DCUCI

Implementing Cisco Data Center Unified Computing

Volume 2

Version 5.0

Student Guide

Text Part Number: 97-3201-01

https://t.me/learningnets

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

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: 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)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED “AS IS.” CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

© 2012 Cisco and/or its affiliates. All rights reserved.

https://t.me/learningnets

Table of Contents

Volume 2

Provision Cisco UCS Compute Resources ***4-1***

Overview 4-1
Module Objectives 4-1

Provisioning the Cisco UCS Cluster **4-3**

Overview 4-3
Objectives 4-3
Configure the Primary Cluster Peer from the Fabric Interconnect Console 4-4
Configure and Join the Secondary Cluster Peer 4-9
Assign a Pool of Management IP Addresses 4-14
Summary 4-19

Provisioning LAN Networking **4-21**

Overview 4-21
Objectives 4-21
Provision VLANs 4-22
Provision VLAN Ranges 4-30
Provision Private VLANs 4-32
Provision Ethernet Uplinks 4-36
Provision Ethernet Uplink Port Channels 4-43
Provision Fabric Port Channels from the Cisco UCS Fabric Interconnect to a Cisco 2208 IOM 4-52
Provision FCoE Storage Ports 4-56
Provision Appliance Ports and Prune VLANs 4-60
Summary 4-64

Provisioning SAN Networking **4-65**

Overview 4-65
Objectives 4-65
Provision VSANs 4-66
Provision Fibre Channel Uplinks and VSAN Trunking 4-75
Provision Fibre Channel Port Channels 4-78
Provision Direct-Attach Fibre Channel Storage Ports and Default Zoning 4-84
Summary 4-90

Provisioning Resource Pools in Cisco UCS Manager **4-91**

Overview 4-91
Objectives 4-91
Provision Server Pools 4-92
Provision Server Pool Autoplacement 4-98
Provision UUID Pools 4-102
Provision MAC Pools 4-107
Provision WWNN Pools 4-110
Provision WWPN Pools 4-114
Provision iSCSI Initiator Pools 4-117
Summary 4-122

Provisioning Server Policies in Cisco UCS Manager **4-123**

Overview 4-123
Objectives 4-123
Provision a Service Profile Using the Expert Service Profile Wizard 4-124
Implement Pools and Policies in the Service Profile 4-128
Associate a Service Profile to a Server 4-152
Cisco UCS Utility Operating System 4-154
Observe the Association Process 4-157
Summary 4-159

https://t.me/learningnets

Provisioning Service Profiles from Templates in Cisco UCS Manager 4-161
Overview 4-161
Objectives 4-161
Requirements of Service Profile Templates 4-162
Differences Between Initial Templates and Updating Templates 4-164
Provision a vNIC Template Using the Template Wizard 4-169
Provision a vHBA Template Using the Template Wizard 4-170
Provision a Service Profile Template Using the Template Wizard 4-171
Provision Multiple Servers from a Service Profile Template 4-180
Clone a Service Profile 4-182
Summary 4-184
Provisioning Cisco UCS C-Series Server Integration in Cisco UCS Manager 4-185
Overview 4-185
Objectives 4-185
Benefits of Cisco C-Series Integration 4-186
Physical Connectivity Requirements for C-Series Integration 4-187
Install Version 1.2 C-Series Server Firmware to Allow Integration 4-192
C-Series Discovery Process 4-195
Summary 4-196
Module Summary 4-197
References 4-198
Module Self-Check 4-199
Module Self-Check Answer Key 4-205
Implement Cisco UCS Server Virtualization Features 5-1
Overview 5-1
Module Objectives 5-1
Provisioning Cisco VM-FEX and Cisco VM-FEX Universal Pass-Through 5-3
Overview 5-3
Objectives 5-3
VMware vSwitch and vDS 5-4
Cisco Nexus 1000V Switching 5-9
Cisco VM-FEX 5-15
Cisco VM-FEX Universal Pass-Through 5-26
Summary 5-32
Provisioning Cisco VM-FEX 5-33
Overview 5-33
Objectives 5-33
Provision VMware ESXi Servers with a Cisco VEM 5-34
Cisco UCS Manager with VMware Integration 5-37
Provision Port Profiles 5-41
Provision Service Profile Components for Cisco VM-FEX 5-45
Add ESXi Hosts to the DVS 5-50
Link a VM to a Port Group 5-54
Summary 5-55

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provisioning Cisco VM-FEX Universal Pass-Through 5-57
Overview 5-57
Objectives 5-57
VMware Requirements for Universal Pass-Through Mode 5-58
Provision a Dynamic vNIC Connection Policy for Universal Pass-Through Mode 5-60
Provision BIOS Policy for Universal Pass-Through Mode 5-62
Associate Universal Pass-Through Policies to a Service Profile 5-64
Provision a Port Profile for Universal Pass-Through Mode 5-66
Provision VMs to Connect to DirectPath I/O Interfaces 5-70
Verify Universal Pass-Through Mode 5-71
Summary 5-73
Module Summary 5-75
References 5-76
Module Self-Check 5-77
Module Self-Check Answer Key 5-80

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module 4

Provision Cisco UCS Compute Resources

Overview

Before you can deploy servers in the Cisco Unified Computing System (UCS), you must build and configure LAN and SAN connectivity, create service profiles, and provide other needed components. Those components include configuration and operational policies, pools, and service profile templates. This module will review the processes of configuring LAN and SAN connectivity, as well as servers.

Module Objectives

Upon completing this module, you will be able to design and configure the connectivity of the Cisco UCS with the LAN and SAN infrastructures in your data center. You will be able to provision servers by leveraging reusable pools, policies, and templates that allow for rapid provisioning and consistency of policy.

This ability includes being able to meet these objectives:

- Perform the initial Cisco UCS cluster setup and provide management IP addresses for blade servers
- Configure VLANs and fabric interconnect uplinks for server connectivity to the Layer 3 data center cloud
- Configure VSANs and fabric interconnect Fibre Channel uplinks for server connectivity to the data center storage cloud
- Configure resource pools for servers, UUIDs, MAC addresses, WWNN, WWPN, and iSCSI
- Configure reusable server policies in Cisco UCS Manager
- Provision service profiles with initial and updating templates
- Provision Cisco UCS C-Series server integration

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 1

Provisioning the Cisco UCS Cluster

Overview

The high-availability cluster is set up during the initial fabric interconnect setup. In this lesson, you will provision the primary and secondary fabric interconnect from the serial console.

You will also configure a pool of management IP addresses to provide management communication with the Cisco Integrated Management Controllers of the server.

Objectives

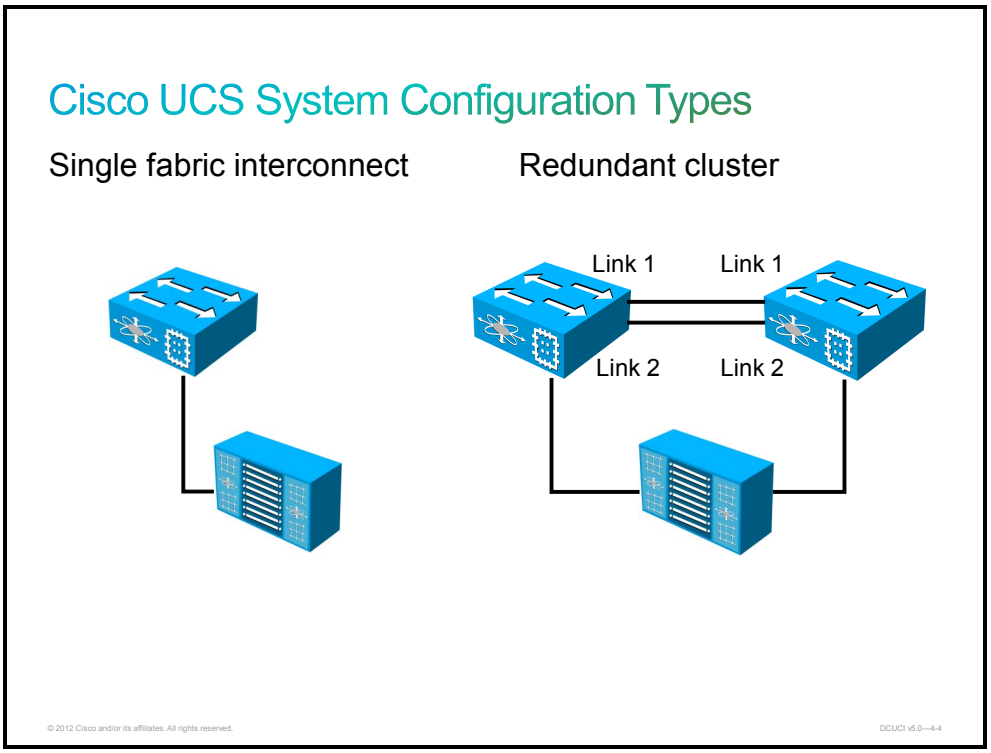
Upon completing this lesson, you will be able to perform initial Cisco Unified Computing System (UCS) cluster setup and provide management IP addresses for blade servers. This ability includes being able to meet these objectives:

- Configure the primary cluster peer from the fabric interconnect console
- Configure the secondary cluster peer from the fabric interconnect console and join to the cluster
- Log into the Cisco UCS Manager GUI and assign a pool of management IP addresses for server management

https://t.me/learningnets

Configure the Primary Cluster Peer from the Fabric Interconnect Console

This topic provides a brief overview of the available Cisco UCS configurations—the single fabric interconnect-based and the high-availability cluster.

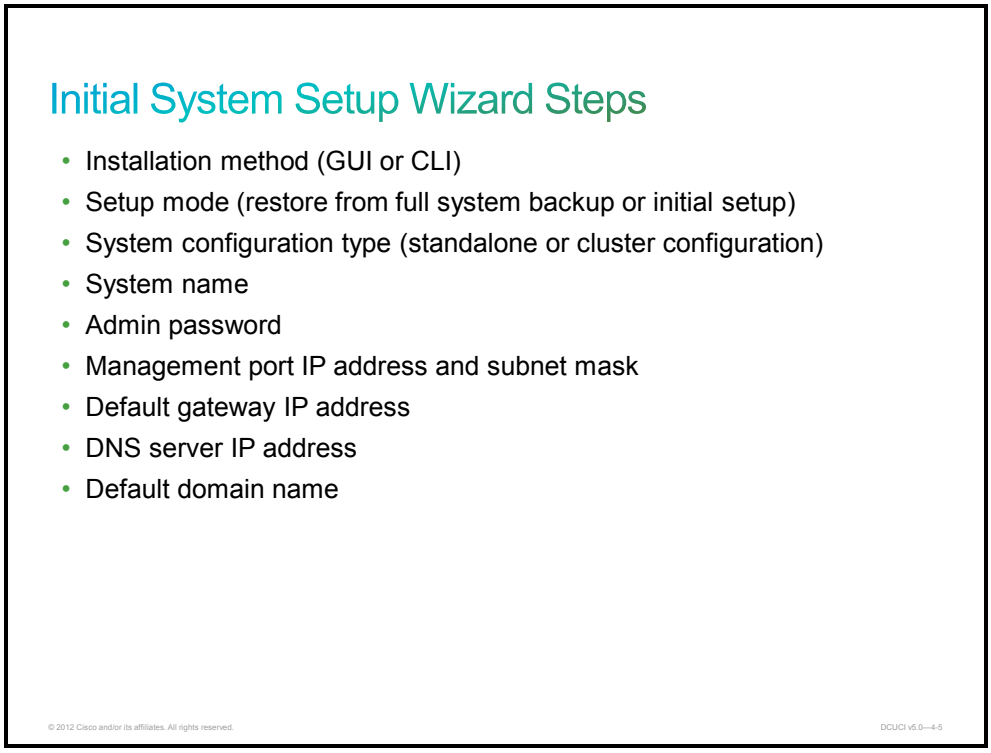


Cisco UCS is managed by an instance of Cisco UCS Manager. A single instance of Cisco UCS Manager can run on a single fabric interconnect Cisco UCS or as a member of a redundant cluster.

The high-availability cluster is formed by two fabric interconnects. The fabric interconnects must be linked to each other using the cluster ports—for example, Link 1 and Link 2. Each I/O module (IOM) in a chassis is connected to only one of the fabric interconnects. In this way, you have two separate and independent data, management, and control paths, through Fabric A and through Fabric B. This provides redundancy. If one of the fabric interconnects becomes unavailable, the other one takes over. The Cisco UCS Manager instance, when it is run on the top of a cluster, will always have an available, operational fabric interconnect.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



The initial system setup wizard is a sequence of questions that you have to answer to provision the initial configuration of the fabric interconnects. This basic configuration is enough to allow you to then connect to Cisco UCS Manager and continue to provision the system.

The initial system setup wizard can be run in two cases:

- A new fabric interconnect
- On a fabric interconnect where the **erase configurations** command is issued; the fabric interconnect automatically reloads and the initial setup wizard starts

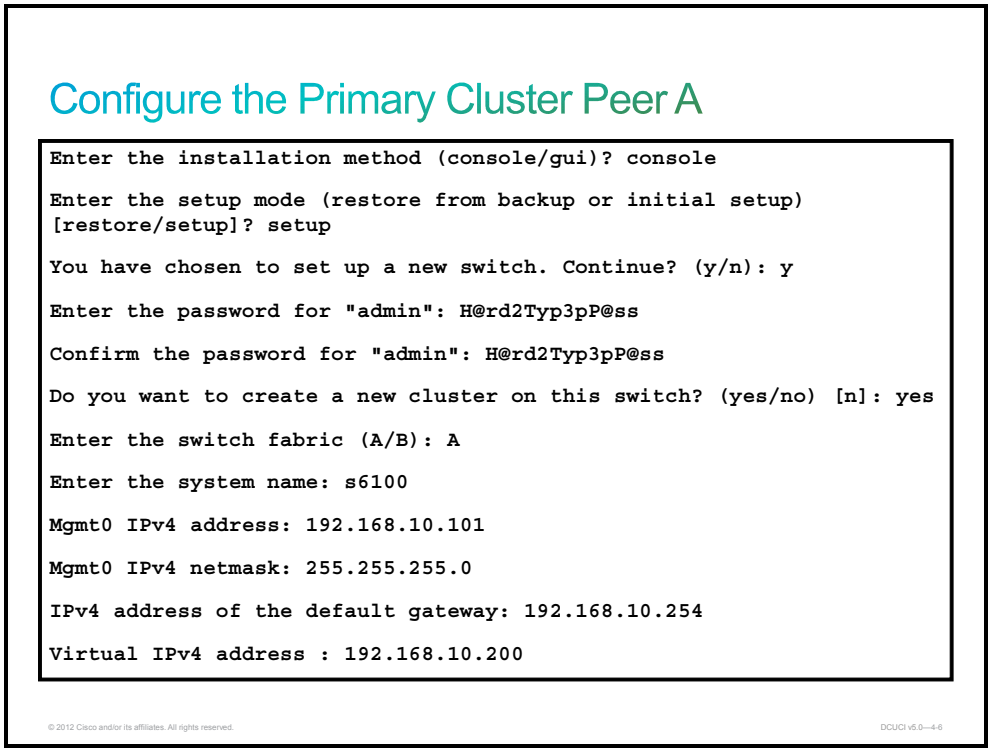
During the initial setup wizard, you are asked for the following information:

- **Installation method:** Select between console or GUI.
- **Setup mode:** Select between initial configuration, or restore the system from a full-state backup.
- **System configuration type:** Select between a standalone fabric interconnect or high-availability cluster.
- **System name**
- **Admin password:** This password is for the user “admin,” which is assigned the administrative role. You need to configure this password because this is the only user that exists initially on the system. You need the password to log into the system. Later, you can perform more configuration related to the users and roles that you will use to access the system.

https://t.me/learningnets

- **Management port IP address:** This is the IP address of interface Mgmt 0. When the initial configuration of a Cisco UCS cluster is performed, you need to separate three IP addresses from the management network:
  - One IP address for the Mgmt 0 interface of fabric interconnect A
  - One IP address for the Mgmt 0 interface of fabric interconnect B. This address is configured during the setup of the second fabric interconnect.
  - One IP address for the cluster, also called VIP. This is the virtual management IP address, which you use to access Cisco UCS Manager. This address floats between the fabric interconnects, depending on which one is designated as primary.
- **Cluster IP address**
- **Default gateway IP address**
- **DNS server IP address**
- **Default domain name**

© 2012 Cisco Systems, Inc.
https://t.me/learningnets



The figure shows the initial system setup wizard for the first fabric.

The primary configuration of the cluster is performed on the first fabric interconnect. Here you configure details such as the system name, admin password, Mgmt 0 IP address of the first fabric interconnect, and the cluster IP address.

To begin the cluster configuration on a new fabric interconnect, connect the serial console to the first member of the cluster (Fabric A). Although there is a GUI Express Start option after fabric interconnect A is configured with an IP address, only the CLI method will be covered.

Like most Cisco devices with an RJ-45 serial console port, you can use a standard Cisco DB-9 to RJ-45 console cable. Configure your favorite terminal emulator for 9600 b/s, 8 data bits, 1 stop bit, and no parity (9600-8-1-none).

https://t.me/learningnets

Configure the Primary Cluster Peer A (Cont.)

```
Configure the DNS Server IPv4 address? (yes/no) [n]: yes

DNS IPv4 address: 20.10.20.10

Configure the default domain name? (yes/no) [n]: yes

Default domain name: cisco.com

Following configurations will be applied:

Switch Fabric = A

System Name = s6100-A

Management IP Address = 192.168.10.101

Management IP Netmask = 255.255.255.0

Default Gateway = 192.168.10.254

Cluster Enabled = yes

Virtual Ip Address = 192.168.10.200

DNS Server = 20.10.20.10

Domain Name = cisco.com

Apply and save the configuration (select 'no' if you want to re-enter)?
(yes/no): yes
```

© 2012 Cisco and/or its affiliates. All rights reserved.

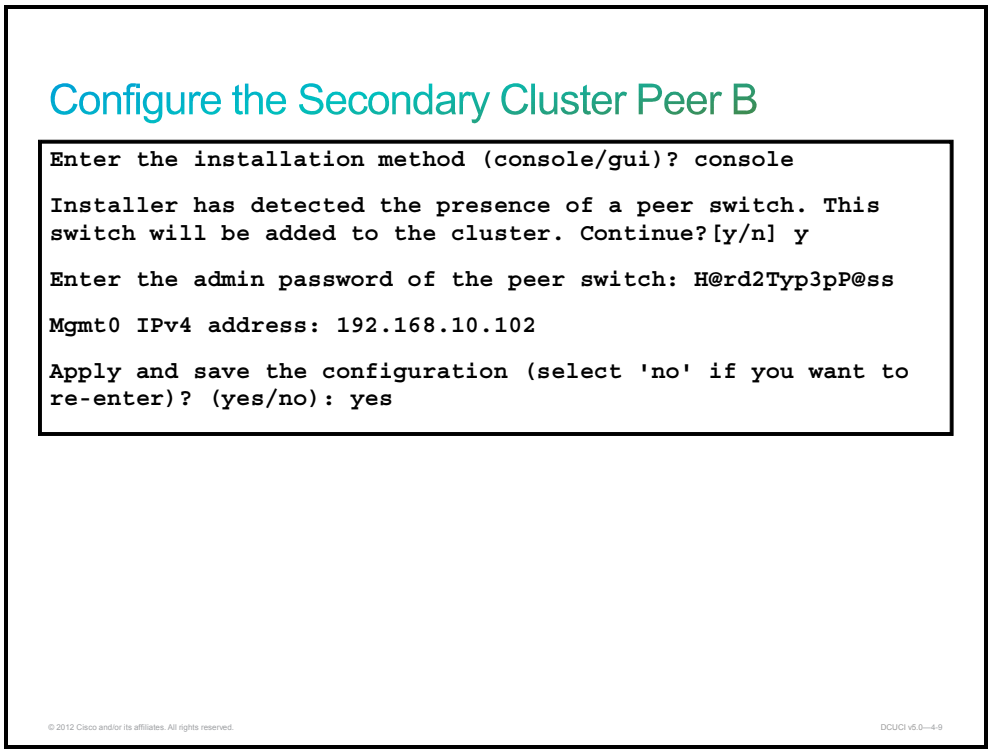
The remainder of the dialog prompts for basic network connectivity options, including Domain Name System (DNS) server and domain. The setup wizard then allows you to review your configuration and make corrections if necessary. When you answer “yes” to apply and save the configuration, the cluster services are configured and enabled on fabric interconnect A.

Note	The hostname and domain name need to be configured correctly to later enroll with a certificate authority (CA). The fully qualified domain name (FQDN) is part of the certificate signing request (CSR). Be certain that the FQDN is unique within your domain.

https://t.me/learningnets

Configure and Join the Secondary Cluster Peer

This topic introduces the initial configuration of the second fabric interconnect of a Cisco UCS cluster.



Assuming that the Link 1 and Link 2 links are connected correctly, the secondary peer will detect the primary peer and ask to join the cluster. Enter the admin password and enter “yes” after reviewing the configuration. The primary peer will perform an initial synchronization from the active management node to the subordinate node. This synchronization includes all elements of the Cisco UCS Manager configuration database and images in the firmware store.

https://t.me/learningnets

Convert Standalone Mode to Cluster

```
S6100-A# connect local-mgmt

S6100-A(local-mgmt)# enable cluster 192.168.10.200

This command will enable cluster mode on this setup. You cannot
change it back to stand-alone. Are you sure you want to continue?
(yes/no): yes


Configure secondary fabric interconnect:

Enter the installation method (console/gui)? console

Installer has detected the presence of a peer switch. This switch
will be added to the cluster. Continue?[y/n] y

Enter the admin password of the peer switch: H@rd2Typ3pP@ss

Mgmt0 IPv4 address: 192.168.10.102

Management IP Address: 192.168.10.102

Apply and save the configuration (select 'no' if you want to
re-enter)? (yes/no): yes
```

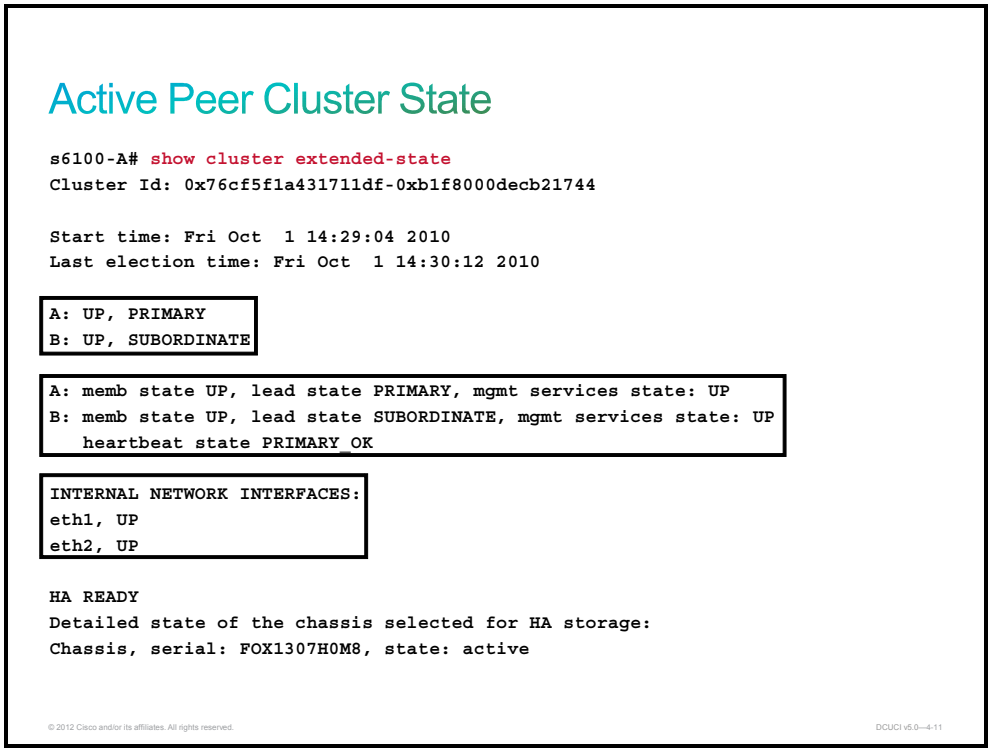
© 2012 Cisco and/or its affiliates. All rights reserved.

One potential scenario that might trigger the need to convert from standalone mode into a cluster is a proof-of-concept lab. Based on your budget to evaluate Cisco UCS, a redundant fabric interconnect might not be an option. After the evaluation is approved for conversion to production use, a secondary fabric interconnect is essential for production data center operation. The command **enable cluster 192.168.10.200** creates a new cluster on the fabric interconnect and defines 192.168.10.200 as the virtual IP address for the cluster.

To complete the cluster, connect Link 1 to Link 1 and Link 2 to Link 2 to enable cluster peer communication. Then, add the secondary peer, as in the previous example.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets



The **show cluster extended-state** command includes information that administrators need to validate cluster configuration and troubleshoot cluster operation. The output shown in the figure indicates that this fabric interconnect is the primary management node. The first fabric interconnect in a cluster is always assigned as Fabric A.

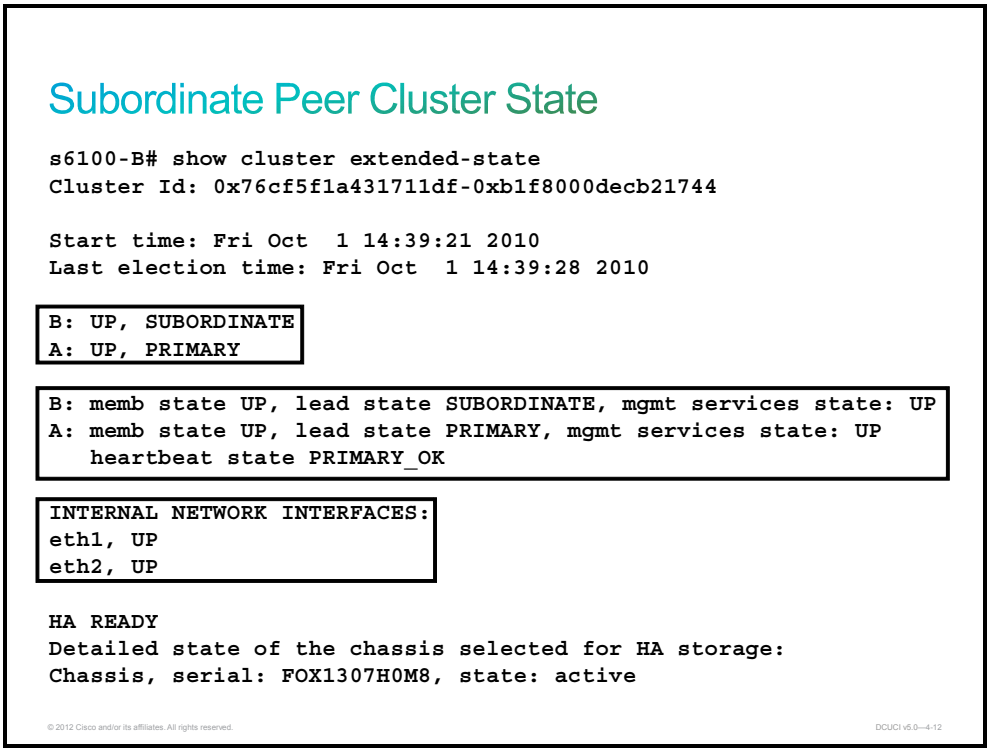
All configuration is performed on the active management node. Before the active node commits a configuration transaction to the data management engine (DME), it first replicates the transaction to the subordinate node. After the subordinate acknowledges that its DME committed the transaction, the primary node commits the transaction.

On the active management node, the management plane and data planes are both active.

All configuration is performed on the active management node. Before the active node commits a configuration transaction to the DME, it first replicates the transaction to the subordinate node. After the subordinate acknowledges that its DME has committed the transaction, the primary node commits the transaction.

On the active management node, the management and data planes are both active.

https://t.me/learningnets



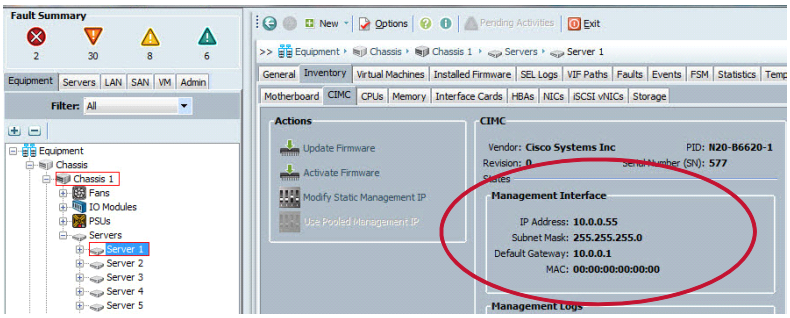
The subordinate node is not in passive standby mode. The DME is active and accepts data that is synchronized from the active management node. Therefore, a distinction is made that it is *subordinate active*. If the active management node fails, the subordinate will wait a predetermined amount of time and then declare the peer dead. At that time, the subordinate node becomes the active management node.

Even when in subordinate mode for the management plane, the data plane is active and forwarding.

© 2012 Cisco Systems, Inc.
https://t.me/learningnets

Server Management IP Address in Cisco UCS

- Assigned to Cisco Integrated Management Controller
- Usage—KVM, SoL, IPMI
- Types of management IP addresses:
  - Static IPv4
  - Static IPv4 from service profile
  - IPv4 address from management pool



© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco UCS Manager communicates with the Cisco Integrated Management Controller of each blade server to provide external access.

The external access that is provided is used for the following:

- Remote keyboard, video, mouse (KVM) console
- Serial over LAN (SoL)
- Intelligent Platform Management Interface (IPMI) protocol

Each Cisco Integrated Management Controller, both on the B-Series and C-Series servers, must be assigned an IP address to be reachable. There are three ways of assigning the IP address:

- Directly assign a static IPv4 address to the Cisco Integrated Management Controller of the server.
- Assign a static management IP address through a service profile. An IP address assigned in this way moves with the service profile. This means that this specific IP address will be used only from the server that is currently associated with this service profile. Also, this IP address will move with the service profile when it is associated with another server. During disassociation and association with a new server, all of the open communication to the previous server, like KVM, SoL, and so on, will be lost.
- In Cisco UCS Manager, create a pool of management IP addresses. These addresses are assigned automatically by Cisco UCS Manager to the controllers of the servers that are under the management of this Cisco UCS Manager instance.

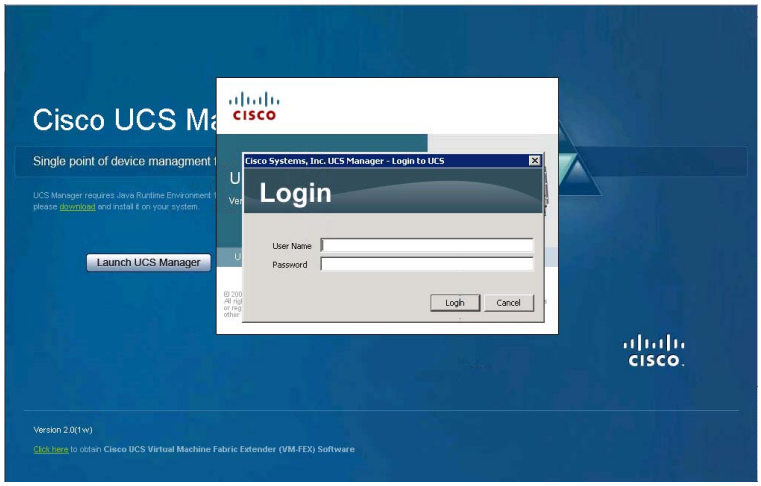
https://t.me/learningnets

Assign a Pool of Management IP Addresses

This topic describes how to log into Cisco UCS Manager and assign a pool of management IP addresses for server management.

Log into Cisco UCS Manager

- Enter the IP address of the Cisco UCS Manager cluster.
- Authenticate at the prompt.



© 2012 Cisco and/or its affiliates. All rights reserved.

To log in and start working with Cisco UCS Manager, you must do the following:

- You must have already performed initial configuration.
- Open an Internet browser and type in the cluster IP address of the Cisco UCS.
- When the initial page loads, enter “admin” as the user and enter the corresponding password that you configured during initial setup.

In this example, you are logging into a newly configured Cisco UCS cluster. When you have a standalone fabric interconnect, use the unicast IP address of the Mgmt 0 interface.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Create a Management IP Address Pool

- To start the Management IP Address Pool wizard, navigate to Admin > All > Communication Management > Management IP Pool (ext-mgmt).

© 2012 Cisco and/or its affiliates. All rights reserved.

To create a pool of management IPv4 addresses, follow these steps:

Step 1 From the navigation pane, click the **Admin** tab.

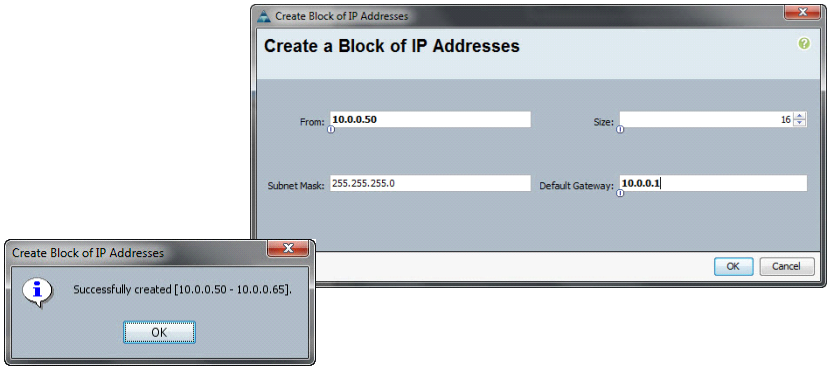
Step 2 From the Admin tab, select **Management IP Pool (ext-mgmt)**, which is under All > Communication Management.

Step 3 In the content pane, click **Create Block of IP Addresses** to start the management IP address pool wizard.

https://t.me/learningnets

Create a Management IP Address Pool (Cont.)

- Specify first IP address
- Specify number of IP addresses
- Specify subnet mask
- Specify default gateway



© 2012 Cisco and/or its affiliates. All rights reserved.

In the Create Block of IP Addresses window, complete the following four fields:

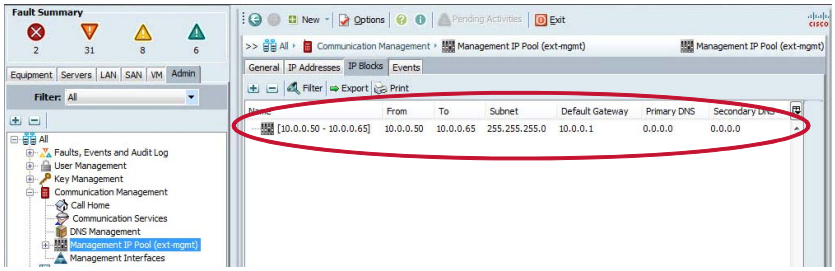
- **From:** In this field, specify the first IP address from the range that you want to configure.
- **Size:** Specify how many IP addresses you need in this range.
- **Subnet Mask:** Specify the network mask.
- **Default Gateway:** Specify the default gateway for this management network.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Management IP Pool Verification

- In the IP Blocks tab, verify the range of IP addresses, subnet mask, and default gateway.



© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco UCS allows for multiple pools of management IP addresses. To check the pools that are configured on the system, select the **IP Blocks** tab in the content pane. From the Admin tab in the navigation pane, navigate to **All > Communication Management > Management IP Pool (ext-mgmt)**.

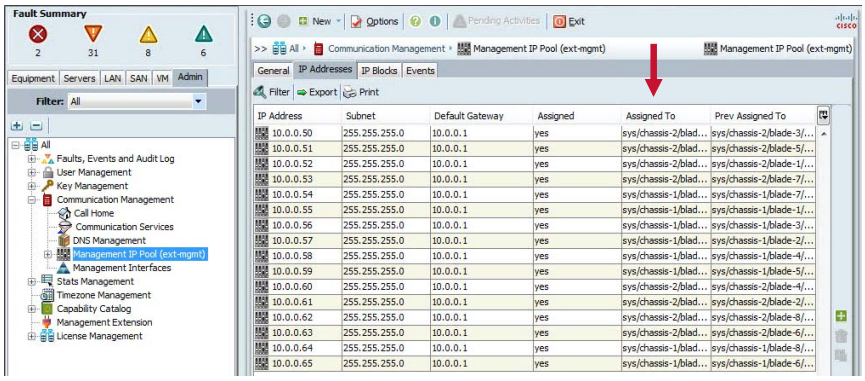
In the IP Blocks tab, you will see a list of the created management IP pools, which will provide you with the following information:

- **Name:** The system uses the range of IP addresses to automatically create a name for this object in Cisco UCS Manager.
- **From:** The first IP address from this range.
- **To:** The last IP address from this range.
- **Subnet:** The network mask for this range.
- **Default Gateway:** The IP address of the default gateway configured for this range.
- **Primary and Secondary DNS:** The configuration of DNS servers related to this pool of management IP addresses.

https://t.me/learningnets

Management IP Pool Address Assignment

- In the IP Addresses tab, verify IP the address assignment to servers.



© 2012 Cisco and/or its affiliates. All rights reserved.

To check the Cisco UCS Manager management IP address assignment to the servers, choose the **IP Addresses** tab. There you will be provided with the following information:

- **IP Address:** A specific IP address from the pool.
- **Subnet Mask**
- **Default Gateway**
- **Assigned:** This field indicates with “yes” or “no” whether this IP address is assigned to a server from the Cisco UCS.
- **Assigned to:** This field indicates to which server this management IP address is assigned.
- **Prev assigned to:** This field indicates the server to which this IP address has been previously assigned.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.

Summary

- The primary fabric interconnect in a cluster is configured through the initial setup wizard.
- The secondary fabric interconnect must be connected through the Link 1 and Link 2 cluster interfaces and, after basic initial configuration is performed, it pulls the configuration from the primary fabric interconnect.
- The management IP address pool for all servers can be configured in Cisco UCS Manager by navigating to Admin > All > Communication Management > Management IP Pool (ext-mgmt).

© 2012 Cisco and/or its affiliates. All rights reserved.

https://t.me/learningnets

© 2012 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 2

Provisioning LAN Networking

Overview

A Cisco Unified Computing System (UCS) must be connected to the LAN infrastructure of the data center to provide access to the applications running on the servers. In this lesson, you will provision LAN networking.

You will provision VLANs, Ethernet uplinks, port channels for uplink communication, Fibre Channel over Ethernet (FCoE) ports, and appliance ports.

Objectives

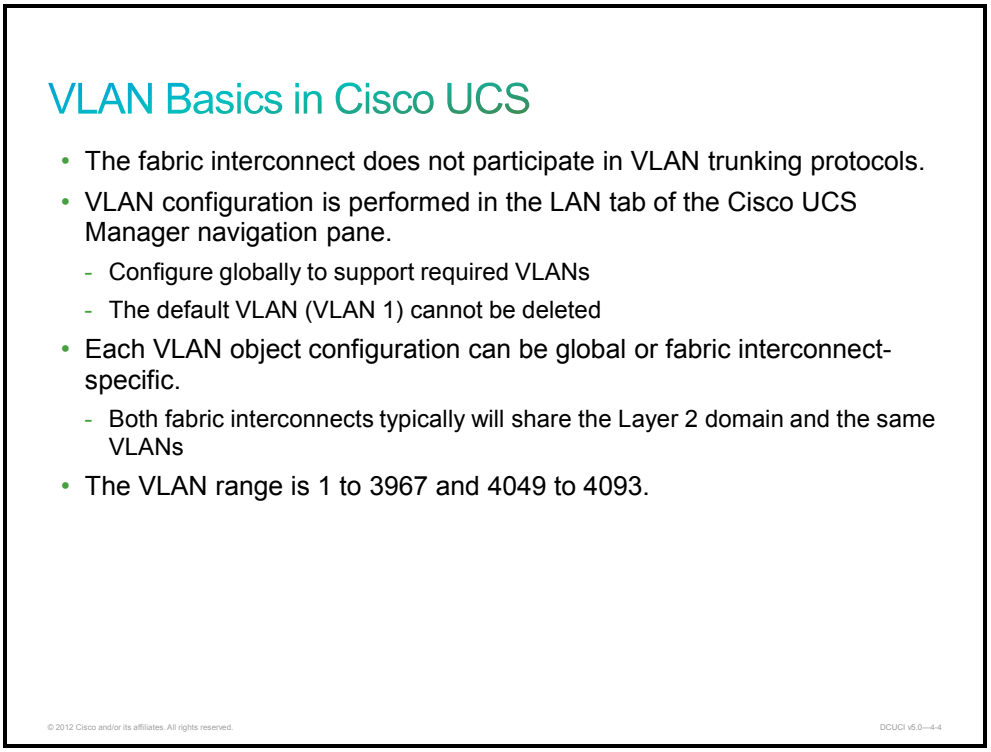
Upon completing this lesson, you will be able to configure VLANs and fabric interconnect uplinks for server connectivity to the Layer 3 data center cloud. This ability includes being able to meet these objectives:

- Provision VLANs for single fabric, both fabrics, and both fabrics configured differently
- Provision VLAN ranges
- Provision private VLANs
- Provision Ethernet uplinks
- Provision Ethernet uplink port channels
- Provision fabric port channels from the Cisco UCS Fabric Interconnect to a Cisco 2204/2208 IOM
- Provision FCoE storage ports
- Provision appliance ports and prune VLANs

https://t.me/learningnets

Provision VLANs

This topic describes how to provision different VLANs in Cisco UCS Manager.



Although all uplinks from the fabric interconnect to the northbound switch are IEEE 802.1Q trunks, no virtual trunking protocol is employed. Therefore, the fabric interconnect requires manual configuration of VLANs.

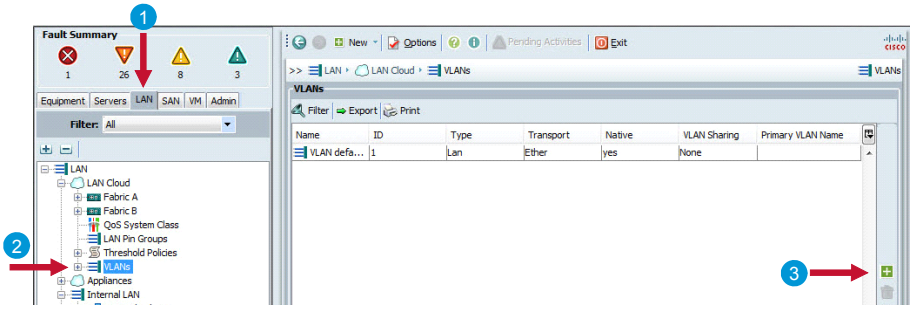
Note	Cisco UCS Manager reserves VLANs 3968 to 4048 and 4094 for system use.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Start the VLAN Creation Wizard

- Start the VLAN wizard



To start the VLAN creation wizard, follow these steps:

Step 1 Select the **LAN** tab in the navigation pane.

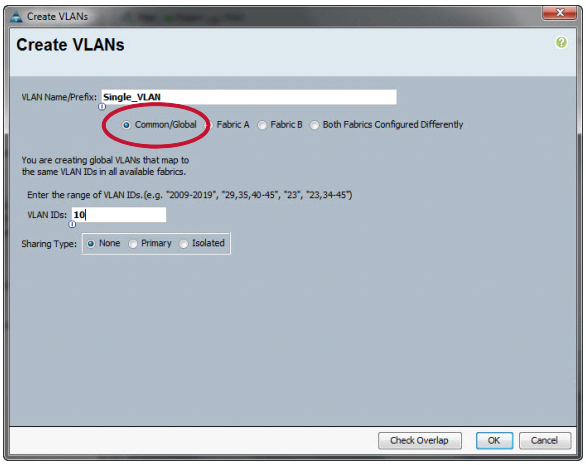
Step 2 Expand **LAN Cloud** and select **VLANs**.

Step 3 You can either right-click **VLANs** and choose **Create VLANs** from the pop-up menu, or you can click the plus sign (+) in the content pane to start the VLAN creation wizard.

https://t.me/learningnets

Provision a Single VLAN

- A VLAN name can be 1 to 32 characters long.



© 2012 Cisco and/or its affiliates. All rights reserved.

In Cisco UCS, VLANs require a name and a VLAN number. VLAN names are always used in the creation of virtual network interface card (vNIC) profiles. This abstraction of the VLAN number allows you to change a VLAN associated with the VLAN names without requiring configuration changes to the server.

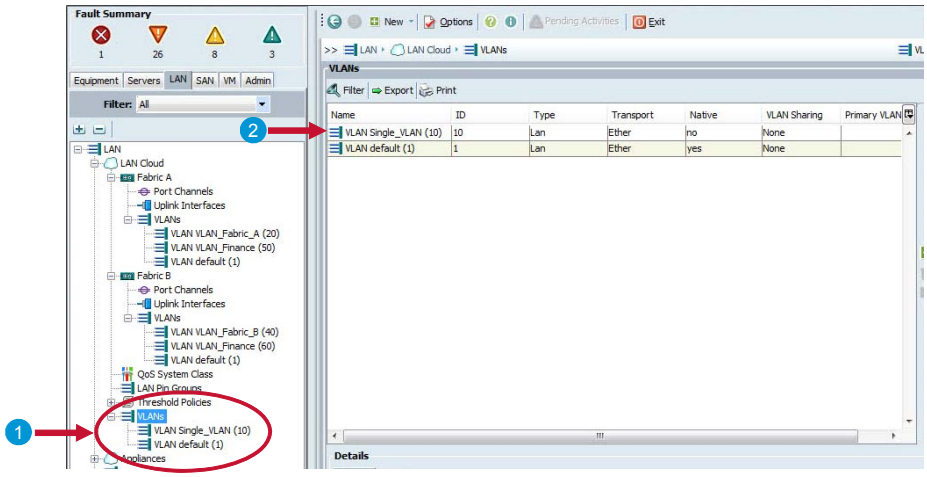
Click **Check Overlap** to verify that the VLAN number is not already defined.

When you click the Common/Global radio button for VLAN creation, the VLAN name and number will be created on both fabric interconnects. This selection is the most common.

https://t.me/learningnets

Verifying Single VLANs

- Common or global VLANs can be seen in the global list.



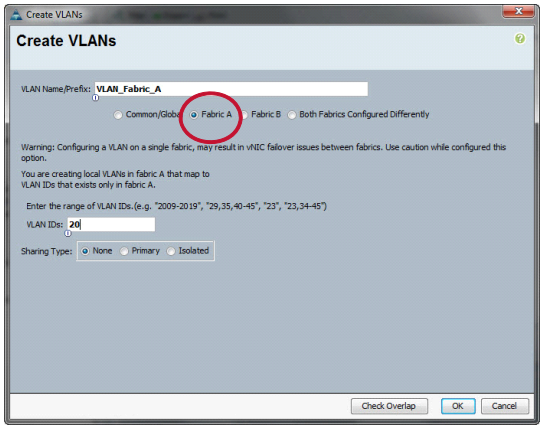
© 2012 Cisco and/or its affiliates. All rights reserved.

By default, when a single VLAN is created, it exists on both of the fabric interconnects and uses the same VLAN ID for the traffic going through both paths. To verify the creation of a single VLAN, from the LAN tab, navigate to LAN Cloud > VLANs. In the content pane, you will see a list of all VLANs that exist on both of the fabric interconnects.

https://t.me/learningnets

Provision Fabric-Only VLANs

- VLAN_Fabric_A is only available to servers connected to Fabric A.

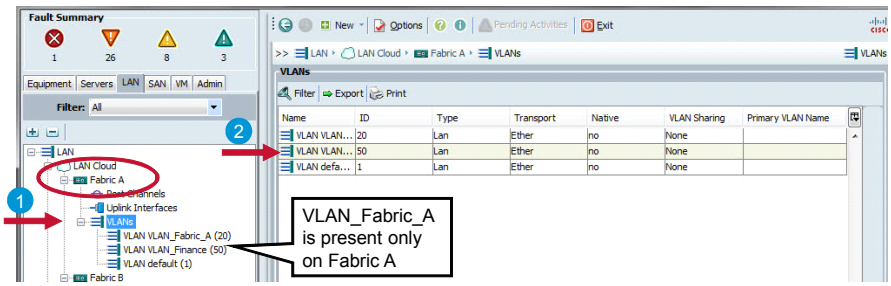


© 2012 Cisco and/or its affiliates. All rights reserved.

Fabric-only VLANs can be created, if desired. In the example, VLAN 20 will be created only on fabric interconnect A. Because this VLAN exists on only one fabric, fabric failover will not be available for this VLAN. For this reason, fabric-only VLANs are generally limited to test use.

Verifying Fabric-Specific VLANs

- Fabric-specific VLANs can be seen in the Fabric VLAN list



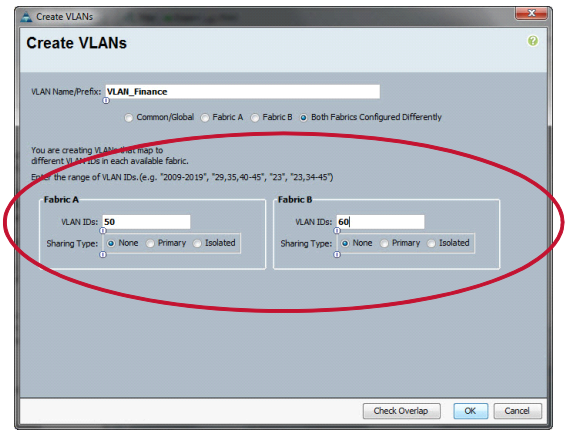
© 2012 Cisco and/or its affiliates. All rights reserved.

To verify the creation of fabric-only VLANs, choose the LAN tab in the navigation pane. Then, navigate to LAN Cloud > Fabric A or B, depending on which fabric contains the VLAN you have created.

https://t.me/learningnets

Provision Both Fabrics Differently

- VLAN_Finance is created with a different VLAN ID on each fabric.



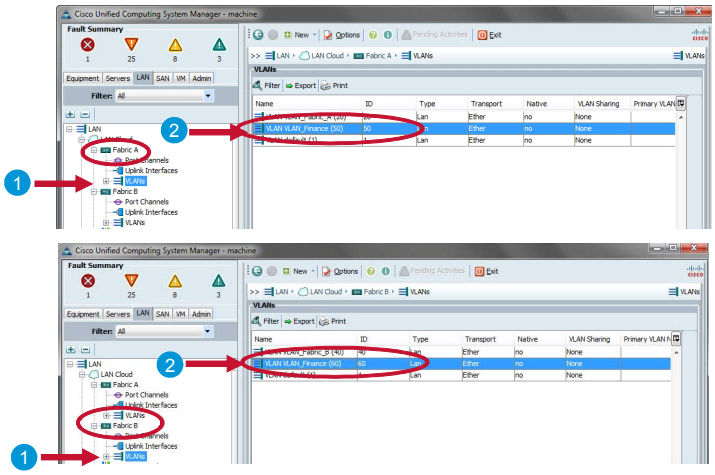
© 2012 Cisco and/or its affiliates. All rights reserved.

You can create and configure a VLAN that will exist on both of the fabric interconnects. However, the traffic will be applied to different VLAN IDs depending on the data path that is taken—through Fabric A or Fabric B. In the example, the VLAN named VLAN_Finance will be created. The traffic for this VLAN that goes through Fabric A will be applied to VLAN ID 50. The traffic for this VLAN that uses the data path through Fabric B will be applied to VLAN ID 60. In the unlikely event that the northbound switches defined a common subnet on two different VLANs, this is a workaround to allow connectivity.

https://t.me/learningnets

Verifying VLANs Configured Differently

- The same VLAN that uses different VLAN IDs must be verified in the VLAN list of both fabric interconnects.



© 2012 Cisco and/or its affiliates. All rights reserved.

When you create a VLAN that is configured differently, it will use different VLAN IDs on Fabric A and on Fabric B. To verify the configuration, you have to check the VLAN on both of the fabric interconnects. To check the VLANs, navigate to LAN Cloud > Fabric A > VLANs. In the content pane, you will see the VLANs that exist on Fabric A.

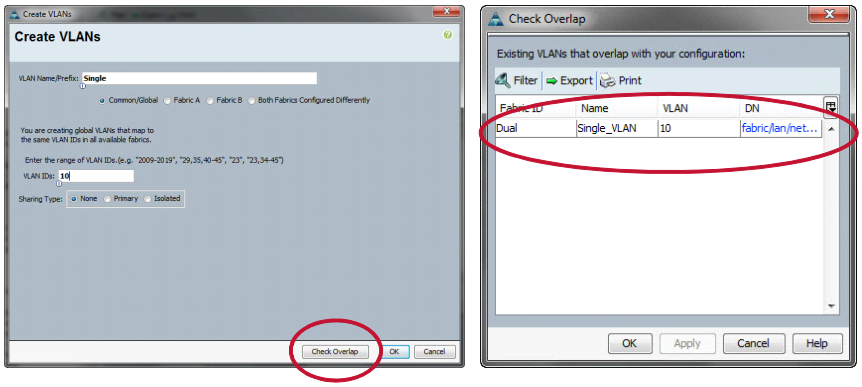
In the same manner, you can verify the VLAN and configured VLAN ID on Fabric B.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Check VLAN Overlap

- Start creating a VLAN that uses an existing ID and click Check Overlap.
- A dialog box will indicate if there is a conflict.



© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco UCS Manager uses multiple VLANs for communication between the blade chassis and fabric interconnects. Some VLANs are used for server data traffic, some are used for control and management communication of Cisco UCS Manager, and some are used as transport VLANs for Fibre Channel over Ethernet (FCoE) communication. The VLANs used for FCoE traffic must be dedicated only for this purpose. To check for overlapping of VLAN IDs, use the Check VLAN Overlap feature when you create a VLAN.

In the VLAN creation wizard, after the VLAN name and ID are configured, click **Check VLAN Overlap**. A new window will open. The window will state if the VLAN ID overlaps with an existing VLAN.

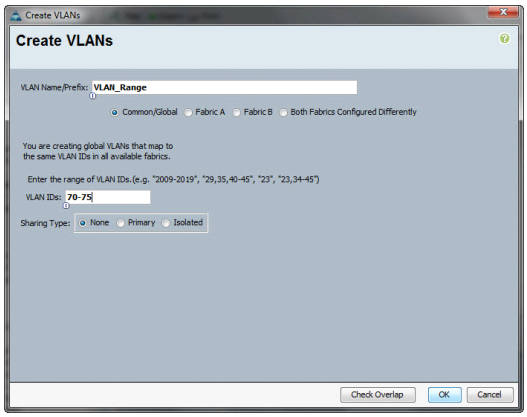
https://t.me/learningnets

Provision VLAN Ranges

This topic describes how to create a range of VLANs.

Define Multiple VLANs Using a Prefix

- This feature is available in Cisco UCS Manager 1.3 and higher.
- Enter the prefix name for the VLAN range to be created.



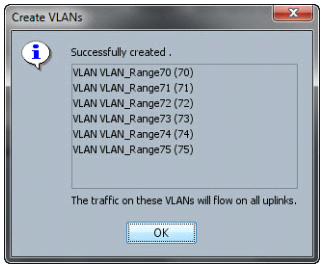
© 2012 Cisco and/or its affiliates. All rights reserved.

Starting from Cisco UCS Manager version 1.3, you can create multiple VLANs at once. For this option, the name that is specified is used as a prefix. The number of VLANs is specified by configuring a range of VLAN IDs. You can specify a range as “start VLAN ID” – “end VLAN ID,” or you can list the VLAN IDs that you want to create. For example, if you want to create VLANs 4, 6, 12, 13, and 14, you have to specify them in the following format: “4, 6, 12–14.” For the names of the newly created VLANs to be unique, the name prefix will be added to the number, which represents the VLAN IDs.

https://t.me/learningnets

VLAN Creation Successful

- Six VLANs were created using the VLAN_Range prefix.



© 2012 Cisco and/or its affiliates. All rights reserved.

The figure shows the successful creation of a range of VLANs. Also, the figure shows how Cisco UCS Manager uses the name prefix and the VLAN ID to form a unique name for each VLAN.

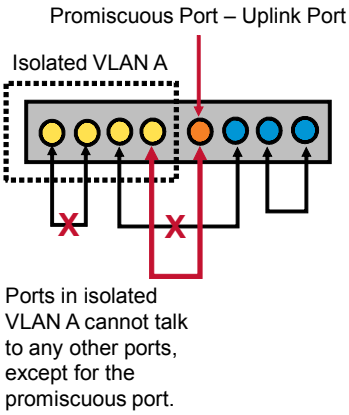
https://t.me/learningnets

Provision Private VLANs

This topic describes how to provision private VLANs in Cisco UCS Manager.

Private VLANs

- Private VLANs subdivide a primary VLAN into secondary VLANs for better control of the communication.
- Cisco UCS Manager supports private VLANs.
- Cisco UCS Manager supports only isolated secondary VLANs.
- Each primary VLAN can have only one isolated VLAN.



© 2012 Cisco and/or its affiliates. All rights reserved.

Private VLANs are used when you want to apply more control over the communication between ports in a VLAN. This VLAN is called primary, and it is subdivided into secondary VLANs. Secondary VLANs can be isolated or community VLANs. The ports from a primary VLAN that belong to an isolated VLAN cannot communicate with each other or with any ports outside of the primary VLAN. The ports in a community VLAN can communicate only with other ports in the same community VLAN. You can allow communication between specific ports only through a special port. This port is called a promiscuous port. Because it is the only point for communication, the communication rules are applied by using access control lists (ACLs).

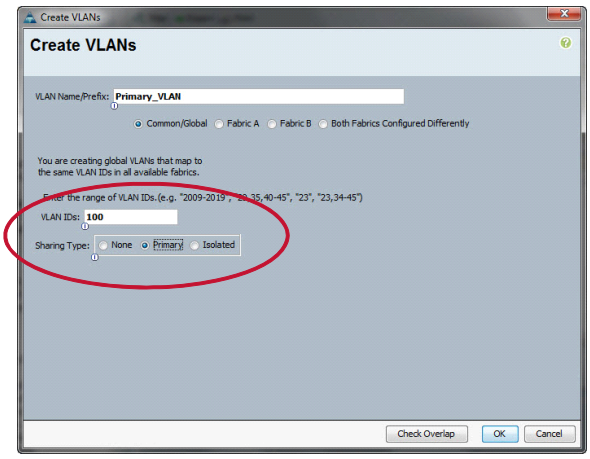
Cisco UCS Manager supports private VLANs. This support is limited, however, because you can have only isolated VLANs as secondary VLANs. The other restriction is that you can have only one isolated VLAN per primary VLAN.

In Cisco UCS Manager, you have isolated ports. The isolated ports are host ports that belong to an isolated VLAN. The communication to and from these isolated ports with other ports is blocked, except for the communication that goes through a promiscuous port. In Cisco UCS Manager, you can have multiple isolated ports.

https://t.me/learningnets

Create a Primary VLAN

- To provision private VLANs, first create a primary VLAN.
- The primary VLAN is the promiscuous VLAN.



© 2012 Cisco and/or its affiliates. All rights reserved.

To use the private VLAN feature, a VLAN that will be subdivided must be specified as a primary VLAN. To specify the VLAN as primary, go to the LAN node at the LAN tab in the navigation pane. Then choose the **VLANs** tab and click the plus sign (+) to open the window for VLAN creation.

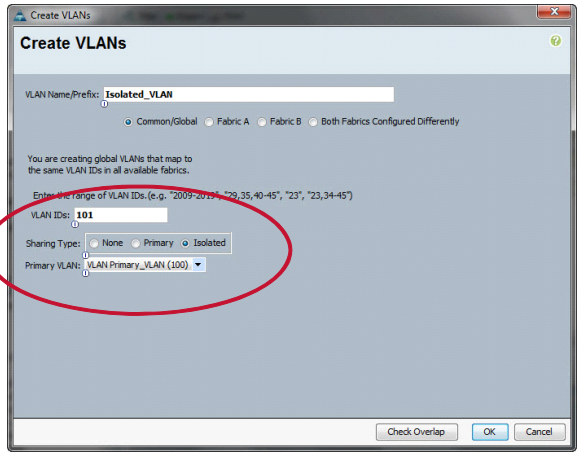
In the new window, specify the VLAN name, where you want the VLAN to be created, and the VLAN ID.

The last option is Sharing Type. Click **Primary** to make this VLAN a primary VLAN.

https://t.me/learningnets

Create an Isolated VLAN

- Create a new VLAN with a sharing type of isolated.
- Bind the isolated VLAN to the primary VLAN from the drop-down menu.



© 2012 Cisco and/or its affiliates. All rights reserved.

Next, create and configure the isolated VLAN for the primary VLAN that you just created. To create the isolated VLAN, follow the same procedure that you used to create the VLAN.

Specify the same attributes—VLAN name, where the VLAN will be created, and VLAN ID.

Finally, for a VLAN to be isolated, click **Isolated** for the Sharing Type.

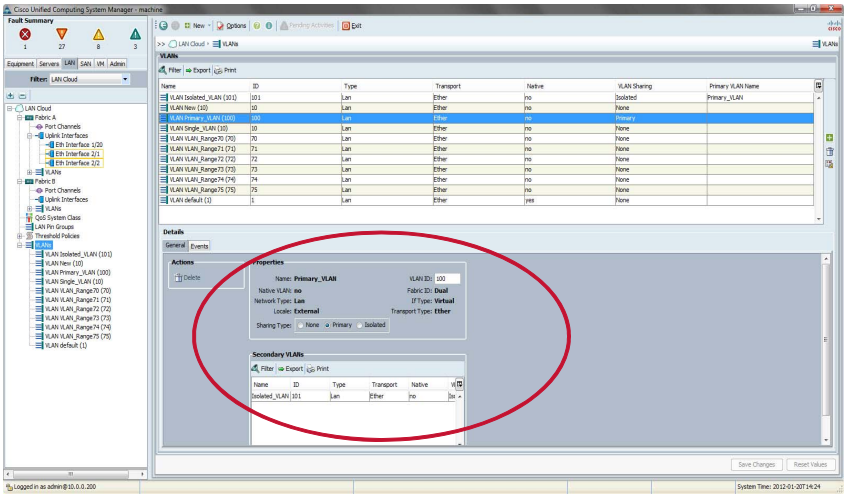
When a VLAN is specified as isolated, a drop-down menu appears under the Sharing Type option. From this menu, choose the primary VLAN for this isolated VLAN.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Verify Private VLANs

- Navigate to LAN > LAN Cloud > VLANs and click the primary VLAN to view the isolated VLANs that are bound to it.



To verify the configuration of the private VLAN, go to the **LAN** tab in the navigation pane. Click **LAN Cloud** and choose **VLANs**.

In the content pane, a list of VLANs that exist in the Cisco UCS Manager will be displayed. In this list, you will see your primary VLAN. Click the primary VLAN, and properties for this VLAN will be displayed in the Details pane. The Sharing Type will show as Primary, and you will see the secondary isolated VLAN that is associated with the primary VLAN.

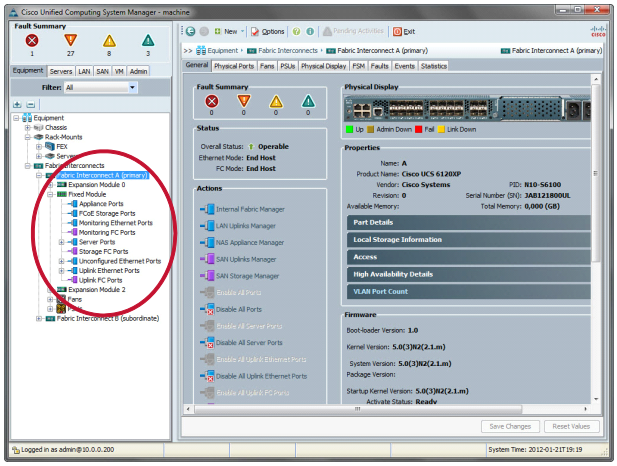
https://t.me/learningnets

Provision Ethernet Uplinks

This topic describes how to provision Ethernet uplinks.

Select the Fabric Interconnect

- In the Equipment tab of the navigation pane, select Fabric Interconnects > Fabric Interconnect A or B.



© 2012 Cisco and/or its affiliates. All rights reserved.

To provide connectivity for Cisco UCS to the Ethernet infrastructure, Ethernet uplink ports must be configured.

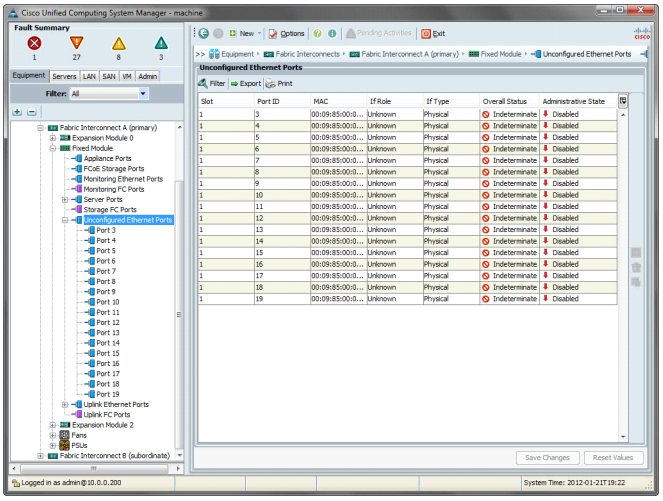
To configure Ethernet ports as uplinks, choose the **Equipment** tab from the navigation pane. Then choose the fabric interconnect on which you want to configure the ports.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Select the Unconfigured Port to Provision

- Choose Fixed Module or Expansion Module and expand Unconfigured Ethernet Ports.



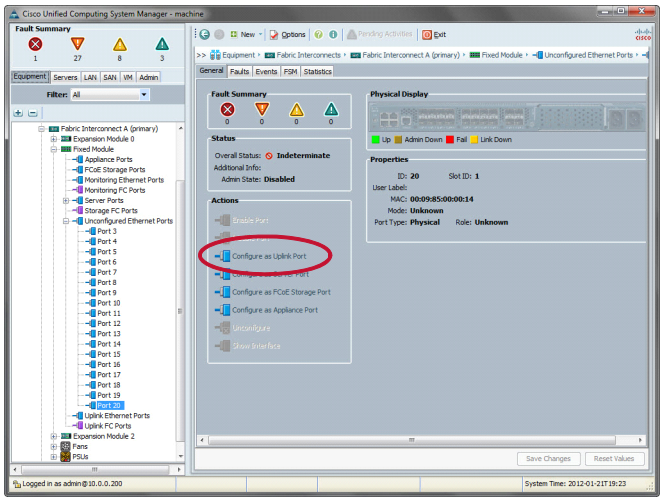
© 2012 Cisco and/or its affiliates. All rights reserved.

On the fabric interconnect, there are fixed and expansion ports. Depending on which ports you want to use, expand either the **Fixed Module** or the **Expansion Module** section.

https://t.me/learningnets

Provision an Unconfigured Port as an Uplink

- Select a port from Unconfigured Ethernet Ports and click **Configure as Uplink Port**.



© 2012 Cisco and/or its affiliates. All rights reserved.

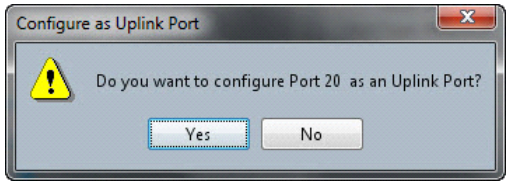
Next, expand **Unconfigured Ethernet Ports** to see a list of all Ethernet ports that are currently not used and do not have any configuration applied.

Click a port to configure. In the content pane, you will see all the available configuration options. Click **Configure as Uplink Port**.

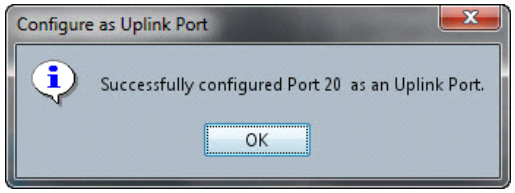
https://t.me/learningnets

Confirm Uplink Port Creation

- Click Yes to confirm the creation of the uplink.



- Click OK to acknowledge the creation of the uplink.



© 2012 Cisco and/or its affiliates. All rights reserved.

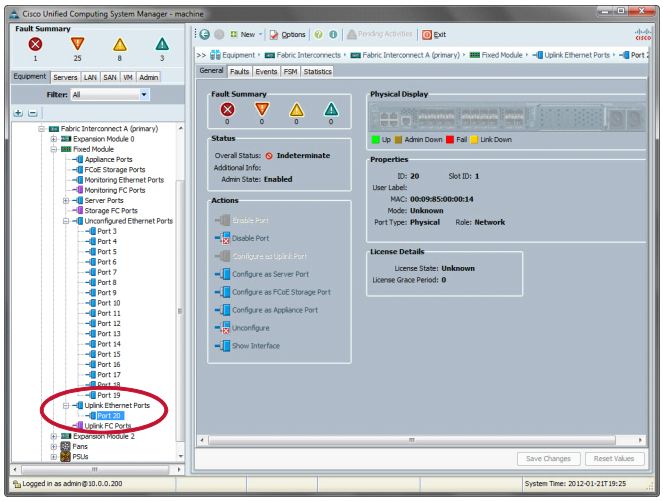
A new window opens where you have to confirm that you want the port to be configured as an uplink port.

The next window confirms successful configuration.

https://t.me/learningnets

Verify Ethernet Uplink Port Creation

- Verify that the port appears under Uplink Ethernet Ports.



© 2012 Cisco and/or its affiliates. All rights reserved.

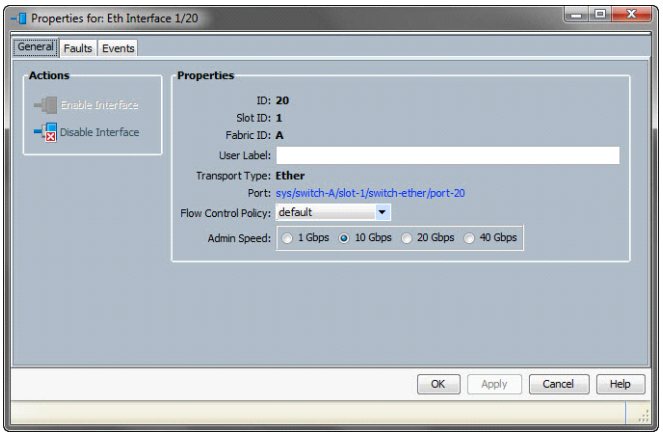
To verify the configuration, expand **Uplink Ethernet Ports**, which will list the configured uplink ports.

Click the port. From the **General** tab of the content pane, select **Show Interface**. A window opens displaying the characteristics for this port.

https://t.me/learningnets

Edit Ethernet Uplink Parameters

- View and edit uplink port properties.



© 2012 Cisco and/or its affiliates. All rights reserved.

Under the General tab of the new window, you can see the properties for the port—port ID, slot ID (if it is from the fixed ports, the slot ID will be 1), and fabric ID. You will also see the full path to the port.

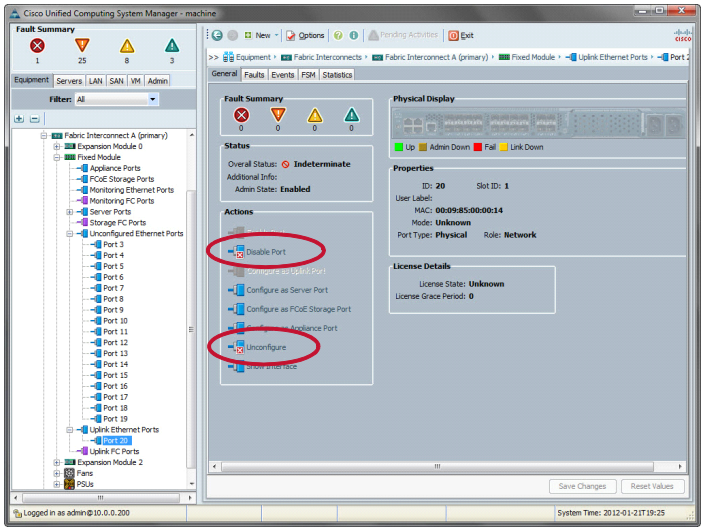
You can also configure the following:

- **Flow control policy:** Choose the flow control policy to specify how the port will send the IEEE 802.3x pause signals.
- **Admin speed:** Choose the speed for the port. Currently, the supported speeds for uplink port channels are limited to 1 Gb/s and 10 Gb/s.

https://t.me/learningnets

Administrative Control of Ethernet Uplinks

- Unconfigure or disable an uplink port.



© 2012 Cisco and/or its affiliates. All rights reserved.

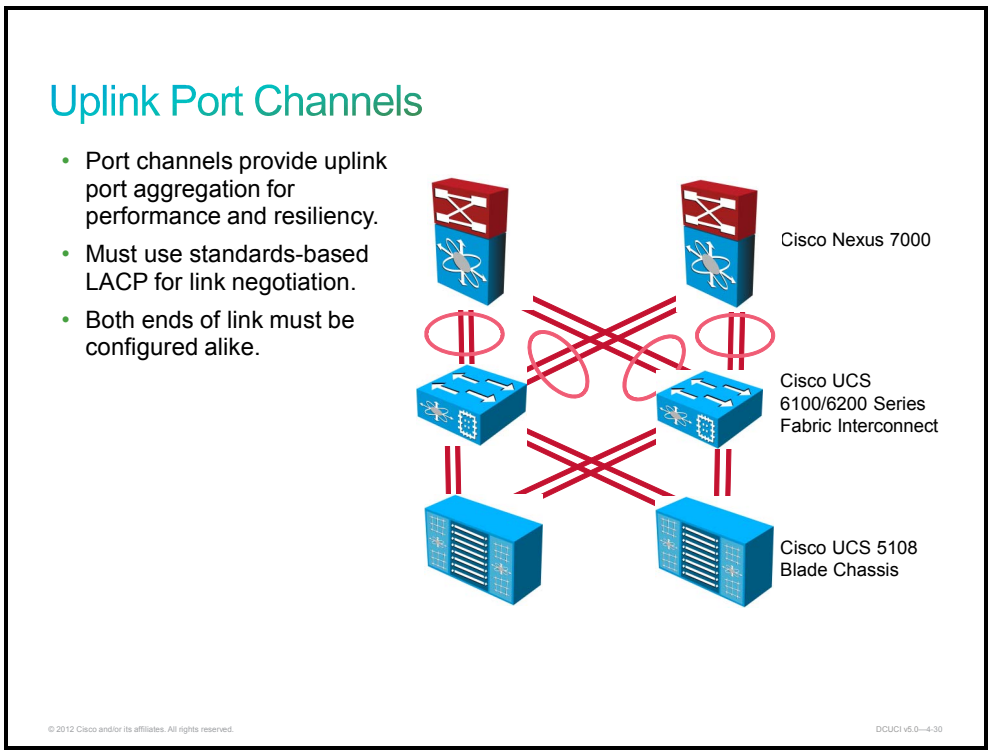
To disable a port, click the port. Then, in the General tab of the content pane, choose **Disable Port**.

If you need to remove the configuration of the port (that is, change the role of a port), choose **Unconfigure** from the General tab. When a port is unconfigured, it will be moved back into the Unconfigured Ports section.

https://t.me/learningnets

Provision Ethernet Uplink Port Channels

This topic describes how to provision uplink port channels.



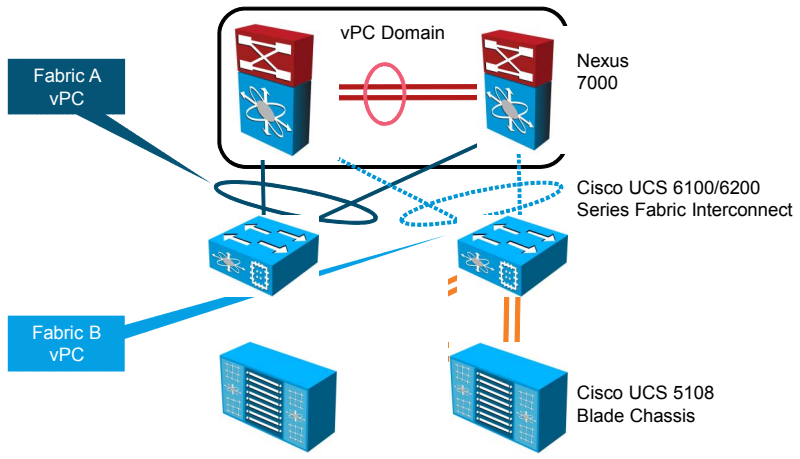
The uplink ports, which are the ports between the fabric interconnects and the upstream Ethernet switches, can be combined in port channels. Port channels add fault tolerance and load balancing, and aggregate the speed of the ports.

Note	On the Cisco UCS Manager, the supported link aggregation protocol is Link Aggregation Control Protocol (LACP). Port Aggregation Protocol (PAgP) is *not* supported. When the port channel is created at the side of the upstream switch, you must use LACP. Otherwise, the ports will not be put in a port channel from the side of the Cisco UCS.

https://t.me/learningnets

Uplink Virtual Port Channels

- A vPC is transparent to the fabric interconnects.
- All vPC-specific configuration is provisioned on the northbound switch.



© 2012 Cisco and/or its affiliates. All rights reserved.

Normally, all links in a port channel must terminate on the same switch. The Cisco Nexus 5000, 5500, and 7000 Series Switches support a feature called virtual port channel (vPC). A vPC allows for bandwidth aggregation like a traditional port channel, but adds the benefit of a redundant path without the need to run Spanning Tree Protocol (STP). Spanning-tree recovery on path failure can be tuned as low as 6 seconds, but a port channel can recover in less than 1 second.

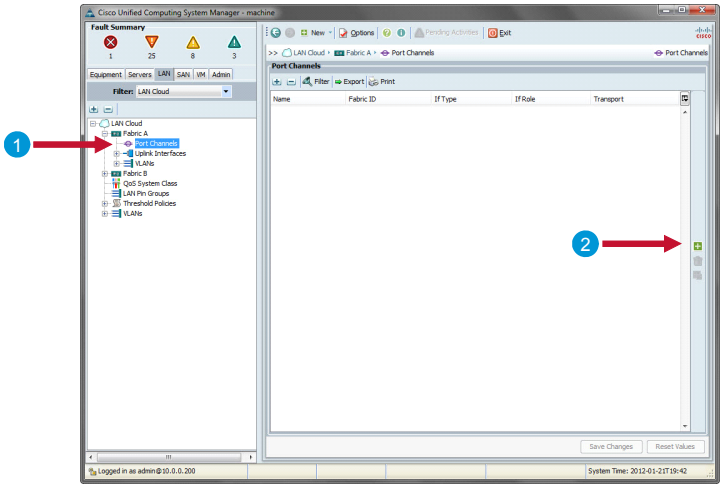
All vPC configuration is performed on the northbound uplink switch. The fabric interconnect is unaware that the port channel is split between two switches.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Start the Port Channel Wizard

- Port channels are created independently on each fabric interconnect.
- Choose Fabric A or Fabric B.

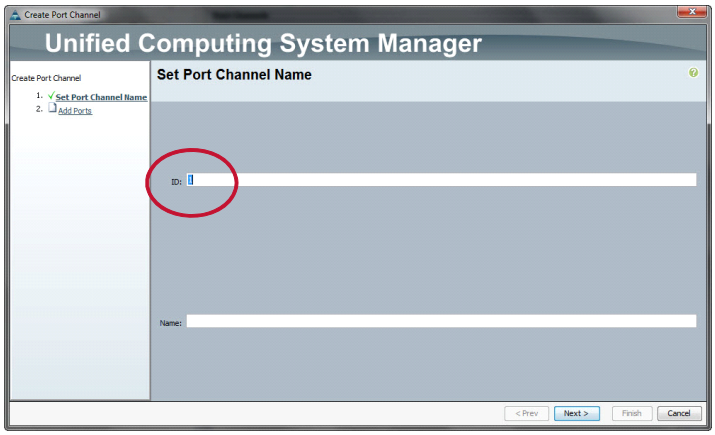


To start the port channel wizard, click **LAN Cloud** in the LAN tab in the navigation pane and expand one of the fabric interconnects. The port channels are created per fabric interconnect. When you click port channels, you can either right-click to start the wizard or click the plus sign (+).

https://t.me/learningnets

Assign a Port Channel ID

- The port channel ID must be a number.
- The name cannot contain spaces.



© 2012 Cisco and/or its affiliates. All rights reserved.

The first step in the port channel wizard is to assign a port channel ID to the new port channel. A port channel ID must be unique on its fabric interconnect. Optionally, a name can be assigned and associated with a port channel ID. The name cannot contain spaces.

The port channel ID can be any number in the range from 1 to 256.

The name can consist of up to 16 alphanumeric characters.

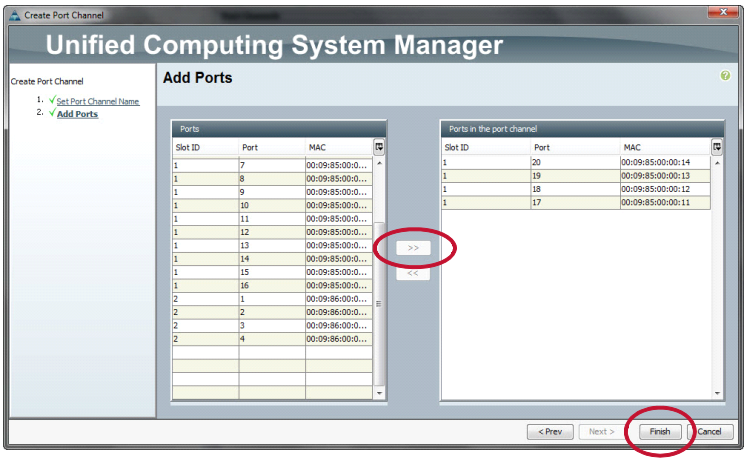
Note	Hyphens and special characters are not allowed.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Select Port Channel Ports

- Select the unused ports that will form the port channel.
- Click Finish to complete the wizard.



© 2012 Cisco and/or its affiliates. All rights reserved.

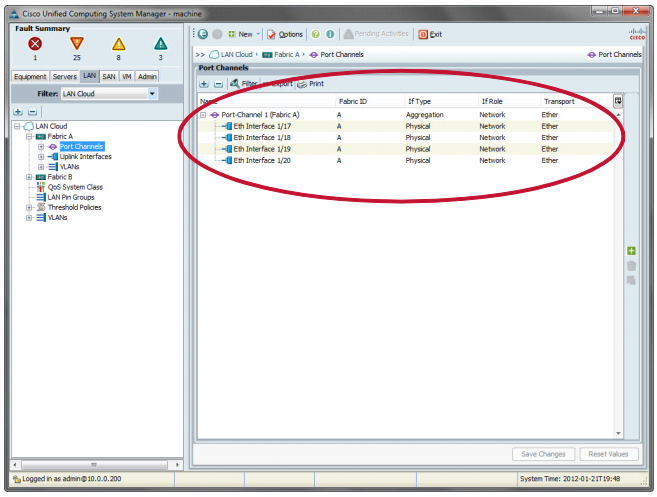
In the left portion of the window, select the interfaces that should participate in a port channel. Click the double right-arrow to move those interfaces into the new port channel. Click **Finish** in the lower-right corner of the dialog box to complete the port channel creation wizard.

The ports that you select are usually the uplink Ethernet ports. If you select an unconfigured port, it will be configured automatically as an uplink port. If you select a server port, the system will issue a warning. If you confirm your selection, then the server port will be reconfigured as an uplink port.

https://t.me/learningnets

Verify the Port Channel

- Port Channel 1 is now available.



© 2012 Cisco and/or its affiliates. All rights reserved.

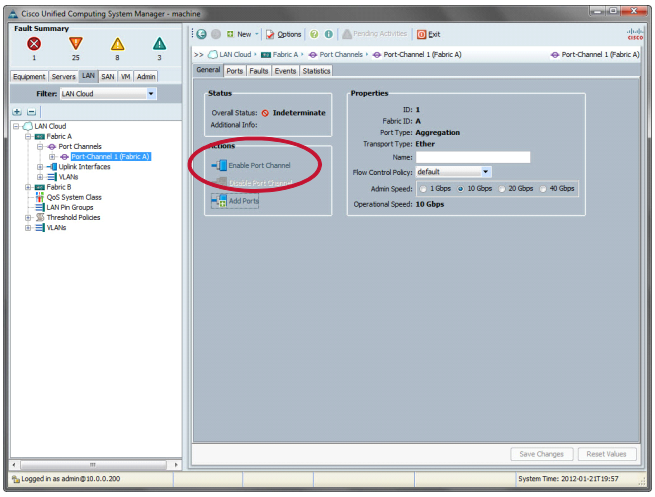
After you finish the port channel wizard, you will see that the port channel was created and is available in the content pane. You will see information for the ports that participate in this port channel and their status.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Enable the Uplink Ethernet Port Channel

- To enable the uplink port channel, click it.



© 2012 Cisco and/or its affiliates. All rights reserved.

To enable a port channel, go to the **LAN** tab, expand **LAN Cloud**, expand the fabric interconnect on which the port channel exists, and select it by clicking it.

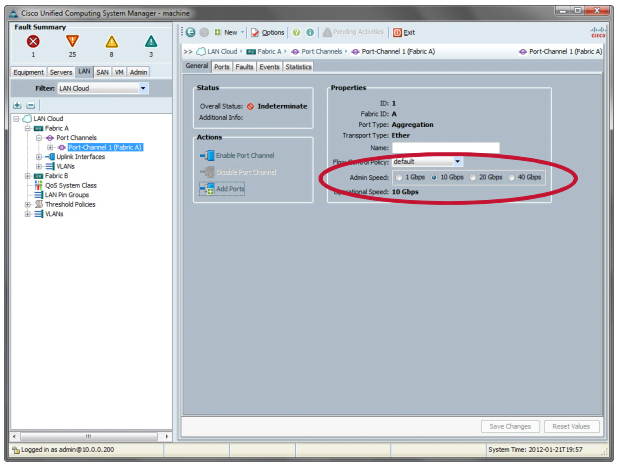
In the content pane, in the General tab, you will see the status of the port channel, the properties, and available actions.

To enable it, click **Enable Port Channel**.

https://t.me/learningnets

Port Channel Speed

- Beginning with Cisco UCS Manager version 1.3, port channels can operate at either 1 Gb/s or 10 Gb/s.*
- Beginning with Cisco UCS Manager version 2.0 the available speeds are 1, 10, 20, or 40 Gb/s.**



* Only certain ports on a generation 1 fabric Interconnect can be configured for 1-Gb/s operation.

** Only generation 2 fabric interconnects support 20-Gb/s and 40-Gb/s operation.

© 2012 Cisco and/or its affiliates. All rights reserved.

From the same location, you can change the port channel speed.

Starting with version 1.3, port channels can operate at speeds of 1 Gb/s or 10 Gb/s.

Beginning with Cisco UCS Manager 2.0, 20-Gb/s and 40-Gb/s speeds can be configured on fabric port channels. Fabric port channels are links from the Cisco 6200 Series Fabric Interconnect to the Cisco 2208 I/O Module (IOM). The only mezzanine card that supports the higher speeds is the Cisco Virtual Interface Card (VIC) 1280.

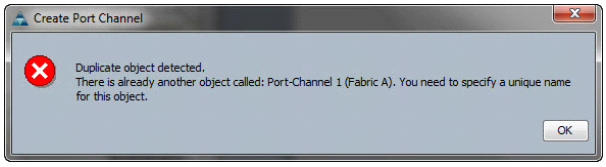
The higher-speed port channels are not available with first-generation fabric interconnects, IOMs, or mezzanine cards.

 © 2012 Cisco Systems, Inc.

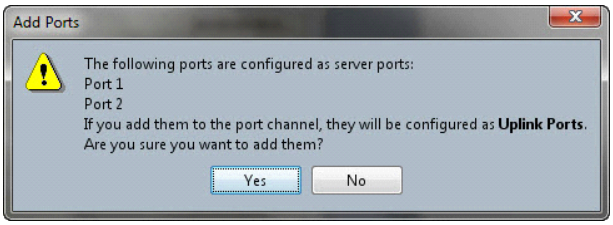
https://t.me/learningnets

Port Channel Errors and Warnings

- The port channel wizard detected a duplicate ID.



- Server ports cannot join a port channel.



© 2012 Cisco and/or its affiliates. All rights reserved.

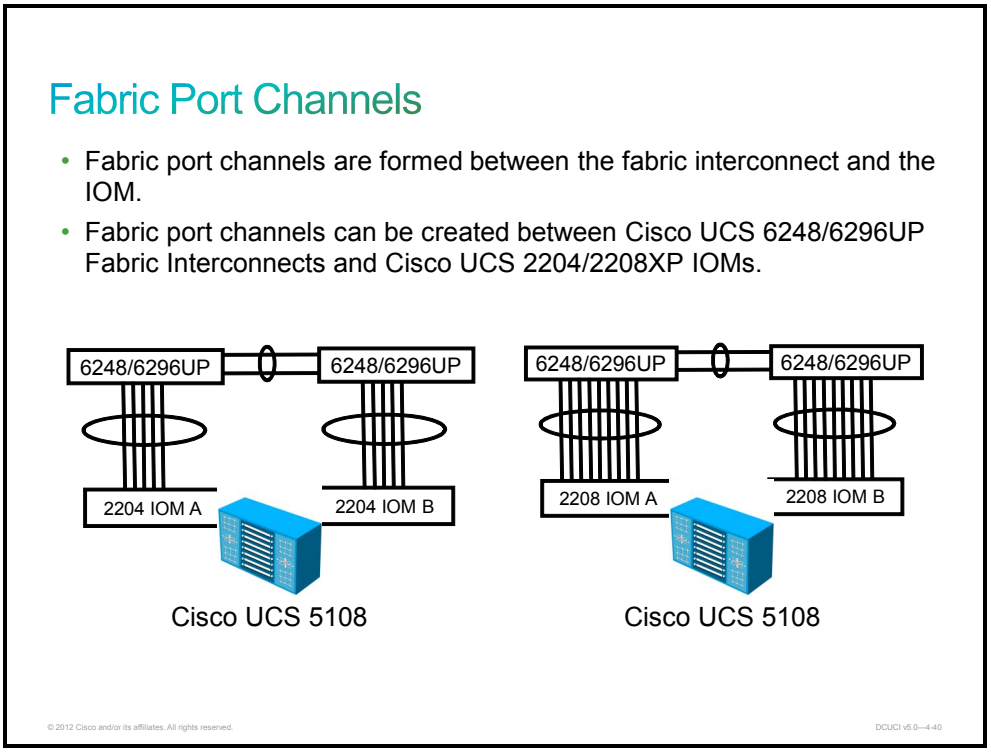
The port channel wizard includes logic to prevent duplicate port channel IDs. When this situation occurs, the system will generate an error message and you will be allowed to continue after you change the port channel ID.

The system also warns you that server links will be converted to uplinks before they can become members of a port channel. This warning message provides a choice. You can continue and reconfigure the server ports as uplink ports or return to the wizard and change the chosen ports.

https://t.me/learningnets

Provision Fabric Port Channels from the Cisco UCS Fabric Interconnect to a Cisco 2208 IOM

This topic shows the steps to provision fabric port channels in Cisco UCS.



Fabric port channels are the port channels that are created on the links between the fabric interconnect and the IOMs. Cisco UCS Manager supports the creation of fabric port channels only between Cisco 6248UP Fabric Interconnects and Cisco 2208 IOMs.

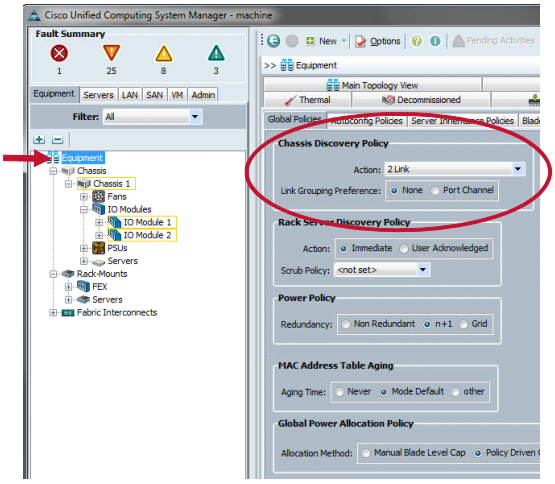
When there is a fabric port channel between a fabric interconnect and an IOM, then the server traffic is pinned to the vPC interface, higher bandwidth is utilized, and there is a load-balancing scheme applied. The load-balancing scheme is *source-dest-mac* and is not user configurable.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Fabric Port Channel Provisioning

- Fabric port channels are formed automatically by the system
- Depends on the global chassis discovery policy
- Port channel ID is assigned automatically
- Action—discover the number of links
- Link grouping preference
  - None (default)
  - Port channel



© 2012 Cisco and/or its affiliates. All rights reserved.

Fabric port channels are formed automatically by Cisco UCS Manager when the appropriate hardware is available and based on the setting in the Global Chassis Discovery Policy.

A port channel ID is assigned automatically by the system. No user intervention is required.

The global chassis discovery policy defines how Cisco UCS Manager discovers the chassis. To access the settings for the global chassis discovery policy, from the Equipment tab, navigate to **Equipment > Global Policies**.

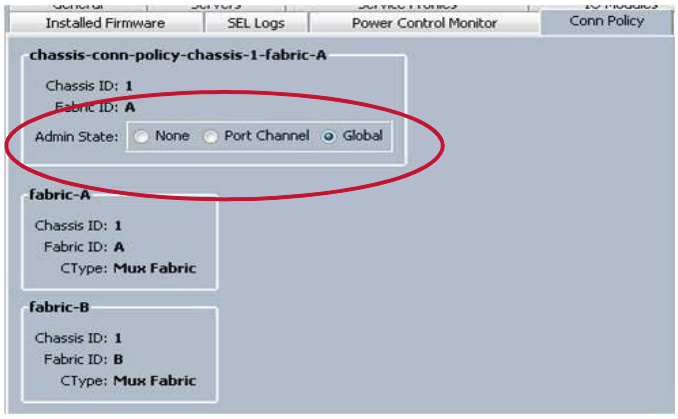
The following are the available settings:

- **Action:** Define the minimum links discovery policy. For example, what is the minimum number of links needed between the fabric interconnect and the IOM for Cisco UCS Manager to discover the chassis?
- **Link Grouping Preference:** Determines how the Cisco UCS Manager treats the available links.
  - **None (default):** The links will be utilized as individual links and then the rules for pinning the traffic from the servers to the IOM uplink ports will be followed.
  - **Port Channel:** This option instructs Cisco UCS Manager to form a fabric port channel from the available links.

https://t.me/learningnets

Fabric Port Channels Per Chassis

- Fabric port channels per individual chassis depend on the chassis connectivity policy.
- The chassis connectivity policy will be available for configuration when Cisco 2208 IOM and 6248UP are present.



© 2012 Cisco and/or its affiliates. All rights reserved.

If you need to specify different behavior for an individual chassis, then you must also configure the chassis connectivity policy. Unlike the configuration of the global chassis discovery policy, which is performed globally and affects all the chassis under the Cisco UCS Manager instance, the chassis connectivity policy is configured on a per-chassis basis.

To access the chassis connectivity policy, from the Equipment tab, navigate to **Equipment > Chassis > Chassis # > Connectivity Policy**.

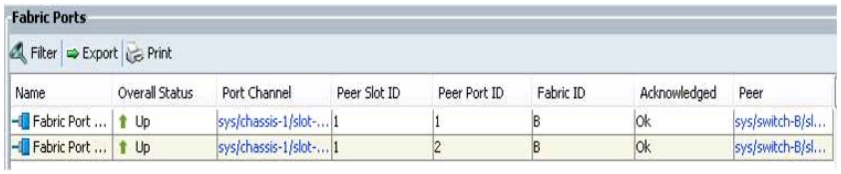
If the supported hardware is available, for example, the Cisco 6248UP Fabric Interconnect and 2208 IOM, you will be allowed to change the Admin State. The following are the available options:

- **None:** The links for this chassis will be treated as individual links. No port channel will be formed.
- **Port Channel:** A port channel will be formed.
- **Global (default):** The settings from the global chassis discovery policy will be inherited.

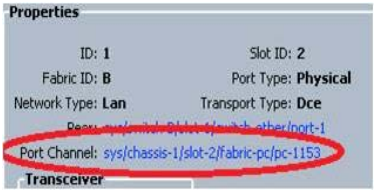
https://t.me/learningnets

Verify Fabric Port Channels

- Fabric ports table



- Fabric ports properties



© 2012 Cisco and/or its affiliates. All rights reserved.

To verify the configuration and operational state of the fabric ports on the IOM, from the **Equipment** tab, navigate to **Equipment > Chassis > Chassis # > IO Modules > IO Module 1/2.** Then choose the **Fabric Ports** tab in the content pane. From that tab, you will see a list of the fabric ports and information describing if they operate as members of a fabric port channel.

To look at the properties of a specific fabric port, from the **Equipment** tab, navigate to **Equipment > Chassis > Chassis # > IO Modules > IO Module 1 or 2 > Fabric Ports > Fabric Port 1/#**.

The content pane will display properties for the fabric port and in which port channel it participates.

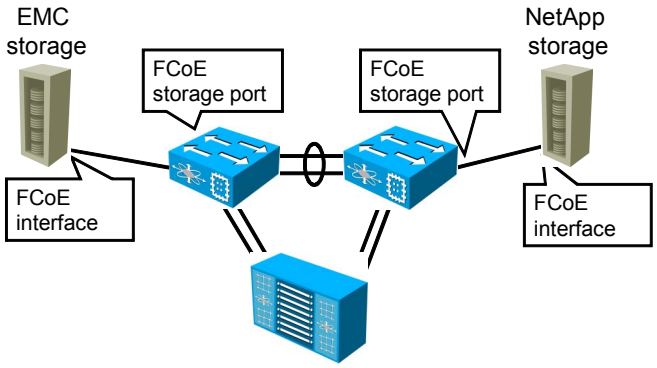
https://t.me/learningnets

Provision FCoE Storage Ports

This topic describes how to provision FCoE storage ports.

FCoE Storage Port Role

- NetApp and EMC storage systems can be connected to FCoE storage ports on the fabric interconnects.
- NetApp and EMC storage systems must be equipped with 10-Gb/s FCoE-capable interfaces.



© 2012 Cisco and/or its affiliates. All rights reserved.

Ethernet ports on the fabric interconnects can be configured as FCoE storage ports. FCoE protocol communication will go through these ports, which requires a minimum bandwidth of 10 Gb/s.

You can connect storage systems that are equipped with FCoE-capable interfaces at 10 Gb/s to FCoE storage ports.

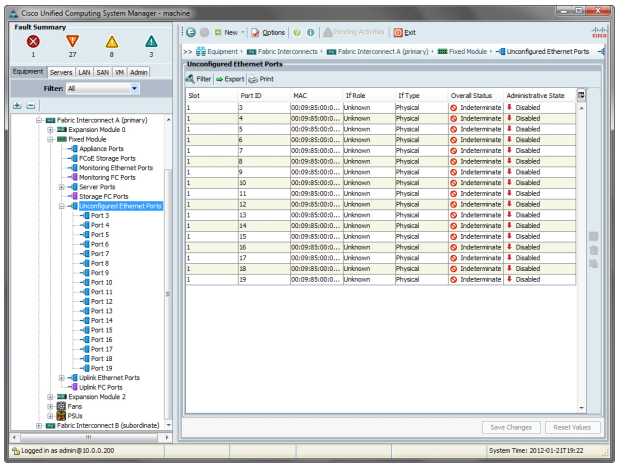
Currently, only EMC and NetApp deliver FCoE-based storage systems. These systems are certified by Cisco for use with Cisco UCS.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision FCoE Storage Ports

- From the navigation pane, navigate to Equipment > Fabric Interconnects > Fabric Interconnect A or B > Fixed or Expansion Module > Unconfigured Ethernet Ports.



© 2012 Cisco and/or its affiliates. All rights reserved.

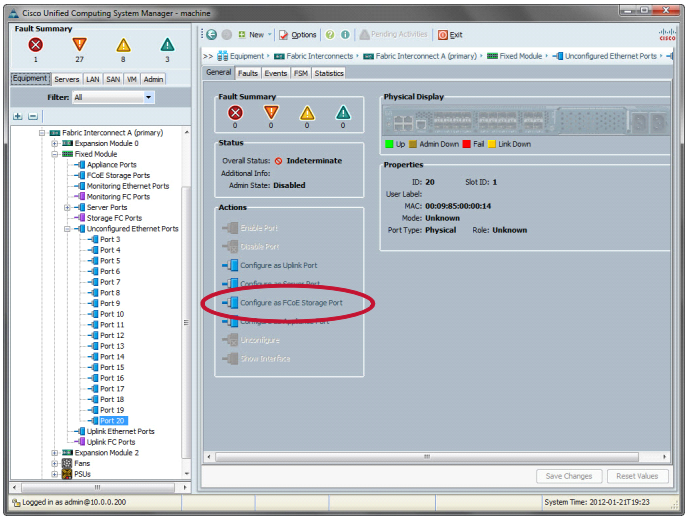
To configure an FCoE port, choose ports from the Fixed Module or the Expansion Module.

Note	To directly attach a storage system, the Fibre Channel switching mode must be set to Switching. FCoE storage ports are not supported in end-host mode.

https://t.me/learningnets

Select an Unconfigured Port

- Select a port from Unconfigured Ethernet Ports.



© 2012 Cisco and/or its affiliates. All rights reserved.

From either the Fixed Module or Expansion Module, expand **Unconfigured Ethernet Ports** and click an available port.

The available commands will be shown in the General tab. Click **Configure as FCoE Storage Port**.

https://t.me/learningnets

FCoE Ports Requirement

- FCoE ports are supported only in Fiber Channel switching mode.
- Prior to configuring an FCoE storage port, ensure the mode is set to FC Switching.

© 2012 Cisco and/or its affiliates. All rights reserved.

A window will open warning that it is required that the Fibre Channel switching mode must be set to Switching to support FCoE storage ports. Confirm the creation of the FCoE storage port.

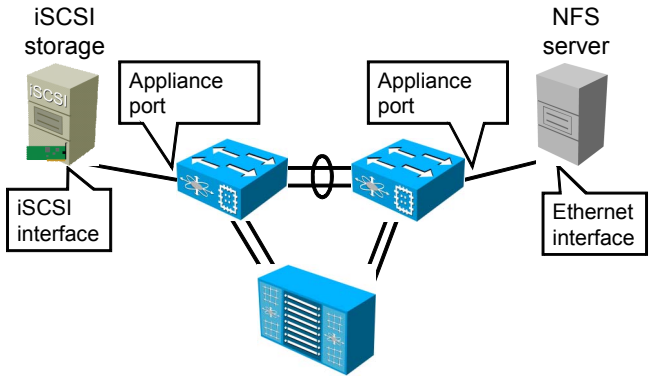
https://t.me/learningnets

Provision Appliance Ports and Prune VLANs

This topic describes how to provision appliance ports.

Appliance Port Role

- Appliance ports are used to directly attach iSCSI storage or NAS filers to fabric interconnects.
- The Cisco Nexus 1010 appliance or security appliance can be connected also.



© 2012 Cisco and/or its affiliates. All rights reserved.

Ethernet ports on the fabric interconnects can be configured as appliance ports. The appliance ports are used to directly attach a storage system with an Internet Small Computing Systems Interface (iSCSI). Cisco UCS Manager version 2.0 supports iSCSI interfaces on VICs for an iSCSI-based boot.

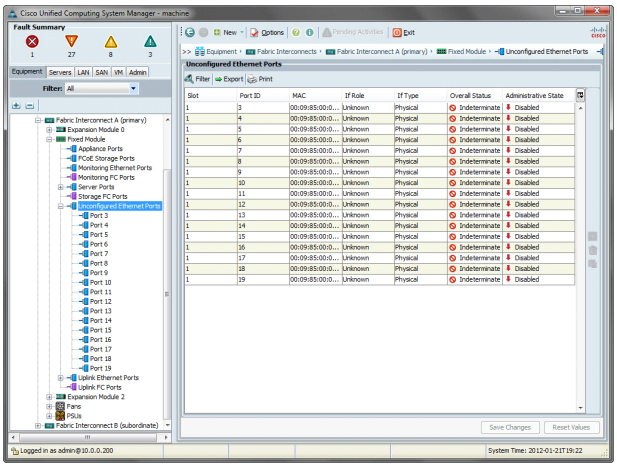
You can attach network-attached storage (NAS) filers, like a Network File System (NFS) server, to the appliance ports.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision Appliance Ports

- From the navigation pane, navigate to **Equipment > Fabric Interconnects > Fabric Interconnect A or B > Fixed or Expansion Module > Unconfigured Ethernet Ports**.



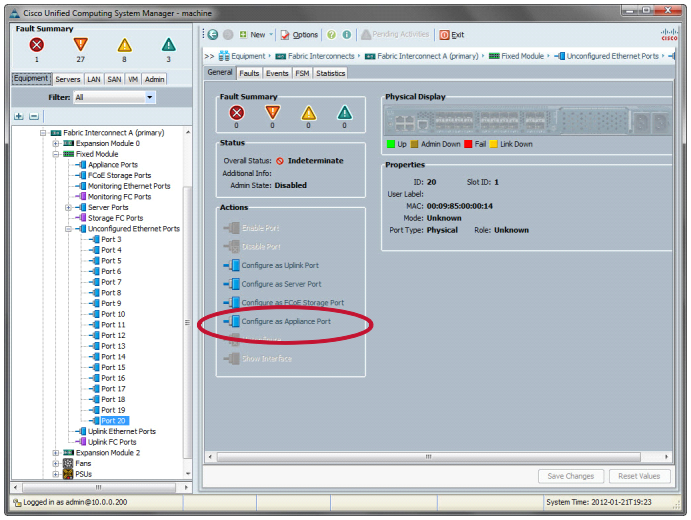
© 2012 Cisco and/or its affiliates. All rights reserved.

DCUCI v5.0—4-51

To configure a port as an appliance port, first choose a port from the Fixed Module or Expansion Module on a fabric interconnect.

Select an Unconfigured Ethernet Port

- Select a port from Unconfigured Ethernet Ports.



© 2012 Cisco and/or its affiliates. All rights reserved.

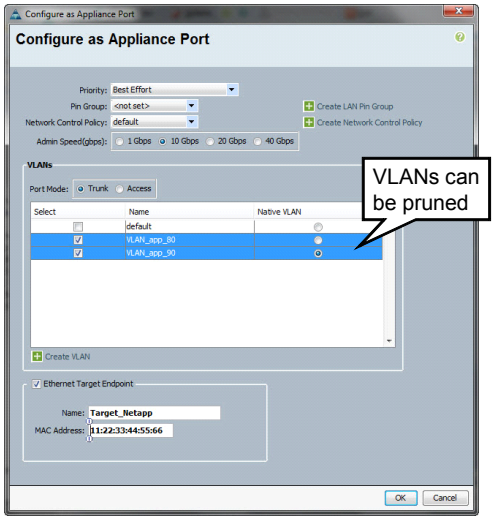
DCUCI v5.0—4-52

Click the selected port. From the content pane, click **Configure as Appliance Port**.

https://t.me/learningnets

Edit Appliance Port Parameters

- Priority
- Pin Group (if available)
- Network Control Policy
- Speed
- VLANs
  - Trunk
  - Access
- Ethernet Target Endpoint
  - Name
  - MAC Address



© 2012 Cisco and/or its affiliates. All rights reserved.

The parameters available for configuration include the following:

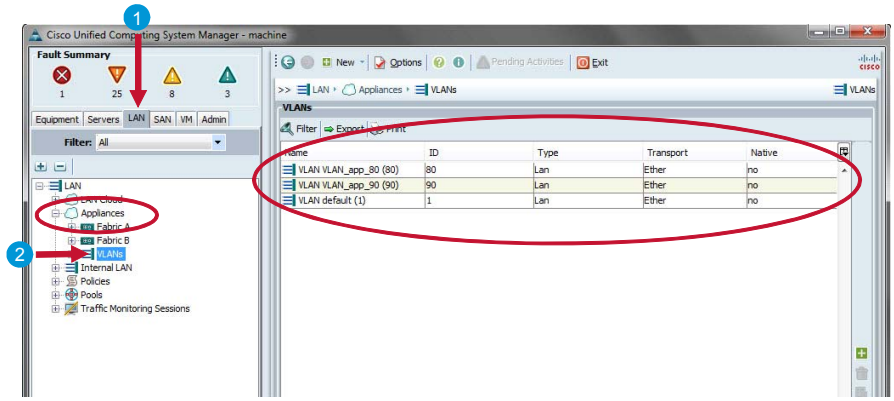
- **Priority:** A drop-down menu to select the quality of service (QoS) setting. Available options include the following:
  - **Fc:** Priority for virtual host bus adapter (vHBA) traffic only.
  - **Platinum:** Priority for vNIC traffic only
  - **Gold:** Priority for vNIC traffic only
  - **Silver:** Priority for vNIC traffic only
  - **Bronze:** Priority for vNIC traffic only
  - **Best Effort:** Not to be used; reserved for Ethernet traffic only
- **Pin Group:** If available, a drop-down menu to select a LAN pin group to pin the traffic for this appliance
- **Network Control Policy**
- **Speed**
- **VLANs:** You can select access or trunk mode and specify the allowed VLANs.
- **Ethernet Target Endpoint:** This is an optional field that defines the MAC address of the appliance that is connected. The available options include the following:
  - **Name:** Up to 16 alphanumeric characters; no hyphens or special characters allowed
  - **MAC address:** The MAC address of the endpoint target

The option to choose which VLANs to allow is called VLAN pruning. With this option, you control which VLANs will be allowed to communicate over this port.

https://t.me/learningnets

Appliance Port VLANs

- VLANs used by appliance ports are locally significant and are called internal VLANs.
- They must be created in LAN > Appliances > VLANs.



© 2012 Cisco and/or its affiliates. All rights reserved.

The VLANs that are used for communication through appliance ports are locally significant. These VLANs are called internal VLANs. They are not configured in the LAN Cloud, but in the Appliances option.

To create them, navigate to **LAN > Appliances > VLANs**.

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.

Summary

- VLANs can be provisioned to exist on both fabric interconnects, only on fabric interconnect A or B, or can be configured to service different VLAN IDs.
- VLAN ranges can be provisioned for easier and quicker VLAN creation.
- Private VLANs can be used to subdivide a VLAN and to isolate communication on server ports.
- Ethernet uplinks are provisioned to provide the connectivity to the LAN infrastructure.
- Ethernet uplink port channels can be used for redundancy and load balancing.
- Fabric port channels can be created automatically by the system between Cisco 6248/6296UP Fabric Interconnects and Cisco 2204/2208XP IOM. Chassis discovery policy must be set globally to Port Channel.
- FCoE storage ports can be provisioned to directly attach an FCoE-capable storage system only in Fiber Channel switching mode.
- Appliance ports can be provisioned to attach directly to NAS filers, iSCSI storage devices, the Cisco Nexus 1010, or security appliances.

© 2012 Cisco and/or its affiliates. All rights reserved.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 3

Provisioning SAN Networking

Overview

A Cisco Unified Computing System (UCS) must be connected to the SAN infrastructure of the data center to provide access to storage resources for the servers. In this lesson, you will provision SAN connectivity.

You will provision virtual storage area networks (VSANs), Fibre Channel uplinks, Fibre Channel trunking, Fibre Channel port channels, and direct-attach Fibre Channel storage ports.

Objectives

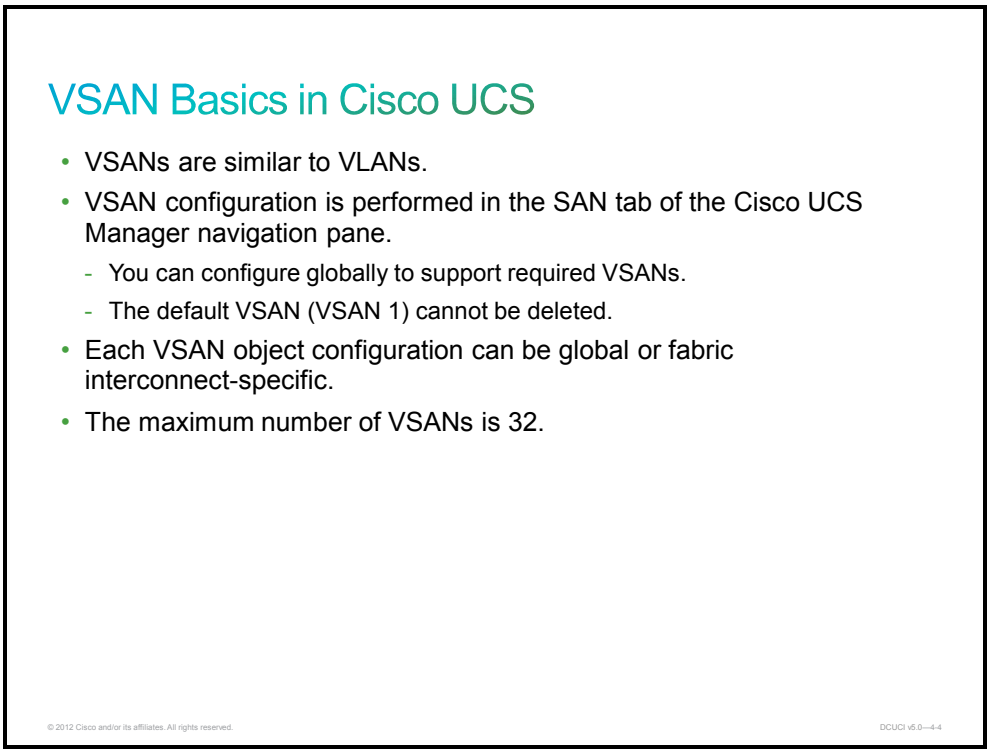
Upon completing this lesson, you will be able to provision VSANs and fabric interconnect Fibre Channel uplinks for server connectivity to the data center storage cloud. This ability includes being able to meet these objectives:

- Provision VSANs for single fabric, both fabrics, and both fabrics configured differently
- Provision Fibre Channel uplinks and VSAN trunking
- Provision Fibre Channel port channels
- Provision direct-attach Fibre Channel storage ports and default zoning

https://t.me/learningnets

Provision VSANs

This topic describes how to provision VSANs that exist on both fabric interconnects, only on Fabric A or B, or on both fabric interconnects but with different configuration.



The VSAN concept is similar to the VLAN concept. VSANs are used to provide logical separation and segmentation for the Fibre Channel Protocol (FCP) communication.

Cisco UCS Manager supports a maximum of 32 active VSANs.

Supported VSAN IDs range from 1 to 4093. VSAN ID 4079 is reserved because it is used by other protocols in SAN infrastructures. In Cisco N-Port Virtualizer (NPV) mode, VSAN IDs 3840 to 4079 are not available.

VSAN objects can be created in three modes in Cisco UCS Manager:

- To exist on both fabric interconnects with one configuration
- To exist only on Fabric A or B
- To exist on both fabric interconnects, but to use different VSAN IDs for each

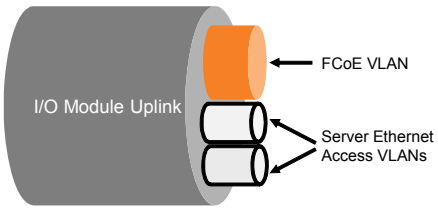
The default VSAN (VSAN 1) exists on the system and cannot be deleted.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

FCoE VLAN

- You must specify an FCoE VLAN for each VSAN.
- All server Fibre Channel traffic is carried via FCoE in dedicated VLANs.
- FCoE VLANs must not conflict with Cisco UCS Manager VLAN objects.
- Select an unused range of VLANs and dedicate that range to FCoE.



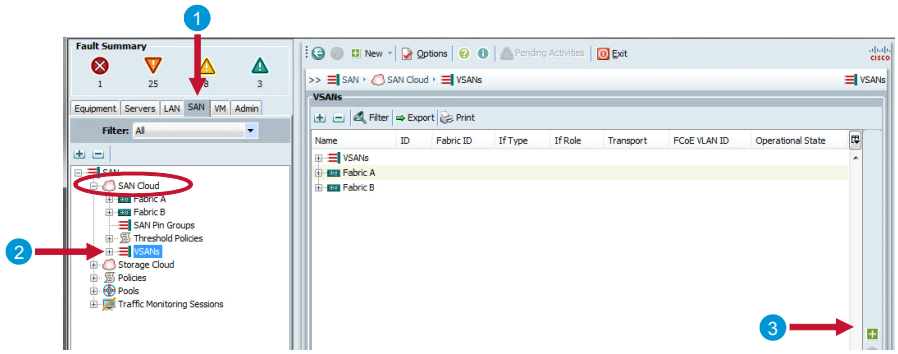
© 2012 Cisco and/or its affiliates. All rights reserved.

Because of the internal Fibre Channel over Ethernet (FCoE) architecture of Cisco UCS, each VSAN supported within the architecture requires a dedicated VLAN to carry FCoE traffic. FCoE VLANs are designated during VSAN configuration and are not created like Ethernet VLANs. FCoE VLANs must not conflict with Ethernet VLAN objects. The relationship between a VSAN and an FCoE VLAN is 1:1. This one-to-one relationship means that for each VSAN, you must have a dedicated FCoE VLAN.

https://t.me/learningnets

Start the VSAN Creation Wizard

- Start the VSAN wizard by navigating to SAN > SAN Cloud > VSANs.



© 2012 Cisco and/or its affiliates. All rights reserved.

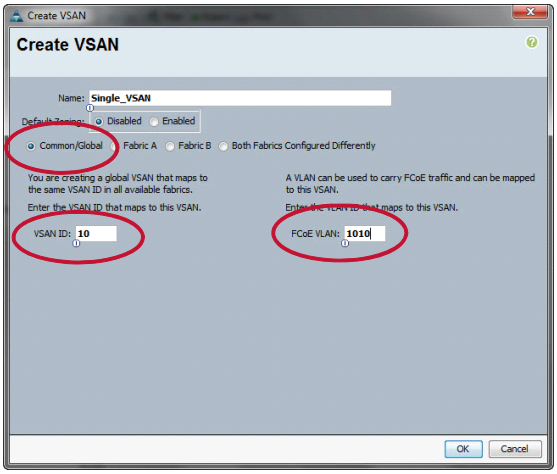
To start the VSAN creation wizard, choose the **SAN** tab from the navigation pane, and then navigate to **SAN Cloud > VSANs**. You can either right-click **VSANs** and choose **Create VSANs** or click the plus sign (+) in the content pane to start the VSAN creation wizard.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision a Single VSAN

- A VSAN name can be up to 32 characters long.
- A single VSAN will exist on both fabric interconnects.



© 2012 Cisco and/or its affiliates. All rights reserved.

In Cisco UCS, VSANs require a name and a number. VSAN names are always used in the creation of virtual host bus adapter (vHBA) profiles. This abstraction of the VSAN number allows a change of VSAN associated with the VSAN names without requiring configuration changes to the server.

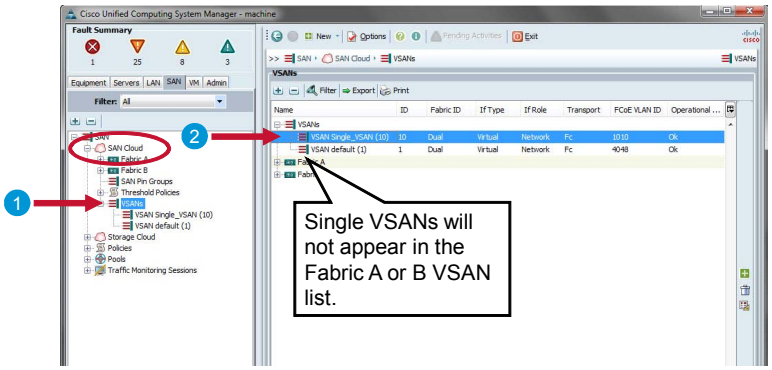
Common or global VSANs are created on both fabric interconnects and will use the same VSAN ID and FCoE VLAN. This type of configuration requires both fabric interconnects to be connected to the same physical Fibre Channel fabric. This configuration is not conducive to a high-availability design because of the single point of failure.

The Default Zoning setting will be discussed later in this lesson.

https://t.me/learningnets

Verifying Single VSANs

- Common or global VSANs can be seen in the global list under SAN Cloud.



© 2012 Cisco and/or its affiliates. All rights reserved.

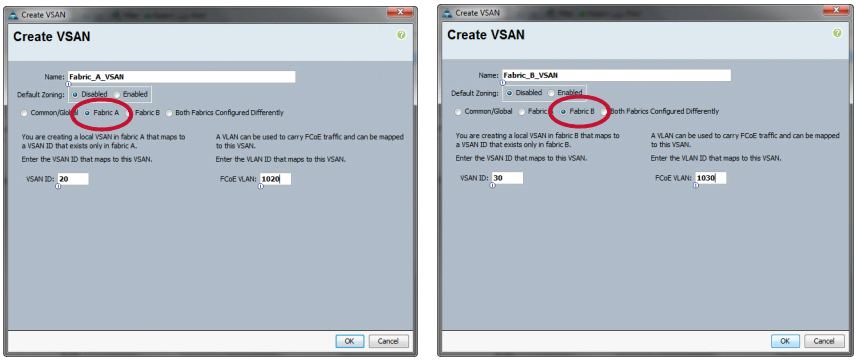
To verify the creation of a common or global VSAN, from the SAN tab choose **SAN Cloud > VSANs**. The newly created VSAN will be in the global VSAN list in the content pane. The common or global VSANs will not appear in the VSAN list for Fabric A or Fabric B.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision Fabric-Only VSANs

- Fabric_A_VSAN is only available to servers connected to Fabric A.
- Fabric_B_VSAN is only available to servers connected to Fabric B.



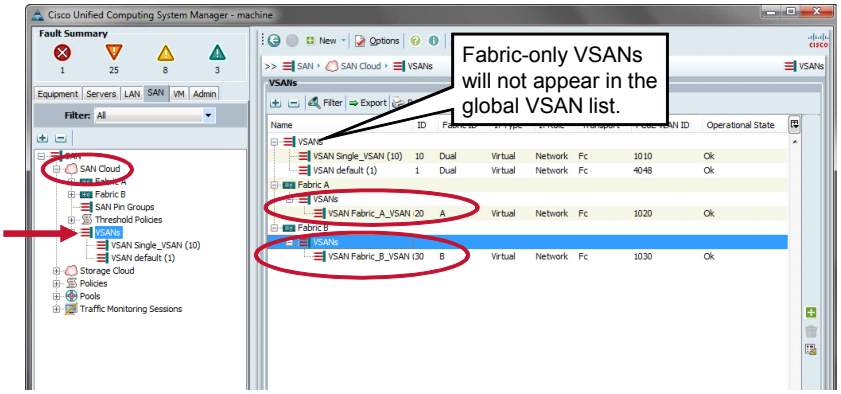
© 2012 Cisco and/or its affiliates. All rights reserved.

Fabric-only VSANs can be created, if desired. Such a VSAN will exist only on Fabric A or only on Fabric B. In the figure, Fabric_A_VSAN will be created only on fabric interconnect A, and Fabric_B_VSAN will exist only on fabric interconnect B. In this configuration, each fabric interconnect would connect to a different upstream Fibre Channel switch. This configuration closely models traditional Fibre Channel designs and maintains the physical separation of the switch fabrics.

https://t.me/learningnets

Verifying Fabric-Only VSANs

- Fabric-only VSANs can be seen in the VSANs list for the specific fabric.



© 2012 Cisco and/or its affiliates. All rights reserved.

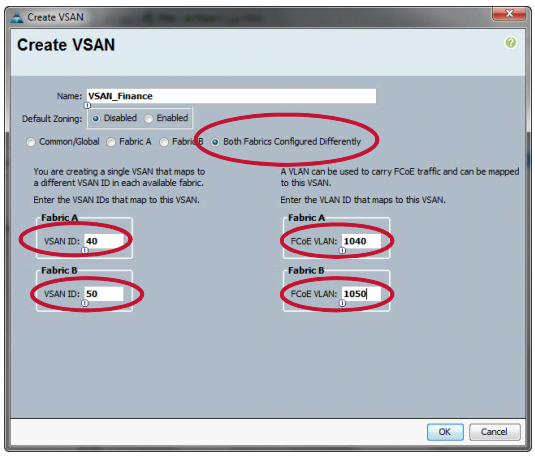
Because fabric-only VSANs exist only on one fabric interconnect, you must navigate to VSANs under SAN Cloud to verify their creation. You must choose a specific fabric interconnect to see the list of fabric-only VSANs for that fabric. You will see the new VSAN in the list. In the example, Fabric_A_VSAN will be available only in the VSAN list of fabric interconnect A and Fabric_B_VSAN will be in the VSAN list of fabric interconnect B.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision Fabric-Specific VSANs

- VSAN_Finance is created with a different VSAN number on each fabric.
- For each VSAN ID, there must be a unique FCoE VLAN configured.



© 2012 Cisco and/or its affiliates. All rights reserved.

When you select the Both Fabrics Configured Differently option, the same VSAN label is applied to two separate VSANs and FCoE VLANs. For this configuration to behave as expected, the same external resources need to be accessible through each of the upstream fabrics.

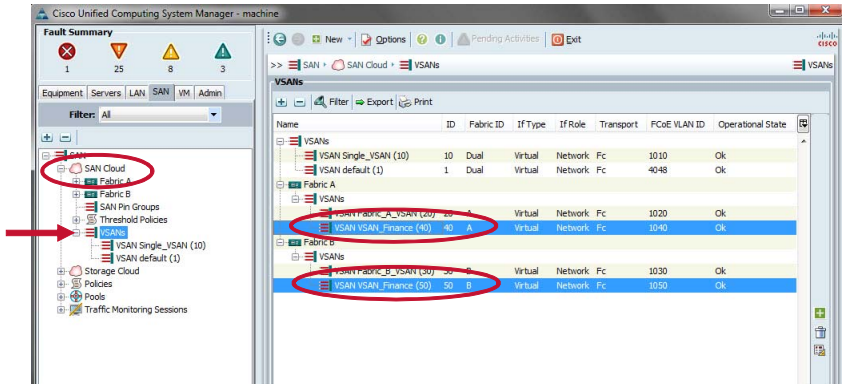
In this situation, you must specify different VSAN IDs for use on Fabric A and on Fabric B. A separate FCoE VLAN must be specified for each of the VSAN IDs.

Using this method to create a VSAN, you will provision a VSAN from one place with one label. Although the VSAN has the same label, the two fabric interconnects will use different VSAN IDs. For the external SAN infrastructure, it will be as if you are using two separate VSANs. From the Cisco UCS perspective, you use the same VSAN with different IDs for the separate communication paths. You will provision the two VSANs from one place, allowing you to stay consistent with the redundant SAN design.

https://t.me/learningnets

Verifying Fabric-Specific VSANs

- Fabric-specific VSANs can be seen in the VSAN list for each fabric using different VSAN IDs.



© 2012 Cisco and/or its affiliates. All rights reserved.

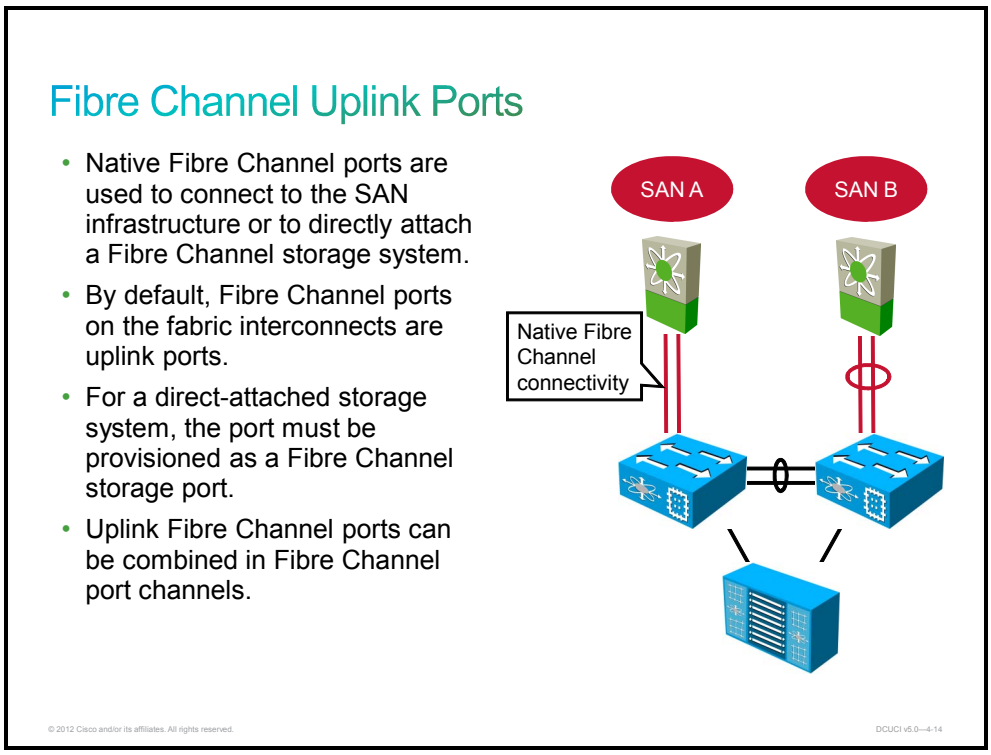
To verify the creation of the fabric-specific VSAN, from the SAN tab, navigate to **SAN Cloud > VSANs**. In the content pane, the VSAN will be visible in the VSAN lists of each fabric interconnect, but it will show the VSAN ID only for the corresponding fabric. In the example, you can see that VSAN_Finance is visible in both of the VSAN lists. You can also see that the Fabric A VSAN ID is 40 and the Fabric B VSAN ID is 50.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision Fibre Channel Uplinks and VSAN Trunking

This topic describes how to provision Fibre Channel uplink ports and enable VSAN trunking.



The fabric interconnects use native Fibre Channel ports to connect to the SAN infrastructure or to directly connect a Fibre Channel storage array. When you connect to upstream Fibre Channel switches, the Fibre Channel ports are uplink ports. You can connect to upstream Cisco MDS switches or to Cisco Nexus 5000 or 5500 switches if they operate in Fibre Channel switching mode.

On the Cisco UCS 6100 Series, you can have Fibre Channel ports only on the expansion ports. The maximum number of Fibre Channel ports for the Cisco UCS 6120 is eight ports at a speed of 4 Gb/s or six ports at a speed of 8 Gb/s. For the Cisco UCS 6140, the port limits are 16 ports at 4 Gb/s or 12 ports at 8 Gb/s. For the Cisco UCS 6248UP, you can have up to 48 Fibre Channel ports, supporting speeds of 1, 2, 4, or 8 Gb/s, depending on the small form-factor pluggable (SFP) used and on the ports at the upstream switch.

Before Cisco UCS Manager version 1.4, each Fibre Channel port supported only one VSAN. Starting with version 1.4, Fibre Channel uplink ports supported VSAN trunking. In both cases, there must be the same configuration on the upstream switch. This means that the VSAN that you allow on the fabric interconnect Fibre Channel uplink port must be the same on the remote port. If you have enabled VSAN trunking on the upstream switch Fibre Channel port, then you must also enable it on the fabric interconnect.

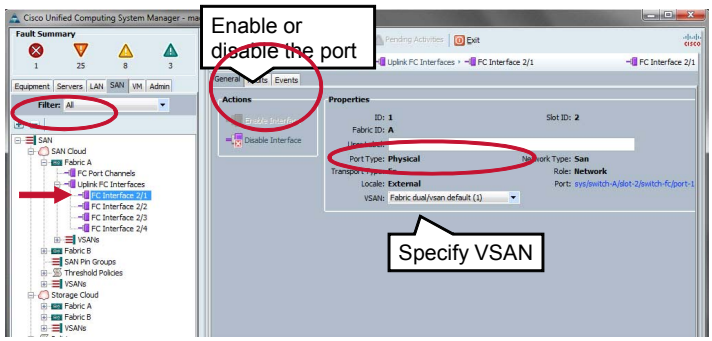
Starting from version 1.4, the Fibre Channel uplink ports can also be combined in Fibre Channel port channels. On the upstream switch, the same configuration must be performed.

Because the fabric interconnects can operate in Cisco NPV (end-host) mode or in Fibre Channel switching mode, the Fibre Channel uplink ports support VSAN trunking and Fibre Channel port channels in both modes.

https://t.me/learningnets

Administer Fibre Channel Uplink Ports

- By default, Fibre Channel ports are uplink ports.
- Navigate to SAN Cloud > Fabric A or B > Uplink FC Interfaces and click a port.



© 2012 Cisco and/or its affiliates. All rights reserved.

By default, all of the Fibre Channel ports on the fabric interconnects are uplink ports. The only option is to configure an uplink port as a Fibre Channel storage port.

To view the Fibre Channel ports on the fabric interconnect, from the SAN tab, navigate to **SAN Cloud > Fabric A** or **B > Uplink FC Interfaces**. As an alternative, you can access the Fibre Channel port from the Equipment tab by navigating to **Equipment > Fabric Interconnects > Fabric Interconnect A** or **B > Expansion Module > Uplink FC Interfaces**.

The content pane displays available options for the Fibre Channel uplink ports:

- Enable or disable the interface.
- Specify which VSAN will be allowed through the interface.

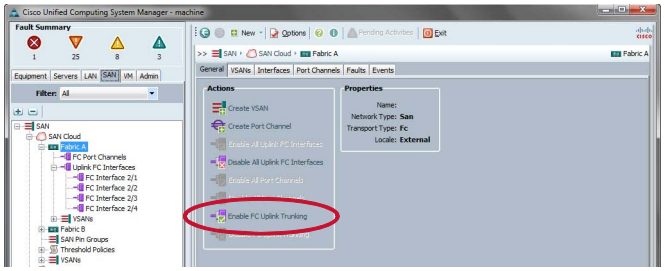
You can also see the following properties for the Fibre Channel uplink port:

- Port ID
- Slot ID
- Fabric ID
- User label
- Port type
- Network type
- Transport type
- Role
- Path to the port

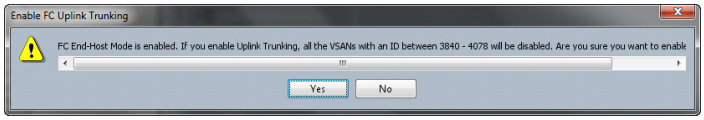
https://t.me/learningnets

Enable VSAN Trunking

- Enable VSAN trunking to allow multiple VSANs on uplink ports and on uplink Fibre Channel port channels.
- VSAN trunking is enabled globally per fabric interconnect.



- In Fibre Channel end-host mode, VSAN IDs 3840 to 4078 will be disabled.



© 2012 Cisco and/or its affiliates. All rights reserved.

Before Cisco UCS Manager version 1.4, uplink Fibre Channel ports supported only one VSAN, meaning that the Fibre Channel ports were operating only in access mode. This fact was important because the server traffic was pinned to the uplink ports based on the VSAN membership.

Since version 1.4, VSAN trunking has been supported. This feature allows Fibre Channel uplink ports and Fibre Channel port channels to operate in trunking mode and allows traffic for all external VSANs that are configured on the fabric interconnects.

The default behavior is the same as in Cisco UCS version 1.3. For example, the Fibre Channel uplink ports, by default, are E ports, allowing only a single VSAN. The VSAN trunking option must be specifically enabled.

VSAN trunking is enabled globally per fabric interconnect and puts all of the Fibre Channel uplink ports and Fibre Channel port channels in trunking mode, which means that all VSANs will be allowed on all uplink ports.

When VSAN trunking is enabled, the ports will flap. For this reason, Cisco strongly recommends that you enable VSAN trunking during maintenance windows.

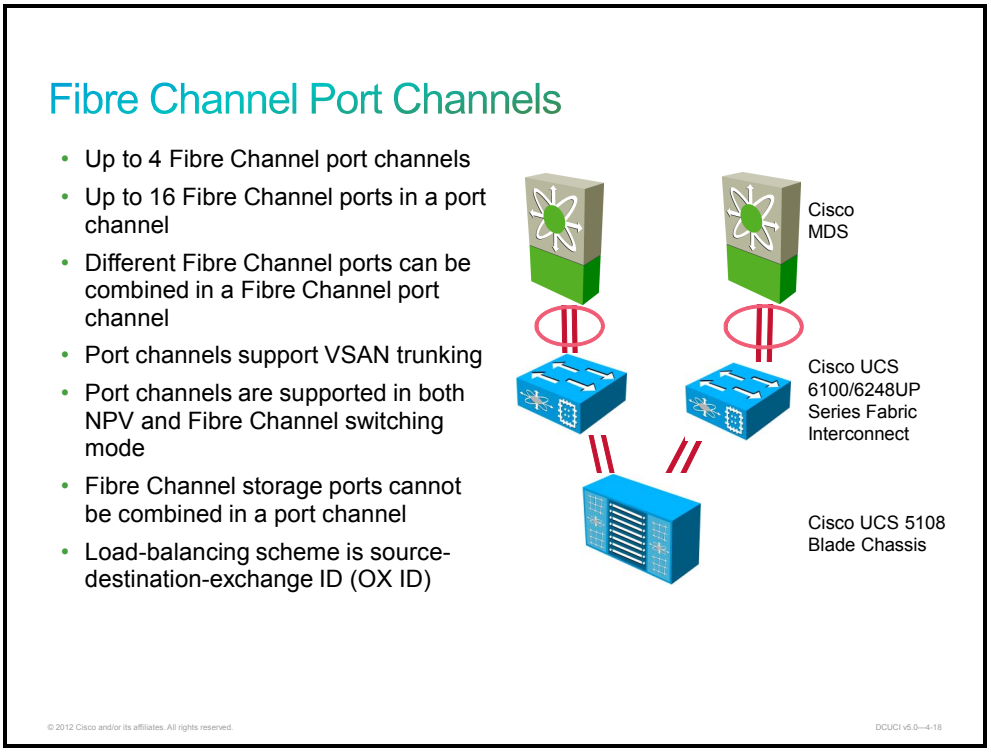
To enable VSAN trunking, under the SAN tab, navigate to **SAN Cloud > Fabric A** or **B**. In the content pane, click **Enable FC Uplink Trunking**.

When the fabric interconnect operates in end-host mode and if you enable VSAN trunking, the system will disable VSAN IDs 3840 to 4078.

https://t.me/learningnets

Provision Fibre Channel Port Channels

This topic describes how to provision Fibre Channel port channels.



Uplink Fibre Channel ports can be combined in Fibre Channel port channels. The benefits are better aggregated bandwidth and added resiliency.

When you combine the Fibre Channel uplink ports in Fibre Channel port channels at the side of the fabric interconnect, the remote ports on the upstream Fibre Channel switch must also be combined in the Fibre Channel port channel.

Cisco UCS Manager supports a maximum of 4 Fibre Channel port channels and a maximum of 16 Fibre Channel ports per port channel. Fibre Channel port channels can be formed by Fibre Channel uplink ports with different speeds.

Fibre Channel port channels support VSAN trunking. As previously mentioned, VSAN trunking is enabled globally, per fabric interconnect. Once it is enabled, all Fibre Channel uplink ports and Fibre Channel port channels are trunking.

Fibre Channel port channels and VSAN trunking are supported both in NPV mode and in Fibre Channel switching mode.

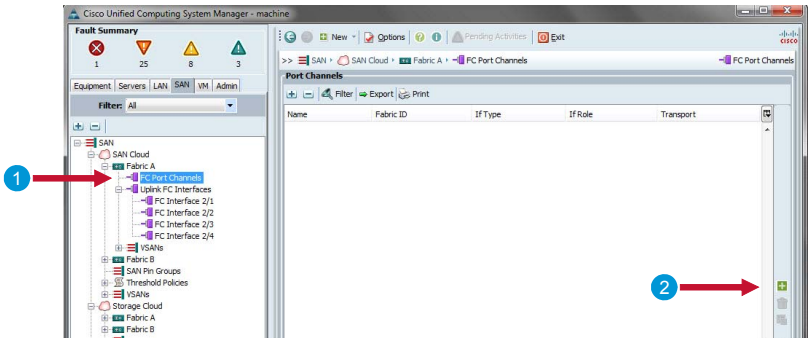
Fibre Channel port channels use a load-balancing scheme like LAN port channels. By default, the load-balancing scheme that is used in Cisco UCS is source-destination-exchange ID, also called originator exchange ID (OX ID).

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Start the Fibre Channel Port Channel Wizard

- Port channels are created independently on each fabric interconnect.
- Under SAN Cloud, choose Fabric A or Fabric B.



© 2012 Cisco and/or its affiliates. All rights reserved.

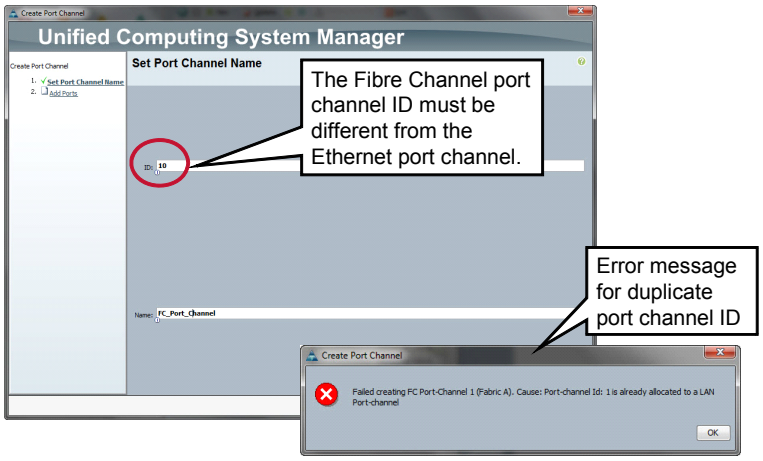
Fibre Channel port channels are created per fabric interconnect. When you want to create a Fibre Channel port channel, you have to select a fabric interconnect for it.

To start the Fibre Channel port channel creation wizard, from the SAN tab, navigate to **SAN Cloud > Fabric A** or **B > FC Port Channels**. Click the plus sign (+) on the right in the content pane.

https://t.me/learningnets

Assign a Fibre Channel Port Channel ID

- The port channel ID must be a number.
- The name cannot contain spaces.



© 2012 Cisco and/or its affiliates. All rights reserved.

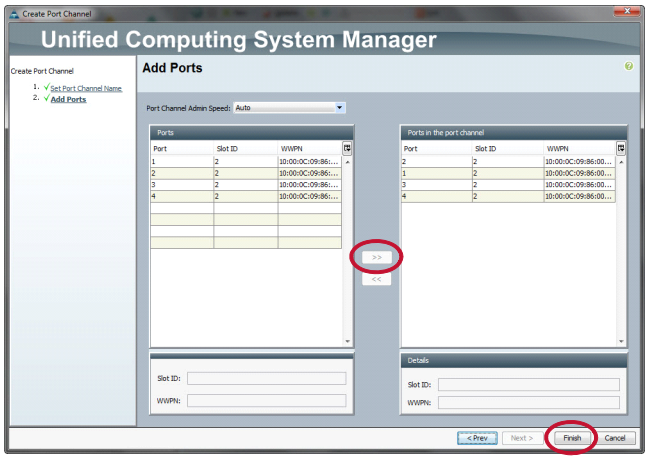
A new window will open. In that window, specify the following attributes:

- **ID:** The ID is a number specifying the unique port channel ID. Cisco UCS requires this ID to be unique and different from the LAN port channel IDs. If you specify a duplicate ID, the system will generate an error message and will not allow you to continue.
- **Name:** This field is optional. You can specify a name, which will provide you with more information for this object.

https://t.me/learningnets

Select Fibre Channel Port Channel Member Ports

- Select from the Fibre Channel uplink ports that will form the port channel.
- Click Finish to complete the wizard.



© 2012 Cisco and/or its affiliates. All rights reserved.

In the next step, you will see a list of available Fibre Channel uplink interfaces on the left. From here, choose the physical Fibre Channel ports that will become members of the Fibre Channel port channel.

Select the Fibre Channel uplink ports from the left and press the right-facing arrows (>>) to add them to the Fibre Channel port channel.

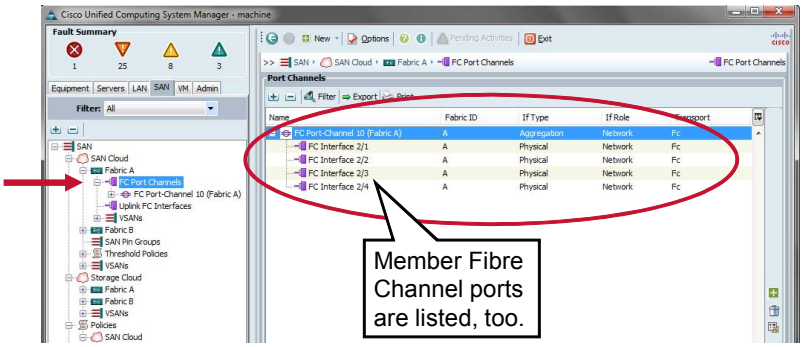
Note In Cisco UCS, you first create the Fibre Channel port channel object and then you add physical ports to it.

To finalize the creation of the Fibre Channel port channel, click **Finish**. The system will generate a message that the Fibre Channel port channel has been created successfully.

https://t.me/learningnets

Verify Fibre Channel Port Channels

- FC Port-Channel 10 is now available.



© 2012 Cisco and/or its affiliates. All rights reserved.

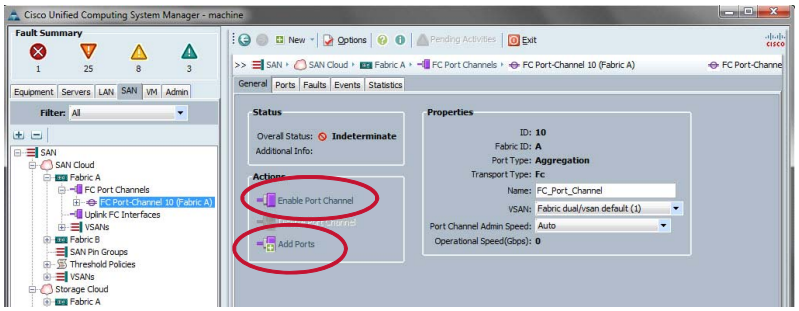
To verify the creation of the new Fibre Channel port channel, from the SAN tab, navigate to **SAN Cloud > Fabric A** or **B**. Next, click **FC Port Channels**. In the content pane, you will see a list of available Fibre Channel port channels. Click a port channel from the list to expand it. You will see information for the physical Fibre Channel member ports.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Administer Fibre Channel Port Channels

- Fibre Channel port channel options include the following:
  - Enable or disable port channel
  - Add ports
  - Change speed to 1, 2, 4, 8, or auto
  - VSANs



© 2012 Cisco and/or its affiliates. All rights reserved.

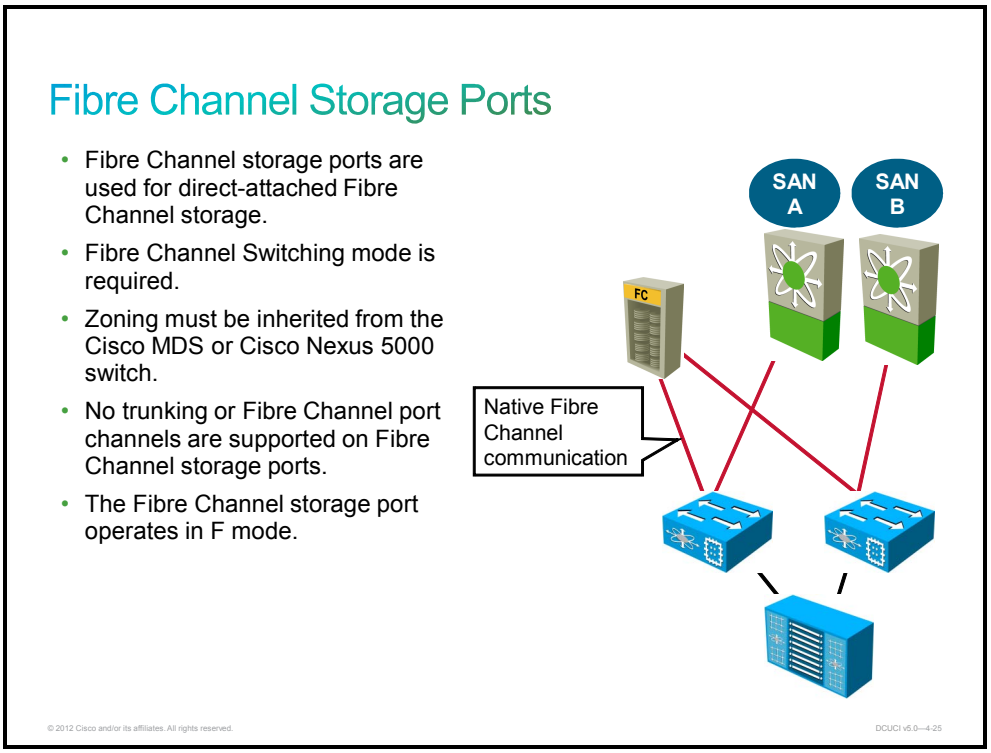
From the SAN tab, navigate to **SAN Cloud > Fabric A** or **B** and expand **FC Port Channels**. You will see the port channels that exist on that fabric interconnect. To see the properties of the Fibre Channel port channel and the available configuration options, you must click the port channel. In the content pane, you will see the following information and options:

- **Status:** Indicates status information
- **Actions:** Shows the available commands that can be executed related to the Fibre Channel port channel:
  - **Enable or Disable Port Channel:** Depending on the status, one of these options will be available and the other will be grayed out.
  - **Add Ports:** This option will allow you to add more Fibre Channel member ports
- **Properties:**
  - **ID:** The Fibre Channel port channel ID.
  - **Fabric ID:** On which fabric interconnect the Fibre Channel port channel exists.
  - **Port type**
  - **Transport type:** Because this is a Fibre Channel port channel, the transport type will be *Fc*.
  - **Name**
  - **VSAN:** Which VSAN is allowed over this virtual interface.
  - **Port Channel Admin Speed:** Define the administrative speed of the port channel. The available options are 1, 2, 4, or 8 Gb/s, or Auto.

https://t.me/learningnets

Provision Direct-Attach Fibre Channel Storage Ports and Default Zoning

This topic describes how to provision direct-attach Fibre Channel storage ports and when to enable default zoning.



By default, Fibre Channel ports on the fabric interconnects operate as Fibre Channel uplink ports to connect to the SAN infrastructure in the data center. Beginning with Cisco UCS Manager version 1.4, there is a new role that is called Fibre Channel storage port, which allows directly attaching a Fibre Channel storage system. There are some conditions for using Fibre Channel ports as Fibre Channel storage ports:

- The fabric interconnect must operate in Fibre Channel switching mode.
- A Fibre Channel uplink port must be reconfigured as a Fibre Channel storage port.
- A storage VSAN must be created.

The Fibre Channel storage ports operate as fiber ports (F ports) and do not support VSAN trunking and Fibre Channel port channels.

Initially there was a topology that was supported that allowed directly connecting a Fibre Channel storage system without any connectivity to the SAN infrastructure. In this topology, fabric interconnects operated in Fibre Channel switching mode, but did not consume domain IDs and zoning was not supported, because fabric interconnects do not natively support zoning configuration.

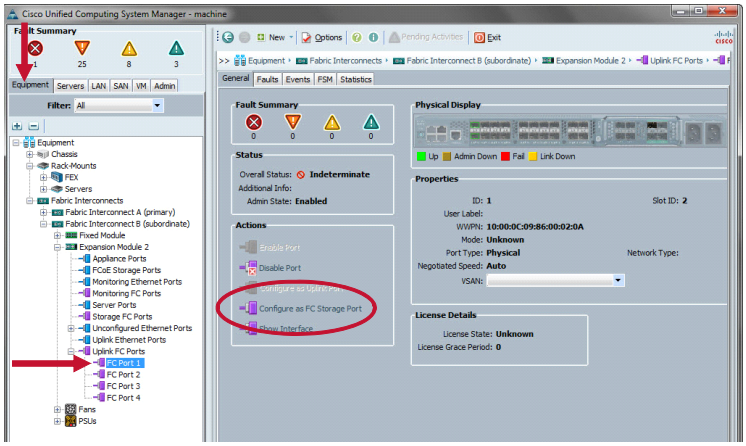
Currently, this topology is not supported. It is required that fabric interconnects connect to an upstream Cisco Nexus 7000, 5000, or 5500 switch to obtain zoning configuration, in case you need to directly attach and access a Fibre Channel storage system, as shown in the figure.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision a Fibre Channel Storage Port

- The Fibre Channel uplink port must be reconfigured as a Fibre Channel storage port.
- Select from Uplink FC Ports.



© 2012 Cisco and/or its affiliates. All rights reserved.

To provision a Fibre Channel storage port, from the Equipment tab, navigate to **Fabric Interconnects > Fabric Interconnect A** or **B > Expansion Module > Uplink FC Ports**. Expand the section and select from the Fibre Channel uplink ports.

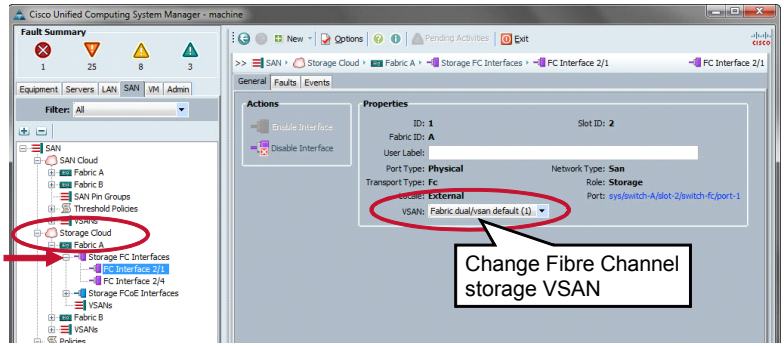
In the content pane, click **Configure as FC Storage Port**. The port will be reconfigured as a Fibre Channel storage port.

The system will warn you if the fabric interconnects are not operating in Fibre Channel switching mode.

https://t.me/learningnets

Verify the Fibre Channel Storage Port

- Fibre Channel storage ports will appear in the Storage FC Interfaces list.
- The Fibre Channel storage port is per fabric interconnect.



© 2012 Cisco and/or its affiliates. All rights reserved.

There are two paths to verify the creation of Fibre Channel storage ports:

- From the Equipment tab, navigate to **Fabric Interconnects > Fabric Interconnect A** or **B > Expansion Module > Storage FC Ports**.
- From the SAN tab, navigate to Storage Cloud > Fabric A or B > Storage FC Interfaces.

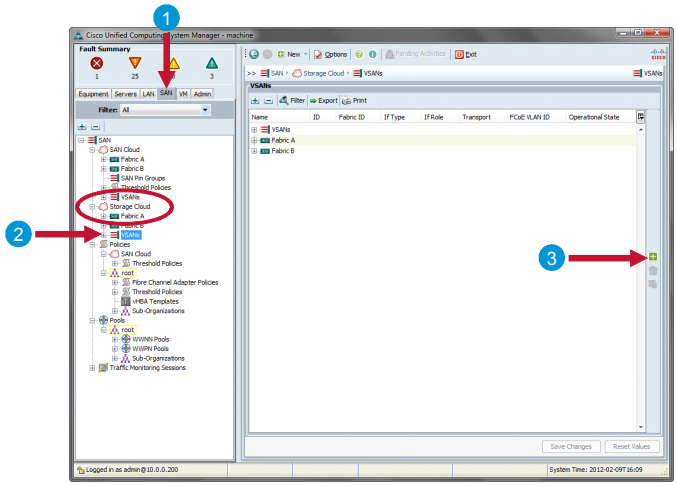
When you click the Fibre Channel storage port, the content pane will display the properties and actions available:

- Actions
  - **Enable or Disable Interface:** The available action will depend on the current operational status of the port.
- Properties
  - **ID**
  - **Slot ID**
  - **Fabric ID**
  - **User Label**
  - **Port Type**
  - **Network Type**
  - **Transport Type**
  - **Role**
  - **Port:** Path to the port object
  - **VSAN:** Which storage VSAN is assigned to this port

https://t.me/learningnets

Provision Fibre Channel Storage VSANs

- Fibre Channel Storage VSANs must be created by navigating to SAN > Storage Cloud > VSANs.



© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco designed the VSAN technology feature to divide the hardware SAN infrastructure into virtual infrastructures to provide better utilization and control over the communication between end devices. It is an internal function between the Cisco MDS switches in the storage infrastructure. End devices, initiators (servers), and targets (storage systems, tape libraries) are not aware to which VSAN their communication belongs. This lack of awareness is because Fibre Channel Protocol (FCP) frames are tagged with VSAN membership information when they enter the MDS switch and on egress the VSAN tag is removed. The Fibre Channel frame arrives at the destination end device in its clear form. If you want to allow communication between two end devices in the SAN infrastructure, the Fibre Channel ports on the MDS switches to which they are attached must belong to the same VSAN. This condition is the first to allow communication between end devices in a SAN infrastructure that is built with Cisco MDS switches.

In Cisco UCS, when there is a directly attached Fibre Channel storage system, it must also be in the same VSAN with the vHBA of the servers that will use its resources. One of the differences in Cisco UCS is that the VSAN tag is applied to the server traffic on the vHBA of the server. For the Fibre Channel storage system-generated traffic, the VSAN tag is applied on the Fibre Channel storage port to which it is connected.

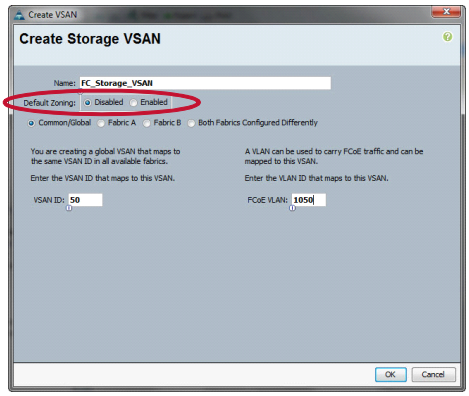
This VSAN is locally significant only on Cisco UCS since it is used only in the communication between the Cisco UCS servers and the directly attached Fibre Channel storage system. However, the VSAN must also exist on the upstream Cisco MDS or Cisco Nexus 5000 switch, where zoning configuration will be performed.

Such VSANs are called storage VSANs. They are created from the SAN tab by navigating to **Storage Cloud > VSANs**. From there, the VSAN creation wizard starts.

https://t.me/learningnets

Storage VSAN Default Zoning

- VSAN ID and corresponding FCoE VLAN
- Default zoning
  - Disabled (default): Zone configuration will be inherited from the Cisco Nexus 5000 or Cisco MDS
  - Enabled: When default zoning on the upstream Cisco Nexus 5000 or Cisco MDS is enabled
  - Zoning is configured per VSAN
  - Cannot be changed after that



© 2012 Cisco and/or its affiliates. All rights reserved.

You must specify the storage VSAN ID. You must also specify if the VSAN will be a common and global VSAN, only on Fabric A or B, or will be created on both fabric interconnects but with different VSAN IDS and FCoE VLANs. The ID of the transport FCoE VLAN must be specified, as well.

You must also set the default zoning behavior. There are two options—enabled and disabled.

Zones are the other security mechanism that is mandatory on Fibre Channel switches to control which initiator will be allowed to communicate with which target. After the end devices are put in the same VSAN, they also must be put in the same zone. The zone feature is standard for all Fibre Channel switches and, on the Cisco MDS and Nexus 5000 switches, it is a per-VSAN function. The zone-related configuration for one VSAN is different from the zone configuration for other VSANs.

On Cisco MDS switches, or in other words, in Cisco FCP implementation, there is also a default zone. Initially, by default, all end devices that are connected to the Fibre Channel switches will be put in the default zone. If the default zone policy on MDS or Nexus 5000 switches is set to “allow,” then all of the devices will be able to communicate with each other. If it is set to “not allow,” then zones must be created to allow communication between end devices.

Zoning configuration is needed because in the Cisco UCS directly attached Fibre Channel storage system topology there is a storage device that must communicate with the servers. Natively, Cisco UCS Manager does not support zoning configuration. It can only inherit zoning configuration from an upstream Cisco MDS or Nexus 5000 switch.

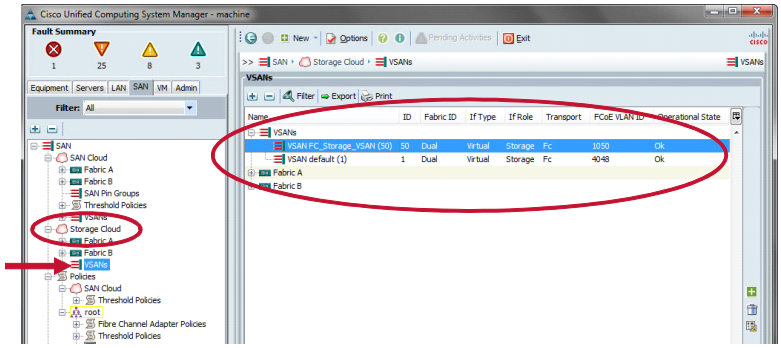
The default zoning setting will depend on the default zone policy on the upstream Cisco MDS or Nexus 5000 switch. If set to “allow,” then in the creation of the storage VSAN it must be set to enabled. If the default zone policy on the upstream switch is “not allow,” then it must be set to disabled.

The fabric interconnects will receive zoning configuration from the zone server for this VSAN, which is operating on the upstream switch for this VSAN. That is why the storage VSAN must also exist on the upstream switch, even though it is not used for any actual communication.

https://t.me/learningnets

Verify the Storage VSAN

- Fibre Channel Storage VSANs will appear under Storage Cloud.



© 2012 Cisco and/or its affiliates. All rights reserved.

To verify the creation of the storage VSAN, from the SAN tab, navigate to **Storage Cloud > VSANs**. The content pane will display a list of available storage VSANs.

You can now go back to the properties of a Fibre Channel storage port and make it a member of this storage VSAN.

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.

Summary

- VSANs can be provisioned to exist on both fabric interconnects, to exist only on Fabric A or B, or to exist on both fabric interconnects using different VSAN IDs.
- Fibre Channel interfaces are uplink ports by default and service only one VSAN. To allow multiple VSANs, trunking must be enabled per fabric interconnect.
- Fibre Channel uplink interfaces can be combined in Fibre Channel port channels for better redundancy and bandwidth.
- Fibre Channel storage ports are used for direct-attached Fibre Channel storage systems. They cannot be part of a Fibre Channel port channel. They require the upstream Cisco MDS or Nexus 5000 switch to provide zoning configuration. Default zoning should be enabled only if it is enabled on the upstream Fibre Channel switch.

© 2012 Cisco and/or its affiliates. All rights reserved.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 4

Provisioning Resource Pools in Cisco UCS Manager

Overview

Identity and resource pools are containers that facilitate consistent application of abstracted identities that are used by service profiles and service profile templates. While administrators are free to track abstracted identities in a spreadsheet or text file, such tracking is difficult to scale in a large system. Server pools provide a means of automating the process of selecting the correct hardware. With Internet Small Computer Systems Interfaces (iSCSIs), Cisco Unified Computing System (UCS) now supports the iSCSI-based boot.

Objectives

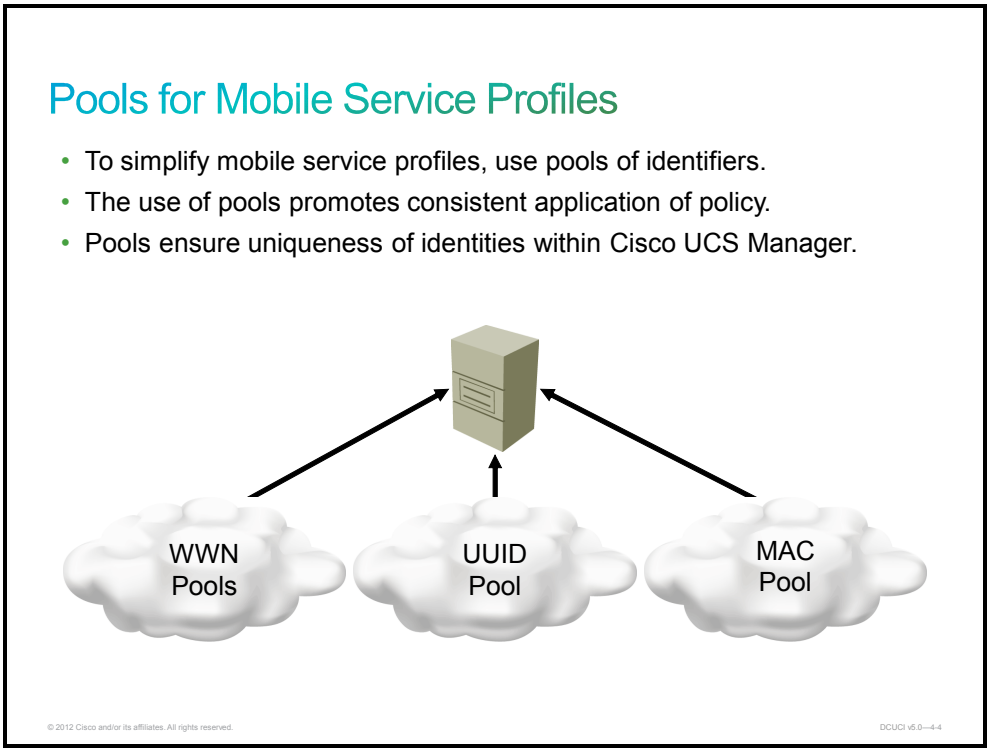
Upon completing this lesson, you will be able to provision identity and resource pools, as well as IP addresses for an iSCSI boot. This ability includes being able to meet these objectives:

- Provision server pools
- Provision server pool autoplacement
- Provision UUID pools
- Provision MAC pools
- Provision WWNN pools
- Provision WWPN pools
- Provision iSCSI initiator pools

https://t.me/learningnets

Provision Server Pools

This topic describes how to provision server pools.



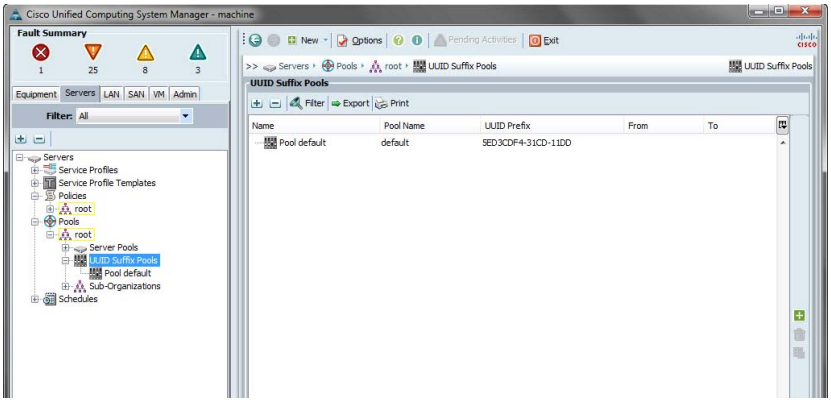
Stateless computing requires unique identity resources for universally unique identifiers (UUIDs), MAC addresses, and world wide names (WWNs) for Fibre Channel. Using pooled resources ensures the consistent application of policy and offers reasonable assurances that identities are unique within Cisco UCS Manager.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Logical Resource Pools

- Identity pools supply abstracted identities to service profiles in service profile templates.
- Logical resource pools are MAC pools, UUID pools, and WWN pools.

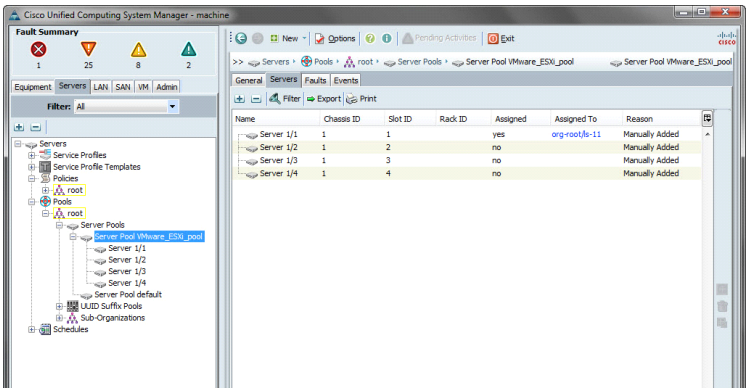


© 2012 Cisco and/or its affiliates. All rights reserved.

Logical resource pools provide abstracted identities that are used by service profiles in service profile templates to facilitate stateless computing.

Physical Resource Pools

- Physical resource pools provide blade server resources to service profiles and facilitate rapid provisioning.



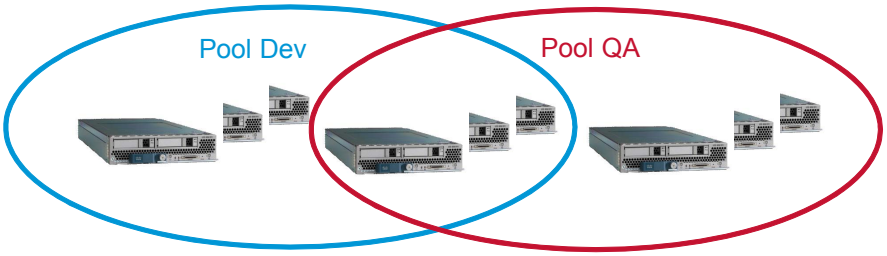
© 2012 Cisco and/or its affiliates. All rights reserved.

Physical resource pools are used to create blade server groupings that are based on arbitrary administrative criteria. These pools can be used with service profile templates to provide rapid provisioning of compute resources.

https://t.me/learningnets

Server Pools

- Server pools can be manually populated or autopopulated.
- Blade servers can be in multiple pools at the same time.
- Associate a service profile with a pool:
  - A compute node is selected automatically from the pool.
  - Cisco UCS Manager will only select a blade server not yet associated with a service profile, and not in the process of being disassociated from a service profile.



© 2012 Cisco and/or its affiliates. All rights reserved.

Pools can be manually populated or autopopulated using a server pool policy.

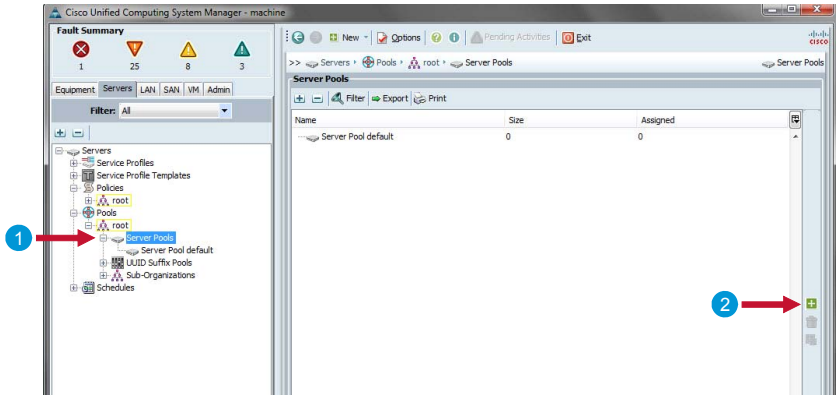
A compute node can be in multiple pools at the same time. The profile that is associated with a specific compute node owns the node, regardless of the number of pools in which the blade server resides.

To use a server pool, associate the service profile with the pool. Cisco UCS Manager automatically selects an available compute node from the pool. An available blade server is one that is currently discovered but not associated with any profile and not in the process of being associated or disassociated.

https://t.me/learningnets

Start the Server Pool Wizard

- To create a new server pool, right-click Server Pools and select Create Server Pool, or click the plus sign (+).

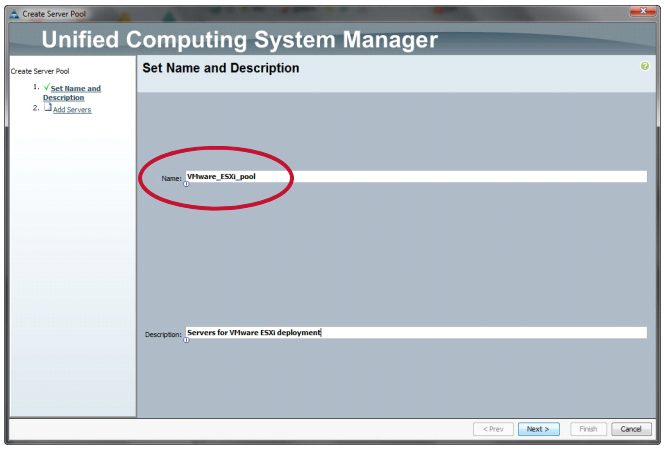


© 2012 Cisco and/or its affiliates. All rights reserved.

Server pools are configured under the LAN tab in the navigation pane. To create a new server pool, right-click **Server Pools** and select **Create Server Pool**, or click the plus sign (+).

Name the Server Pool

- Select a unique name for the server pool.
- Optionally, provide a description.



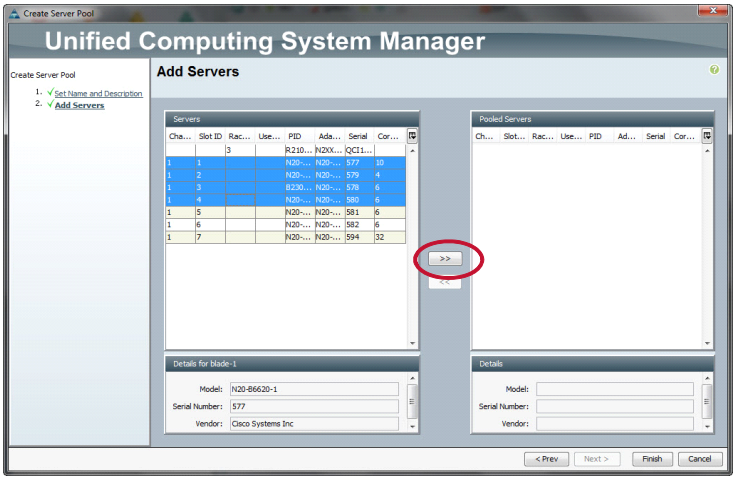
© 2012 Cisco and/or its affiliates. All rights reserved.

Enter a unique name and, optionally, a description for the new server pool, and click **Next**.

https://t.me/learningnets

Select Server Pool Members

- Select servers for the pool.
- Click the right-facing arrows (>>) to add the servers to the pool.

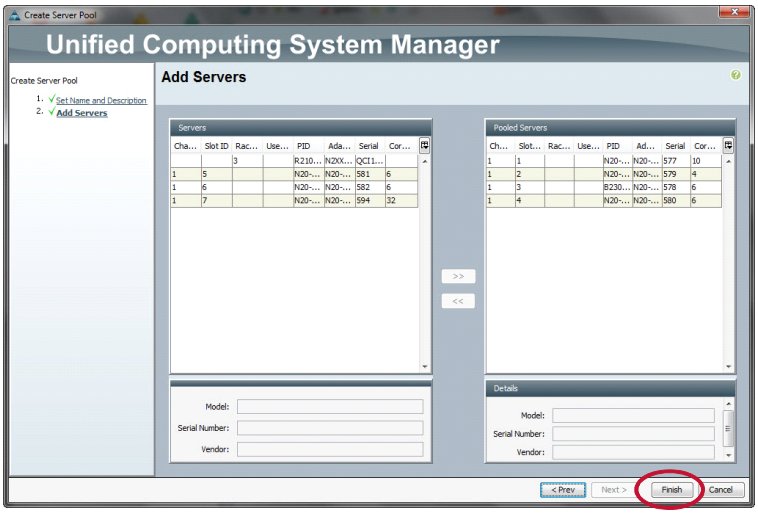


© 2012 Cisco and/or its affiliates. All rights reserved.

Use the mouse to populate the new server pool. Hold down the shift key to select a range of servers. Click the right-facing arrows (>>) to move the selected servers into the pool.

New Server Pool Members

- Click Finish to close the wizard and save the pool.



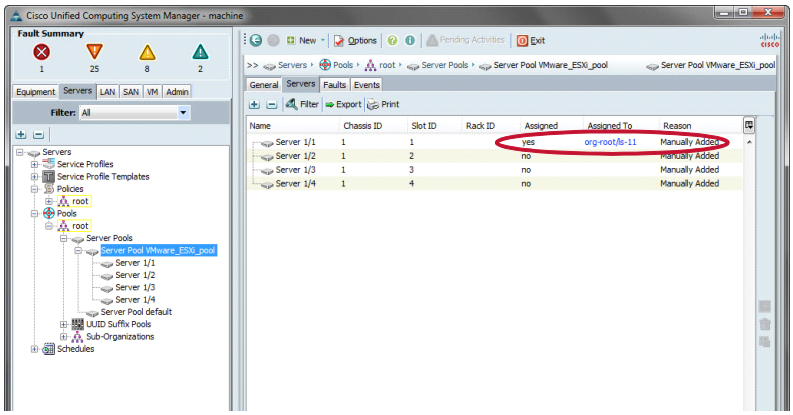
© 2012 Cisco and/or its affiliates. All rights reserved.

Verify that the desired servers are members of the new pool. Click **Finish** to complete the wizard.

https://t.me/learningnets

Server Pool Created

- Server pool members are listed.
- Links are provided once a server is assigned to a service profile.



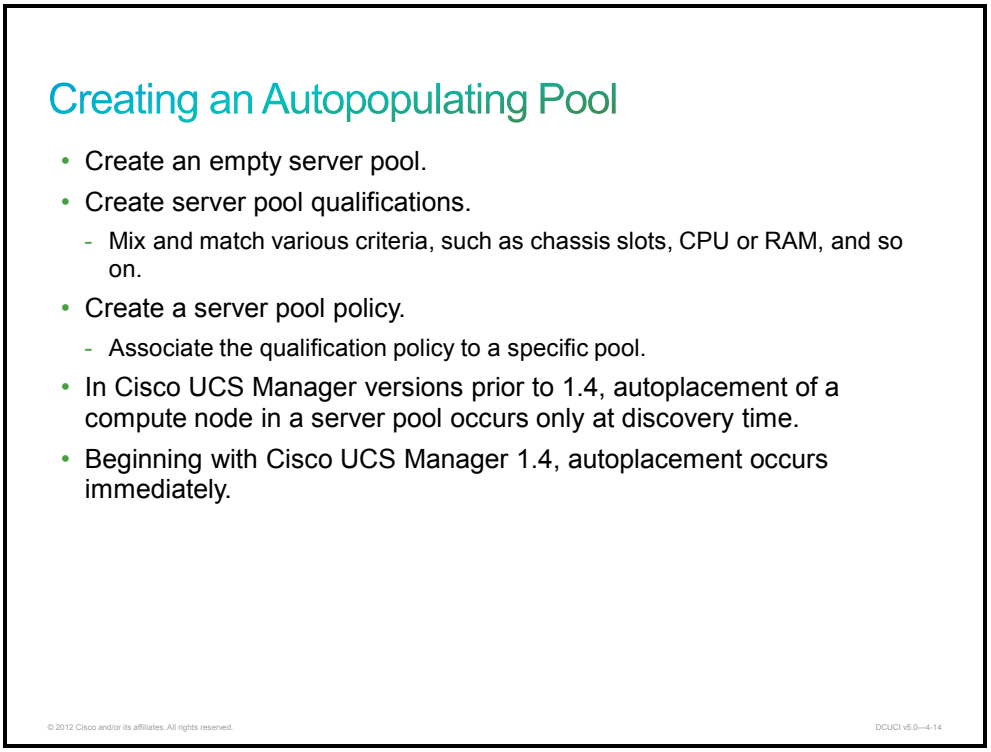
© 2012 Cisco and/or its affiliates. All rights reserved.

The content pane displays the IDs of the servers that were added to the pool. You will see information about whether each server has been assigned. If assigned, a link to the service profile of the server will display in the Assigned To column.

https://t.me/learningnets

Provision Server Pool Autoplacement

This topic describes how to provision an autopopulated server pool.



The autopopulation feature lets you do the following:

- Specify qualifications that will be used for matching specific blade servers
- Specify server pool policies, which will put every blade server that matches a particular qualification into a particular server pool

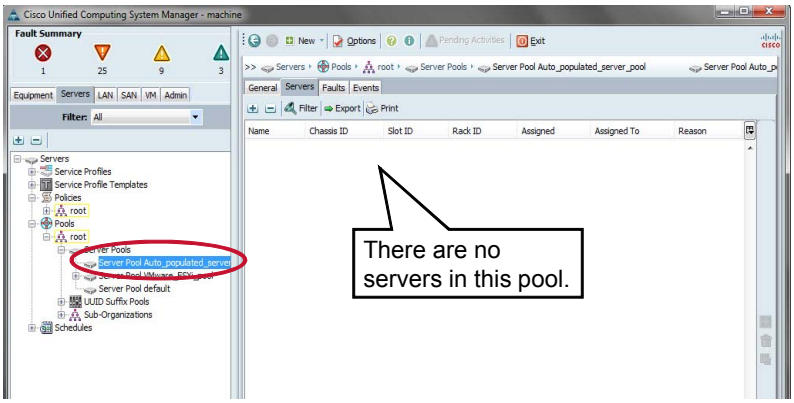
Beginning with Cisco UCS Manager version 1.4, the qualification policy runs against all present servers and autoplacement is done immediately. All of the newly installed servers will be evaluated at the time of discovery.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

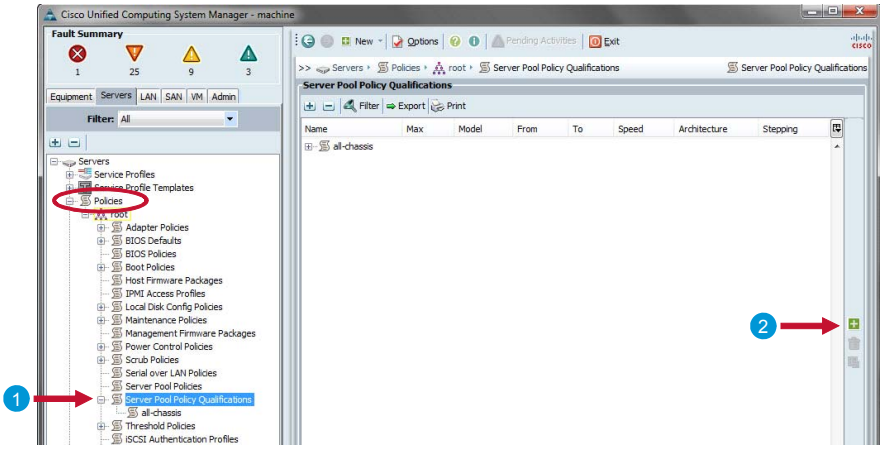
Create an Empty Server Pool

- Create an empty server pool as a standard one.
- Do not select any servers for it.



Create an empty server pool where servers matching the qualification criteria will be placed.

Create a New Qualification Policy

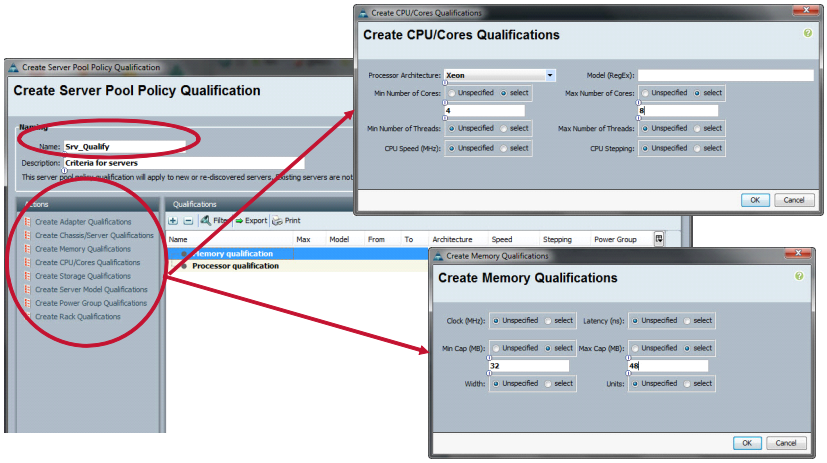


In the **Servers** tab of the navigation pane, expand **Policies**. Right-click **Server Policy Pool Qualification** and select **Create Server Pool Policy Qualification**.

https://t.me/learningnets

Server Selection Criteria

- Specify a unique name.
- Choose server selection criteria from the Actions box.

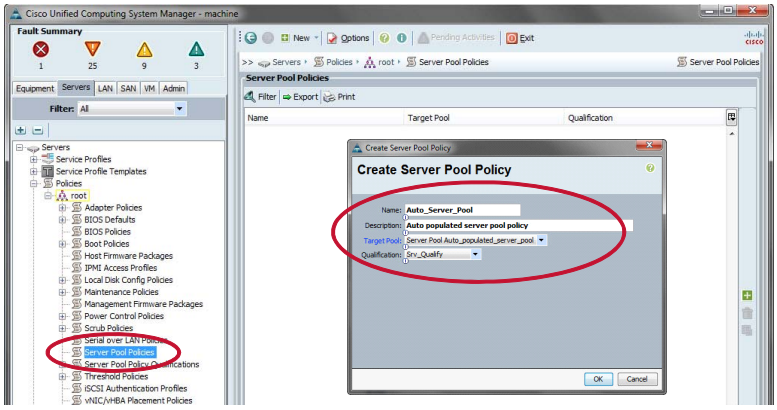


© 2012 Cisco and/or its affiliates. All rights reserved.

In the Actions section of the policy wizard, there is a list of categories that can be used for selection criteria. Specify a unique name for the policy. In the figure, requirements for CPU and memory are specified. The servers will have to match these requirements to be put in the empty server pool.

Create a Server Pool Policy

- Create a new server pool policy.
- Map the qualification policy to the empty server pool.



© 2012 Cisco and/or its affiliates. All rights reserved.

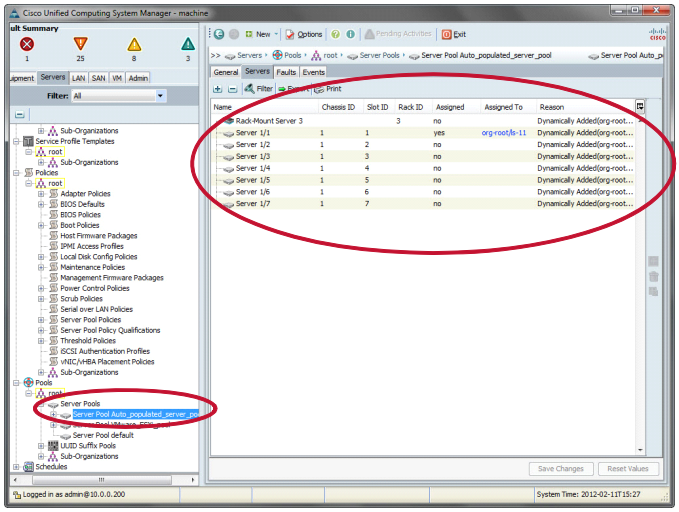
The next step is to create a server pool policy. The purpose of this policy is to map a qualification policy to the empty pool that was created earlier.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Servers Autopopulated After Discovery

- Servers that meet the qualification policy are populated in the server pool.



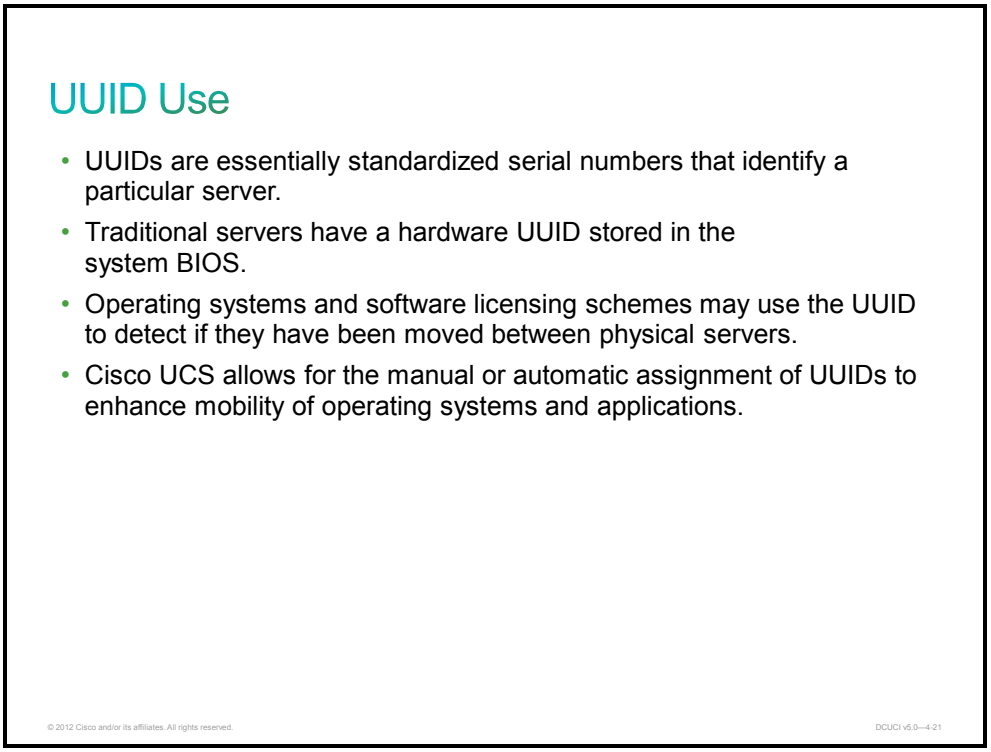
© 2012 Cisco and/or its affiliates. All rights reserved.

The example shows that the servers with the appropriate hardware were automatically added to the pool. A new blade server that is inserted into a chassis will be evaluated by all qualification policies that have been configured.

https://t.me/learningnets

Provision UUID Pools

This topic describes how to provision UUID suffix pools.



UUIDs are designed as globally unique identifiers for each compute node on a network. UUIDs are used in a number of different ways. In the context of Cisco UCS, the UUID refers to a 128-bit identifier coded into the compute node BIOS.

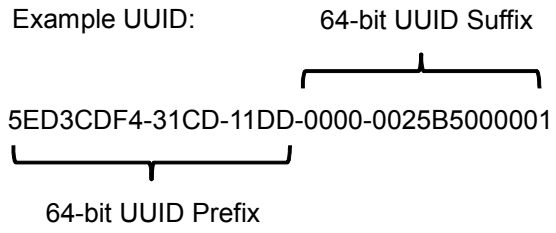
Operating systems, hypervisors, and applications can leverage the UUID for processes like activation, internal disk labels, and so on. Some applications may use the UUID as an internal root value propagated very tightly within data structures. Therefore, UUIDs should be locally administered in the service profile instead of derived from the BIOS. UUIDs within a service profile are mobile. If the underlying compute node fails, the service profile carries the UUID to the replacement compute node, eliminating the need for potentially time-consuming search-and-replace operations.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

UUID Format

- UUIDs are globally unique 128-bit numbers.
- Many schemes exist to define or generate the UUID.
- Cisco UCS Manager uses a configurable 64-bit prefix and allows you to specify a range of 64-bit suffixes for use by compute nodes.
- The prefix and suffixes are concatenated to form the 128-bit UUID.

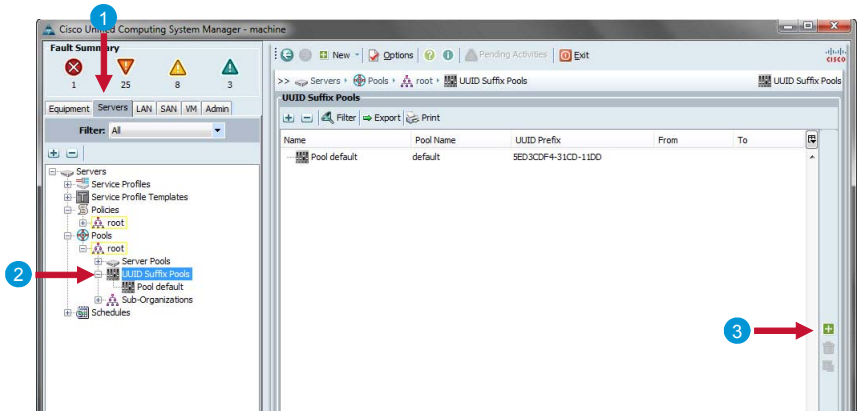


© 2012 Cisco and/or its affiliates. All rights reserved.

There are many schemas for deploying and formatting UUIDs. It is the responsibility of Cisco UCS administrators to determine what values to encode in the UUID prefix and suffix.

Start the UUID Suffix Pool Wizard

- To create a new UUID pool, right-click UUID Suffix Pools and select Create UUID Suffix Pools or click the plus sign (+).



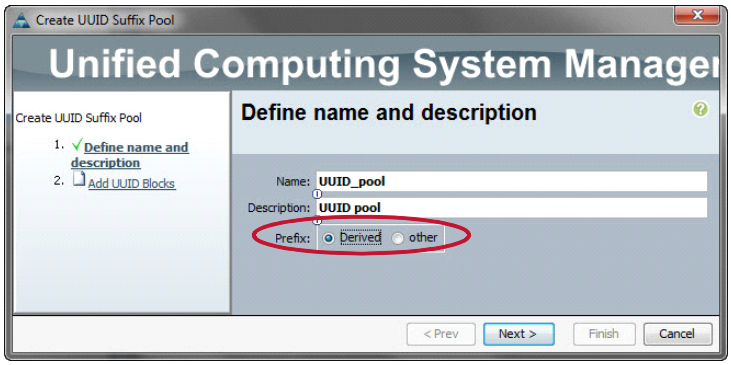
© 2012 Cisco and/or its affiliates. All rights reserved.

To create a UUID pool, navigate to the **Servers** tab in the navigation pane. Navigate to **Pools** and the organization in which the pool should be created. Right-click **UUID Suffix Pools** and choose **Create UUID Suffix Pool**. Or, click the plus sign (+) on the right.

https://t.me/learningnets

Name the UUID Suffix Pool

- Select a unique name for the UUID pool.
- Optionally, provide a description.
- Specify how the prefix will be formed.



© 2012 Cisco and/or its affiliates. All rights reserved.

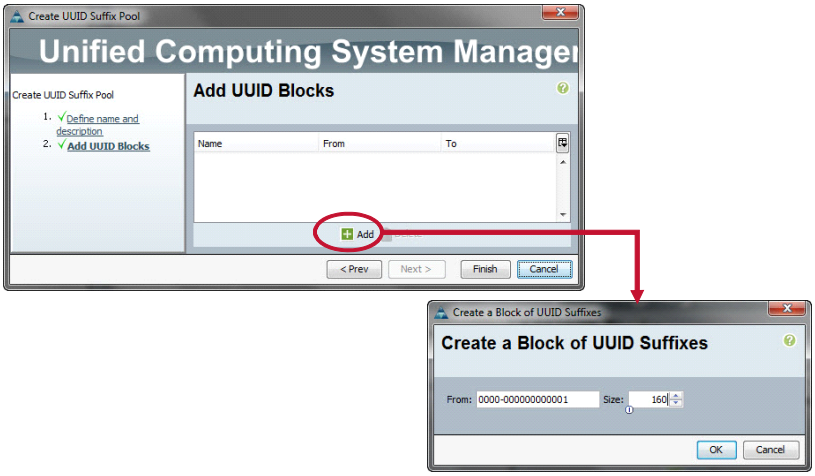
Assign a name and optional description for the pool. There are two choices for creating the UUID prefix. The prefix represents the first 8 bytes of the 16-byte value. If you select Derived, Cisco UCS Manager supplies the prefix. If you select Other, Cisco UCS Manager will prompt you to supply the first 16 bits of the UUID.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Create a Block of UUID Suffixes

- Click Add, enter a suffix starting point, and choose how many UUIDs will populate the pool.



© 2012 Cisco and/or its affiliates. All rights reserved.

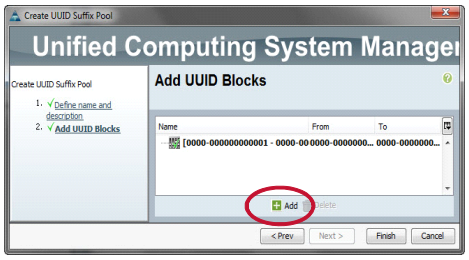
Click **Add** to create a starting point for the 16-bit UUID suffix. The current maximum number of compute nodes in Cisco UCS is 320.

Note	It is a best practice to only preallocate the number of identities in a given pool that are based on the current and near-term forecast. Every identity resource that is allocated is a managed object in the Cisco UCS Manager database.

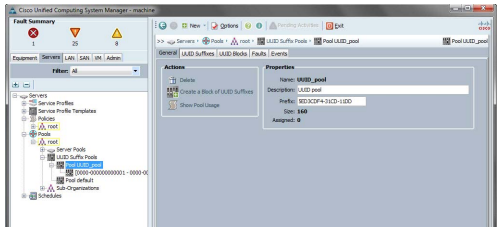
https://t.me/learningnets

UUID Pool

- Additional blocks can be added.



- UUIDs are now available for assignment.



© 2012 Cisco and/or its affiliates. All rights reserved.

Before you finish the wizard for creating the UUID suffix pool, you can add more ranges of suffixes, if needed.

Immediately after you finish the wizard, the pool is created and the UUIDs are available for use.

 © 2012 Cisco Systems, Inc.

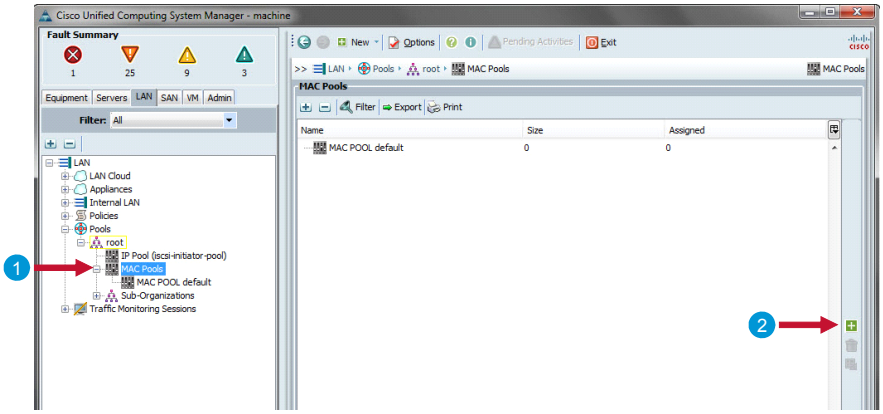
https://t.me/learningnets

Provision MAC Pools

This topic describes how to provision MAC pools.

Start the MAC Pool Wizard

- Right-click MAC Pools or click the plus sign (+) to start the MAC pool wizard.



© 2012 Cisco and/or its affiliates. All rights reserved.

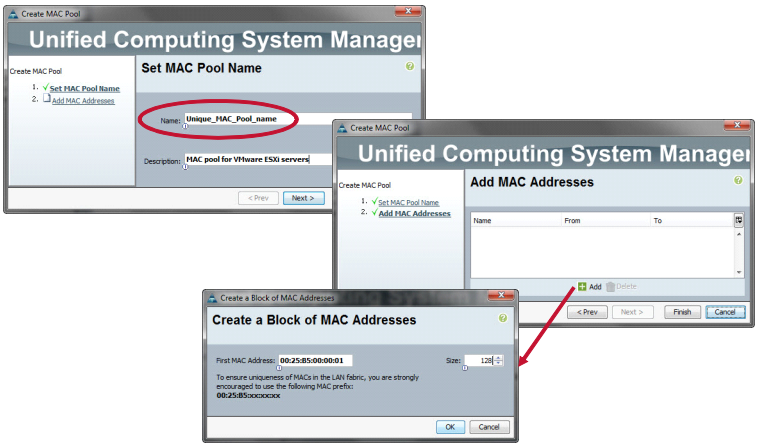
A MAC pool consists of one or more ranges of MAC addresses. You can create the MAC pool and assign a name. With MAC pools, Cisco UCS administration is made easier when scaling server deployment of service profiles by prompting stakeholders to define a set of MAC addresses before actual deployment.

To create a MAC pool, navigate to the LAN tab in the navigation pane. Then navigate to **Pools > MAC Pools**. Right-click **MAC Pools** and choose **Create MAC Pool** to start the wizard, or click the plus sign (+) on the right.

https://t.me/learningnets

Name the MAC Pool and Create a MAC Block

- Select a unique name for the MAC pool and, optionally, provide a description.



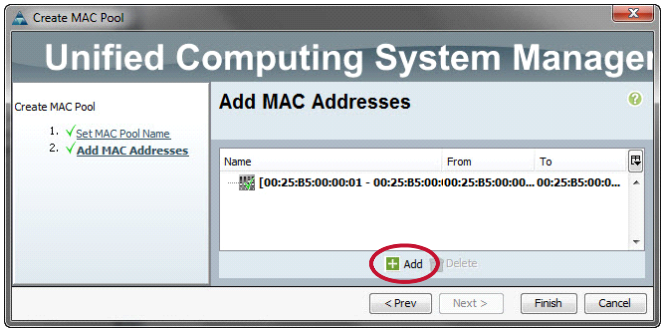
© 2012 Cisco and/or its affiliates. All rights reserved.

Provide the MAC pool with a unique name and, optionally, a description. Click **Next** and decide how many MAC addresses should be created in the pool. Cisco provides a 3-byte Organizationally Unique Identifier (OUI) assigned by the IEEE. It is recommended that you do not modify the prefix.

https://t.me/learningnets

Verify the MAC Block and Finish the Wizard

- Verify that the MAC pool is correct or click <Prev to go back to creating addresses.
- Click Finish to complete the wizard.

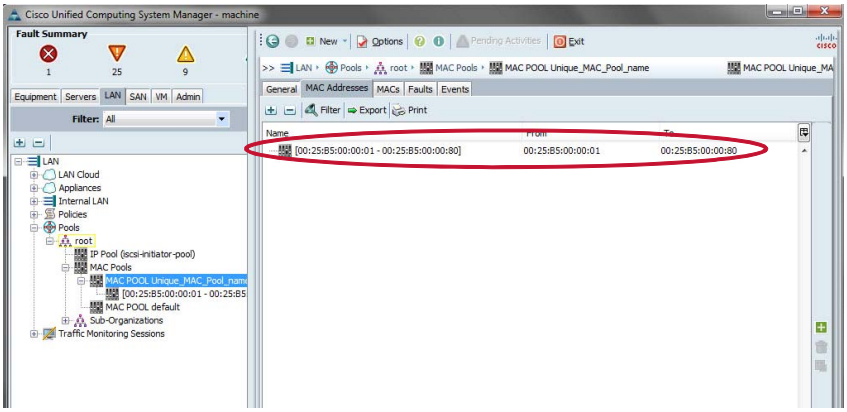


© 2012 Cisco and/or its affiliates. All rights reserved.

When the MAC pool has been created, there is an opportunity to verify the addresses and go back to the previous window if a mistake has been made. You can also add more MAC address ranges by adding more blocks. When you are done, click **Finish** to complete the wizard.

Verify MAC Pool Creation

- The MAC pool is now available for assignment.
- The blocks of MAC addresses are shown.



© 2012 Cisco and/or its affiliates. All rights reserved.

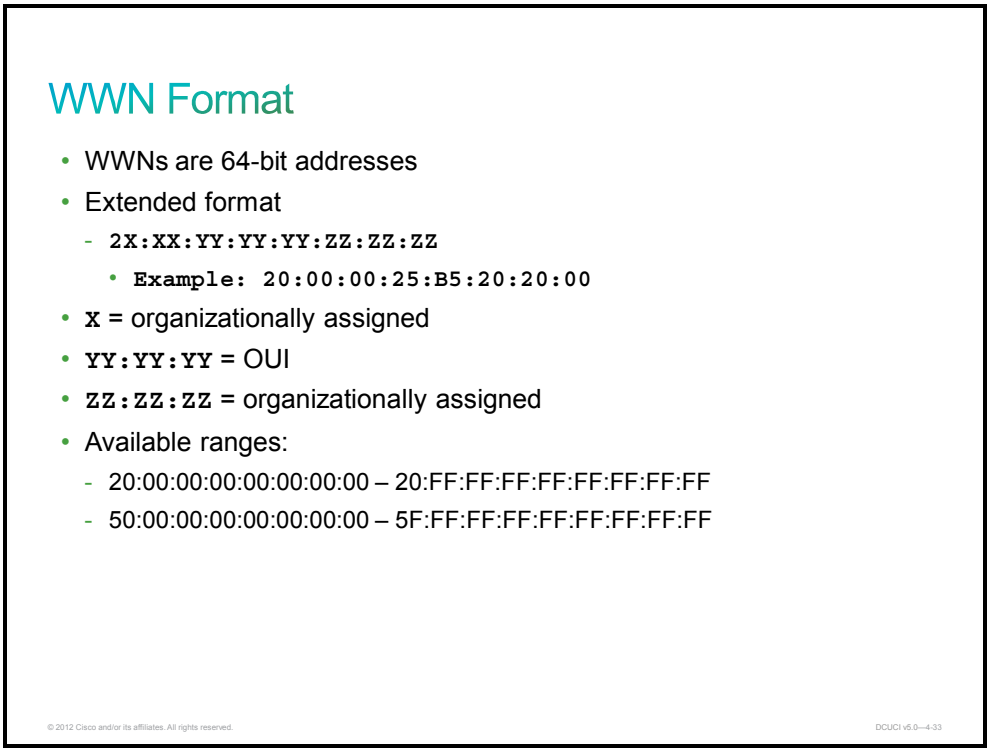
Now the pool is available and can be used in service profiles.

When you click it, the content pane will show general information for the pool. If you select the MAC Addresses tab, you will get information for the ranges of MAC addresses in this pool.

https://t.me/learningnets

Provision WWNN Pools

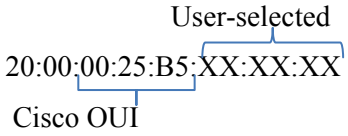
This topic describes how to provision WWNN pools.



WWNs are 64-bit addresses that have many possible formats. The example in the figure is shown for reference only, as Cisco UCS Manager enforces a specific format in all WWN pools.

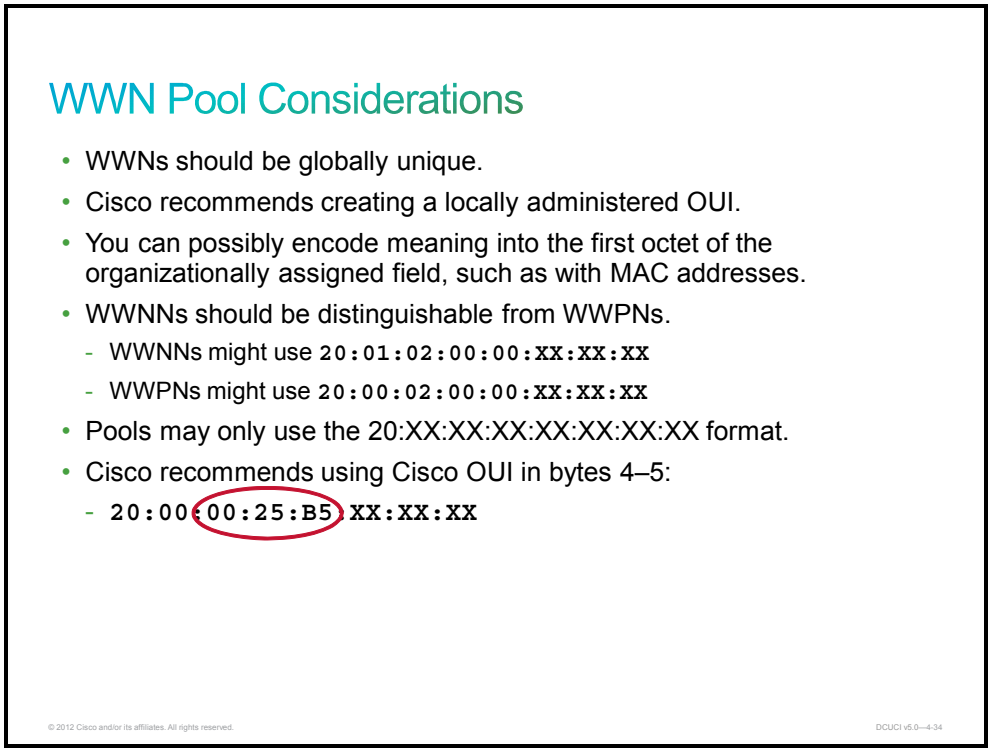
A WWN pool can include only world-wide node names (WWNNs) or world-wide port names (WWPNs) in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved.

To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, you should use the following WWN prefix for all blocks in a pool:



© 2012 Cisco Systems, Inc.

https://t.me/learningnets

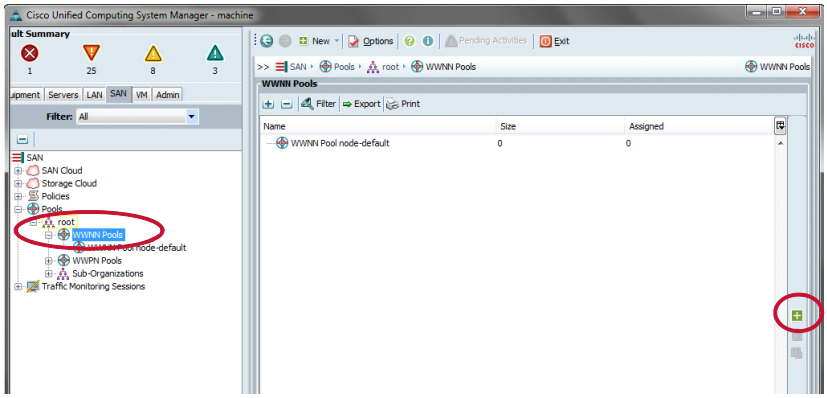


Cisco UCS Manager enforces the use of WWNNs that begin with "20." All WWN pools must begin with that value, while you create any remaining values. In keeping with the global standards set for WWNs, it is recommended that a locally administered OUI of 00:25:B5 be selected and used as the third through fifth octets. Additionally, it is useful if the WWNN and WWPN values are easily distinguishable. Because the second octet of a WWN can be organizationally assigned, that octet might be used to encode meaning for the WWNN or WWPN. This convention and address block should be agreed upon by all stakeholders in the initial implementation phase of a Cisco UCS deployment.

https://t.me/learningnets

Start the WWNN Pool Wizard

- From the SAN tab, navigate to Pools > WWNN Pools.
- Right-click WWNN Pools or click the plus sign (+).

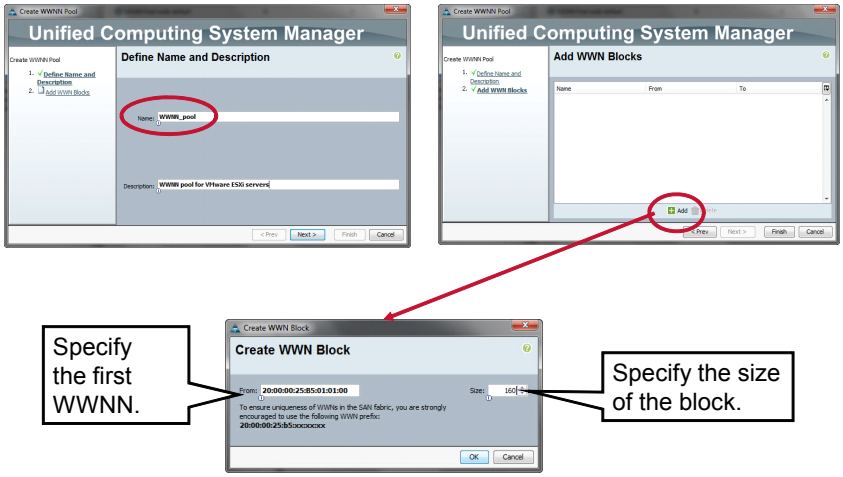


© 2012 Cisco and/or its affiliates. All rights reserved.

To create a WWNN pool, navigate to the **SAN** tab in the navigation pane. Then navigate to **Pools > WWNN Pools**. Right-click **WWNN Pools** and choose **Create WWNN Pool** to start the wizard, or click the plus sign (+) on the right.

Name the Pool and Create a WWNN Block

- Select a unique name for the WWNN pool.
- Optionally, provide a description.



© 2012 Cisco and/or its affiliates. All rights reserved.

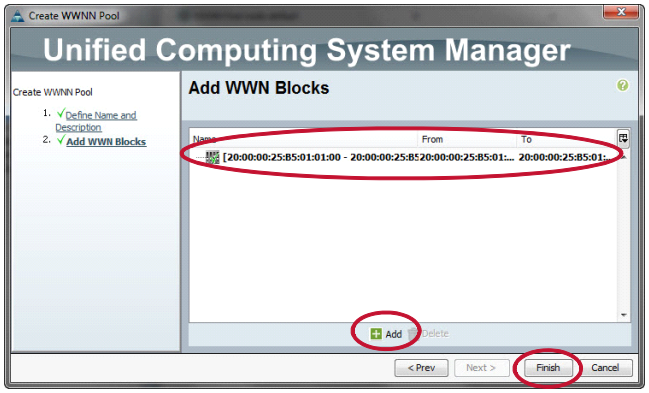
Cisco supplies the first 4 bytes of the WWNN prefix by combining “20” with one of the 3-byte OUIs provided by Cisco. One WWNN is used by each service profile. In the example that is shown in the figure, the administrator has decided to preallocate 160 addresses.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Verify the WWNN Block and Finish the Wizard

- Verify that the WWNN pool is correct or click <Prev to go back to the addresses.
- Click Finish to complete the wizard.

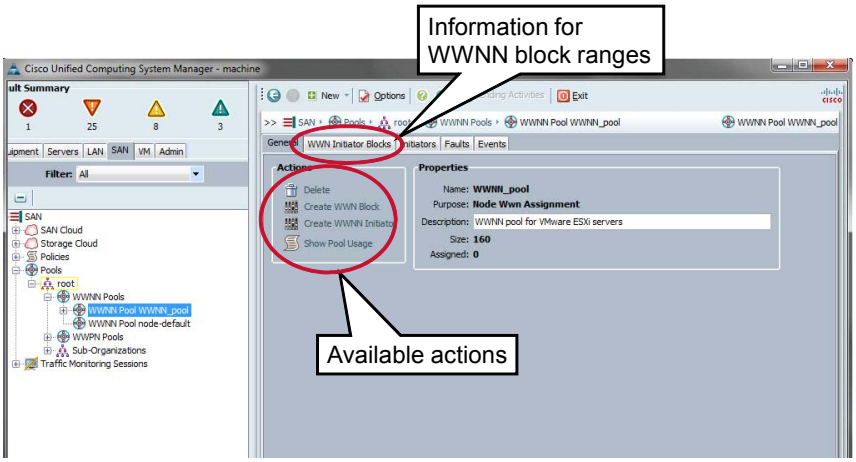


© 2012 Cisco and/or its affiliates. All rights reserved.

After the WWNN pool has been created, there is an opportunity to verify the addresses and go back to the previous window if you notice a mistake. Otherwise, click **Finish** to complete the wizard.

Verify WWNN Pool Creation

- From the SAN tab, navigate to **Pools > WWNN Pools**.



© 2012 Cisco and/or its affiliates. All rights reserved.

Now the pool is available. From the SAN tab, navigate to **Pools > WWNN Pools** and click the pool. In the General tab of the content pane, you will see information for the properties of the pool and the available actions. In the WWN Initiators Block tab, you will see the ranges of WWNN addresses.

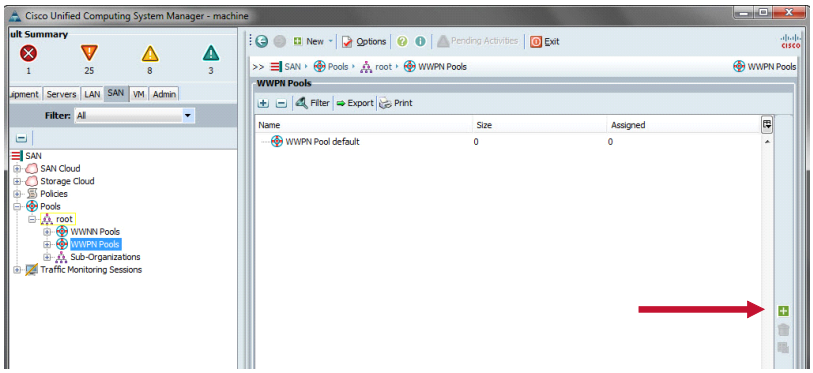
https://t.me/learningnets

Provision WWPN Pools

This topic describes how to provision WWPN pools in Cisco UCS.

Start the WWPN Pool Wizard

- From the SAN tab, navigate to **Pools > WWPN Pools**.
- Right-click **WWPN Pools** or click the plus sign (+).



© 2012 Cisco and/or its affiliates. All rights reserved.

The process of provisioning WWPN pools is similar to the one used for WWNN pools. The first difference is that you create a pool with identity values for different usage than the WWNN pools. The second difference is that you have to start the wizard from a different location.

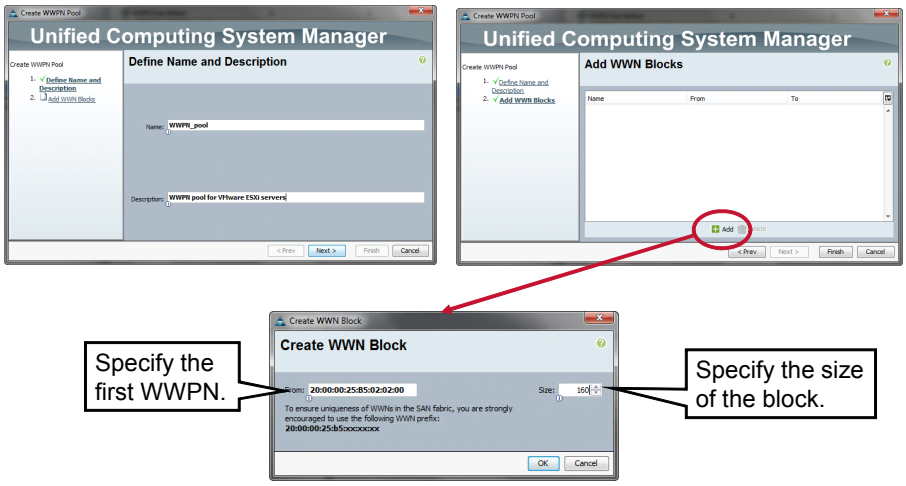
To create a WWPN pool, navigate to the **SAN** tab in the navigation pane. Then navigate to **Pools > WWPN Pools**. Right-click **WWPN Pools** and choose **Create WWPN Pool** to start the wizard, or click the plus sign (+) on the right.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Name the Pool and Create a WWPN Block

- Select a unique name for the WWPN pool and, optionally, provide a description.

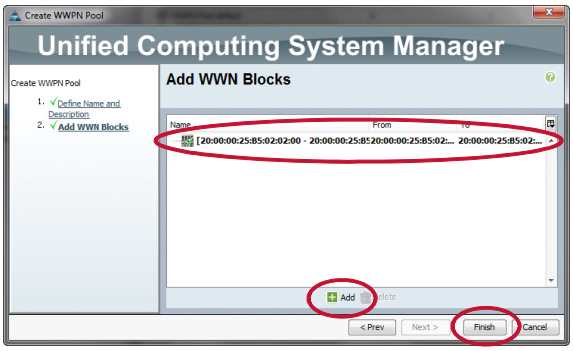


© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco supplies the first 4 bytes of the WWPN prefix by combining "20" with one of the 3-byte OUIs provided by Cisco. One WWPN is required for each virtual host bus adapter (vHBA). In the example shown in the figure, a WWPN pool is created with 160 addresses.

Verify the WWPN Block and Finish the Wizard

- Verify that the WWPN pool is correct or click <Prev to go back to create addresses.
- Click Finish to complete the wizard.



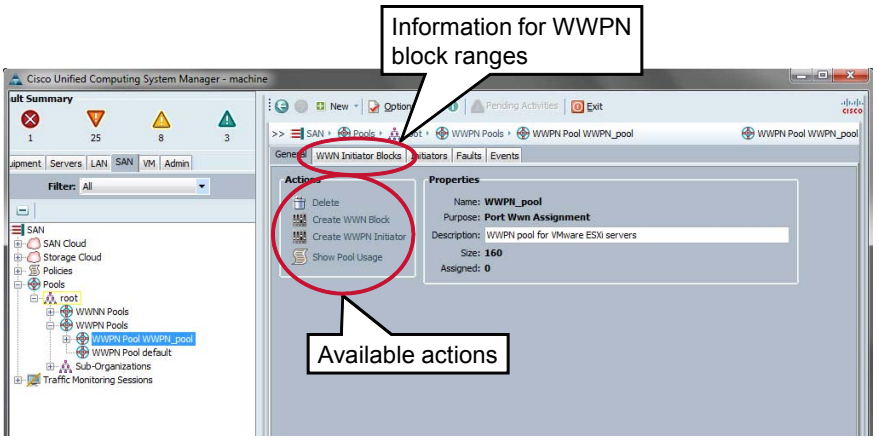
© 2012 Cisco and/or its affiliates. All rights reserved.

After the WWPN pool has been created, there is an opportunity to verify the addresses and go back to the previous window if you notice a mistake. Also, the blocks of WWPN addresses will be shown, and you can add additional addresses. When you are done, click **Finish** to complete the wizard.

https://t.me/learningnets

Verify WWPN Pool Creation

- From the SAN tab, navigate to **Pools > WWPN Pools**.



© 2012 Cisco and/or its affiliates. All rights reserved.

To verify the creation of the new WWPN pool, from the SAN tab, navigate to **Pools > WWPN Pools**.

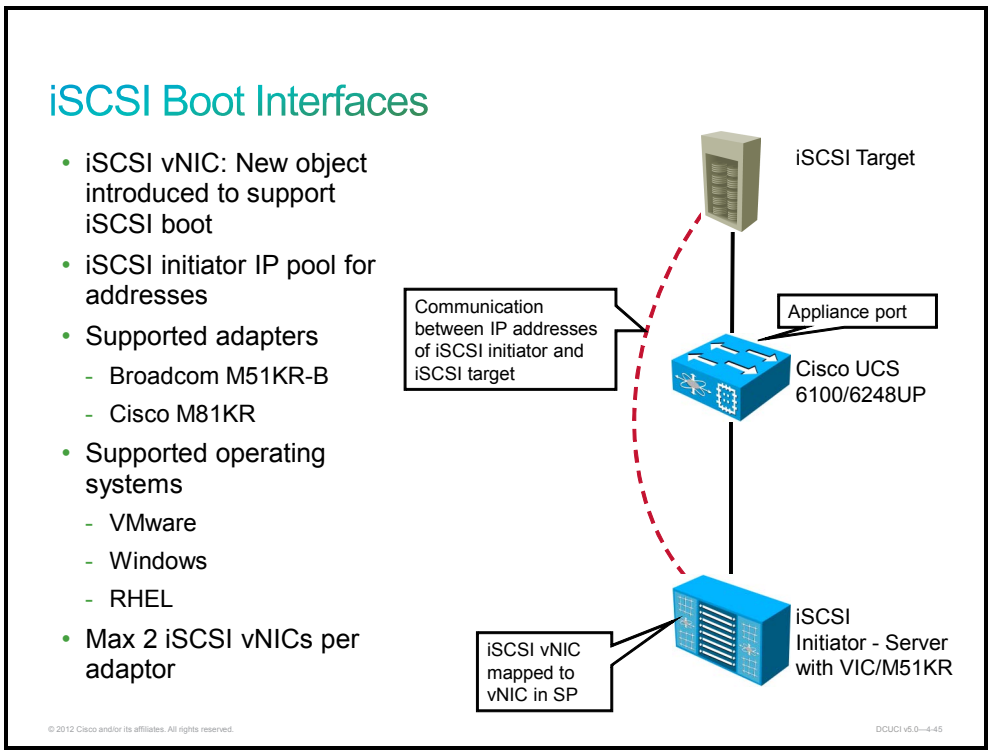
Click the new pool to select it. The content pane will show all the information that is related to the pool. The Actions section will list the available commands. You can delete the pool, create a new WWPN initiator, or look at the usage of the WWPN addresses from the pool when you click **Show Pool Usage**.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision iSCSI Initiator Pools

This topic describes how to provision iSCSI initiator IP pools.



Cisco UCS version 2.0 introduced a new object—the iSCSI virtual network interface card (vNIC). The iSCSI vNIC is an interface that allows a server to boot from an iSCSI storage system that is attached to an appliance port on the fabric interconnect. The supported iSCSI storage devices are from NetApp and EMC.

Since iSCSI communication is IP-based, for the server to communicate and boot from an iSCSI device, the iSCSI interface must be linked to a network interface. The vNIC provides the IP connectivity and is called an overlay vNIC. The iSCSI vNIC provides the iSCSI processing and configuration.

The server in this communication is called an iSCSI initiator. The iSCSI vNIC holds all the settings for the initiator. The settings must specify the iSCSI target IP address, logical unit number (LUN) ID, and so on. Also, the configuration of the iSCSI vNIC must specify the iSCSI initiator IP address. To provision an IP address in Cisco UCS, iSCSI initiator IP pools must be used.

The iSCSI vNIC is provisioned in the service profile and is mapped to an overlay vNIC. Currently, only two iSCSI vNICs are supported per service profile.

https://t.me/learningnets

The following are supported adapters for the servers:

- Cisco Virtual Interface Card (VIC) 1280
- Broadcom M51KR-B. This adapter also supports the host bus adapter (HBA) mode, also known as offload mode. In this mode, the iSCSI communication processing, which is the encapsulation of SCSI into IP packets and vice versa, is performed in the hardware.

The following are supported operating systems for iSCSI boot:

- Windows
- VMware
- RHEL

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Start the iSCSI Initiator IP Pool Wizard

- Select **Pools** from the LAN tab.
- Select **IP Pool (iscsi-initiator-pool)**.

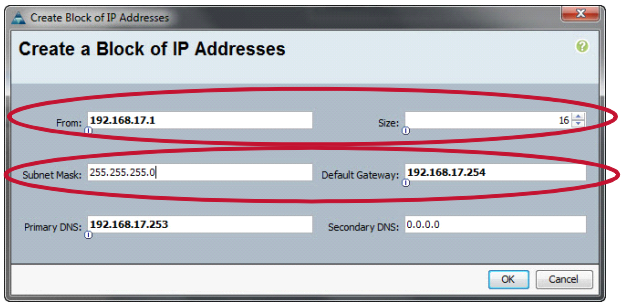
© 2012 Cisco and/or its affiliates. All rights reserved.

To provision an iSCSI initiator IP pool, from the LAN tab, navigate to **Pools > IP Pool (iscsi-initiator-pool)**. Click **Create Block of IP Addresses** to start the creation wizard.

https://t.me/learningnets

Create a Block of Addresses

- Specify start IP address and size.
- Specify the subnet mask, default gateway, and DNS.



© 2012 Cisco and/or its affiliates. All rights reserved.

After you click **Create Block of IP Addresses**, a new window opens, allowing you to specify all the settings for the pool.

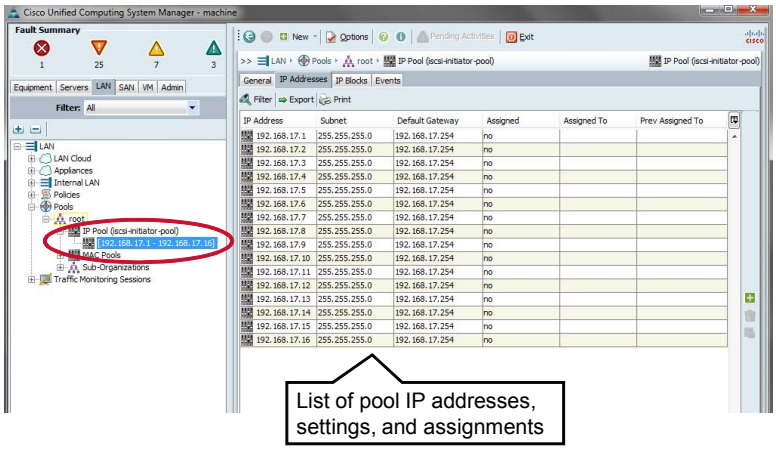
- **From:** The first IP address in the range that you want to specify.
- **Size:** How many IP addresses you need in the pool.
- **Subnet Mask:** The IP addresses must be either from the same subnet of the iSCSI storage device, or there must be Layer 3-based connectivity.
- **Default Gateway**
- **Primary and Secondary DNS:** Optional fields to specify DNS servers if needed.

Click **OK** to finish and create the iSCSI initiator IP pool.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

iSCSI Initiator IP Pool Verification



© 2012 Cisco and/or its affiliates. All rights reserved.

When you have finished with the pool creation, the new pool will appear under the LAN tab. From the **LAN** tab, navigate to **Pools > IP Pool (iscsi-initiator-pool)**. When you select the new iSCSI initiator IP pool, the content pane will display all of the information that is related to it. In the IP Addresses tab of the content pane, you can see a list of the IP addresses in the pool, the specified default gateway, and their assignments (which IP address is used by which server).

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.

Summary

- Server pools are a union of multiple servers with equal or similar hardware characteristics. When you provision server pools, servers are added manually.
- Server pools can be provisioned with autoplacement. When the server pool policy is created, it links an empty server pool with server pool policy qualification.
- UUID suffix pools are provisioned to supply UUID values for service profiles. The UUID suffix can be derived or manually generated.
- MAC address pools are provisioned in the LAN tab and are consumed in the service profile by vNICs.
- WWNN pools are created in the SAN tab and are consumed in the service profile by vHBAs.
- WWPN pools are created in the SAN tab and are consumed in the service profile by vHBAs.
- iSCSI initiator IP pools are provisioned in the LAN tab to supply IP addresses for the iSCSI vNICs and to support the iSCSI boot process.

© 2012 Cisco and/or its affiliates. All rights reserved.

https://t.me/learningnets

Lesson 5

Provisioning Server Policies in Cisco UCS Manager

Overview

Service profiles are the structural elements of the compute node. Service profiles contain all of the identity resources and policies that are required to operate a blade server. The service profile makes stateless computing possible by abstracting identity and policy information from the physical server. If the compute node that a service profile is associated with becomes unavailable, the service profile is simply reassociated with another compatible compute node. When the operating system or hypervisor reboots on the replacement compute node, it believes that it is running on the same hardware.

Objectives

Upon completing this lesson, you will be able to provision service profiles and related policies. You will know how to use identity and server pools, and how to associate and disassociate service profiles with compute nodes. This ability includes being able to meet these objectives:

- Provision a service profile using the expert service profile wizard
- Implement pools and policies in the service profile
- Associate a service profile to a server
- Describe the Cisco UCS Utility Operating System
- Observe the association process using the FSM

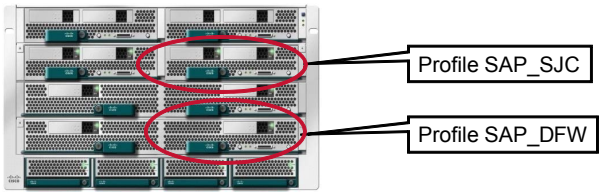
https://t.me/learningnets

Provision a Service Profile Using the Expert Service Profile Wizard

This topic describes how to provision service profiles by using the service profile wizard in expert mode.

Service Profile Basics

- Service profiles contain identity and state information for a logical server.
- LAN and SAN connectivity to a compute node is unavailable without a service profile associated with it.
- Every compute node needs its own unique service profile.
- There is a 1:1 relationship. One compute node can be associated with only one service profile at a time.

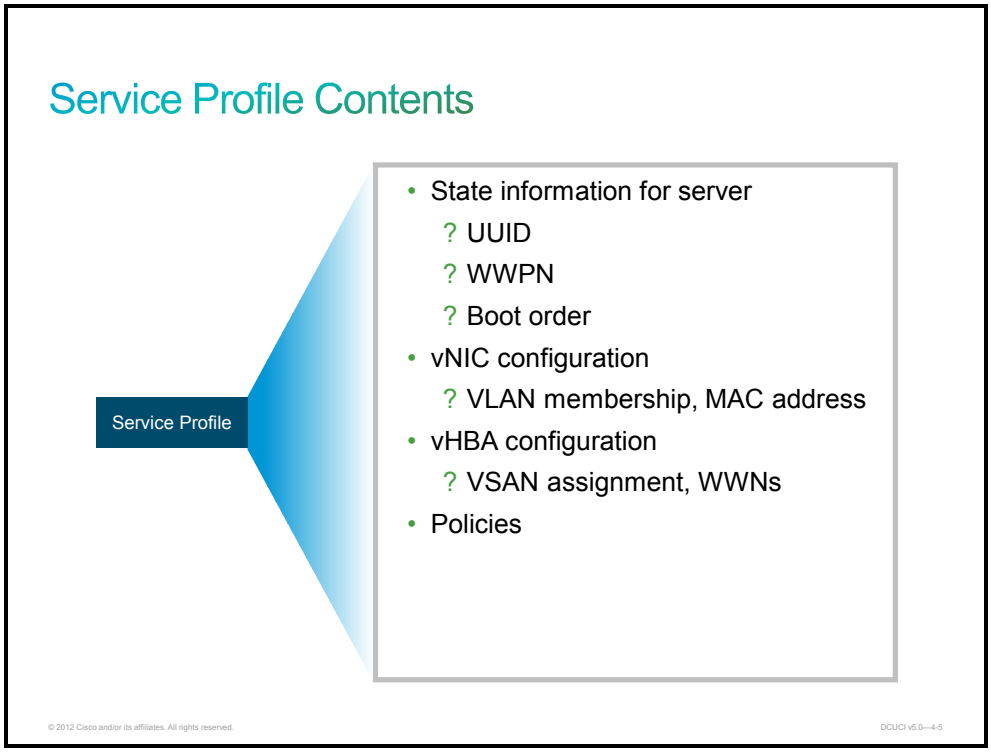


© 2012 Cisco and/or its affiliates. All rights reserved.

Stateless computing requires unique identity resources for universally unique identifiers (UUIDs), MAC addresses, and world wide names (WWNs) for Fibre Channel. Using pooled resources ensures the consistent application of policy and provides reasonable assurances that identities are unique within Cisco Unified Computing System (UCS) Manager.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets



The service profile represents a logical view of a server without any ties to a specific physical device. The profile object contains all of the elements of server function. This identity contains the unique information for that server, including MAC address, world-wide port name (WWPN), UUID, boot order, and so on. Each profile can only be associated with a single blade server at any given time, and every blade server requires a unique service profile.

Service profiles facilitate server mobility. Mobility is the ability to transfer server identities seamlessly between compute nodes so that the underlying operating system or hypervisor does not detect any changes in server hardware.

In environments where blades are managed as traditional individual servers, service profiles are still required. Service profiles provide LAN and SAN connectivity configuration. Configuring service profiles in this way is similar to the need to configure individual LAN and SAN ports for traditional rack servers.

https://t.me/learningnets

Service Profile Wizards

- The basic wizard is a single-page form that allows the creation of a service profile using all derived values.
- Service profiles created with the basic wizard do not support stateless computing and have limited options.
- The expert service profile wizard provides the administrator with a rich set of options for identity and policy assignment.
- The expert wizard allows the creation of mobile service profiles that can be moved from compute node to compute node without the need to modify parameters in the operating system or applications.

© 2012 Cisco and/or its affiliates. All rights reserved.

The primary difference between the simple service profile wizard and the expert service profile wizard is the scope of tools available to manipulate within the wizard. The simple wizard provides a fast, single-page form for the rapid provisioning of a blade server using all derived identity values. The expert service profile wizard allows for the granular configuration of policies, identities, and thresholds.

Comparison of Service Profile Wizards

Basic Wizard	Expert Wizard
Assign single-access VLAN	Assign access VLAN or trunk
Use derived MAC address only	Assign locally administered MAC address or use pool
Use derived WWNN only	Assign locally administered WWNN or use pool
Use derived WWPN only	Assign locally administered WWPN or use pool
Use derived UUID only	Assign locally administered UUID or use pool
Only two devices in the boot order	More than two devices in the boot order
No policy or threshold assignment	Policy and threshold assignment for each element in the service profile

© 2012 Cisco and/or its affiliates. All rights reserved.

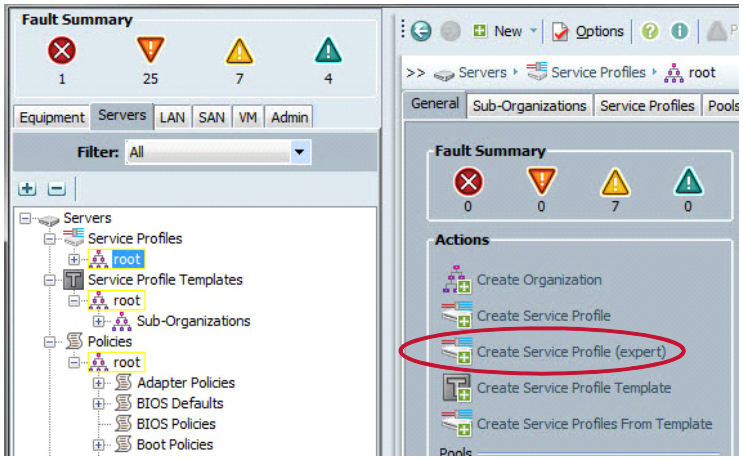
The figure summarizes the most important differences between the simple and expert service profile wizards.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Launch the Expert Service Profile Wizard

- Select the organization where the new service profile should be created.
- Select Create Service Profile (expert).

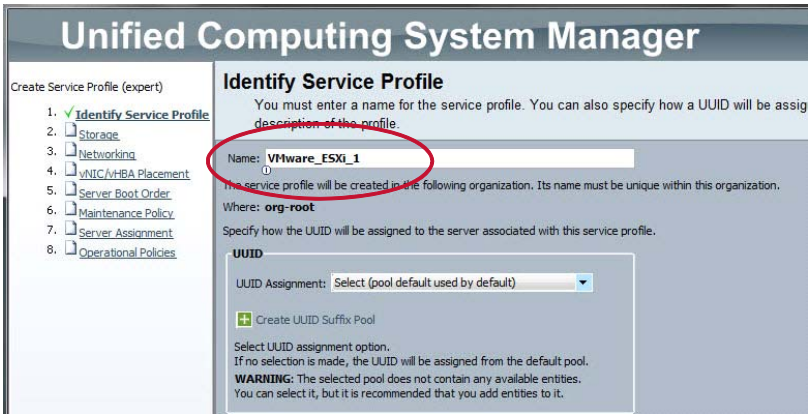


© 2012 Cisco and/or its affiliates. All rights reserved.

To start the service profile wizard, select the **Servers** tab from the navigation pane. Navigate to **Servers > Service Profiles**. Choose the organization under which you want to create the service profile and click it. In the content pane, you will see all of the available commands for the organization. Click **Create Service Profile (expert)**.

Name the Service Profile

- The wizard goes through eight steps.
- Select a name to identify the service profile.



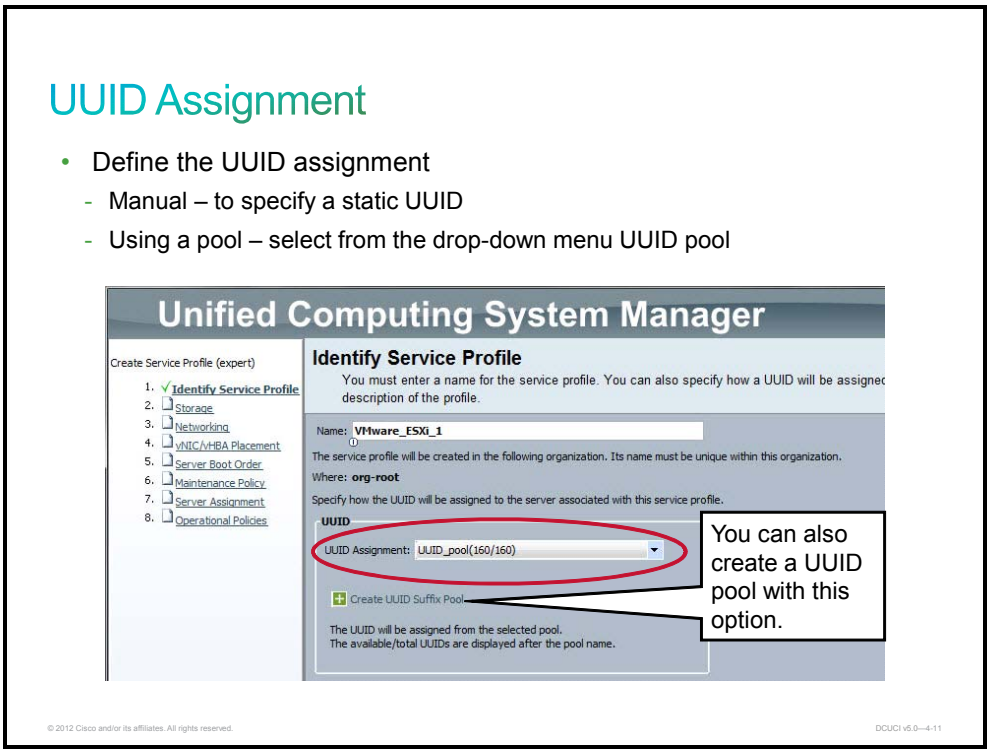
© 2012 Cisco and/or its affiliates. All rights reserved.

The wizard window will open. The wizard will guide you through the eight major steps to build the service profile. In the first step, the first setting to specify is the name of the service profile. The name must be up to 16 characters and may not include special characters or spaces.

https://t.me/learningnets

Implement Pools and Policies in the Service Profile

This topic describes how to implement pools and policies during the creation of the service profile.



You must specify the UUID assignment method. When you click the drop-down menu, the following options are available:

- **Hardware default:** The service profile will use the burned-in UUID in the BIOS of the server. This option does not allow mobility for the service profile.
- **Manual using an Organizationally Unique Identifier (OUI):** Manually creates the UUID.
- **Pools:** Select from preprovisioned UUID pools.

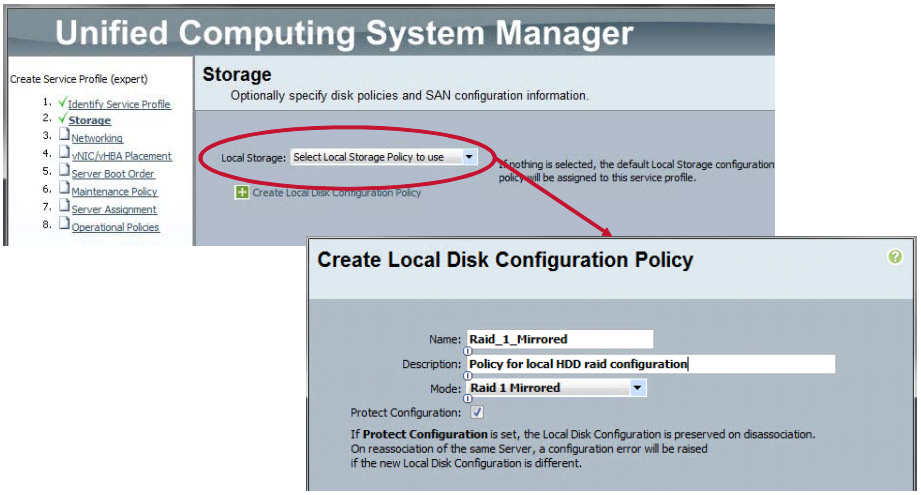
If you begin the service profile wizard and realize that you have forgotten to first create a UUID pool, you can create a new pool from within the wizard by clicking **Create UUID Suffix Pool**.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Local Storage Policy

- Choose the local storage policy or create a local storage policy.



© 2012 Cisco and/or its affiliates. All rights reserved.

The second step of the service profile wizard is to provision the storage. First, you must specify the local storage policy. If you have not already provisioned a local storage policy, then you can click **Create Local Disk Configuration Policy**.

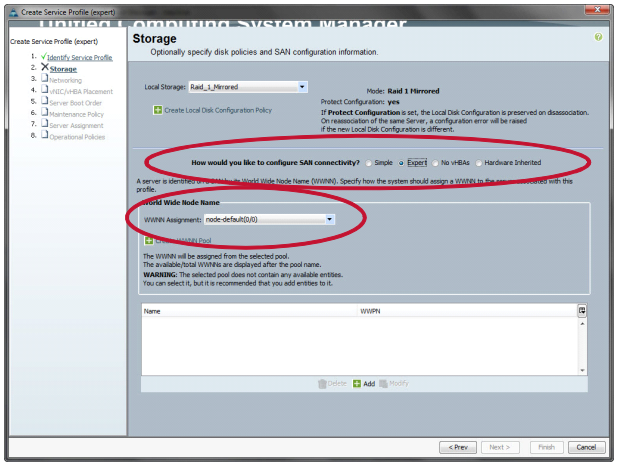
The Protect Configuration check box is checked by default. This feature is used to protect the local storage configuration. When the service profile is disassociated, the server retains the local storage configuration. If a new service profile is associated, it must have a matching local storage policy. If the new local storage policy is different, an error message will appear.

You have to specify a name for the policy and the Redundant Array of Independent Disks (RAID) mode in which the local storage must operate. As the local storage policy defines the behavior of the RAID controller, it is important to know the characteristics of the hardware. If you define a mode that is not supported by the RAID controller of the compute node, you will receive an error message from the system during association.

https://t.me/learningnets

WWNN Assignment

- Switch to expert view.
- Assign a WWNN manually or from an existing or newly created pool.



© 2012 Cisco and/or its affiliates. All rights reserved.

To be allowed to create virtual host bus adapters (vHBAs), you have to switch to expert view. Even if you began the wizard in expert mode, you will be presented with the simple view at this point in the process. The same situation occurs during the third step of network provisioning.

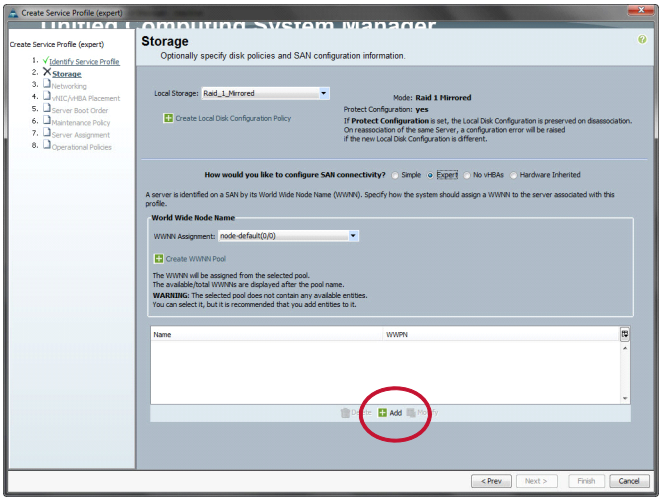
Once you have switched to expert view, the second task is to specify the world wide node name (WWNN) assignment method. Here again, the options are to manually generate a WWNN address or to specify a WWNN pool. The options are available from the drop-down menu.

If you want to use a WWNN pool, but one has not already been provisioned, then click **Create WWNN Pool**.

https://t.me/learningnets

Begin Creation of vHBAs

- Click Add to create the first vHBA.

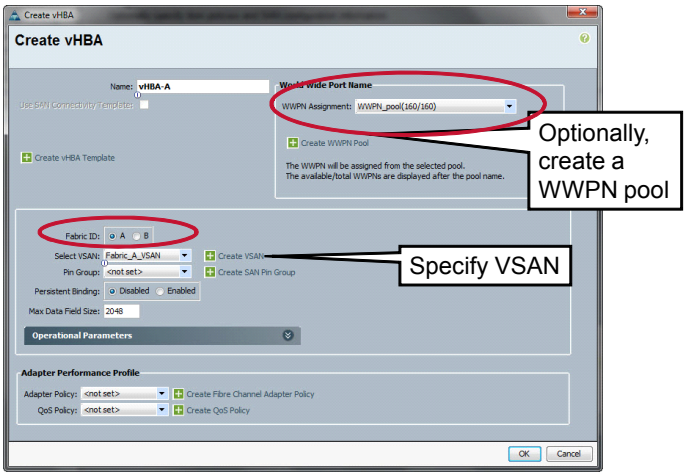


© 2012 Cisco and/or its affiliates. All rights reserved.

The next step is to create the vHBAs for the compute node. Click the plus sign (+) to open a dialog box to create the vHBA for fabric A.

Create vHBA for Fabric A

- Define the configuration parameters for Fabric A.
- Specify the WWPN assignment method.



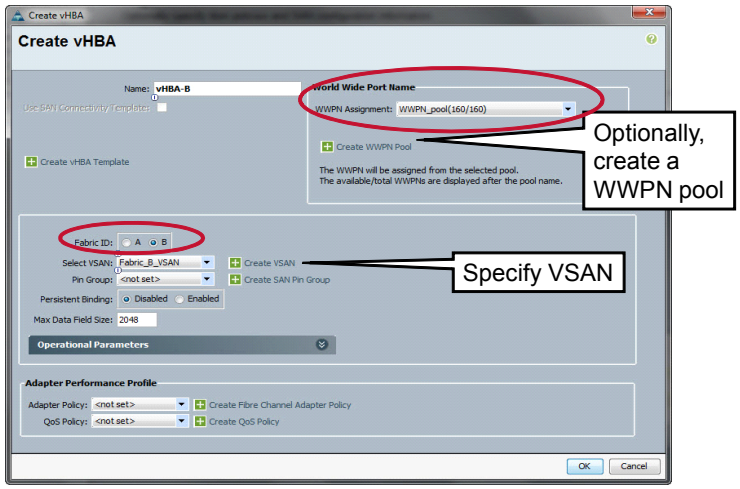
© 2012 Cisco and/or its affiliates. All rights reserved.

The vHBA requires a name, WWPN assignment, virtual storage area network (VSAN) assignment, and fabric assignment. The figure shows the creation of a new vHBA named vHBA-A. The vHBA will pull its WWPN assignment from a pool named WWPN_pool, which is a member of Fabric_A_VSAN, and is associated with Fabric A.

https://t.me/learningnets

Create vHBA for Fabric B

- Define the configuration parameters for Fabric B.
- Specify the WWPN assignment method.



© 2012 Cisco and/or its affiliates. All rights reserved.

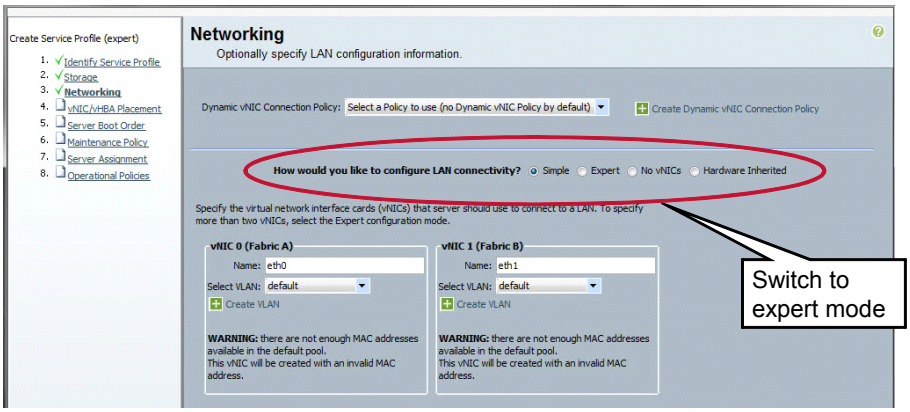
Repeat the steps that you used to create the vHBA on Fabric A to create the vHBA on Fabric B. Be certain to select a different VSAN for Fabric B. Click **Next** to continue the wizard.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Simple View for Networking

- The networking section of the wizard defaults to simple view.
- In simple view, you can create two vNICs and trunking is not supported.



The expert wizard defaults to simple view for networking configuration. This view limits you to selecting derived MAC addresses and a single VLAN.

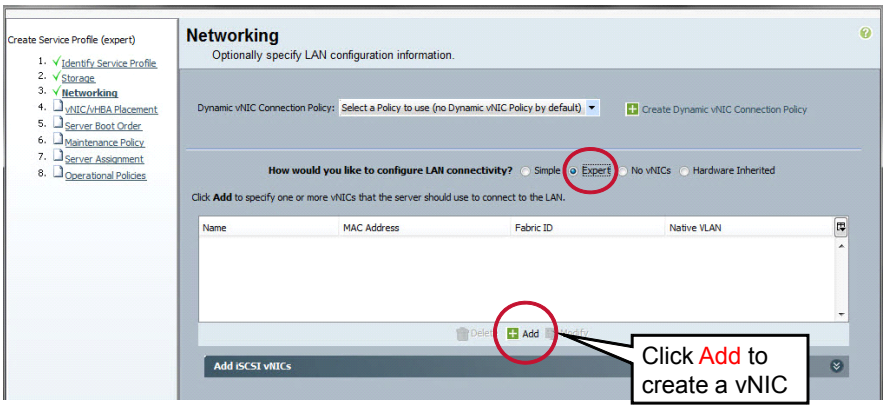
Note	The Cisco UCS MK81-KR virtualization adapter does not have burned-in MAC addresses. Pooled or manual address assignment is required on this mezzanine adapter.

Click the **Expert** radio button to reveal the complete suite of networking configuration tools that are available within the expert wizard.

https://t.me/learningnets

vNIC Provisioning for Networking

- Provision new vNICs.
- In expert mode, you can create more than two vNICs.

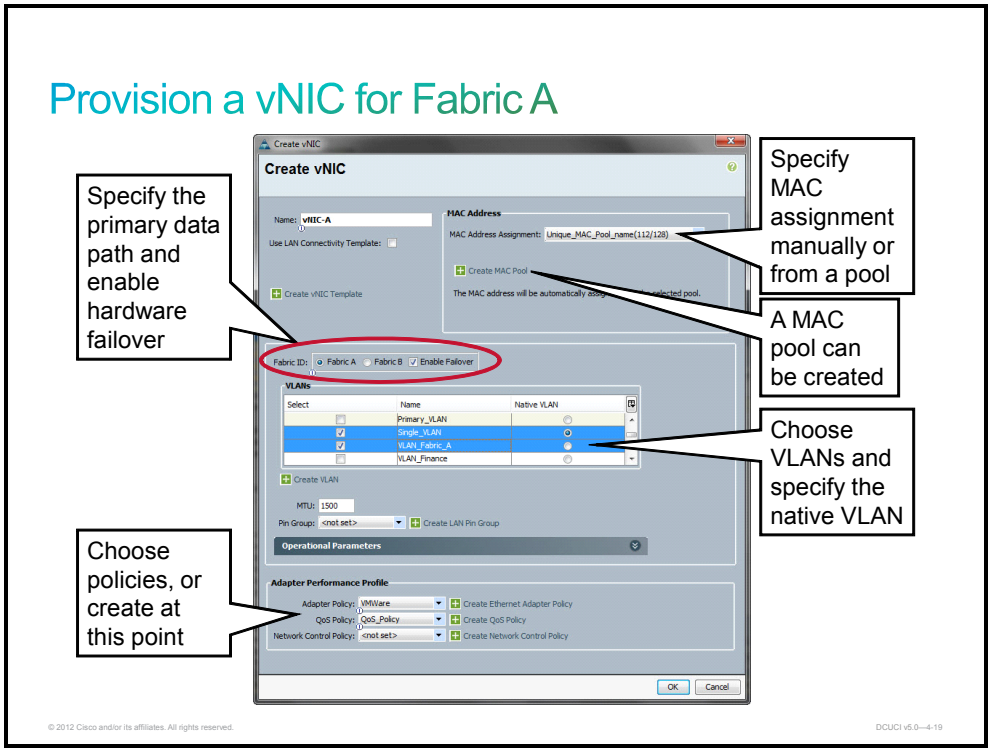


© 2012 Cisco and/or its affiliates. All rights reserved.

Click **Add** to open the dialog box and define a new virtual network interface card (vNIC).

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets



The new vNIC requires the following configuration elements:

- Name
- MAC address assignment method
- Fabric assignment and failover
- Select which VLAN or VLANs will be allowed
- Select which VLAN will be the native VLAN
- Policies

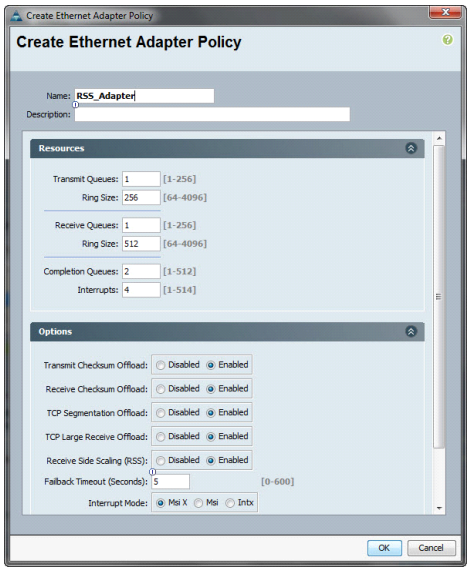
In the Policies section, you can either choose from preprovisioned policies or create the policies that you need. You can specify or provision and then specify the adapter policy, quality of service (QoS) policy, and network control policy.

Note	Hardware-based failover is offered in the Cisco UCS VIC 1280, M81KR, M71KR-E, and M71KR-Q.

https://t.me/learningnets

Provision an Adapter Policy

- Specify the host-side behavior of the vNIC.
- There are preconfigured adapter policies for different operating systems in Cisco UCS.
- Adapter policy settings depend on operating system requirements.



© 2012 Cisco and/or its affiliates. All rights reserved.

The operating system might have requirements for the low-level hardware configuration of the network adapter it will use. To define the behavior of the network adapter, the vNIC, you have to create an Ethernet adapter policy.

There are preprovisioned adapter policies in the Cisco UCS for the following operating systems:

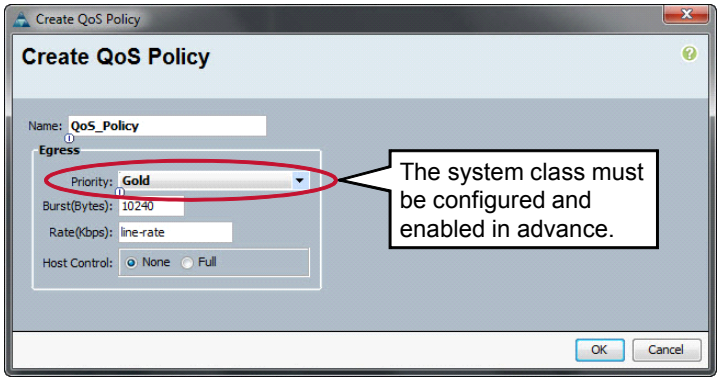
- Windows
- VMware
- Linux

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision a QoS Policy

- Assign the QoS system class to server traffic at the vNIC or vHBA.
- Specify the QoS policy in the vNIC or vHBA configuration.
- Before the creation of a QoS policy, the needed QoS system class must be enabled.



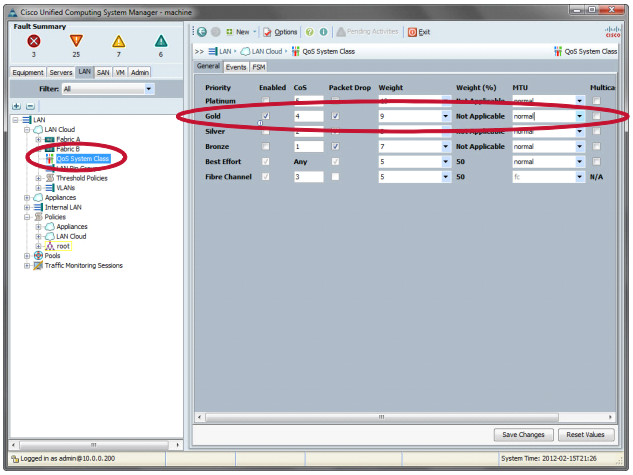
© 2012 Cisco and/or its affiliates. All rights reserved.

To assign a QoS system class to the traffic that originates from the compute node and uses the vNIC, you have to create a QoS policy. You must specify a name and priority. The priority is the system class that will be assigned to the traffic of the server.

https://t.me/learningnets

Define the QoS System Class

- By default, two QoS system classes are enabled—Fibre Channel and Best Effort.
- To use any other system class in a QoS policy, enable it.



© 2012 Cisco and/or its affiliates. All rights reserved.

In Cisco UCS, there are two default QoS system classes that are preprovisioned and enabled:

- **Fibre Channel:** Uses no-drop policy, class of service (CoS) 3, and is used for Fibre Channel over Ethernet (FCoE) traffic.
- **Best Effort:** Uses drop policy and is applied to basic Ethernet traffic.

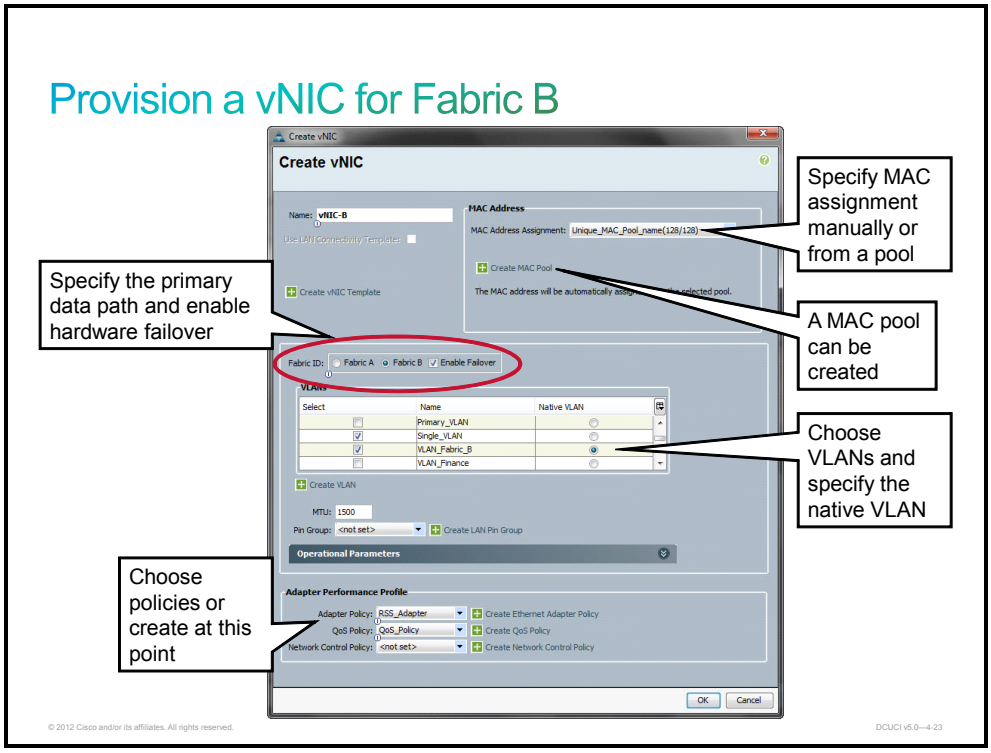
There are other available system classes:

- Platinum
- Gold
- Silver
- Bronze

All of these classes are configurable. You must enable a system class to use it in a QoS policy.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

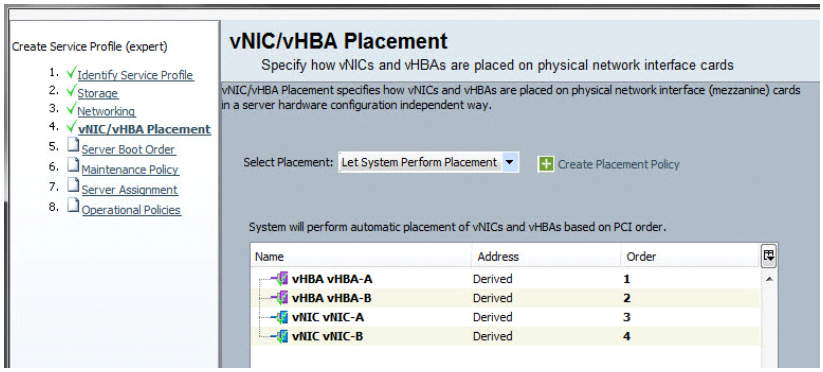


Repeat the process to create the vNIC for Fabric B. You must create a unique name and assign it to Fabric B. All other parameters will be identical to the vNIC for Fabric A.

https://t.me/learningnets

Dual Mezzanine vNIC and vHBA Placement

- Full-slot blades have two mezzanine cards.
- vNIC placement can be automatic or manual.



© 2012 Cisco and/or its affiliates. All rights reserved.

The Cisco UCS B250 and B440 full-slot blade servers include two slots for mezzanine cards. Because a vNIC is a virtual definition of a network interface card (NIC), it could be placed on the appropriate fabric on either of the mezzanine cards present in the full-slot server.

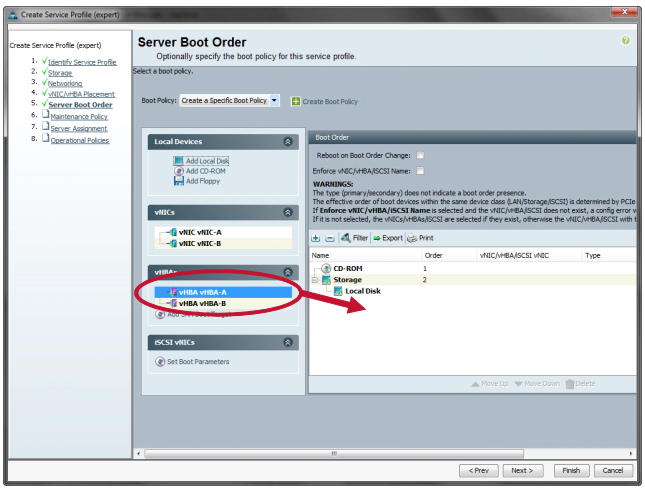
In a half-slot blade with a single mezzanine card, simply allow the system to select the only mezzanine card. If manual control is desired, select **Specify Manually** from the Select Placement drop-down list. vCon1 maps a vNIC to the left mezzanine slot, and vCon2 maps a vNIC to the right mezzanine slot (as viewed from the front panel of the blade server). Click **Next** to continue.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Boot Order Creation

- Specify the boot order for the compute node.
- Drag and drop vHBAs into the boot order.

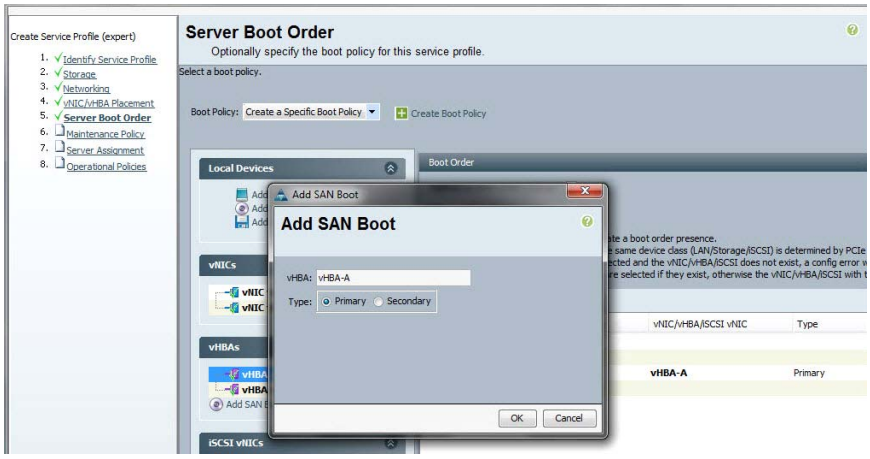


© 2012 Cisco and/or its affiliates. All rights reserved.

To select vHBAs to boot from a logical unit number (LUN), click and drag the first vHBA into the boot order whitespace.

Drag and Drop Pop-Up for Fabric A

- Select the vHBA for Fabric A as the primary boot device.
- This will be the primary path to the storage system.



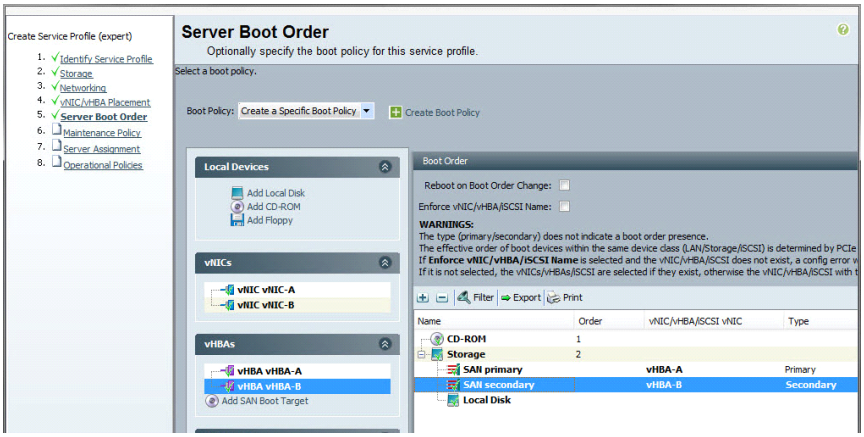
© 2012 Cisco and/or its affiliates. All rights reserved.

A pop-up window will open with the name of the vHBA and the choice to make it the primary or secondary boot device. Select **Primary** for the vHBA on Fabric A, and then click **OK**.

https://t.me/learningnets

Drag and Drop Pop-Up for Fabric B

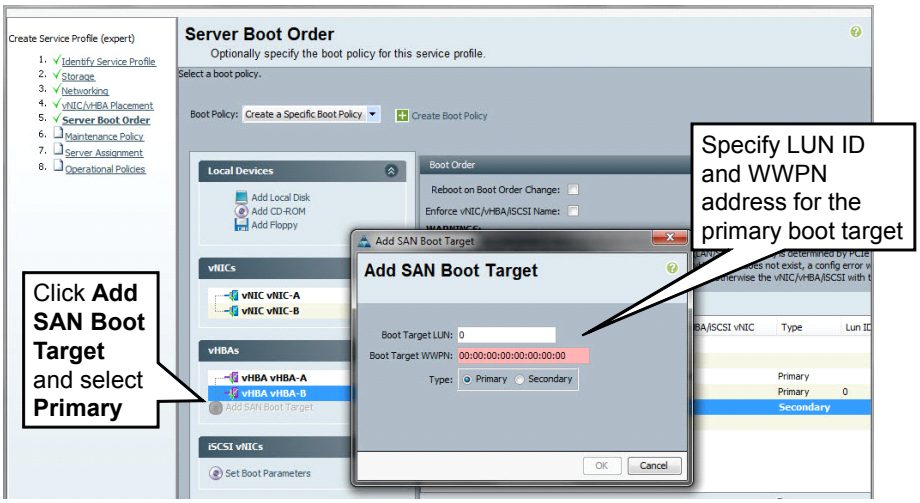
- The vHBA for Fabric B will be the secondary boot device.



© 2012 Cisco and/or its affiliates. All rights reserved.

Repeat the procedure to specify vHBA-B as the secondary path to the storage system.

Set the Primary Boot Target



© 2012 Cisco and/or its affiliates. All rights reserved.

Click **Add SAN Boot Target** and select **Add SAN Boot Target to SAN Primary**.

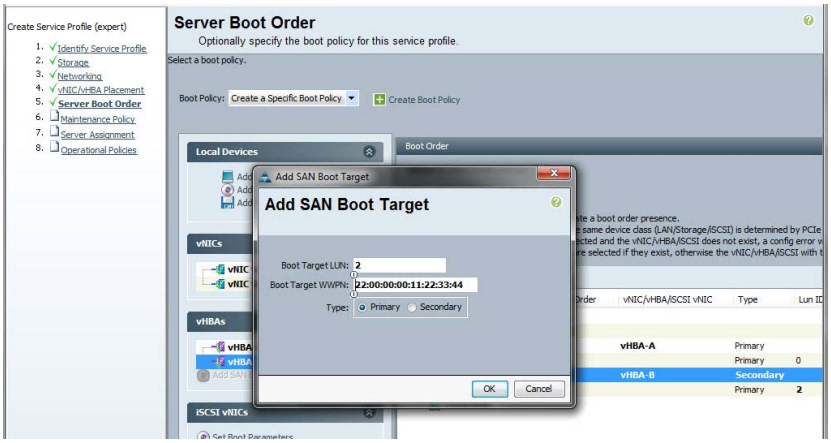
In the pop-up window, enter the boot LUN (always LUN 0 on a Cisco UCS), the WWPN of the boot target, and set the type to **Primary**.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Set the Secondary Boot Target

- Specify the secondary SAN boot target.
- Follow the same procedure.



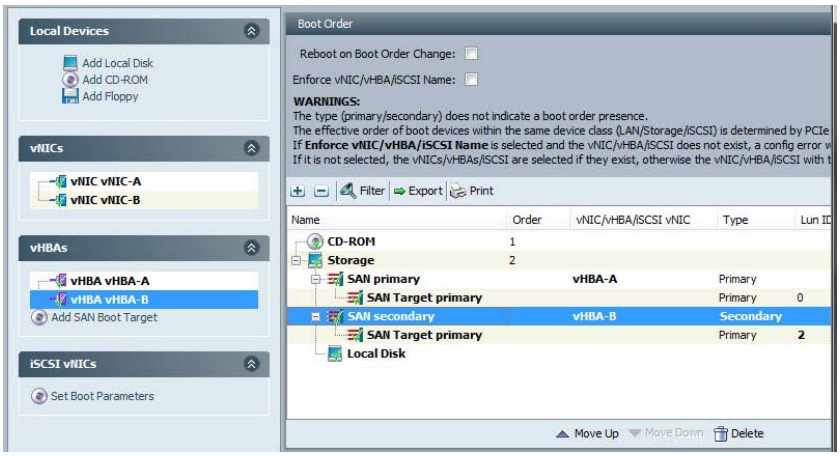
© 2012 Cisco and/or its affiliates. All rights reserved.

Repeat the steps that are required to set the primary boot device, but set the type to **Secondary**. If the primary boot device fails, the secondary device will attempt to boot the system from the other vHBA.

https://t.me/learningnets

Boot Order Summary

- Check the boot order.
- Check the WWPN settings for the SAN targets.



© 2012 Cisco and/or its affiliates. All rights reserved.

After boot devices are configured, the boot order summary window allows you to verify and make modifications to the boot order before committing the configuration.

There are two check boxes:

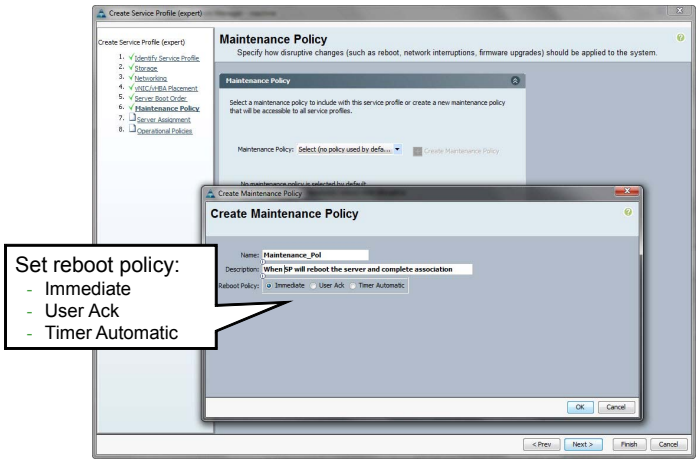
- **Reboot on Boot Order Change:** This option requires that the blade associated with the service profile reboot immediately.
- **Enforce vNIC/vHBA/iSCSI Name:** This option means that the system uses any vNICs or vHBAs in the order that is shown in the Boot Order table. If this option is not checked, the system uses the priority that is specified in the vNIC or vHBA.

Note	If the configuration of a vHBA is changed (other than the boot order), the system will immediately reboot.

https://t.me/learningnets

Provision a Maintenance Policy

- Create a maintenance policy.
- The policy defines when the compute node will be rebooted to finish association with a service profile or on service profile change.



© 2012 Cisco and/or its affiliates. All rights reserved.

The next step in the service profile wizard is to specify the maintenance policy.

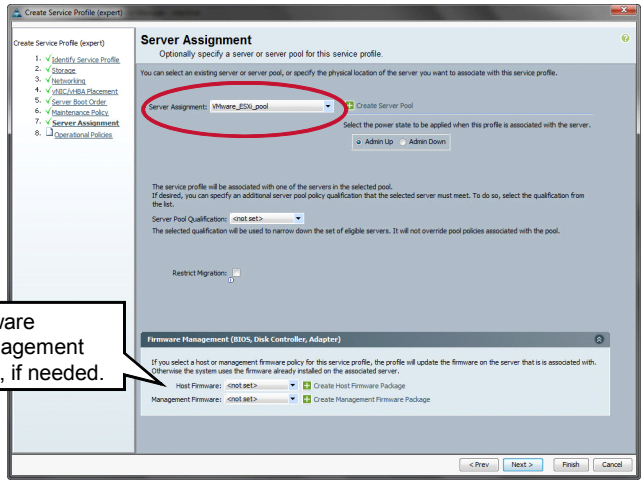
The maintenance policy defines when the compute node will be rebooted after service profile association or changes in the service profile that require rebooting. The following are the available options:

- Immediate
- User Ack
- Timer Automated, which can be a specified schedule

https://t.me/learningnets

Assign a Service Profile to a Server from a Pool

- Select a server pool from the drop-down list.
- Specify the initial power state for the compute node.



© 2012 Cisco and/or its affiliates. All rights reserved.

From the Server Assignment drop-down list, choose an available pool. Cisco UCS Manager will remove that server from all of the pools of which it is currently a member and associate the service profile with that blade.

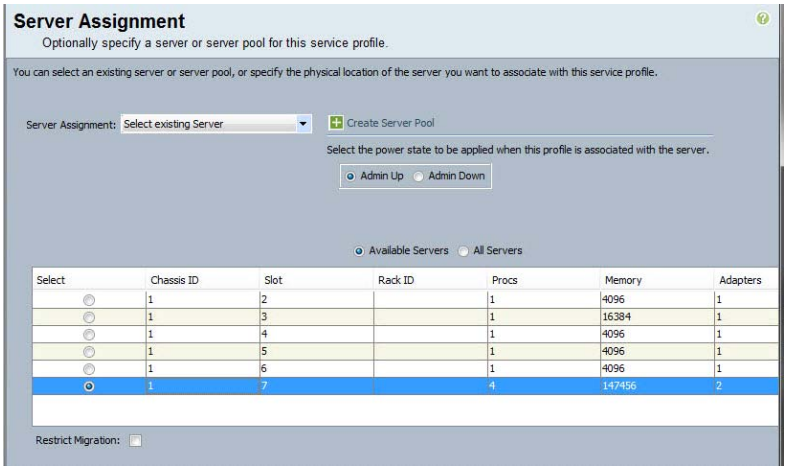
Also during this step, you can specify a host firmware and management firmware package.

Click **Next** to continue the wizard.

https://t.me/learningnets

Assign a Service Profile Directly

- Select a server from all unassociated server blades.
- Information for basic server hardware characteristics is provided.



© 2012 Cisco and/or its affiliates. All rights reserved.

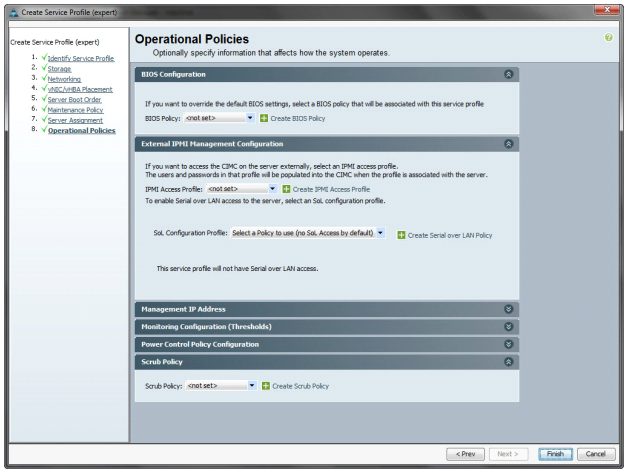
Choose **Select Existing Server** from the Server Assignment drop-down list. Click the radio button of an unassociated server.

The power state radio button allows you to choose the initial power state after the service profile has been successfully associated with the blade server. If the SAN team has not provisioned a boot LUN in time for the service profile, you should leave the power state down.

https://t.me/learningnets

Provision Service Profile Policies

- The last step allows for the provisioning of server-related policies.
- BIOS policy, IPMI and SoL policy, and scrub policy can be defined at this point or in advance.



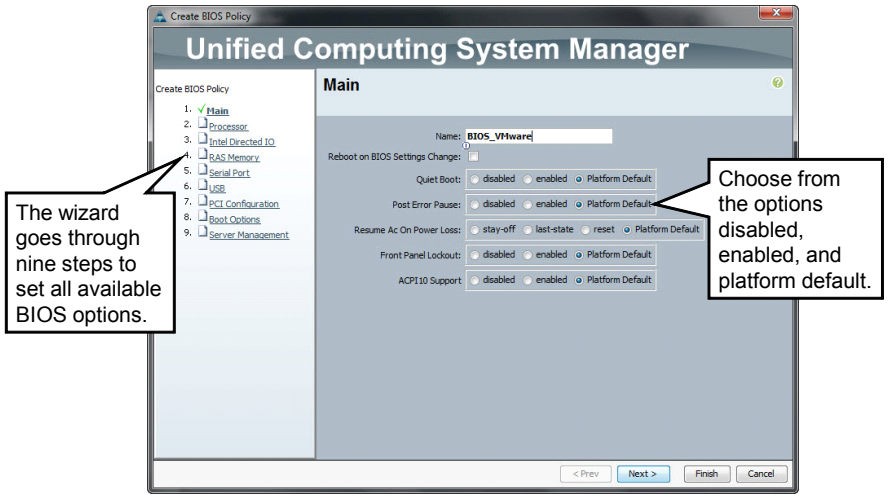
© 2012 Cisco and/or its affiliates. All rights reserved.

Defining operational policies is the last step of the wizard. From here, you can select preprovisioned policies for the BIOS configuration, the Intelligent Platform Management Interface (IPMI) and Serial over LAN (SoL) access, scrub policy, and so on. If you have not preprovisioned the operational policies that you need, you can create them at this point.

https://t.me/learningnets

Provision a BIOS Policy

- Click Create BIOS Policy to start the wizard.
- This configuration will be applied to the BIOS of the server.



Depending on the requirements of the operating system, you might need specific configuration of the BIOS of the server. In Cisco UCS, there are two methods. You can use the default BIOS settings or create a BIOS policy that will be included in the service profile.

BIOS policy provisioning is done through a wizard, which allows you to set all of the BIOS options, as if you are working directly with the BIOS of the server.

The options are divided into nine sections:

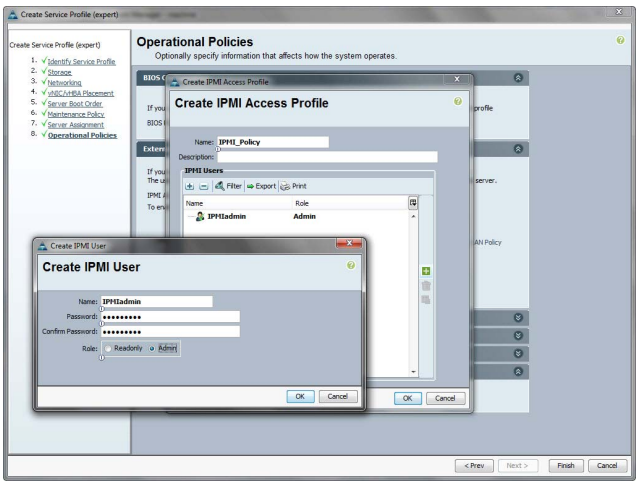
- Main
- Processor
- Intel Direct IO
- RAS Memory
- Serial Port
- USB
- PCI Configuration
- Boot Options
- Server Management

All of these settings depend on the hardware capabilities and the requirements of the server operating system.

https://t.me/learningnets

Provision an IPMI Policy

- Enable IPMI by provisioning an IPMI access profile.
- You must also specify the IPMI users.

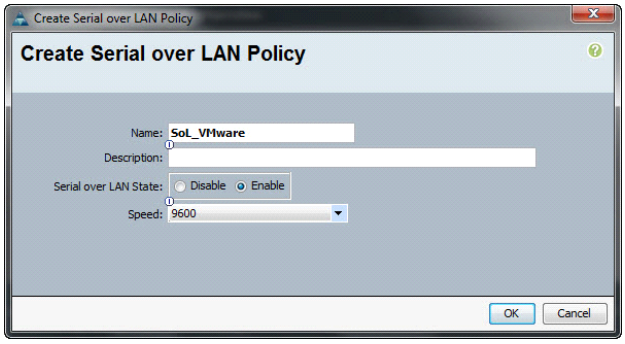


© 2012 Cisco and/or its affiliates. All rights reserved.

To provision an IPMI policy, you must create an IPMI profile. You must specify a name for the profile. You must also create users and assign privileges to these users who will be allowed to access the server via IPMI.

Provision a SoL Policy

- The SoL policy can be provisioned.
- You can define whether SoL is enabled or disabled and set the speed.



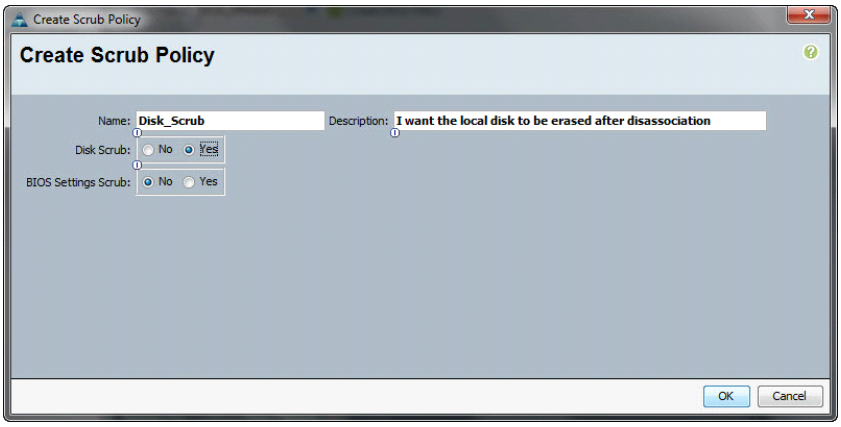
© 2012 Cisco and/or its affiliates. All rights reserved.

You have to specify a name for the SoL policy and define the emulated speed.

https://t.me/learningnets

Provision a Scrub Policy

- You can define whether local disks will be erased on disassociation.
- You can define whether the BIOS will be reset to default.



© 2012 Cisco and/or its affiliates. All rights reserved.

The scrub policy defines what will happen with the BIOS settings and the data on the local hard drives at the time of disassociation. If you need the content of the local drives to be erased, you have to specify **Yes** next to Disk Scrub. You must also decide if you want to scrub the BIOS settings.

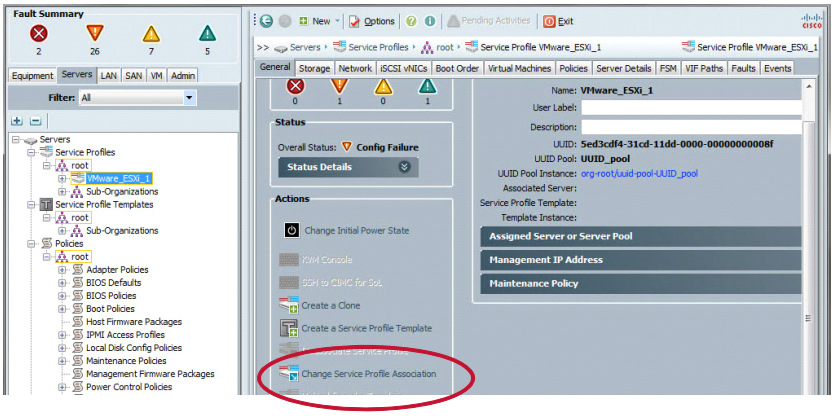
https://t.me/learningnets

Associate a Service Profile to a Server

This topic describes how to associate a service profile with a compute node.

Associate a Service Profile with a Compute Node

- A service profile can be associated later or the association can be changed.
- Select an unassociated service profile and click Change Service Profile Association.



© 2012 Cisco and/or its affiliates. All rights reserved.

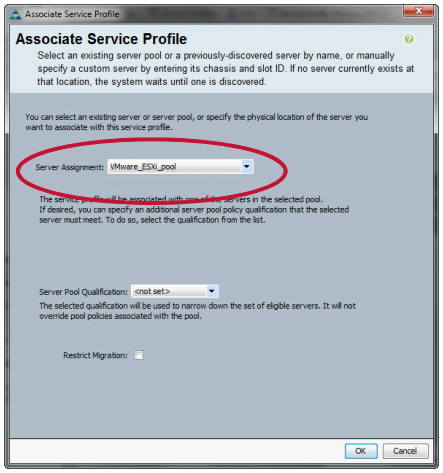
If you previously chose not to immediately assign a service profile to a compute node, you can assign the profile later by selecting the desired service profile in the navigation pane. In the **General** tab of the content pane, click **Change Service Profile Association**.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Associate a Service Profile with a Server Pool

- Select the appropriate server pool from the Server Assignment drop-down list.
- The service profile will immediately choose a server from the server pool.

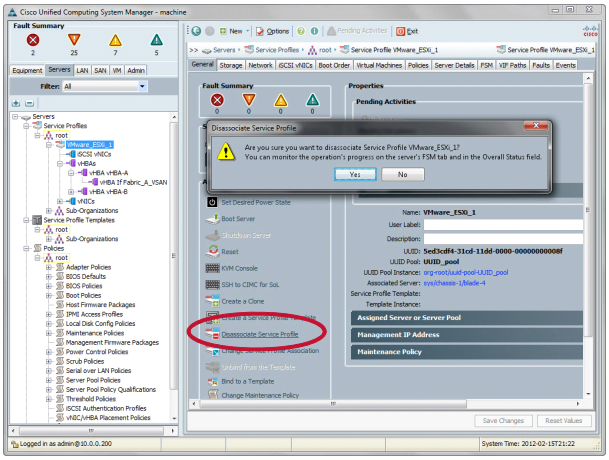


© 2012 Cisco and/or its affiliates. All rights reserved.

A pop-up dialog box prompts you to select either from an existing unassociated server or a server pool. Unlike service profile templates, service profiles that are not bound to a template are not required to select a server from a pool only. Click **OK** to begin the association process.

Disassociate a Service Profile from a Compute Node

- Select the service profile and click Disassociate Service Profile.
- Click Yes in the warning dialog box to confirm the action.
- Monitor the process in the FSM tab.



© 2012 Cisco and/or its affiliates. All rights reserved.

To disassociate a service profile from its compute node, select the service profile in the navigation pane. In the content pane, click **Disassociate Service Profile**. A pop-up warning dialog asks you to verify the operation. Note also the suggestion to observe the process in the FSM tab.

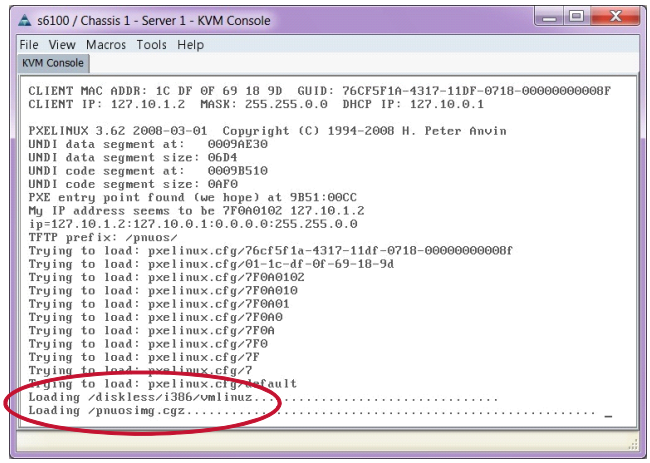
https://t.me/learningnets

Cisco UCS Utility Operating System

This topic describes the Cisco UCS Utility Operating System.

What Happens During Service Profile Association?

- A small Linux kernel is PXE-booted using an internally isolated network in the fabric interconnect.



© 2012 Cisco and/or its affiliates. All rights reserved.

The processes that occur during service profile association and disassociation are interesting. The first step in associating a service profile to a compute node begins with powering up the server. Next, the server Preboot Execution Environment (PXE) boots a small Linux distribution over a private network connection to the fabric interconnect.

The screenshot in the figure highlights the term “pnuosimg.” Before Cisco UCS was released to the public, this Linux operating system was referred to as Processor Node Utility Operating System (PNuOS). The official name is now Cisco UCS Utility Operating System. The old terminology still appears in some contexts.

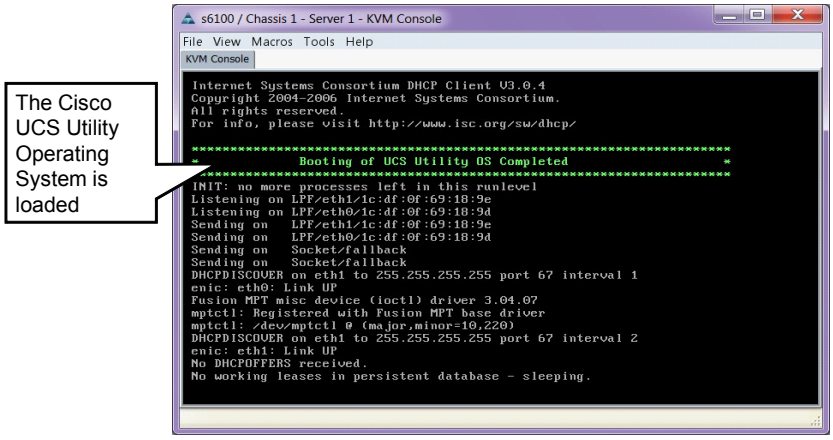
For readability, the black text on white background was reversed from the standard keyboard, video, mouse (KVM) output of white text on black background in a graphics program. The KVM does not provide a choice of text or background colors.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS Utility Operating System

- The Cisco UCS Utility Operating System that is PXE-booted from the fabric interconnect applies all configuration and policy elements of the service profile to a compute node, then exits and reboots the compute node.



© 2012 Cisco and/or its affiliates. All rights reserved.

During PXE boot, the server obtains a DHCP address over the private network. This network is completely isolated from the in-band and out-of-band connections that are processed by the fabric interconnect and servers.

The purpose of booting this Linux operating system is to program the compute node. You will see identity information such as UUID, MAC address, WWNN, WWPN, BIOS configuration, adapter policies, and so on.

https://t.me/learningnets

Changes that Trigger the Cisco UCS Utility Operating System

- When a service profile is associated with a compute node, certain changes made to the service profile trigger a Cisco UCS Utility Operating System update (and instant server reboot).

Configuration Change	Triggers UCSuOS to Run?
Change pooled identity	Yes
Change non-pooled identity	Yes
Change Fibre Channel boot target	Yes
Change boot order	Maybe
Change BIOS config policy	Yes
Change vNIC failover	Yes
Change adapter policy	No
Change VSAN on vHBA	No
Change VLAN on vNIC	No
Change from access VLAN to trunk	No

UCSuOS = Cisco UCS Utility Operating System

© 2012 Cisco and/or its affiliates. All rights reserved.

It is important to understand what types of service profile modifications can be made outside of a change-control maintenance window. The table summarizes changes that will trigger the Cisco UCS Utility Operating System to run. As of Cisco UCS Manager version 1.2, the system alerts you to the changes that will result in the compute node being immediately rebooted.

 © 2012 Cisco Systems, Inc.

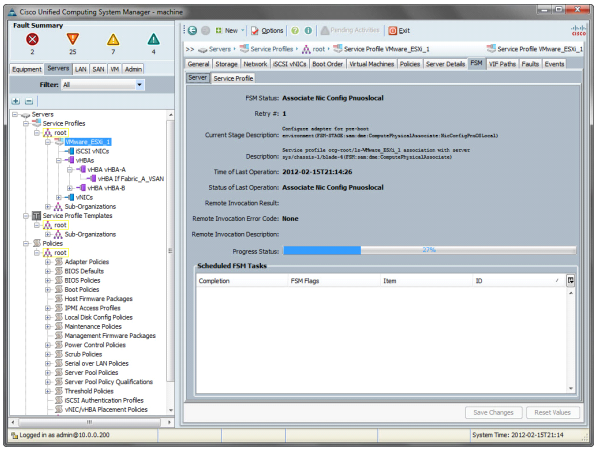
https://t.me/learningnets

Observe the Association Process

This topic describes how to observe association and disassociation processes using the finite state machine (FSM).

Observe the FSM Status During Service Profile Association

- You can observe the association process in the FSM tab in the content pane of the service profile.
- FSM provides information for all stages of the process.



© 2012 Cisco and/or its affiliates. All rights reserved.

You can follow the complete process of association by clicking the FSM tab in the content pane. The service profile association and disassociation are complex processes that are assigned to an FSM.

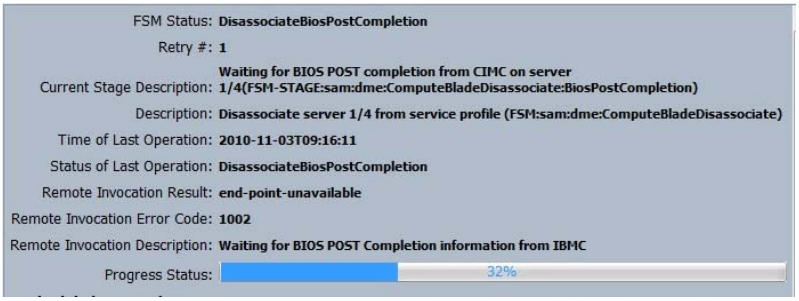
If the service profile is unable to associate with the compute node that is selected, the FSM will provide information about which step of the process caused the failure to occur. This information is useful for troubleshooting service profile association issues.

Note	Be aware that the FSM status indicator may appear to stop and lock up. Some stages of the association process can take 1 minute or longer to complete, which is normal.

https://t.me/learningnets

FSM Status During Service Profile Disassociation

- You can observe the disassociation process in the FSM tab in the content pane of the service profile.



© 2012 Cisco and/or its affiliates. All rights reserved.

Both association and disassociation processes are monitored by the FSM. Click the FSM tab in the content pane to observe the process of disassociation.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.

Summary

- The service profile wizard expert mode allows the most flexibility to create a service profile.
- During the configuration of a service profile, you can create and use operational and configuration policies and identity and server pools.
- A service profile can be associated with a compute node during the creation of the service profile or at a later stage. The options are to manually choose from the available servers or to specify a server pool.
- Cisco UCS Utility Operating System applies service profile settings, policies, and an identity to the physical server.
- The association process can be observed using the FSM, which provides information for the stages of the association process.

© 2012 Cisco and/or its affiliates. All rights reserved.

https://t.me/learningnets

© 2012 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 6

Provisioning Service Profiles from Templates in Cisco UCS Manager

Overview

Service profile templates build on the idea of manually created service profiles. With the potential for a large population of blade servers in a given Cisco Unified Computing System (UCS), manual creation of service profiles would be both slow and error-prone. The use of templates provides the Cisco UCS administrator with the ability to create server definitions in a consistent and rapid process.

Unlike manually created service profiles, service profile templates must use pools for identity and server assignment. Derived hardware values are never used.

Objectives

Upon completing this lesson, you will be able to provision service profile templates, provision service profiles from the templates, and manage the templates. You will know how to use the different types of templates, generate service profiles for large deployments, and clone service profiles. This ability includes being able to meet these objectives:

- Describe the requirements of service profile templates
- Describe the difference between initial templates and updating templates, including operational caveats
- Provision a vNIC template using the template wizard
- Provision a vHBA template using the template wizard
- Provision a service profile template using the template wizard
- Provision multiple servers from a service profile template
- Clone a service profile

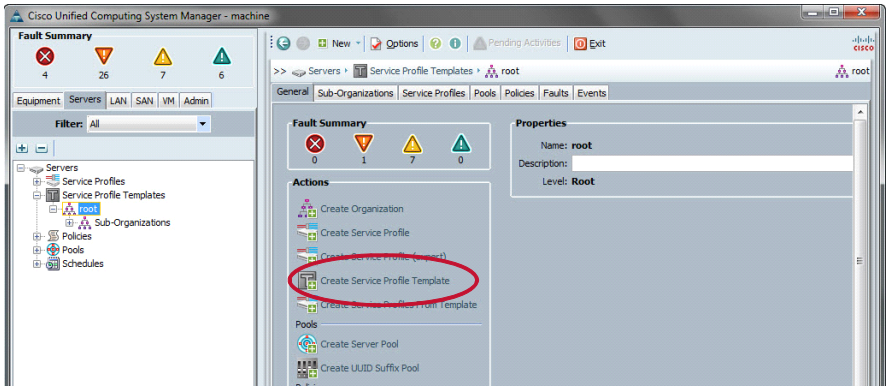
https://t.me/learningnets

Requirements of Service Profile Templates

This topic describes the requirements of service profile templates.

Service Profile Template Requirements

- Similar process to service profile creation
- Requires server pool (cannot select individual blade)
- Requires pooled identities (UUID, MAC, WWNN, WWPN)



© 2012 Cisco and/or its affiliates. All rights reserved.

The process of creating a service profile template is nearly identical to creating a service profile manually. The principal difference is that service profile templates cannot be directly applied to a compute node and no hardware elements can use a derived value.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Using Templates for Differentiated Policy

- The use of templates allows for the consistent application of policy to meet application requirements in heterogeneous computing environments.
- The use of templates allows for quick deployments.

Oracle RAC	SAP	Web Server
B250-M2	B230-M1	B200-M2
256 Gb RAM	128 Gb RAM	8 Gb RAM
Local HD for swap	No local HD	Local HD
M81-KR VIC x 2	M71-KR-Q	M71-KR-E
Xeon 5660 x2	Xeon 6560 x2	Xeon 5620 x 1
RSS support	RSS support	RSS support
Intel VT-d BIOS on	Intel VT-d BIOS off	Intel VT-d BIOS off
Jumbo frames	Jumbo frames	Standard MTU
Hyperthreading off	Hyperthreading on	Hyperthreading on

© 2012 Cisco and/or its affiliates. All rights reserved.

The figure shows the power and flexibility of using templates for differentiated policy. Because groups of applications share similar or identical requirements, service profile templates can be created to seamlessly provide the identity of server resources that are needed to serve the application. One of the important operational benefits to this approach is the consistency of policy across the entire class of applications.

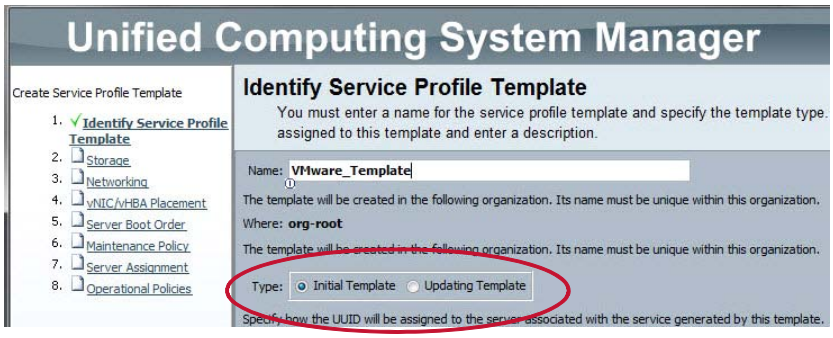
https://t.me/learningnets

Differences Between Initial Templates and Updating Templates

This topic describes the difference between initial and updating templates.

Template Types

- Initial templates
  - Updates to templates are not propagated to service profiles that are created using the initial template.
- Updating templates
  - Changes to templates are propagated to service profiles that are created using the updating template.



© 2012 Cisco and/or its affiliates. All rights reserved.

There are two types of templates:

- **Initial templates:** This type of template maintains no connection to service profiles that are created from this definition. Changes to the template do not propagate to service profiles that are created from the template.
- **Updating templates:** This type of template maintains a semipermanent link to service profiles that are spawned from this definition. Any changes to an updating template will be immediately propagated to all service profiles that are created from the template.

For both types, profiles that are created from a template cannot be modified. The ability to bind or unbind a service profile from its template will be discussed later in this lesson.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Updating Template Issues to Consider

- Updating templates is a great way to update policy on a large number of service profiles.
- The danger is that changing some parameters in the template will cause *all* linked compute nodes to reboot simultaneously.

Policy Change	Result of Change
UUID pool	Reboot all linked compute nodes
WWNN pool	Reboot all linked compute nodes
WWPN pool	Reboot all linked compute nodes
MAC pool	Reboot all linked compute nodes
Boot order	Reboot can be avoided
vNIC and vHBA placement	Reboot all linked compute nodes
Local disk policy	Reboot all linked compute nodes
BIOS policy	Reboot all linked compute nodes
IPMI, SoL, and scrub policies	No reboot

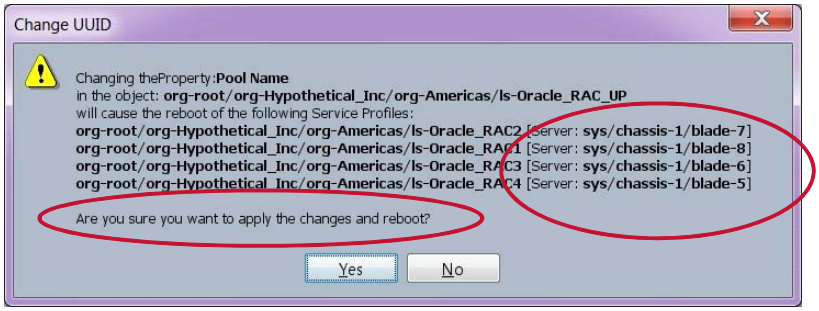
© 2012 Cisco and/or its affiliates. All rights reserved.

Changes to updating templates are immediately propagated to any service profiles that were generated from that template and bound to it. If none of the generated service profiles are associated to a compute node, there is no risk to an update. However, if certain changes are made to the updating template, it will cause all linked compute nodes to reboot. A summary of template modifications and their associated reactions is shown in the figure.

https://t.me/learningnets

Updating Template Warning

- When a change to an updating template will result in the disruption of compute operations, a warning dialog box opens.
- Disruptive changes should only be performed in a planned maintenance window to allow all operating systems and hypervisors to be gracefully shut down.



© 2012 Cisco and/or its affiliates. All rights reserved.

Beginning with Cisco UCS Manager version 1.2, the system warns you that if the modification to the updating template is executed, all impacted compute nodes will reboot immediately.

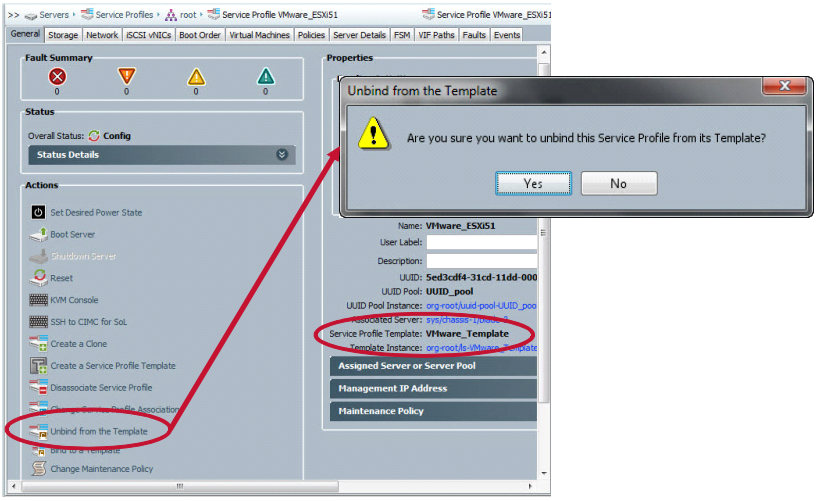
The best practice in this case is to perform the update in a scheduled and approved maintenance window. This practice provides for the graceful shutdown of all compute nodes that the change will affect.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Unbind a Service Profile from Its Template

- Service profiles bound to a template are in a read-only state.
- To modify the service profile, unbind the profile from the template.

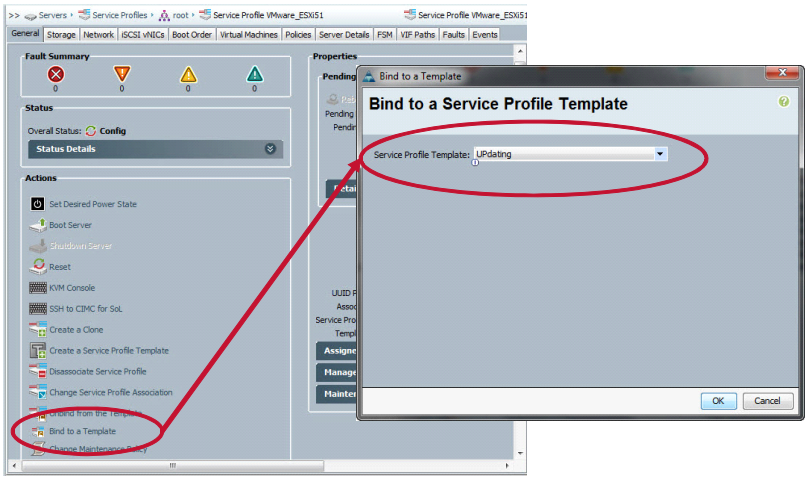


One of the consequences of generating service profiles from an updating template is that the resulting service profiles are created in a read-only state. The Cisco UCS administrator cannot make any changes to the service profile unless it is unbound from the template. By clicking the unbind link, a small dialog box opens asking the administrator to confirm the operation. When the operation is confirmed, the service profile no longer displays the warning or its link to its parent template.

https://t.me/learningnets

Bind a Service Profile to a Template

- Standalone service profiles can be bound to a template at a later time.
- Choose the template.



© 2012 Cisco and/or its affiliates. All rights reserved.

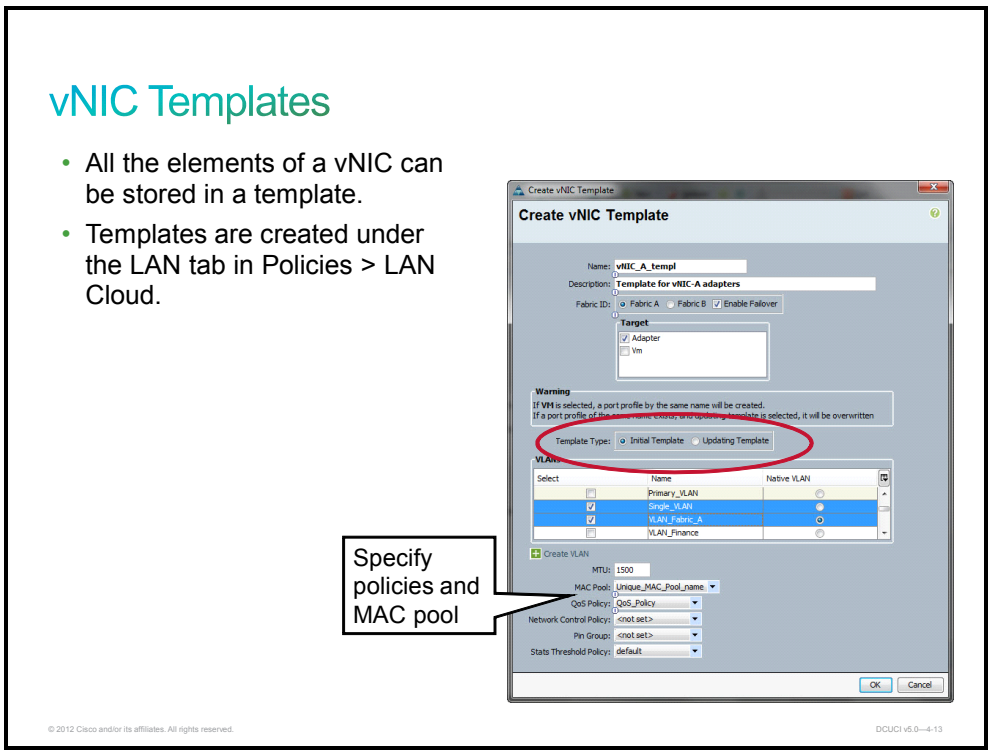
It is also possible to bind a manually created service profile to a template. If the previously created service profile is bound to an initial or updating template, it will retain the identity information for the universally unique identifiers (UUIDs), world wide node name (WWNN), world wide port name (WWPN), and MAC address unless the template uses different pools. If the template uses a different pool, identity information will be replaced with data pulled from the pools of the template.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision a vNIC Template Using the Template Wizard

This topic describes how to provision a virtual network interface card (vNIC) template.



vNIC templates allow Cisco UCS administrators to speed up the repetitive task of entering vNIC parameters in many templates or service profiles. These templates are especially useful when many VLANs must be selected for a trunk interface.

The vNIC templates can also be initial or updating.

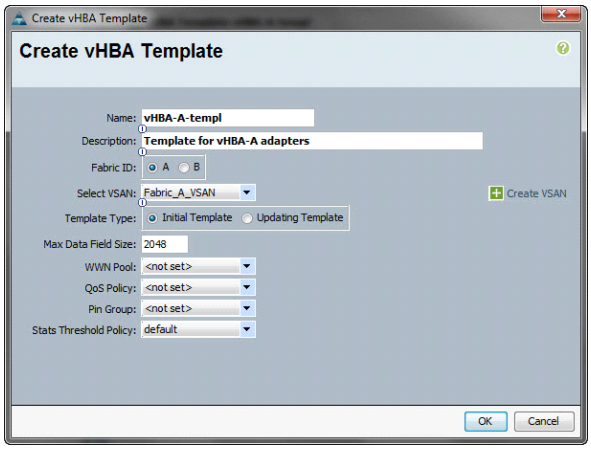
https://t.me/learningnets

Provision a vHBA Template Using the Template Wizard

This topic describes how to provision a virtual host bus adapter (vHBA) template.

vHBA Templates

- All the elements of a vHBA can be stored in a template.
- Templates are created under the SAN tab in Policies.



© 2012 Cisco and/or its affiliates. All rights reserved.

vHBA templates allow Cisco UCS administrators to speed up the repetitive task of entering vHBA parameters in many templates or service profiles. You can enter the information once in the template and never have to set it again.

© 2012 Cisco Systems, Inc.

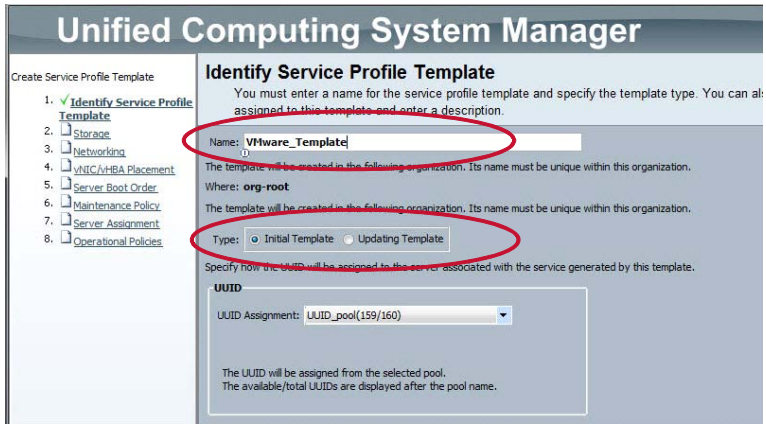
https://t.me/learningnets

Provision a Service Profile Template Using the Template Wizard

This topic describes how to provision a service profile template.

Template Name and Type

- Similar process to service profile creation
- Specify name
- Specify the type—initial or updating



© 2012 Cisco and/or its affiliates. All rights reserved.

Service profile templates require a name, just like manually created service profiles. Templates can also contain an optional description.

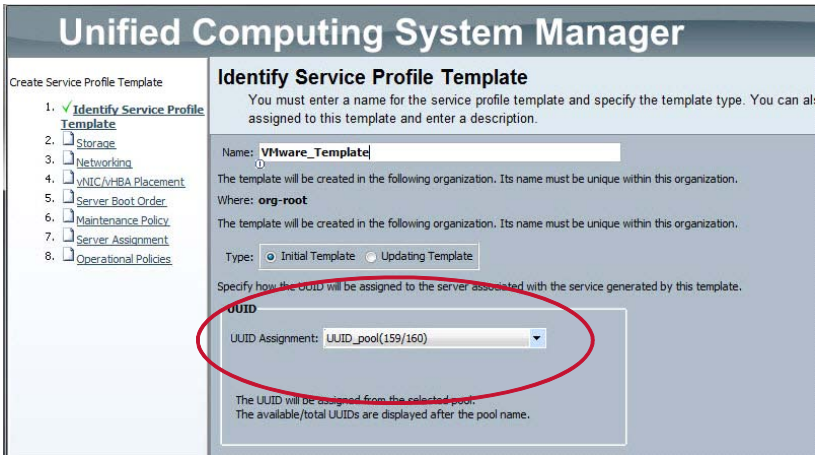
You must specify whether the service profile template type is initial or updating.

Optionally, you can specify a description.

https://t.me/learningnets

Apply a UUID Pool

- All service profiles that are created from this template will use pooled UUIDs.
- Optionally, a description can be specified.



© 2012 Cisco and/or its affiliates. All rights reserved.

To facilitate stateless computing, the UUID must be assigned from a pool. The UUID is unique in that it is the only identity resource that has the option of using the hardware default in the BIOS. Click **Next** to continue the wizard.

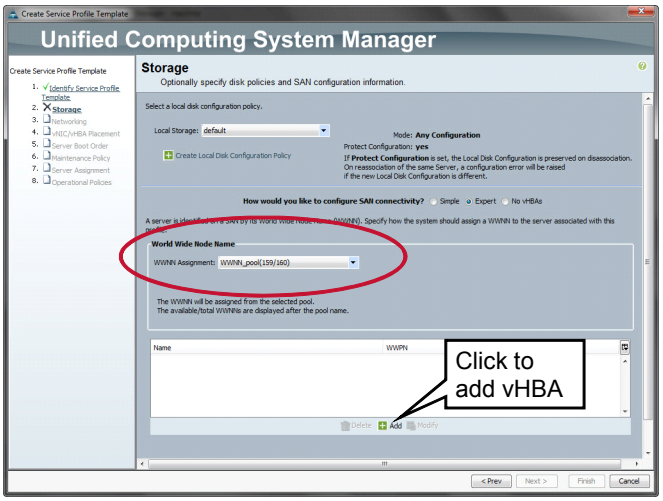
Note	The UUID pool must already be created. Unlike in the service profile wizard, there is no link to create a pool at this point.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Apply a WWNN Pool

- All service profiles that are created from this template will use pooled WWNNs.
- Switch to expert view.



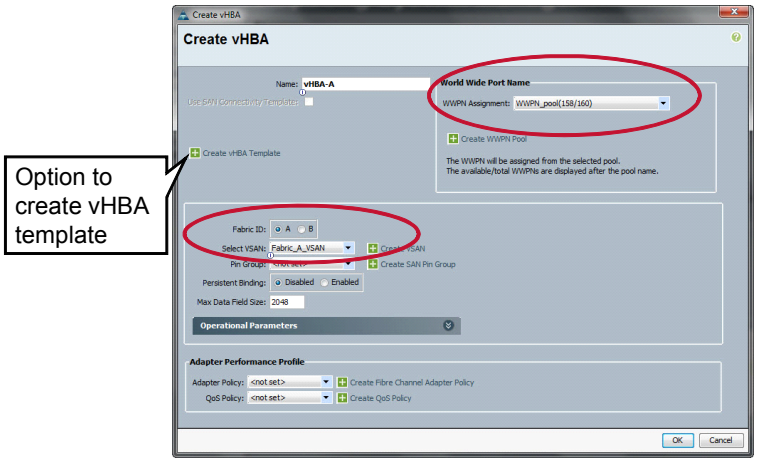
© 2012 Cisco and/or its affiliates. All rights reserved.

To enable Fibre Channel over Ethernet (FCoE) support to service profiles that are generated from this template, enter the name of the WWNN pool.

Switch to expert view to be allowed to create vHBA adapters.

Create a vHBA for Fabric A

- All service profiles that are created from this template will use pooled WWPNs.
- Specify the correct VSAN for Fabric A.



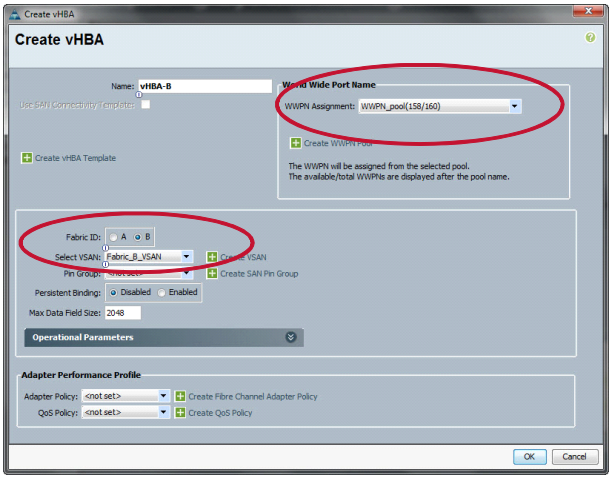
© 2012 Cisco and/or its affiliates. All rights reserved.

Click **Add** to create the vHBA for Fabric A. Like the service profile creation wizard, you must enter a name, fabric affiliation, virtual storage area network (VSAN), and WWPN pool.

https://t.me/learningnets

Create a vHBA for Fabric B

- All service profiles that are created from this template will use pooled WWPNs.
- Specify the correct VSAN for Fabric B.

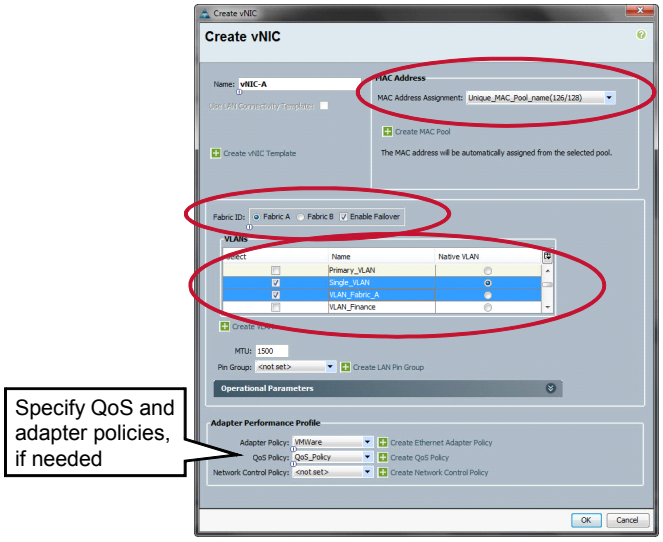


© 2012 Cisco and/or its affiliates. All rights reserved.

Click **Add** to create the vHBA for Fabric B. Like the service profile creation wizard, you must enter a name, fabric affiliation, VSAN, and WWPN pool.

Create a vNIC for Fabric A

- All service profiles that are created from this template will use pooled MACs.



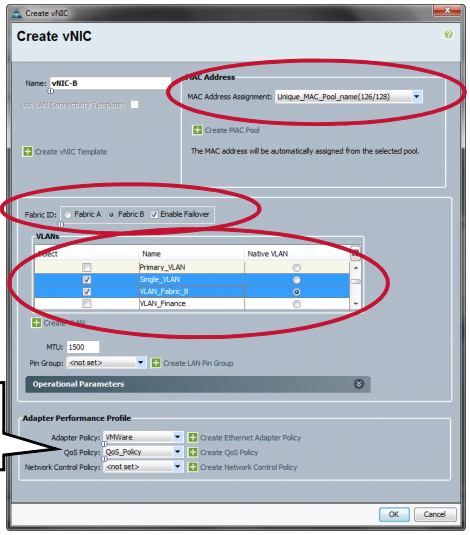
© 2012 Cisco and/or its affiliates. All rights reserved.

The definition of a vNIC in the service profile template wizard is identical to the way that the definition is created in the manual service profile wizard. Enter a name for the vNIC, a MAC address pool, the access VLAN or VLANs associated with an IEEE 802.1Q trunk, any static PIN group, and adapter performance profiles. In this example, the quality of service (QoS) policy named QoS_Policy and the Cisco UCS preconfigured VMware adapter policy will be bound to every service profile that is generated from this template.

https://t.me/learningnets

Create a vNIC for Fabric B

- All service profiles that are created from this template will use pooled MACs.



Specify QoS and adapter policies, if needed

© 2012 Cisco and/or its affiliates. All rights reserved.

The definition of the vNIC for Fabric B is identical to the creation of the vNIC for Fabric A, except for the name.

https://t.me/learningnets

Boot Order and Boot Target

- Create the boot order as if it were a service profile, not a template.
- When SAN boot is used, no local storage is allowed in the boot order.

© 2012 Cisco and/or its affiliates. All rights reserved.

The Cisco UCS administrator has two options regarding the boot order. The figure illustrates a SAN boot policy in which every initiator is mapped to the same target logical unit number (LUN). This mapping is only possible if the storage system maps the source WWPN with a unique LUN. This method is very useful if the SAN administrators can provide premapped WWPNs to LUNs.

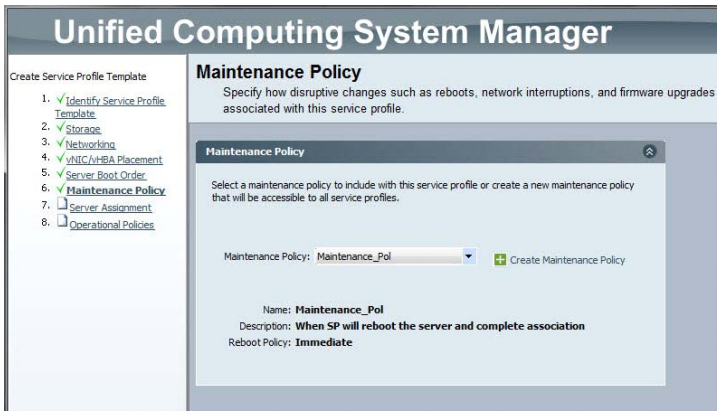
The second option is to define the vHBAs as bootable, but leave the boot target definition for a later time.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision a Maintenance Policy

- This policy specifies when compute nodes will reboot after a configuration change.
- The policy will be used by all service profiles that are generated from this template.

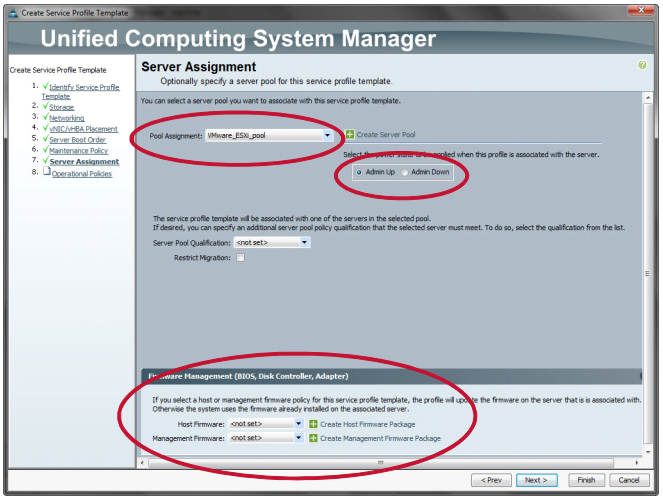


© 2012 Cisco and/or its affiliates. All rights reserved.

Just like in the service profile wizard, you must provision a maintenance policy. The policy will specify the behavior of the service profiles that are generated from this template when disruptive configuration changes are to be applied, and will control when the association will happen.

Template Server Assignment

- Templates can only assign servers from a server pool.
- Specify the power state of the compute nodes.



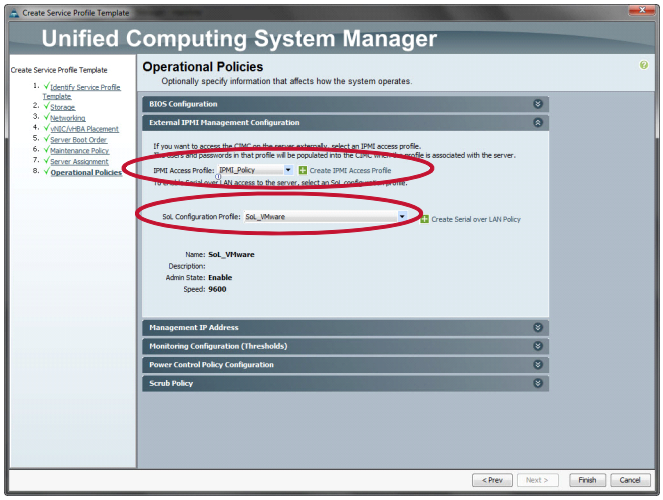
© 2012 Cisco and/or its affiliates. All rights reserved.

It is clear from the server assignment drop-down list that manual assignment is not an option. Servers must be assigned from a pool.

https://t.me/learningnets

IPMI and SoL Policy Assignment

- Add IPMI and SoL policies that were created earlier, or create them now.

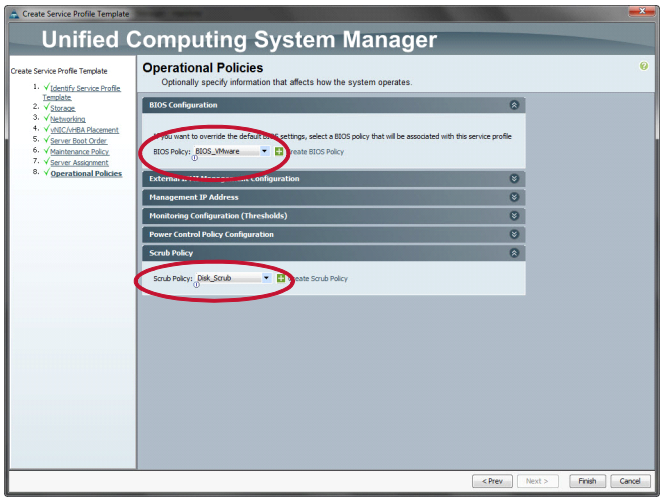


© 2012 Cisco and/or its affiliates. All rights reserved.

The Intelligent Platform Management Interface (IPMI) and Serial over LAN (SoL) policies that were created earlier can be applied to the template. All service profiles that are generated from this template will inherit both policies.

BIOS and Scrub Policy Assignment

- Add a BIOS policy.
- Add a scrub policy.



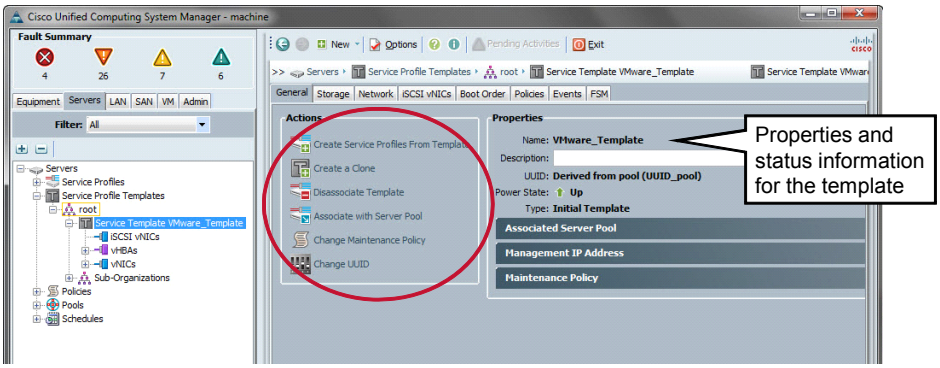
© 2012 Cisco and/or its affiliates. All rights reserved.

The BIOS and scrub policies are applied to the template, and will be assigned automatically to every service profile generated by the template.

https://t.me/learningnets

Modify Templates

- Pool assignments and policies can be changed after template creation.
- Association can be controlled from here.



© 2012 Cisco and/or its affiliates. All rights reserved.

After a service profile template has been generated, it can be modified in a manner very similar to that of a manually created service profile. Certain changes that are made to an updating template will be propagated to every service profile that was generated by the template and bound to it.

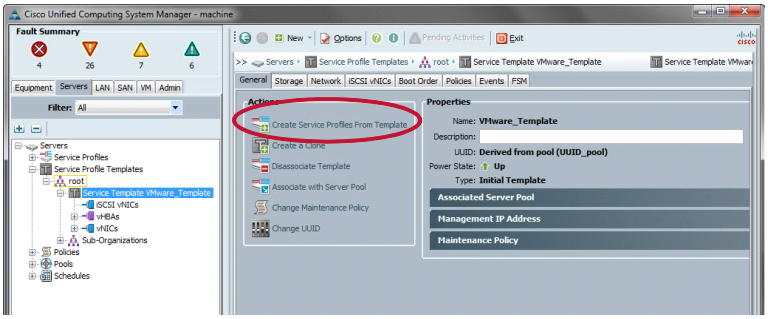
https://t.me/learningnets

Provision Multiple Servers from a Service Profile Template

This topic describes how to provision service profiles from a template.

Creating Service Profiles from a Template

- Creating from a template allows simultaneous provisioning of multiple profiles.
- Service profiles will take identity values from the logical pools immediately.
- Service profiles will associate with compute nodes depending on the server pool and maintenance policy.



© 2012 Cisco and/or its affiliates. All rights reserved.

Another benefit of using service profile templates is that the Cisco UCS administrator can automate the provisioning of anywhere from one to hundreds of compute nodes into simple operations. After a service profile template is built and points to identity and resource pools with sufficient resources, automation can begin.

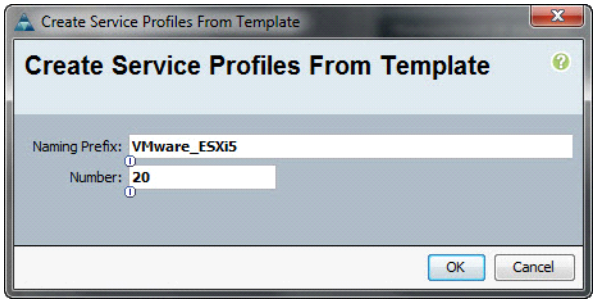
Select the service profile template and the organization where the new service profiles are to be created in the navigation pane. In the content pane, click **Create Service Profiles From Template**.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Select a Prefix and the Number of Profiles

- Provide a naming prefix and the number of service profiles that will be based on the service profile template.
- In the example, the naming prefix would create service profiles VMware_ESXi51 through VMware_ESXi520.



© 2012 Cisco and/or its affiliates. All rights reserved.

The dialog box prompts you for a naming prefix and the number of service profiles to be generated with that prefix. Immediately after you click **OK**, service profiles will appear under the organization. If the server assignment in the template points to a server pool, a new service profile will immediately begin to associate with the next available server in the pool, depending on the maintenance policy. In the example in the figure, 20 service profiles will be generated from this service profile template.

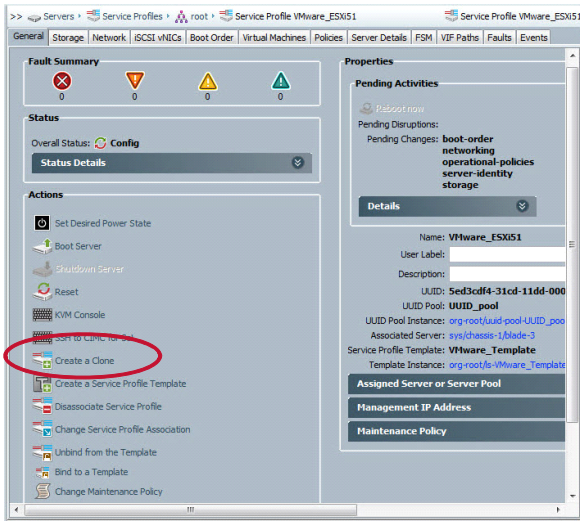
https://t.me/learningnets

Clone a Service Profile

This topic describes how to clone a service profile.

Service Profile Cloning

- All pool associations are replicated to a cloned template.



© 2012 Cisco and/or its affiliates. All rights reserved.

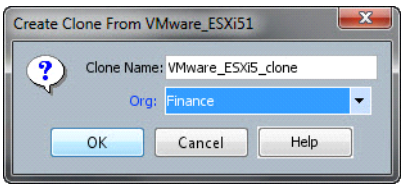
Service profiles and service profile templates both can be cloned. Simply right-click the name of the service profile or service profile template and select **Create a Clone**, or click the plus sign (+) in the content pane. The result of this operation is that all pooled identities in the clone will be refreshed with unique values. The boot order is cloned verbatim.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Clone Destination

- Unique values for MAC and WWN will be immediately assigned to the profile from the appropriate pool.
- Select the destination organization where the clone should be created.



© 2012 Cisco and/or its affiliates. All rights reserved.

When you commit to creating a clone, a pop-up dialog box prompts you for the name of the clone and the destination organization where the clone will be created.

Note	Remember that once an object is created in a particular organization, it cannot be moved or renamed. If an object is created in the wrong organization, it must be deleted and then re-created in the correct organization.

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.

Summary

- Service profile templates require the use of pools for identity values and server assignments.
- Initial templates do not preserve any link with the service profiles that are created from them. The updating templates will propagate any changes to the service profiles that are created from them.
- A vNIC template can be provisioned to automate the tasks of creating vNIC adapters.
- A vHBA template can be provisioned to automate the tasks of creating vHBA adapters.
- The service profile template wizard is similar to the service profile wizard.
- You can provision multiple service profiles at once from a service profile template. The name prefix and number of service profiles wanted must be specified.
- Service profiles and service profile templates can be cloned.

© 2012 Cisco and/or its affiliates. All rights reserved.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 7

Provisioning Cisco UCS C-Series Server Integration in Cisco UCS Manager

Overview

Cisco Unified Computing System (UCS) C-Series Servers are Cisco rack-mount servers. They can operate in standalone mode or can be integrated as a component of Cisco UCS. This integration allows for centralized management of rack servers by Cisco UCS Manager. The integration also provides the benefit of using service profiles to support large deployments and allows better utilization of the available hardware in the data center.

Objectives

Upon completing this lesson, you will be able to provision Cisco UCS C-Series server integration. You will know the requirements for physical connectivity and the required version of the C-Series firmware. You will know how to install the firmware on C-Series servers to allow integration with Cisco UCS. This ability includes being able to meet these objectives:

- Describe the benefits of C-Series integration
- Describe the physical connectivity requirements for C-Series integration
- Install version 1.2 C-Series server firmware to allow integration with Cisco UCS prior to version 2.0(2xx)
- Describe the C-Series discovery process

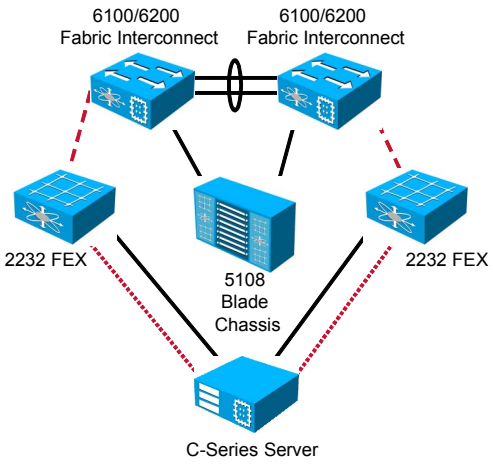
https://t.me/learningnets

Benefits of Cisco C-Series Integration

This topic describes the benefits of Cisco C-Series server integration.

C-Series UCS Integration Benefits

- Cisco C-Series servers can be integrated with Cisco UCS.
- Cisco UCS C200 M2, C210 M2, C220 M3, C240 M3, C250 M2, C260 M2, and C460 M2 can be integrated.
- Cisco UCS Manager provides central management.
- C-Series servers are configured through service profiles.
- You cannot directly access the C-Series Cisco Integrated Management Controller.



© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco C-Series servers are rack-mount servers. They can operate in standalone mode and behave like traditional servers, or they can be integrated with Cisco UCS.

When C-Series servers are integrated with Cisco UCS, they become a component of the Cisco UCS and are managed by Cisco UCS Manager. This integration also means that you must create and use service profiles to provision and utilize the servers. When C-Series servers are part of the Cisco UCS, you cannot directly access the Cisco Integrated Management Controller of the server.

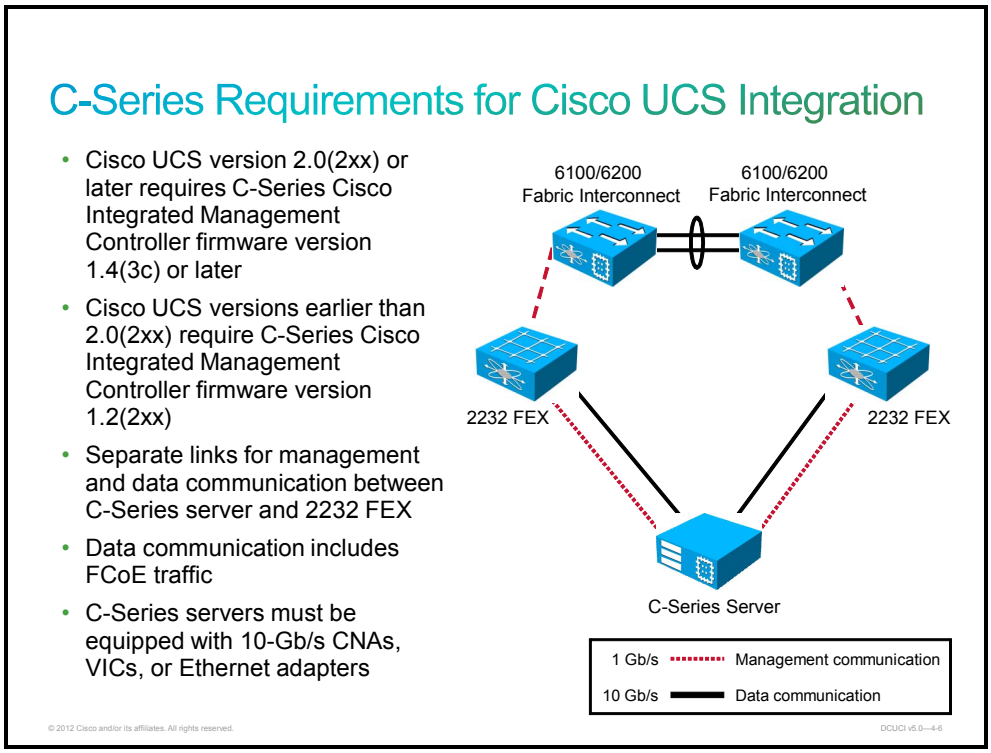
The centralized management, which is performed by Cisco UCS Manager, and the use of service profiles allow for better utilization of available server hardware and for the support of large-scale deployments.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Physical Connectivity Requirements for C-Series Integration

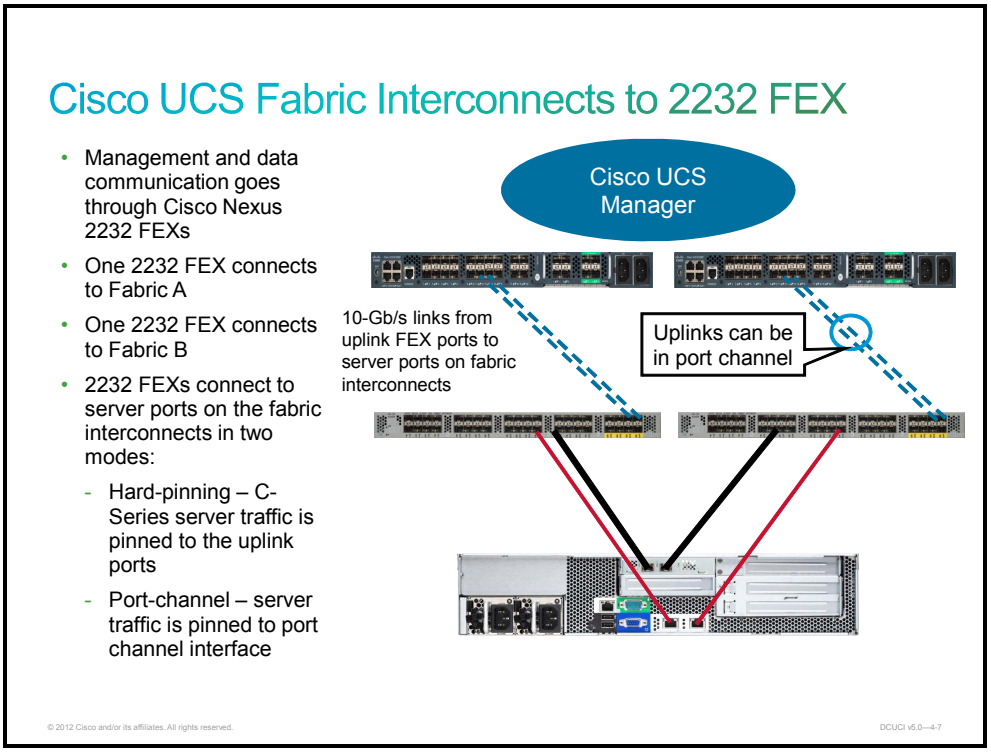
This topic explains the physical connectivity that is required for C-Series server integration with Cisco UCS.



When C-Series servers are integrated with Cisco UCS, they are connected in a specific way. The management and data communications utilize separate dedicated paths to Cisco Nexus 2232 Fabric Extenders (FEXs).

For data communication, C-Series servers utilize the same media for both Ethernet data traffic and access to the SAN infrastructure. This media usage means that the servers use Fibre Channel over Ethernet (FCoE)-based communication. For this reason, the connectivity requirements for data communication state that the links must be at least 10 Gb/s. C-Series servers can be equipped with Converged Network Adapters (CNAs), virtual interface cards (VICs), or Ethernet adapters, if no access to storage systems will be needed.

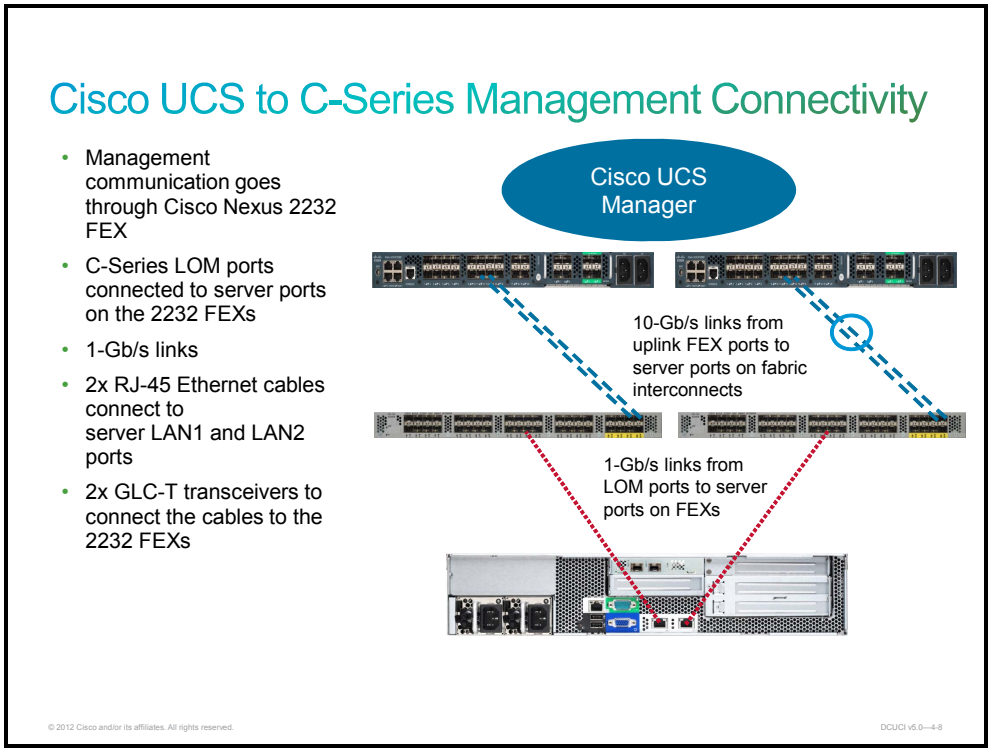
https://t.me/learningnets



The Cisco C-Series server connectivity goes through two 2232 FEXs in the following way:

- One 2232 FEX connects to Fabric A.
- One 2232 FEX connects to Fabric B.
- The 2232 FEXs connect to server ports on the fabric interconnects in two modes:
  - **Hard-pinning:** C-Series server traffic is pinned to the uplink ports on the FEXs.
  - **Port-channel:** Server traffic is pinned to the port channel uplink interface.

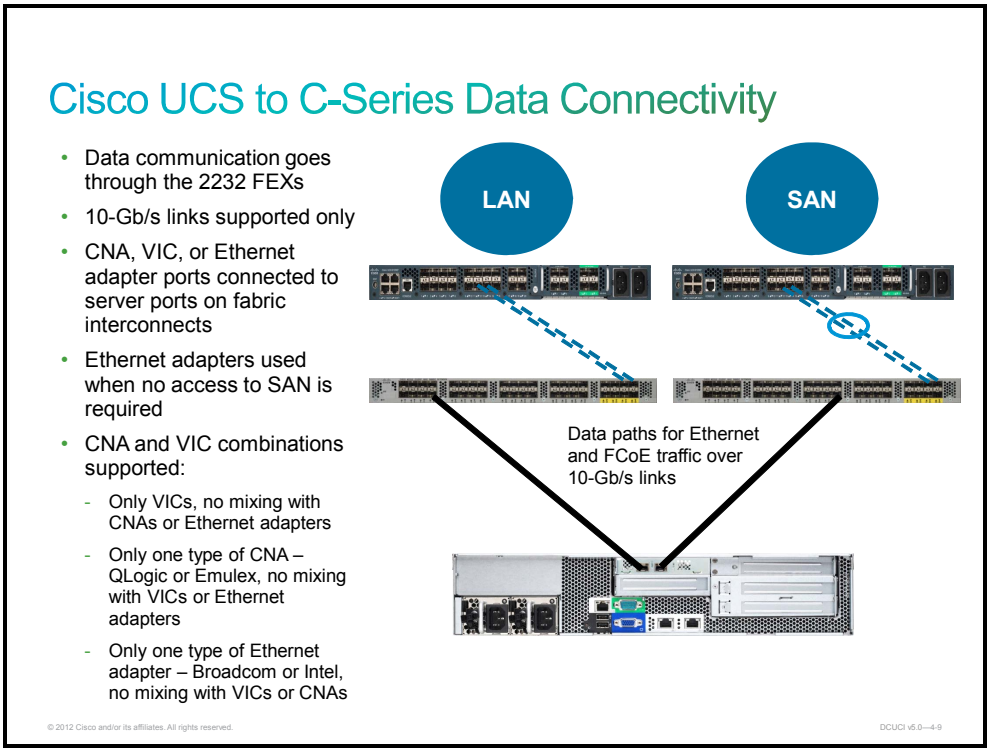
© 2012 Cisco Systems, Inc.
https://t.me/learningnets



The management connectivity is realized as follows:

- Cisco C-Series LAN-on-motherboard (LOM) ports connected to server ports on the 2232 FEXs
- 1-Gb/s links
- Two RJ-45 Ethernet cables connect to server LAN1 and LAN2 ports
- Two GLC-T transceivers connect the cables to the 2232 FEXs

https://t.me/learningnets

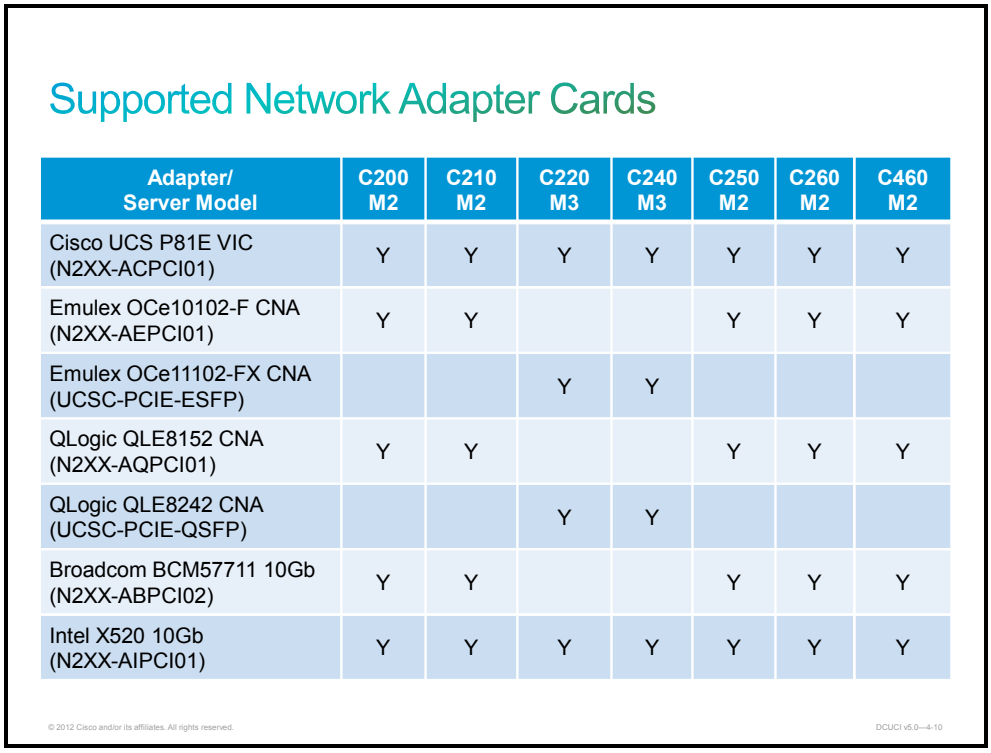


Data connectivity is realized by using 10-Gb/s small form-factor pluggable (SFP) cables. In the Cisco C-Series server, a CNA, VIC, or Ethernet adapter must be installed. One port from the server adapter is connected to one server port at one of the Cisco Nexus 2232 FEXs. Another port from the server is connected in the same manner to the other 2232 FEX.

There are rules for adapters that are installed in the server:

- Only 10-Gb/s links are supported.
- CNA, VIC, or Ethernet adapter ports are connected to server ports on fabric interconnects.
- Ethernet adapters are used when no access to SAN is required.
- The following CNA and VIC combinations are supported:
  - Only VICs, no mixing with CNAs or Ethernet adapters.
  - Only one type of CNA—QLogic or Emulex—no mixing with VICs or Ethernet adapters.
  - Only one type of Ethernet adapter—Broadcom or Intel—no mixing with VICs or CNAs.

© 2012 Cisco Systems, Inc.
https://t.me/learningnets



The table in the figure shows which network adapter cards are supported on which Cisco C-Series server models.

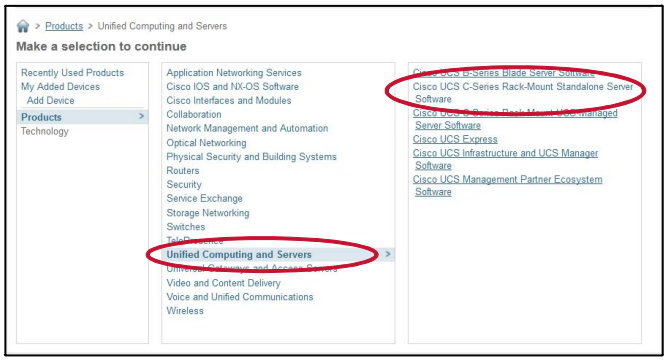
https://t.me/learningnets

Install Version 1.2 C-Series Server Firmware to Allow Integration

This topic describes how to install firmware version 1.2 on C-Series servers.

Prepare to Install Version 1.2 C-Series Server Firmware

- C-Series firmware version 1.2(2XX) is required to allow Cisco UCS integration with Cisco UCS versions earlier than 2.0(2xx).
- From Cisco.com, download C-Series Standalone Server Software.



© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco C-Series servers require firmware version 1.2(2XX) to integrate with Cisco UCS instances that use a version earlier than 2.0(2xx).

To install the needed firmware, you must first download the Host Upgrade Utility image from Cisco.com.

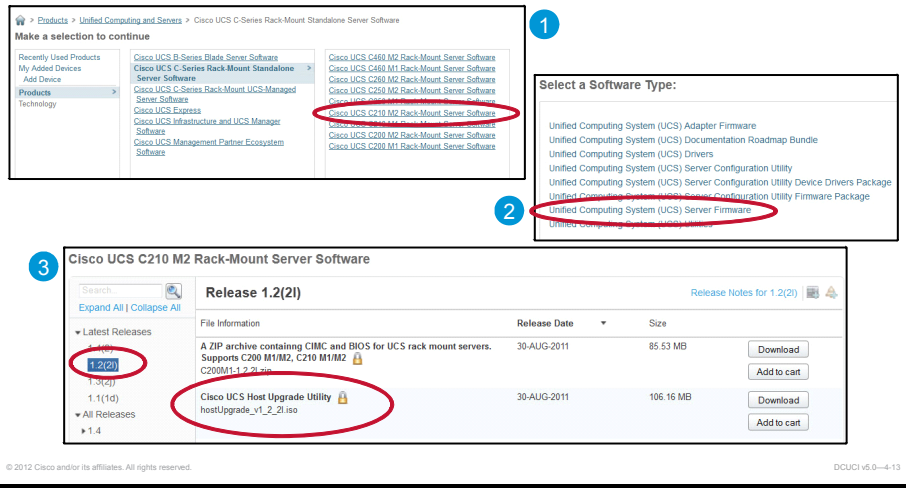
From Cisco.com, navigate to **Unified Computing and Servers > Cisco UCS C-Series Rack-Mount Standalone Server Software**.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Download Host Upgrade Utility Version 1.2(2XX)

- Choose server model server firmware version 1.2(2XX) and download Host Upgrade Utility
- Extract and use as virtual media or prepare image on local media



Follow these steps to download firmware version 1.2:

Step 1 Choose the server model.

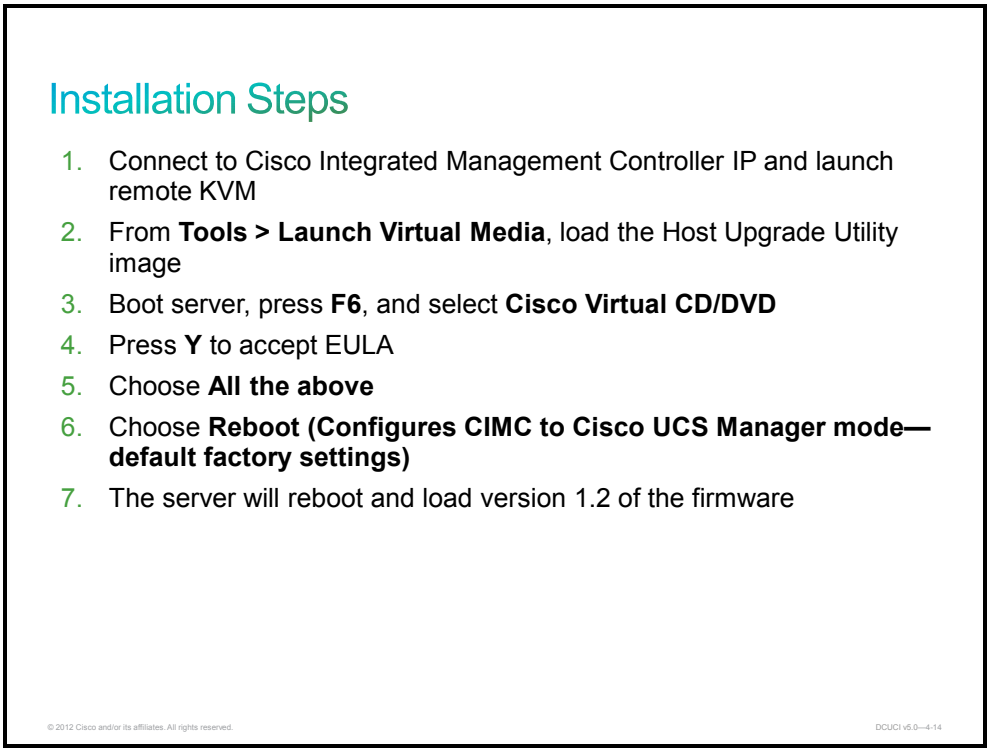
Step 2 Choose **Unified Computing System (UCS) Server Firmware**.

Step 3 Choose version **1.2(2XX)**.

Step 4 Choose the correct Cisco UCS Host Upgrade Utility ISO file and download it.

Step 5 Locally, extract the image file.

https://t.me/learningnets



Now that you have the image file, the following steps describe the installation procedure:

Step 1 Connect to the Cisco Integrated Management Controller.

Step 2 Launch the remote keyboard, video, mouse (KVM) console.

Step 3 In the KVM console, navigate to **Tools > Launch Virtual Media**.

Step 4 Click **Add Image** and choose the image file of the Host Upgrade Utility.

Step 5 Boot the server and press **F6**.

Step 6 Choose **Cisco Virtual CD/DVD**.

Step 7 The installation will start.

Step 8 Accept the EULA agreement.

Step 9 From the menu, choose the number that corresponds to **All the above**.

Step 10 When the installation has finished, choose the number for **Reboot (Configures CIMC to Cisco UCS Manager mode—default factory settings).**

Step 11 The server will reboot and load the new version of the firmware.

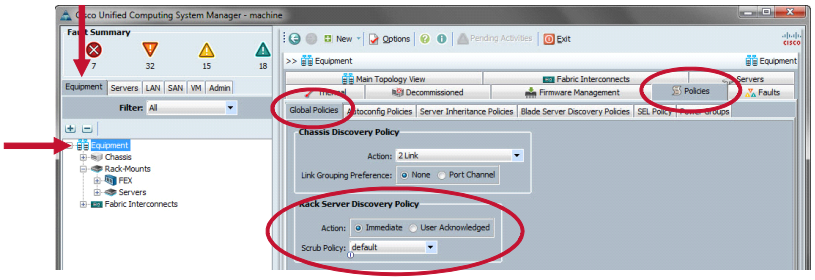
© 2012 Cisco Systems, Inc.
https://t.me/learningnets

C-Series Discovery Process

This topic describes how to provision the Rack Server Discovery Policy in Cisco UCS.

Cisco UCS Rack Server Discovery Policy

- The rack server discovery policy defines how Cisco UCS discovers C-Series servers.
- The policy defines the scrub policy and whether server discovery occurs immediately.
- When the Cisco Nexus 2232 FEX is decommissioned or recommissioned, the C-Series servers must be re-acknowledged in Cisco UCS Manager.



© 2012 Cisco and/or its affiliates. All rights reserved.

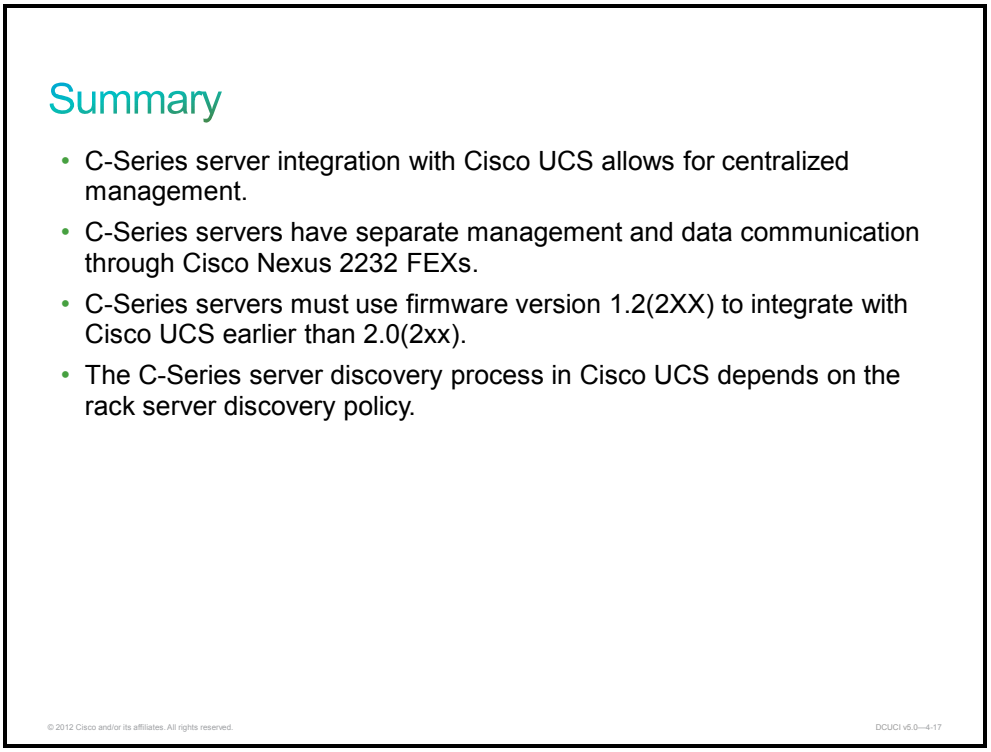
How Cisco UCS discovers C-Series servers depends on the setting of the rack server discovery policy. This policy defines whether the server will be discovered immediately or after the acknowledgement of an administrator. Also, this policy defines if a scrub policy will be used for the server.

To provision the rack server discovery policy, go to the **Equipment** tab and choose **Equipment**. In the content pane, go to the **Policies** tab and choose the **Global Policies** subtab.

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.



© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module Summary

This topic summarizes the primary points that were discussed in this module.

Module Summary

- To provision a Cisco UCS cluster, first provision the primary fabric interconnect, then boot to perform the initial configuration on the secondary fabric interconnect.
- Cisco UCS upstream Ethernet connectivity is realized by uplink ports. The ports can form port channels. You have to provision the correct VLANs. Fabric port channels can be created between Cisco UCS 6200UP Fabric Interconnects and Cisco 2204 IOMs. Appliance ports are used for direct attachment of iSCSI, NAS devices, Cisco Nexus 1010, or security appliances.
- Cisco UCS upstream SAN connectivity is realized by uplink Fibre Channel ports. The correct VSANs must be provisioned on the Cisco UCS. A directly attached Fibre Channel storage system can be used when the fabric interconnects operate in Fibre Channel switching mode.

© 2012 Cisco and/or its affiliates. All rights reserved.

Module Summary (Cont.)

- Logical resource pools provide the identity values that are used in service profiles and assigned to compute nodes. Server pools are used to combine servers with similar hardware characteristics.
- Service profiles are the virtual servers in Cisco UCS. All the configuration related to servers is specified in service profiles, as are all related policies.
- Service profile templates can be used for large-scale deployments, allowing for the generation of multiple identical service profiles. Service profile template types are updating and initial.
- Cisco C-Series servers can be integrated with Cisco UCS and become a component of the system. When integrated, they are under the management of Cisco UCS Manager.

© 2012 Cisco and/or its affiliates. All rights reserved.

https://t.me/learningnets

References

For additional information, refer to these resources:

- Cisco, Inc. *Cisco UCS Manager GUI Configuration Guide, Release 2.0*: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/2.0/b_UCSM_GUI_Configuration_Guide_2_0.html
- Cisco, Inc. *Cisco UCS C200 Installation and Service Guide*: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C200M1/install/c200M1.html
- Cisco, Inc. *Cisco UCS C210 Installation and Service Guide*: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C210M1/install/C210M1.html
- Cisco, Inc. *Cisco UCS C250 Server Installation and Service Guide*: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C250M1/install/c250M1.html
- Cisco, Inc. *Release Notes for Cisco UCS Software, Release 2.0*: http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_25363.html
- Cisco, Inc. *Release Notes for Cisco UCS Software, Release 1.4*: http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_24086.html
- Cisco, Inc. *Cisco UCS 6100 and 6200 Series Configuration Limits for Cisco UCS Manager, Release 2.0*: http://www.cisco.com/en/US/partner/docs/unified_computing/ucs/sw/configuration_limits/2.0/b_UCS_Configuration_Limits_2_0.html

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) How many fabric interconnects form a high-availability cluster? (Source: Provisioning the Cisco UCS Cluster)

A) 1
B) 2
C) 3
D) 4

Q2) In which two ways can you access the initial startup wizard for the Cisco UCS 6100 or 6200 Series Fabric Interconnects? (Choose two.) (Source: Provisioning the Cisco UCS Cluster)

A) from a new system when started for the first time
B) after issuing the **erase configuration** command from the Cisco UCS Manager CLI
C) issue the **start wizard** command from the Cisco UCS Manager CLI
D) issue the **setup** command in the Cisco UCS CLI

Q3) How many management IP addresses must be allocated for a high-availability Cisco UCS cluster? (Source: Provisioning the Cisco UCS Cluster)

A) 1
B) 2
C) 3
D) 4

Q4) Which two commands provide information about the state of the high-availability cluster? (Choose two.) (Source: Provisioning the Cisco UCS Cluster)

A) **show cluster state**
B) **show high-availability state**
C) **show cluster extended-state**
D) **show cluster status**

Q5) Which three methods are supported for assigning management IP addresses to the Cisco Integrated Management Controllers of the B-Series and C-Series servers under the management of Cisco UCS Manager? (Choose three.) (Source: Provisioning the Cisco UCS Cluster)

A) directly assign a static IP address
B) assign an IP address through a service profile
C) by a DHCP server
D) from the management IP pool in Cisco UCS Manager
E) by a switch
F) no IP address is needed

https://t.me/learningnets

Q6) Which three ways of creating VLANs are available in Cisco UCS Manager? (Choose three.) (Source: Provisioning LAN Networking)

A) on both fabric interconnects with the same configuration
B) on both fabric interconnects with different configurations per fabric interconnect
C) only on Fabric A or B
D) on a per-server basis
E) per upstream switch
F) VLANs are migrated from upstream switches

Q7) What is the role of an Ethernet port on the fabric interconnect that is used to connect to the upstream LAN switch? (Source: Provisioning LAN Networking)

A) upstream
B) switch
C) uplink
D) trunk

Q8) Which protocol is supported when you form an uplink port channel? (Source: Provisioning LAN Networking)

A) PAgP
B) LACP
C) none
D) both PAgP and LACP

Q9) Which combination of hardware is needed to support fabric port channels? (Source: Provisioning LAN Networking)

A) Cisco 6120 Fabric Interconnect and 2104 IOM
B) Cisco 6248UP and 2104 IOM
C) Cisco 6248UP and 2208 IOM
D) Cisco 6140 Fabric Interconnect and 2208 IOM

Q10) Which of these must be the Fibre Channel mode of operation to use a direct-attach FCoE storage system on FCoE storage ports? (Source: Provisioning LAN Networking)

A) Fibre Channel switching mode
B) NPV
C) combined
D) supported in both modes

Q11) How many active VSANs can currently be supported in Cisco UCS Manager? (Source: Provisioning SAN Networking)

A) 10
B) 32
C) 1024
D) 4093

Q12) Which two types of ports can be provisioned as Fibre Channel uplink ports? (Choose two.) (Source: Provisioning SAN Networking)

A) native Fibre Channel ports
B) Ethernet ports with FCoE
C) unified ports
D) USB adapter ports

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Q13) Which mode supports trunking for uplink Fibre Channel ports and port channels? (Source: Provisioning SAN Networking)

A) Fibre Channel switching mode
B) NPV mode
C) both Fibre Channel switching mode and NPV mode
D) End Host mode

Q14) How many Fibre Channel port channels and Fibre Channel port members per port channel are supported in Cisco UCS Manager? (Source: Provisioning SAN Networking)

A) 4 Fibre Channel port channels, 16 Fibre Channel port members per port channel
B) 8 Fibre Channel port channels, 8 Fibre Channel port members per port channel
C) 16 Fibre Channel port channels, 4 Fibre Channel port members per port channel
D) 16 Fibre Channel port channels, 8 Fibre Channel port members per port channel

Q15) Which two statements are true about zoning configuration on the fabric interconnects in Fibre Channel switching mode? (Choose two.) (Source: Provisioning SAN Networking)

A) Zoning is configured per fabric interconnect.
B) Zoning is configured in Cisco UCS Manager.
C) Zoning configuration is inherited from an upstream Cisco MDS or Cisco Nexus 5000 switch.
D) Zoning is not needed in Fibre Channel switching mode.
E) Zoning configuration is per-VSAN.

Q16) Which two types of pools can be provisioned in Cisco UCS Manager? (Choose two.) (Source: Provisioning Resource Pools in Cisco UCS Manager)

A) logical resource pools
B) physical resource pools
C) mixed resource pools
D) Fibre Channel resource pools

Q17) What is the Cisco OUI? (Source: Provisioning Resource Pools in Cisco UCS Manager)

A) 00:15:B5
B) 10:05:B5
C) 00:25:B5
D) 00:B5:25

Q18) Which four pool types are logical identity resource pools? (Choose four.) (Source: Provisioning Resource Pools in Cisco UCS Manager)

A) MAC pools
B) WWNN pools
C) OUI pools
D) WWPN pools
E) UUID pools
F) server pools
G) UCS pools
H) local user pools

https://t.me/learningnets

Q19) Which two adapters are supported for iSCSI boot? (Choose two.) (Source: Provisioning Resource Pools in Cisco UCS Manager)

A) QLogic M71KR
B) Broadcom M51KR-B
C) Emulex M71KR
D) Cisco M81KR

Q20) How many iSCSI vNICs are supported per adapter? (Source: Provisioning Resource Pools in Cisco UCS Manager)

A) 2
B) 4
C) 8
D) 16

Q21) In which two modes can the service profile wizard be run? (Choose two.) (Source: Provisioning Server Policies in Cisco UCS Manager)

A) complicated
B) expert
C) professional
D) simple
E) advanced

Q22) What are the identity values that the service profile wizard works with in simple mode? (Source: Provisioning Server Policies in Cisco UCS Manager)

A) pooled
B) statically defined
C) hardware values that are provided by the physical server
D) provided by the DHCP server

Q23) How many burned-in MAC addresses are available on the Cisco M81KR VIC? (Source: Provisioning Server Policies in Cisco UCS Manager)

A) 0
B) 56
C) 116
D) 128

Q24) Which two identity values must be specified in the service profile to support service profile mobility (that is, to be independent from the physical server hardware)? (Choose two.) (Source: Provisioning Server Policies in Cisco UCS Manager)

A) pooled
B) burned-in
C) manually generated
D) vendor-specified

Q25) What must be done before you can create a QoS policy? (Source: Provisioning Server Policies in Cisco UCS Manager)

A) create a service profile
B) enable and configure a QoS system class
C) create a vNIC
D) create a service profile template
E) create a server pool

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Q26) What are the identity values that you can work with when you create a service profile template? (Source: Provisioning Service Profiles from Templates in Cisco UCS Manager)

A) pooled
B) burned-in
C) manually generated
D) DHCP assigned

Q27) Which two types of service profile templates can be provisioned? (Choose two.) (Source: Provisioning Service Profiles from Templates in Cisco UCS Manager)

A) advanced
B) initial
C) simple
D) elementary
E) updating
F) complicated

Q28) Which four operational policies can be used in a service profile? (Choose four.) (Source: Provisioning Service Profiles from Templates in Cisco UCS Manager)

A) scrub
B) IPMI
C) clean
D) BIOS
E) SoL
F) SSH
G) FCIP
H) DHCP

Q29) Which two items must be specified when you generate service profiles from a template? (Choose two.) (Source: Provisioning Service Profiles from Templates in Cisco UCS Manager)

A) name prefix
B) name suffix
C) number of service profiles
D) destination organization

Q30) Which two items must be specified when you clone a service profile or a service profile template? (Choose two.) (Source: Provisioning Service Profiles from Templates in Cisco UCS Manager)

A) number of clones
B) name prefix
C) name
D) destination organization
E) source organization

Q31) Which model of Cisco Nexus 2200 FEXs are needed for C-Series server integration with Cisco UCS? (Source: Provisioning Cisco UCS C-Series Server Integration in Cisco UCS Manager)

A) 2224 FEX
B) 2228 FEX
C) 2232 FEX
D) 2248 FEX

https://t.me/learningnets

Q32) Which three of these are needed for the management connectivity of C-Series servers that are integrated with Cisco UCS? (Choose three.) (Source: Provisioning Cisco UCS C-Series Server Integration in Cisco UCS Manager)

A) Cisco Nexus 2232 FEXs
B) 1-Gb/s RJ-45 cables
C) LOM ports
D) Cisco Catalyst 6509
E) 10-Gb/s SFP cables
F) Cisco ASR9000 routers

Q33) Where are the data ports of the Cisco C-Series servers connected? (Source: Provisioning Cisco UCS C-Series Server Integration in Cisco UCS Manager)

A) server ports on the fabric interconnect
B) uplink ports on the fabric interconnect
C) appliance ports on the fabric interconnect
D) server ports on the Cisco Nexus 2232 FEX

Q34) Which three types of interface adapters can be installed in Cisco C-Series servers for data communication in Cisco UCS? (Choose three.) (Source: Provisioning Cisco UCS C-Series Server Integration in Cisco UCS Manager)

A) VICs
B) Ethernet adapters
C) HBAs
D) CNAs
E) expander cards
F) USB adapter cards

Q35) Which Cisco C-Series firmware version is required for integration with Cisco UCS earlier than 2.0(2xx)? (Source: Provisioning Cisco UCS C-Series Server Integration in Cisco UCS Manager)

A) 1.2
B) 1.3
C) 1.4
D) 2.0

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module Self-Check Answer Key

Q1) B

Q2) A, B

Q3) C

Q4) A, C

Q5) A, B, D

Q6) A, B, C

Q7) C

Q8) B

Q9) C

Q10) A

Q11) B

Q12) A, C

Q13) C

Q14) A

Q15) C, E

Q16) A, B

Q17) C

Q18) A, B, D, E

Q19) B, D

Q20) A

Q21) B, D

Q22) C

Q23) A

Q24) A, C

Q25) B

Q26) A

Q27) B, E

Q28) A, B, D, E

Q29) A, C

Q30) C, D

Q31) C

Q32) A, B, C

Q33) D

Q34) A, B, D

Q35) A

https://t.me/learningnets

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module 5

Implement Cisco UCS Server Virtualization Features

Overview

Cisco Unified Computing System (UCS) provides the infrastructure for applications in the data center and extensive support for virtualizing operating systems, such as VMware vSphere, Microsoft Hyper-V, and Citrix Xen. In addition to support for the flexible management of hardware, Cisco UCS offers extended support for connectivity up to the level of the virtual machines. This module describes the unique features of the Cisco UCS Virtual Machine Fabric Extender (VM-FEX) and Cisco VM-FEX universal pass-through mode features.

Module Objectives

Upon completing this module, you will be able to implement virtualization features unique to Cisco UCS that improve performance and manageability. This ability includes being able to meet these objectives:

- Describe Cisco VM-FEX and Cisco VM-FEX universal pass-through mode
- Provision Cisco VM-FEX
- Provision Cisco VM-FEX universal pass-through

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 1

Provisioning Cisco VM-FEX and Cisco VM-FEX Universal Pass-Through

Overview

The implementation of virtualization technologies created a new network layer in the data center—the virtual access network layer. Initially, network administrators did not have access to or control of virtual machine (VM) networking. Now, Cisco technologies and products, such as the Cisco Nexus 1000V software switch, have put networking back into the hands of network teams. Additionally, the Cisco Unified Computing System (UCS) supports direct provisioning of VM networking by using Cisco virtual interface cards (VICs). This technology is called the Cisco Virtual Machine Fabric Extender (VM-FEX). In this lesson, this technology will be described, as well as the two supported modes of operation—standard and universal pass-through.

Objectives

Upon completing this lesson, you will be able to describe Cisco VM-FEX and Cisco VM-FEX universal pass-through mode. This ability includes being able to meet these objectives:

- Describe VMware vSwitch and vDS
- Describe Cisco Nexus 1000V switching
- Describe Cisco VM-FEX
- Describe Cisco VM-FEX universal pass-through

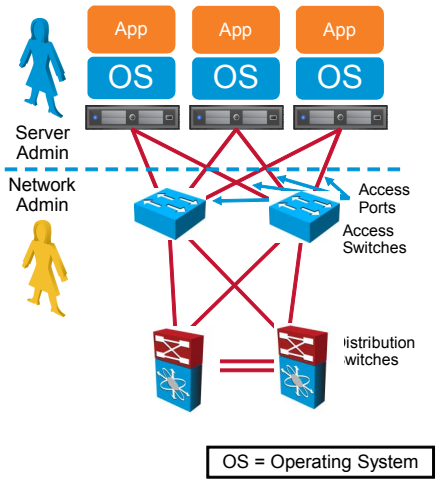
https://t.me/learningnets

VMware vSwitch and vDS

This topic describes switching in VMware ESX/ESXi.

Evolution of Virtual Networking: Before Virtualization

- One-to-one ratio between servers, operating system, or application and network port
- Physical servers connected into the network via access ports (single VLAN)
- Each host, operating system, or application with its own network policy controlled by the network admin
- Clear demarcation between server admin and network admin roles and responsibilities



© 2012 Cisco and/or its affiliates. All rights reserved.

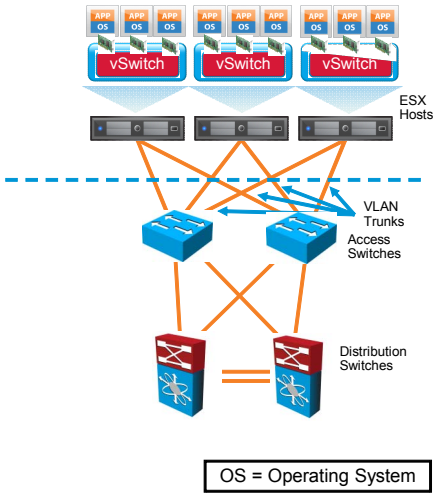
Before virtualization, each server ran its own operating system, usually with a single application running in addition to the operating system. Network interface cards (NICs) were connected to physical access layer switches to provide redundancy. Network security, quality of service (QoS), and management policies were created on these access layer switches and applied to the access ports that corresponded to the appropriate server.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

VMware vSwitch

- Layer 2 switches become embedded within the ESX hypervisor to switch packets between virtual servers (VMs) and the outside world (vSwitch).
- Multiple VMs are required to share the same physical uplinks (VM NICs) to the network, as well as the same network policy.
- VM vNICs connected to vSwitch.
- vSwitch performs local switching.
- Segmentation between VMs is provided by 802.1Q VLANs using port groups.
- One or more vSwitches per ESX/ESXi host.



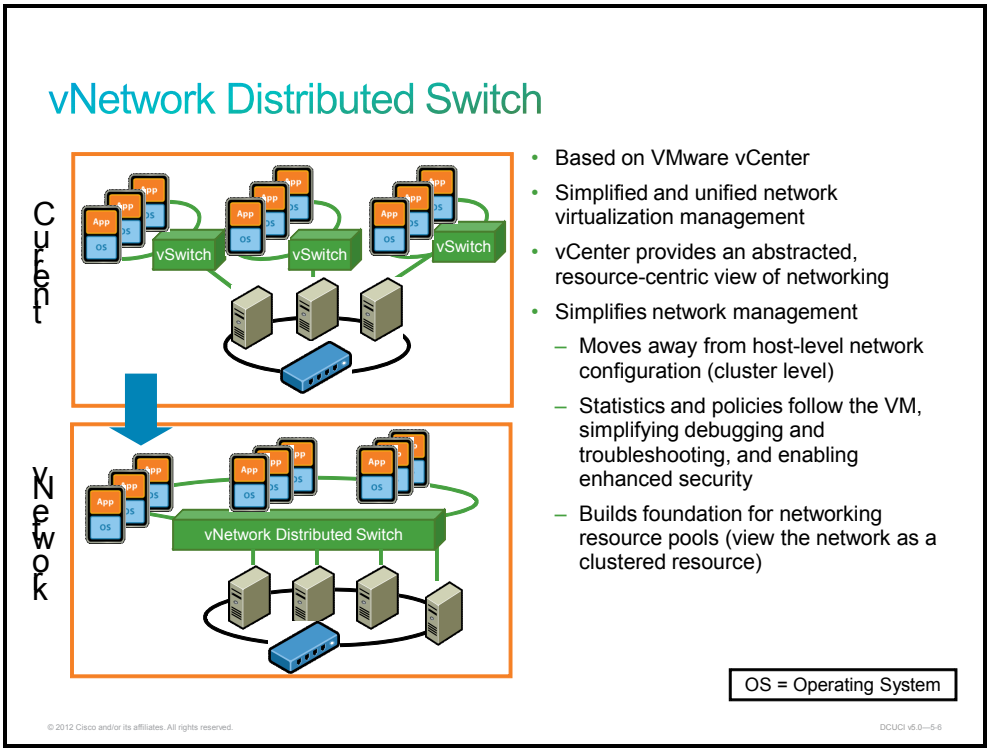
© 2012 Cisco and/or its affiliates. All rights reserved.

The VMware server-virtualization solution extends the access layer into the VMware ESX server by using the VM networking layer. Several components are used to implement server-virtualization networking:

- **Physical networks:** Physical devices connect ESX hosts for resource sharing. Physical Ethernet switches are used to manage traffic between ESX hosts, like in a regular LAN environment.
- **Virtual networks:** Virtual networks include devices that run on the same system for resource sharing.
- **Virtual Ethernet switch (vSwitch):** Like a physical switch, the vSwitch maintains a table of connected devices. This table is used for frame forwarding. The vSwitch can be connected, via uplink, to a physical switch by using a physical VM NIC. The vSwitch does not provide the advanced features of a physical switch.
- **Port group:** A port group is a subset of ports on a vSwitch for VM connectivity.
- **Physical NIC (VM NIC):** The VM NIC is used to uplink the ESX host to the external network.

The vSwitch is a software switch, which means that VM traffic processing is performed in software. The vSwitch is created per ESX host and one or more vSwitches can exist on one ESX host.

https://t.me/learningnets

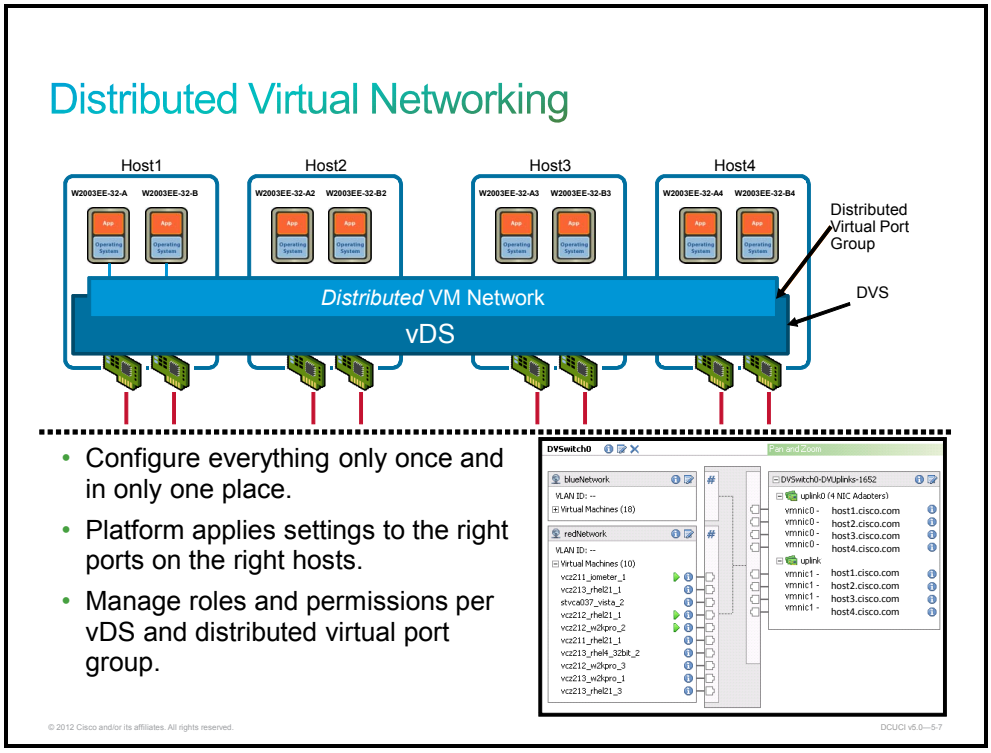


VMware vSphere 4 introduced the VMware vNetwork Distributed Switch (vDS)—a distributed virtual switch (DVS). With vDS, multiple vSwitches within an ESX cluster can be configured from a central point. The vDS automatically applies changes to the individual vSwitches on each ESX host.

The feature is licensed and relies on the VMware vCenter Server. The vDS cannot be used for individually managed hosts.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

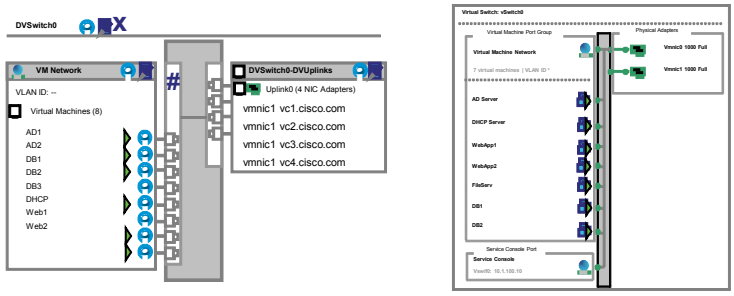


The vDS adds functionality and simplified management to the VMware network. The vDS adds the ability to use private VLANs (PVLANs), perform inbound rate limiting, and track VM port state with migrations. Additionally, the vDS is a single point of network management for VMware networks, which allows for the support of features like VMware VMotion.

https://t.me/learningnets

vSwitch and vDS

- VMware vDS and vSwitch are not mutually exclusive.
  - Physical NIC ports are assigned to either a vSwitch or vDS.
  - Separate ports can be assigned to a vSwitch and vDS on the same VMware ESX host.



© 2012 Cisco and/or its affiliates. All rights reserved.

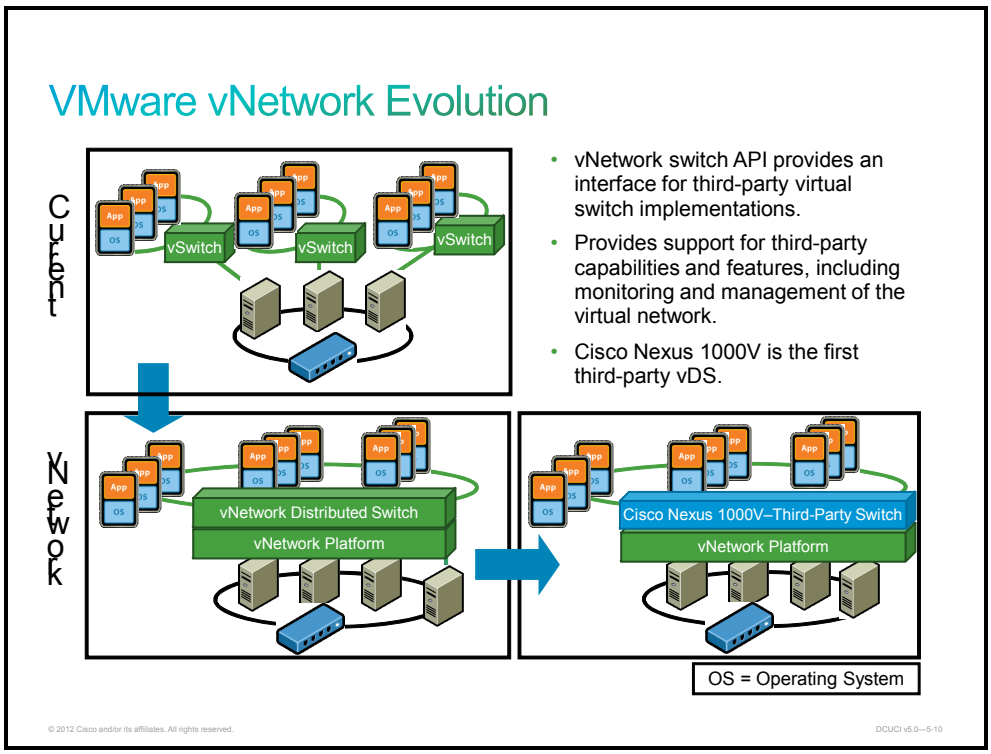
The VMware vSwitch and vDS are not mutually exclusive and can coexist within the same VMware vCenter management environment. Physical VM NICs may be assigned to either the vSwitch or the vDS on the same VMware ESX or ESXi host.

You can also migrate the ESX service console and VMware VMkernel ports from the vSwitch, where they are assigned by default during ESX installation, to the vDS. This migration facilitates a single point of management for all virtual networking within the vCenter data center object.

https://t.me/learningnets

Cisco Nexus 1000V Switching

This topic describes Cisco Nexus 1000V switching.



The Cisco server virtualization solution uses technology that was jointly developed by Cisco and VMware. The network access layer is moved into the virtual environment to provide enhanced network functionality at the VM level.

This solution can be deployed as a hardware- or software-based solution, depending on the data center design and demands. Both deployment scenarios offer VM visibility, policy-based VM connectivity, policy mobility, and a nondisruptive operational model.

Cisco Nexus 1000V

The Cisco Nexus 1000V is a software-based solution that provides VM-level network configurability and management. The Cisco Nexus 1000V solution works with any upstream switching system to provide standard networking controls to the virtual environment.

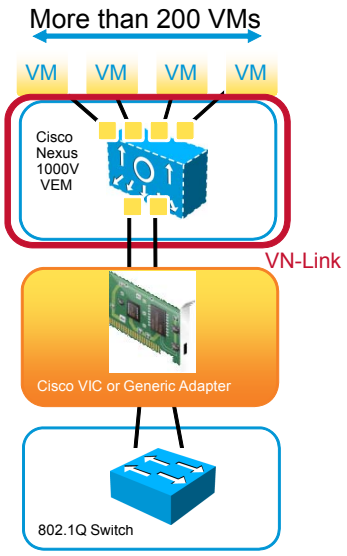
VN-Link

Cisco Virtual Network Link (VN-Link) technology was jointly developed by Cisco and VMware and has been proposed to the IEEE for standardization. The technology is designed to move the network access layer into the virtual environment to provide enhanced network functionality at the VM level.

https://t.me/learningnets

VN-Link Deployment: Cisco Nexus 1000V

- Cisco Nexus 1000V
  - Performs packet forwarding and applies advanced networking features
  - Uses port security, VLAN, and ACLs, policy maps for QoS treatment for VM traffic, console and VMotion or VMkernel
- Generic adapter on generic x86 server, or Cisco VIC (recommended)
- Generic upstream switch



© 2012 Cisco and/or its affiliates. All rights reserved.

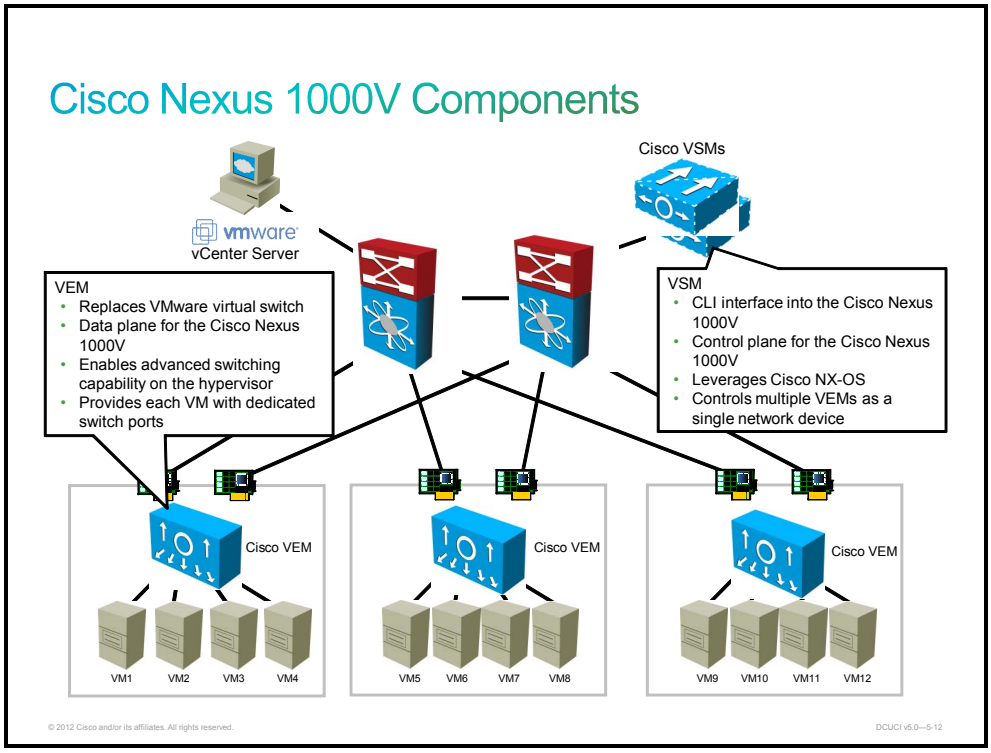
The Cisco Nexus 1000V was developed with VMware to deliver transparency to various server hardware platforms. The Cisco Nexus 1000V may be used with generic NICs on generic x86-based servers or with Cisco VICs. In addition, the upstream physical access layer switch can also be generic.

This generic support enables the Cisco Nexus 1000V to be installed and configured within existing architectures, minimizing disruption and maximizing functionality.

The following features are supported with Cisco Nexus 1000V:

- Layer 2 VLAN, PVLAN, port channels, Internet Group Management Protocol (IGMP) snooping, jumbo frame support
- QoS classification and marking, traffic policing
- Ingress and egress access control lists (ACLs), Layer 2 ACLs, port ACLs, IP Source Guard, port security, Dynamic Address Resolution Protocol (ARP) Inspection, DHCP snooping
- NetFlow

https://t.me/learningnets



The Cisco Nexus 1000V provides Layer 2 switching functions in a virtualized server environment. The Cisco Nexus 1000V DVS replaces virtual switches within the ESX servers. This replacement allows users to configure and monitor the virtual switch by using the Cisco Nexus Operating System (NX-OS) CLI. Cisco Nexus 1000V also provides visibility into the networking components of the ESX servers and access to the virtual switches within the network.

The vCenter server defines the data center that the Cisco Nexus 1000V will manage. Each server is represented as a line card and is managed as if it were a line card in a physical Cisco switch.

Two components are part of the Cisco Nexus 1000V implementation:

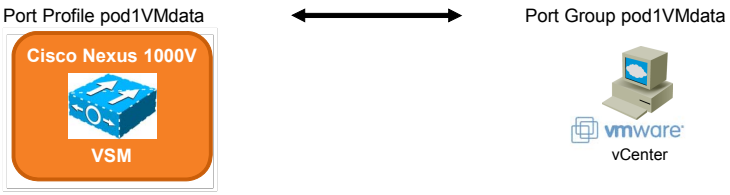
- **Cisco Nexus 1000V Virtual Supervisor Module (VSM):** The Cisco Nexus 1000V VSM is the control software of the Cisco Nexus 1000V DVS. The VSM runs either on a VM or as an appliance, and is based on Cisco NX-OS.
- **Cisco Nexus 1000V Virtual Ethernet Module (VEM):** The Cisco Nexus 1000V VEM actually switches the data traffic and runs on a VMware ESX 4.0 host or later. VSM can control several VEMs, with the VEMs forming a switch domain that should be in the same virtual data center that is defined by VMware vCenter.

https://t.me/learningnets

Cisco Nexus 1000V Port Profiles and VMware Port Groups

- Port profiles correspond to port groups within VMware.
- By default, the port group created within VMware for each port profile will have the same name.
- VMware administrators use the port group to assign network settings to VMs and uplink ports.

```
VSM-1(config)# port-profile type vEthernet pod1VMdata
VSM-1(config-port-prof)# switchport mode access
VSM-1(config-port-prof)# switchport access vlan 102
VSM-1(config-port-prof)# vmware port-group pod1VMdata
VSM-1(config-port-prof)# no shut
VSM-1(config-port-prof)# state enabled
```



© 2012 Cisco and/or its affiliates. All rights reserved.

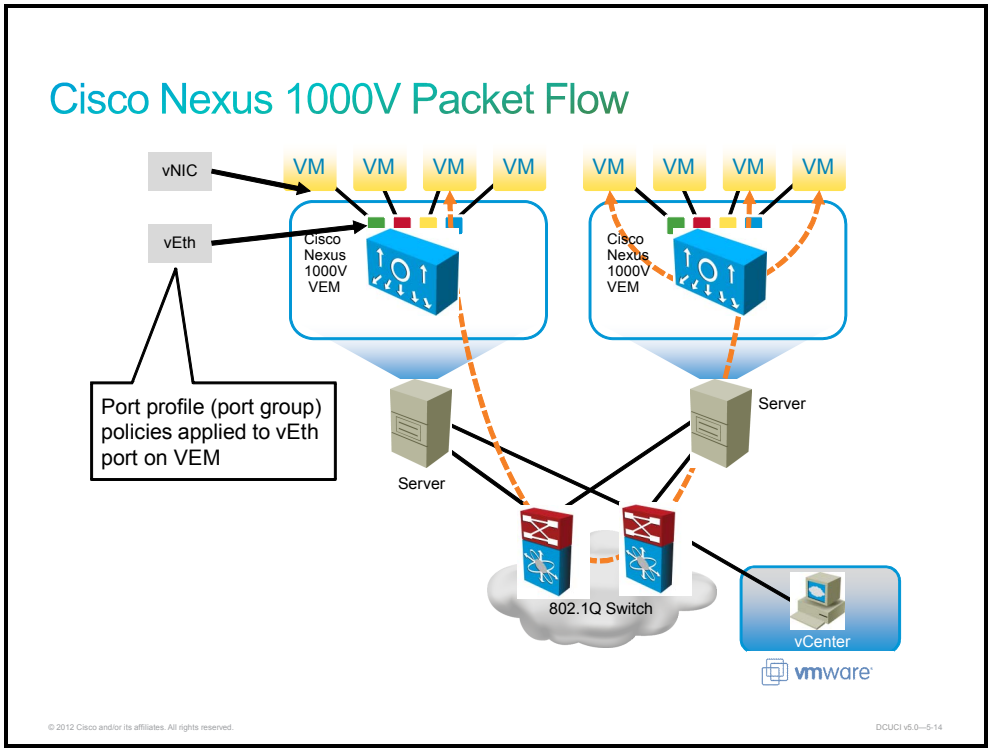
When you work with VMware vSwitch or vDS, the network configuration is applied to the VMs by using port profiles. When you work with Cisco Nexus 1000V, all the configuration is performed on the Cisco Nexus 1000V VSM. This configuration must be communicated to the VMware vCenter, where a port group must be created, because the VM must be linked to a port group. For this reason, there is integration between vCenter Server and the VSM.

In the Cisco Nexus 1000V VSM, you create port profiles that contain the configuration and the policies for the VMs.

When a port profile is created and enabled, a corresponding port group is created in VMware. By default, this port group has the same name as the profile, but this name is configurable. VMware administrators use the port profile to assign network settings to VMs and uplink ports. When a VMware ESX host port (a physical VM NIC) is added to a DVS that is controlled by the Cisco Nexus 1000V switch, an available uplink port group is assigned and those settings are applied. When a NIC is added to a VM, an available VM port group is assigned and the network settings that are associated with that profile are inherited.

A NIC in VMware is represented by a VM NIC interface. The VM NIC number is allocated during VMware installation.

https://t.me/learningnets



The Cisco Nexus 1000V is similar to physical Ethernet switches. For packet forwarding, the Cisco Nexus 1000V uses the same techniques that other Ethernet switches apply, keeping a MAC address-to-port mapping table that is used to determine where packets should be forwarded. The Cisco Nexus 1000V maintains forwarding tables in a slightly different manner than other modular switches. Unlike physical switches with a centralized forwarding engine, each VEM maintains a separate forwarding table. No synchronization exists between forwarding tables on different VEMs. In addition, there is no concept of forwarding from a port on one VEM to a port on another VEM. Packets that are destined for a device that is not local to a VEM are forwarded to the external network, which in turn may forward the packets to a different VEM.

https://t.me/learningnets

Virtual Switch Options

Virtual Switch	Model	Details
vSwitch	Host based: 1 or more per ESX host	• Same as vSwitch in ESX 3.5

vDS	Distributed:
	1 or more per data center
		• Requires VMware vCenter
		• Expanded feature set
		  - PVLANs
		  - Bidirectional traffic shaping
		  - Network VMotion
		• Simplified management

Cisco Nexus 1000V	Distributed: 1 or more per data center	• Requires VMware vCenter • CLI similar to Cisco IOS CLI • Same remote management as Cisco Nexus physical switches • Different feature set compared to Cisco Nexus physical switches

Virtual networking concepts are similar with all virtual switch alternatives.

© 2012 Cisco and/or its affiliates. All rights reserved.

With the introduction of vSphere 4, VMware customers enjoy the benefits of three virtual networking solutions: vSwitch, vDS, and Cisco Nexus 1000V.

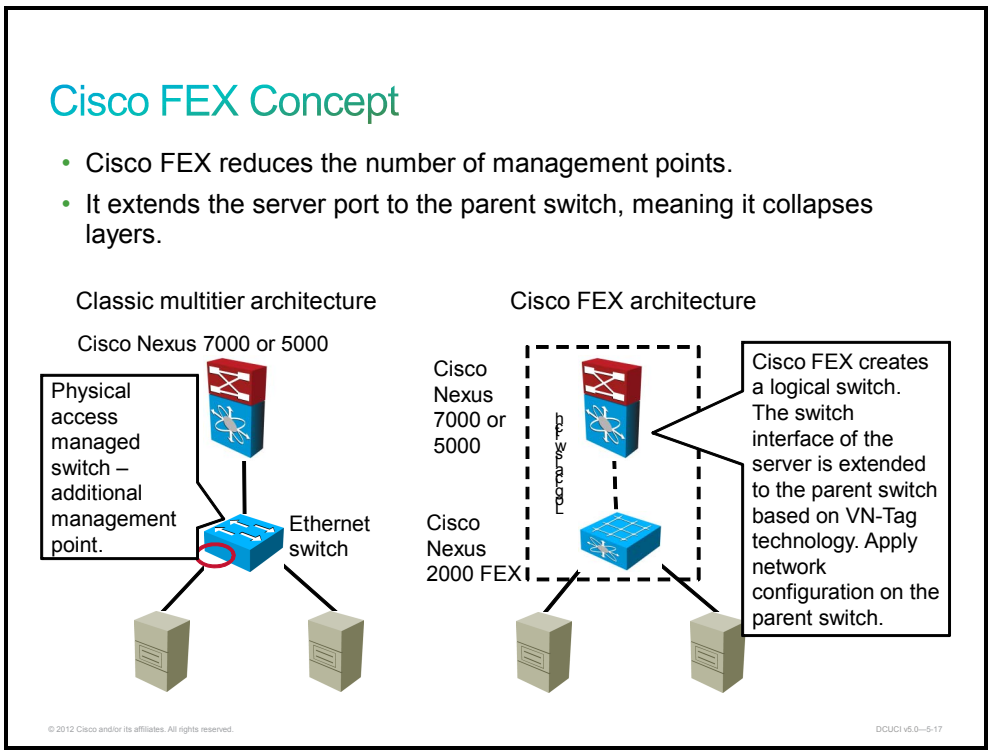
The Cisco Nexus 1000V bypasses the VMware vSwitch with a Cisco software switch. This model provides a single point of configuration for the networking environment of multiple ESX hosts. Additional functionality includes policy-based connectivity for the VMs, network security mobility, and a nondisruptive software model.

VM connection policies are defined in the network and applied to individual VMs from within vCenter. These policies are linked to the universally unique ID (UUID) of the VM and are not based on physical or virtual ports.

https://t.me/learningnets

Cisco VM-FEX

This topic describes the Cisco VM-FEX technology.

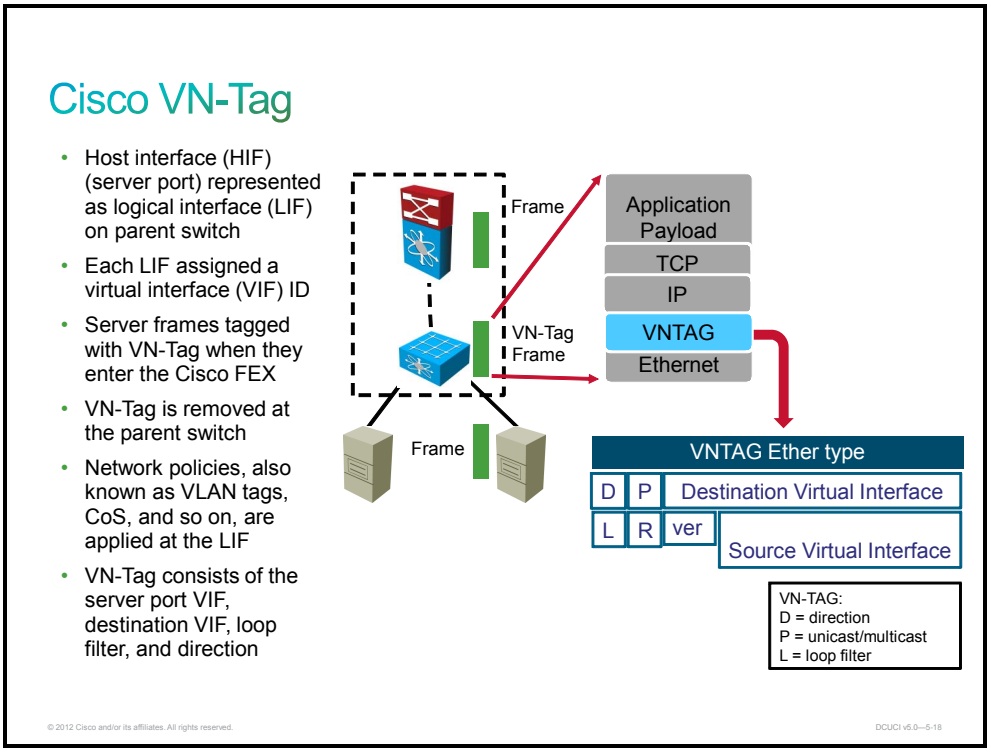


Cisco FEX technology was introduced along with Cisco Nexus switches and Cisco UCS.

In a classic data center, there are distinct access, aggregation, and core network layers. Each layer consists of switches that must be managed.

With Cisco FEX technology, which is based on the Cisco virtual networking tag (VN-Tag), you can collapse network layers. This ability means that the access switches are replaced by unmanaged devices, fabric extenders such as the Cisco Nexus 2000 or the Cisco UCS I/O module (IOM) and Cisco VICs, and the server port is extended up to the first managed device. This function allows all the configurations for the server port to be performed on the parent switch and thus you have physical devices forming the access layer, but you manage only the devices from the upper layer.

https://t.me/learningnets



The Cisco FEX is an unmanaged device to which the server is connected. You use a parent switch on which the Cisco FEX is installed. You provision the network configuration for the server from the parent switch. The parent switch must have a way to access, control, and apply configuration to the fabric extender. This configuration is achieved by using VN-Tag technology.

With VN-Tag, each port to which a server is connected on the fabric extender is called a host interface (HIF). The HIF is represented on the parent switch as a logical interface (LIF). Each LIF is identified by a virtual interface (VIF) ID. With the VIFs, each HIF is represented on the parent switch. The HIF can be managed directly at the parent switch.

Because network policies and configuration of the server traffic are applied to the LIF on the parent switch, there must also be a way to identify traffic from and to multiple servers connected to the HIF on the Cisco FEX. The VN-Tag, an additional tag in the Ethernet frame, is used for this identification. The tag is applied on the HIF of the Cisco FEX when the frame of the server enters, and the tag is stripped away on the parent switch. This process is an internal process between the Cisco FEX and the parent switch.

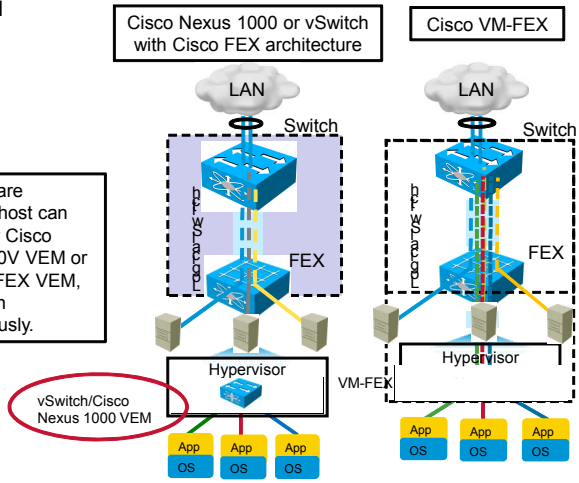
VN-Tag technology allows remote, unmanaged interfaces to be visible and managed on a parent device. Also, this technology allows segmentation of traffic from different servers that are connected in this manner.

© 2012 Cisco Systems, Inc.
https://t.me/learningnets

Cisco VM-FEX

- Extends Cisco FEX up to the level of the VMs
- Collapses physical access and virtual access layers in physical aggregation layer
- Needs Cisco VIC
- No Nexus 1000V or vSwitch
- Supports VMotion

Each VMware ESX/ESXi host can have either Cisco Nexus 1000V VEM or Cisco VM-FEX VEM, but not both simultaneously.



© 2012 Cisco and/or its affiliates. All rights reserved.

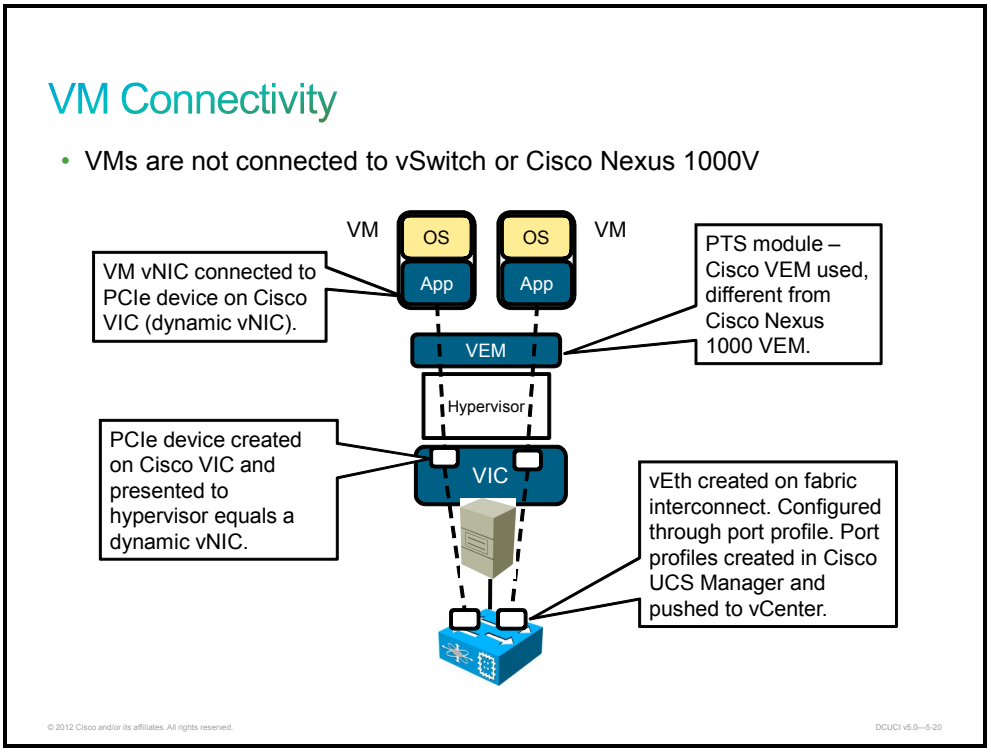
The Cisco VM-FEX extends the Cisco FEX up to the level of the VMs. This extension allows you to collapse both the virtual access network layer and the physical access network layer in the aggregation network layer.

The Cisco FEX is the Cisco VIC. The VM vNICs are connected to the Peripheral Component Interconnect Express (PCIe) devices that are created in the Cisco VIC dynamic vNICs. The VN-Tag is used between the dynamic vNICs and the fabric interconnects, on which LIFs are created, called virtual Ethernet (vEth) interfaces.

With Cisco VM-FEX, there is no software switch. Switching is performed on the Cisco UCS fabric interconnects.

Because there is not a Cisco Nexus 1000V VSM, the network configuration is created on Cisco UCS Manager.

https://t.me/learningnets



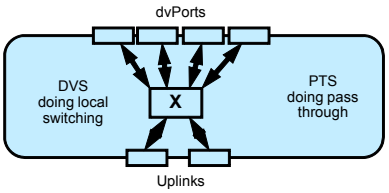
There are two Cisco VM-FEX modes—standard and universal pass-through. Universal pass-through mode is discussed later in this lesson.

In standard mode, the VM vNIC is linked to a port group. This port group is created as a port profile in Cisco UCS Manager and is communicated to vCenter. When the VM vNIC is connected to such a port group, the vNIC is linked through the Cisco VM-FEX VEM module, which is called a pass-through switch, to a PCIe device that is created on the Cisco VIC. This PCIe device is called a dynamic vNIC. On the Cisco VIC, you can create static vNICs, virtual host bus adapters (vHBAs), and dynamic vNICs. The dynamic vNIC is identified by a VIF and appears on the fabric interconnect as a vEth. The port profile configuration is applied on the vEth.

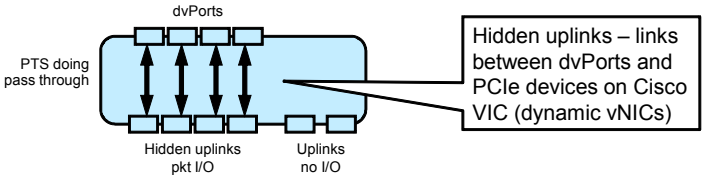
© 2012 Cisco Systems, Inc.
https://t.me/learningnets

vCenter View

- vCenter view:
  - Each VM is connected to a hypervisor network interface (dvPort).



- Cisco VM-FEX view:



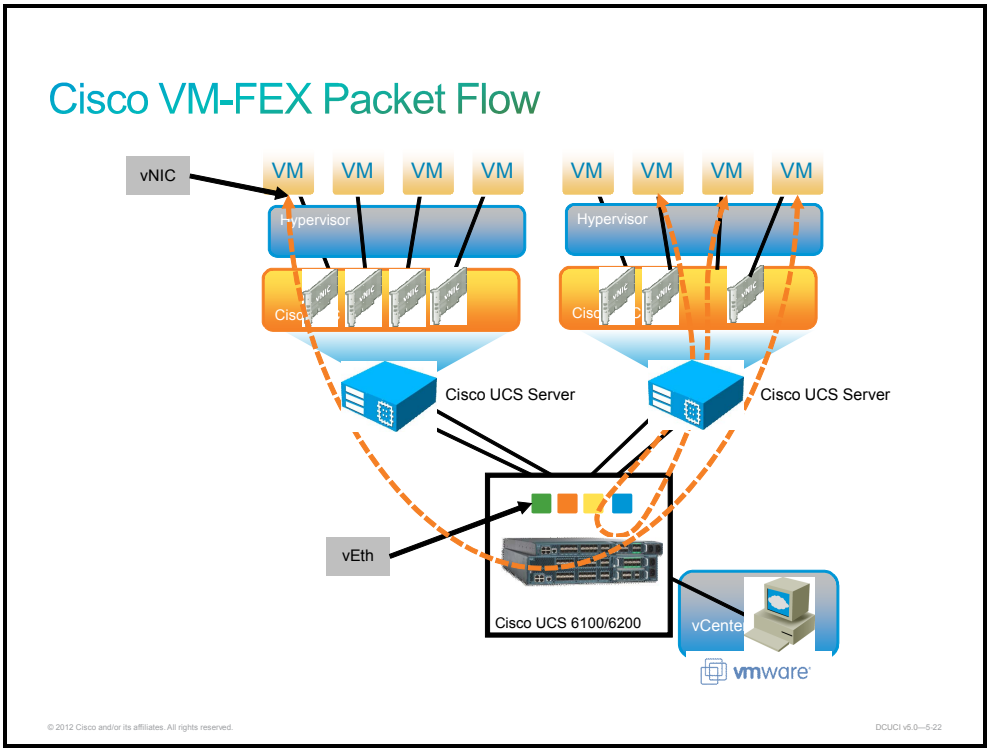
© 2012 Cisco and/or its affiliates. All rights reserved.

This type of connectivity is seen differently by the vCenter and Cisco UCS.

The vCenter sees only the ports on the Cisco VM-FEX VEM to which VM vNICs are connected. These ports are identified as distributed virtual ports (dvPorts) or hypervisor network ports. The vCenter does not see the dynamic vNICs on the Cisco VIC.

Actually, each dynamic vNIC communicates through the physical DCE interfaces with the fabric interconnects. These uplinks are hidden from the vCenter. Each DVPort is connected to one dynamic vNIC through the pass-through switch module. The VM data communication goes only through the hidden uplinks. The static vNICs are not used for VM data communication.

https://t.me/learningnets

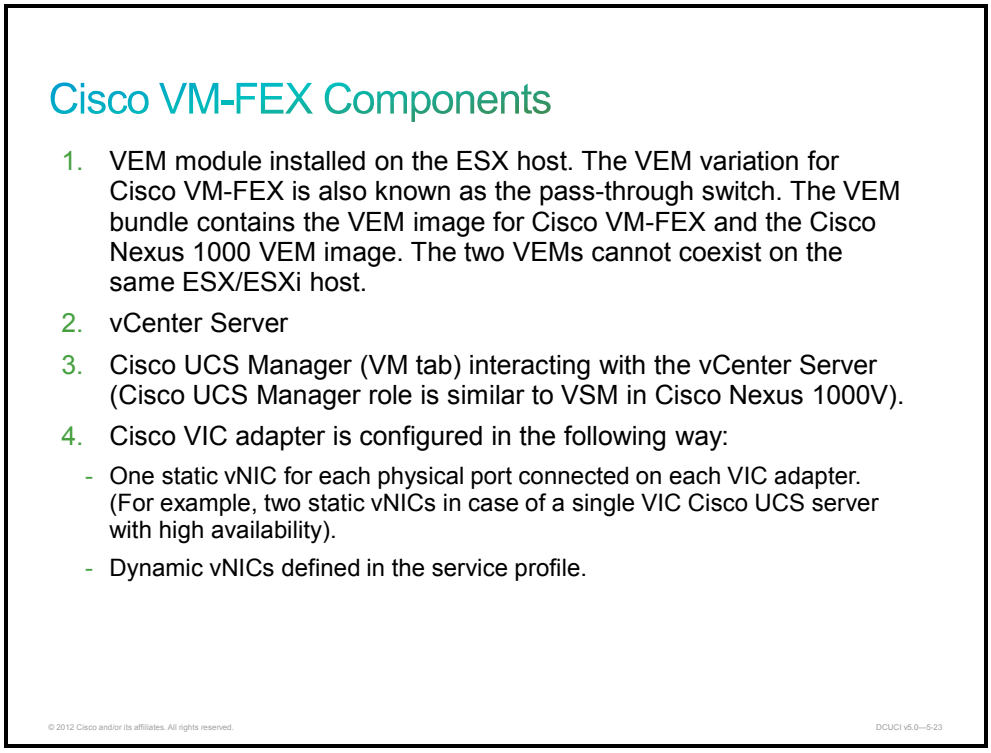


As the port profile configuration is applied on the vEth interface for each VM on the fabric interconnect. Because the VM Ethernet frames go between the VM through the Cisco VIC and up to the fabric interconnect only carrying the VN-Tag, all processing is performed on the fabric interconnects.

The communication between a VM and any other VM or server is processed on the fabric interconnect. This process means that there is no local switching with the Cisco VM-FEX, even for communication between two VMs on the same ESX/ESXi host.

Because traffic is processed in hardware, and there is no forwarding decision that is made by a software switch, the performance is much higher.

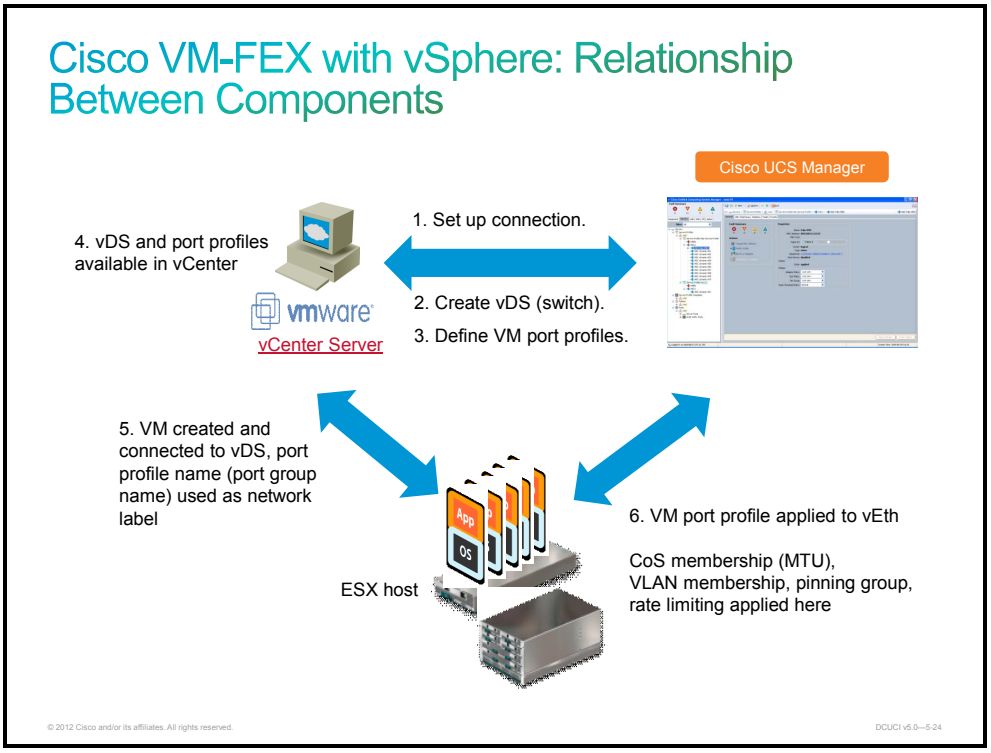
© 2012 Cisco Systems, Inc.
https://t.me/learningnets



The following are Cisco VM-FEX components:

- **The VEM module that is installed on the ESX host:** The VEM variation for Cisco VM-FEX is also known as a pass-through switch. The VEM bundle contains the VEM image for Cisco VM-FEX and the Cisco Nexus 1000 VEM image. Two VEMs cannot coexist on the same ESX/ESXi host. When dynamic vNICs are used, the VEM operates in Cisco VM-FEX mode. When there are no dynamic vNICs, the VEM will operate in Cisco Nexus 1000V mode.
- **vCenter Server:** There is a close integration between vCenter and Cisco UCS Manager. The network configuration for VMs is created as port profiles on Cisco UCS Manager. These port profiles are communicated to the vCenter where the vCenter Server converts them to port groups. After that, the VM vNICs can be linked to the appropriate port group. Also, when communication between vCenter and Cisco UCS Manager is created, a DVS is created in vCenter Server.
- Cisco UCS Manager (VM tab): Cisco UCS Manager interacts with vCenter Server. (The Cisco UCS Manager role is similar to VSM in Cisco Nexus 1000V.)
- Cisco VIC adapter: This adapter is configured in the following way:
  - One static vNIC for each physical port that is connected on each VIC adapter (for example, two static vNICs in a single VIC Cisco UCS server with high availability)
  - Dynamic vNICs defined in the service profile

https://t.me/learningnets



These are the relationships and the sequence for the Cisco VM-FEX components:

Step 1 Cisco UCS Manager creates a connection with vCenter Server.

Step 2 Cisco UCS Manager creates a DVS or multiple DVSs (up to eight).

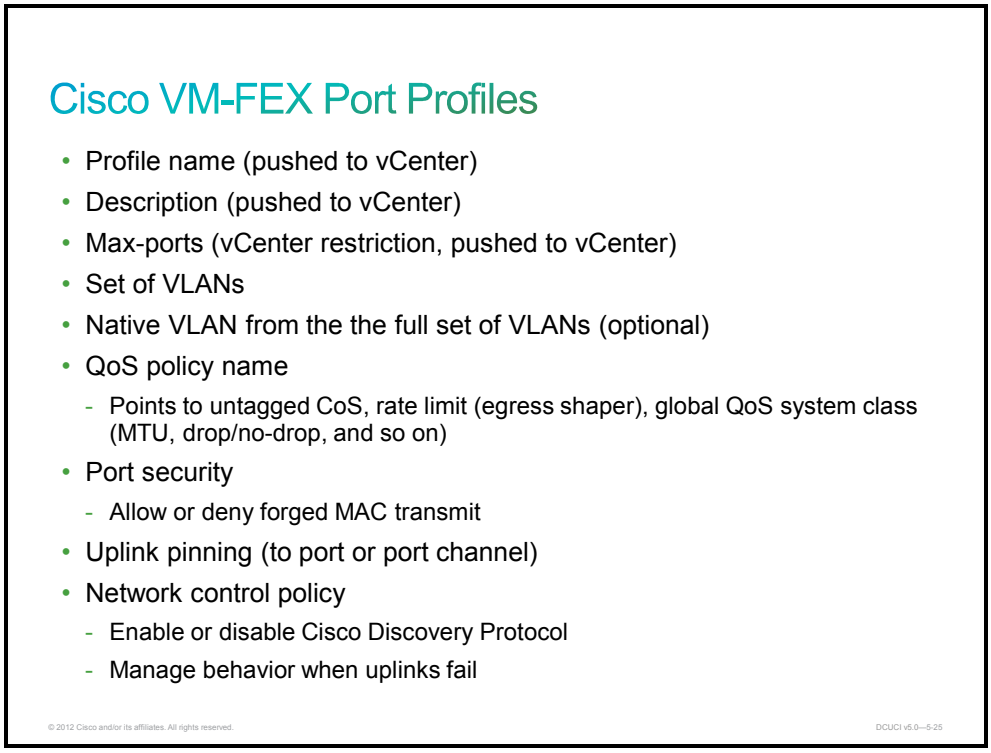
Step 3 Cisco UCS Manager creates VM port profiles.

Step 4 Cisco UCS DVS and VM port profiles are pushed to the vCenter Server. Cisco UCS DVS and VM port groups appear in vCenter server.

Step 5 In vCenter, VMs are created and linked to VM port groups from the Cisco UCS DVS. Thus the VM vNIC is connected to a dynamic vNIC on the Cisco VIC.

Step 6 Cisco UCS Manager creates the vEth on the fabric interconnect and port profile configuration is applied on it.

© 2012 Cisco Systems, Inc.
https://t.me/learningnets



The following are port profiles that are created in Cisco UCS Manager:

- Profile name (pushed to vCenter)
- Description (pushed to vCenter)
- Max-ports (vCenter restriction, pushed to vCenter)
- Set of VLANs
- Native VLAN from the full set of VLANs (optional)
- QoS policy name
- Points to untagged class of service (CoS), rate limit (egress shaper), global QoS system class (maximum transmission unit [MTU], drop/no-drop, and so on)
- Port security
- Allow or deny forged MAC transmit
- Uplink pinning (to port or port channel)
- Network control policy
- Enable or disable Cisco Discovery Protocol
- Manage behavior when uplinks fail

https://t.me/learningnets

Advantages of VM-FEX

- VMotion supported
- Network management domain separation from server or VM (vCenter) management domain (thanks to port profiles)
- Fine-grained control of VM interface configuration enforced fabricwide (VLAN membership, MAC security, QoS, rate limiting, and so on)
  - Precise traffic scheduling and shaping
- VM direct path mode for high performance available within the Cisco VM-FEX operational model
- Higher scalability of networking workloads
- Cisco VM-FEX supported also on Red Hat KVM

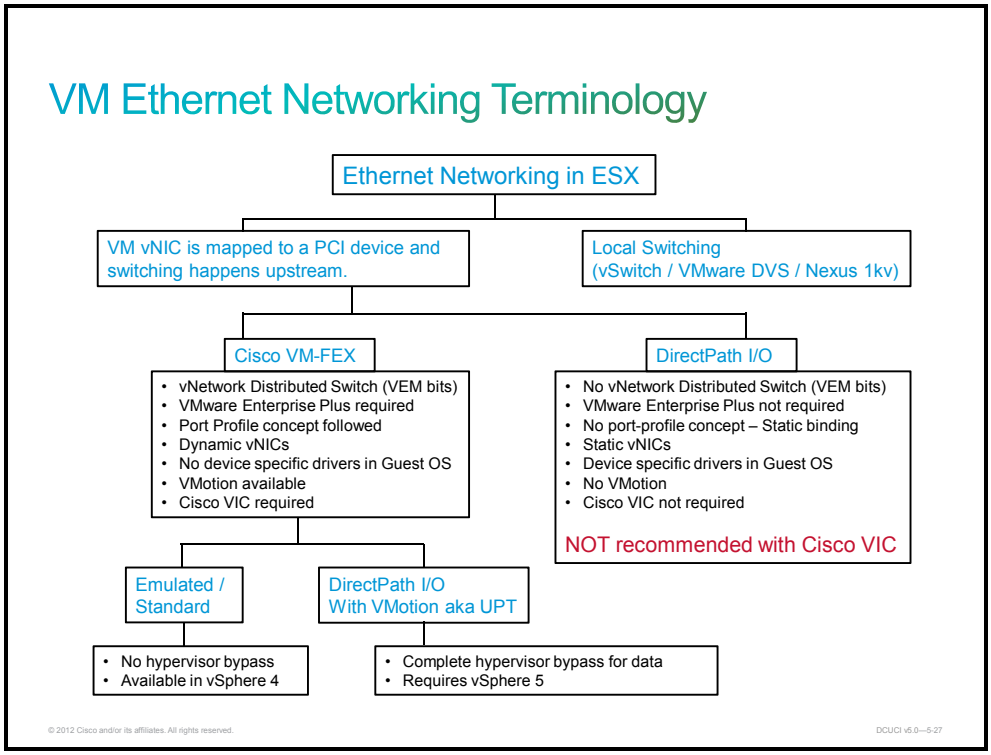
© 2012 Cisco and/or its affiliates. All rights reserved.

The VM-FEX software extends Cisco fabric extender technology to the virtual machine with the following capabilities:

- **Separation of administrative domains:** Network configuration for VMs is performed on Cisco UCS Manager by the network team. Each virtual machine includes a dedicated interface on the parent switch.
- **Better control on the VM interface configuration:** The vEth interface for the VM vNIC is created and configured on the fabric interconnect. All virtual machine traffic is sent directly to the dedicated interface on the switch.
- **Cisco VM-FEX allows for better performance, as the VM traffic processing in software is limited:** In universal pass-through mode, performance is much better as the VM traffic is processed only in hardware. The software-based switch in the hypervisor is eliminated.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



There are distinctions between all these technologies in the virtual access network layer:

- Software switches: vSwitch, VDS, Cisco Nexus 1000V (support for local switching)
- VM vNICs mapping to PCIe devices in the hardware:
  - Cisco VM-FEX
    - Pass-through switch emulated mode, usage of a pass-through switch module, support for VMotion
    - Universal pass-through mode: DirectPath I/O with VMotion
  - DirectPath I/O is not a Cisco technology and does not support VMotion. It is not recommended for use with the Cisco VIC.

https://t.me/learningnets

Cisco VM-FEX Universal Pass-Through

This topic describes Cisco VM-FEX universal pass-through mode.

Cisco VM-FEX Universal Pass-Through Overview

- Cisco VM-FEX universal pass-through is a mode of a VM vNIC attached to Cisco UCS with Cisco VM-FEX.
- VM vNIC attached to a Cisco VM-FEX can either be in standard mode or universal pass-through mode.
  - In standard mode, data traffic from VM vNIC goes through ESX before reaching the hardware.
  - In universal pass-through mode, data traffic from VM vNIC goes directly to hardware.
- Other names for universal pass-through are DirectPath I/O with VMotion (VMware official name), CiscoVM-FEX high-performance mode, and DirectPath I/O Gen 2 (in some older documents).
- Cisco VM-FEX universal pass-through is a successor to fixed pass-through, which is also known as DirectPath I/O. Fixed pass-through does not support VMotion.

© 2012 Cisco and/or its affiliates. All rights reserved.

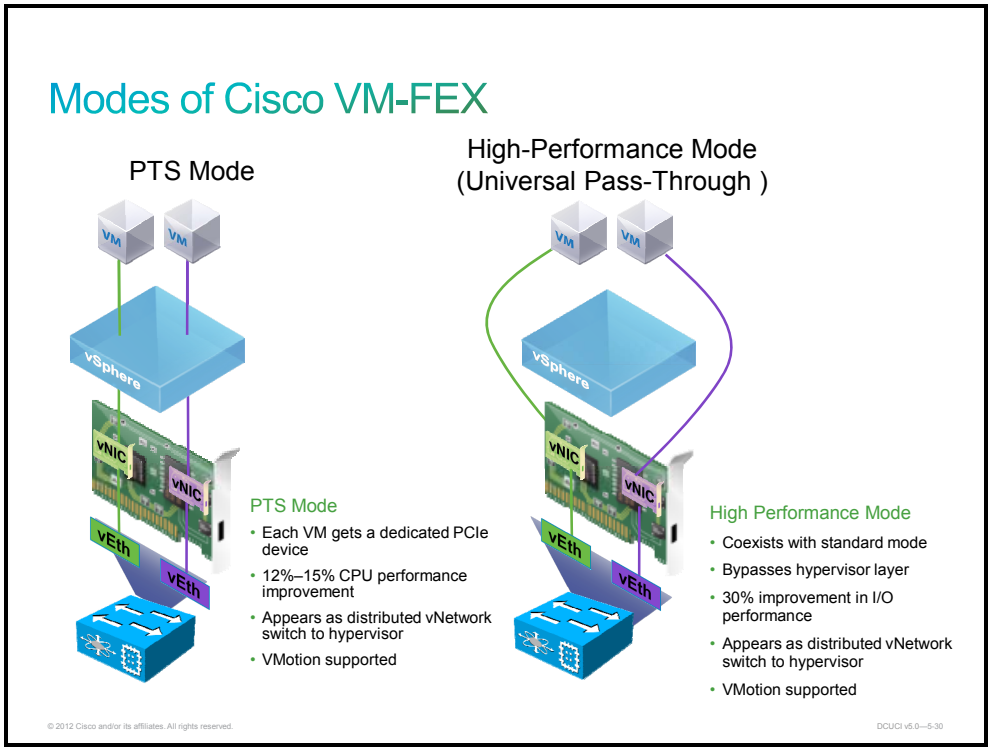
Cisco VM-FEX operates in two modes:

- **Standard:** The VM vNIC is connected to a dynamic vNIC on the Cisco VIC through the pass-through switch module.
- **Universal pass-through:** The VM vNIC is directly connected to a dynamic vNIC, and bypasses the hypervisor.

Other names for universal pass-through are DirectPath I/O with VMotion (the official VMware name), Cisco VM-FEX High Performance Mode, and DirectPath I/O Gen 2 (in some older documents). Universal pass-through is a successor to fixed pass-through, also known as DirectPath I/O. Fixed pass-through does not support VMotion.

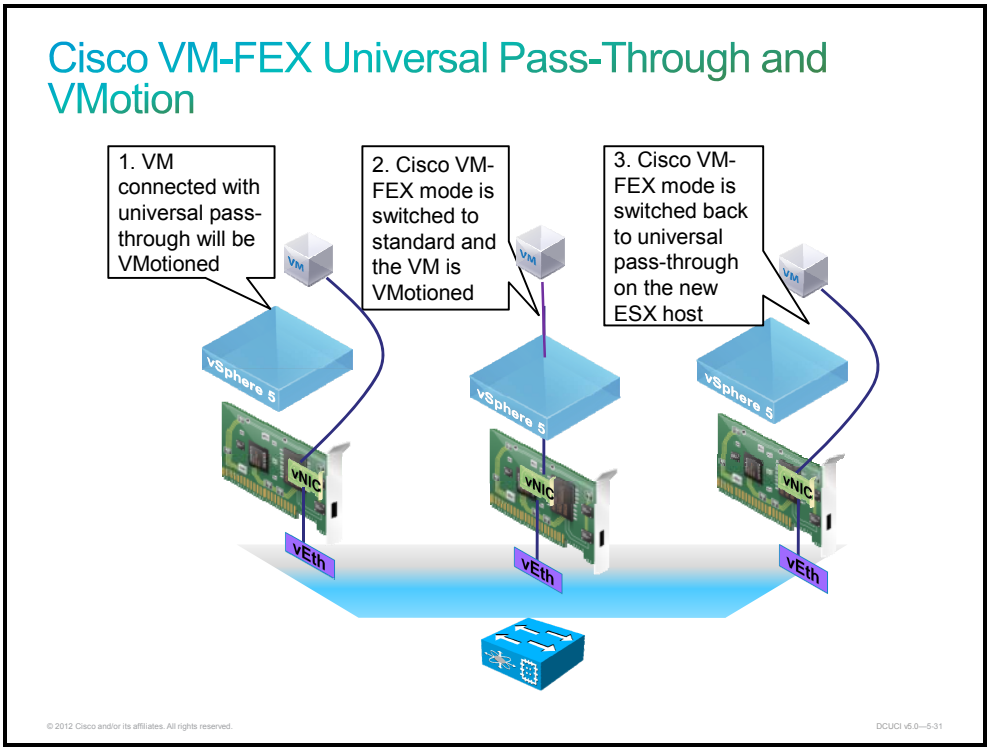
© 2012 Cisco Systems, Inc.

https://t.me/learningnets



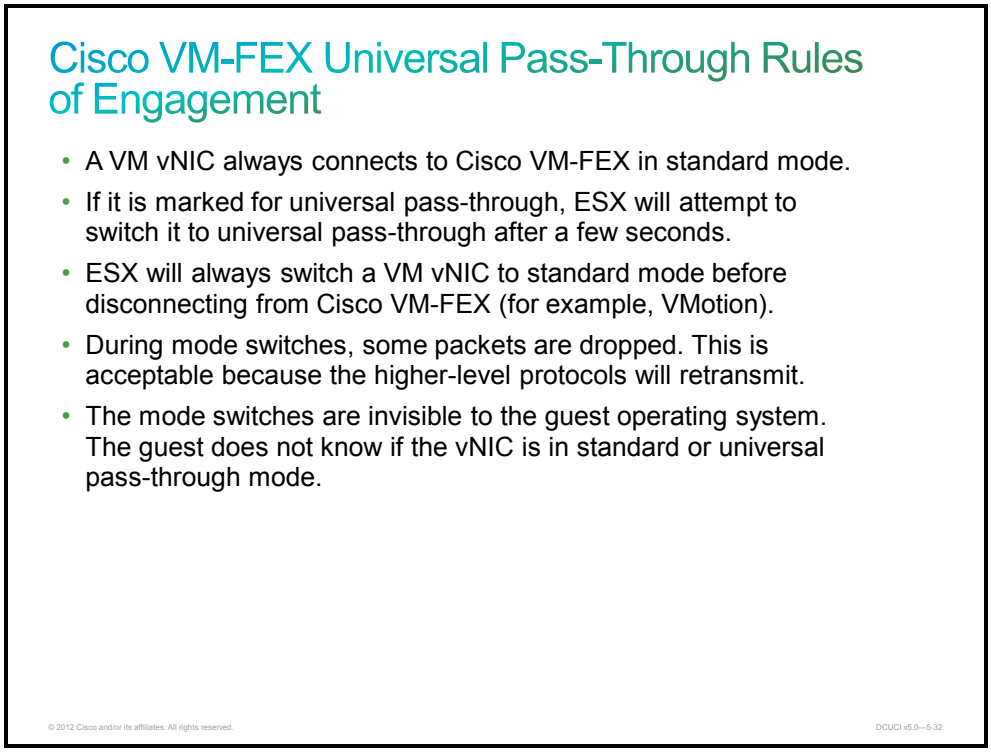
Standard and universal pass-through modes can coexist. In universal pass-through mode, VM traffic is processed in hardware. Immediately after it originates on the VM, it is sent to the Cisco VIC. From there, the traffic is tagged with the VN-Tag and sent to the fabric interconnect for network configuration to be applied and for any Layer 2 Forwarding decisions to be made. This process results in much better performance.

https://t.me/learningnets



VMotion is supported in both standard and universal pass-through modes. In universal pass-through mode, when a VM is moved by VMotion, the Cisco VM-FEX falls back to standard mode. After that, the VM is moved to the other ESX host. On the new ESX host, if there are no restrictions, the VM will be switched back to universal pass-through mode.

© 2012 Cisco Systems, Inc.
https://t.me/learningnets



The following are Cisco VM-FEX universal pass-through rules of engagement:

- A VM vNIC always connects to Cisco VM-FEX in standard mode. If it is marked for universal pass-through, ESX will attempt to switch it to universal pass-through after a few seconds.
- ESX will always switch a VM vNIC to standard mode before disconnecting from Cisco VM-FEX (for example, VMotion).
- During mode switches, some packets are dropped. The drops are acceptable because the higher-level protocols will retransmit.
- The mode switches are invisible to the guest operating system. The guest does not know if the vNIC is in standard or universal pass-through mode.

https://t.me/learningnets

Cisco VM-FEX Universal Pass-Through Requirements

- Cisco VM-FEX universal pass-through mode is only supported on the following VM guest operating systems:
  - Windows 2008 SP2
  - Windows 2008 R2
  - RHEL 6.0
  - SLES 11, SLES 11 SP1
- VM vNIC must be of type VMXNET3 and the guest operating system must be running the supported universal pass-through VMXNET3 driver.
- All memory of the VM must be reserved.

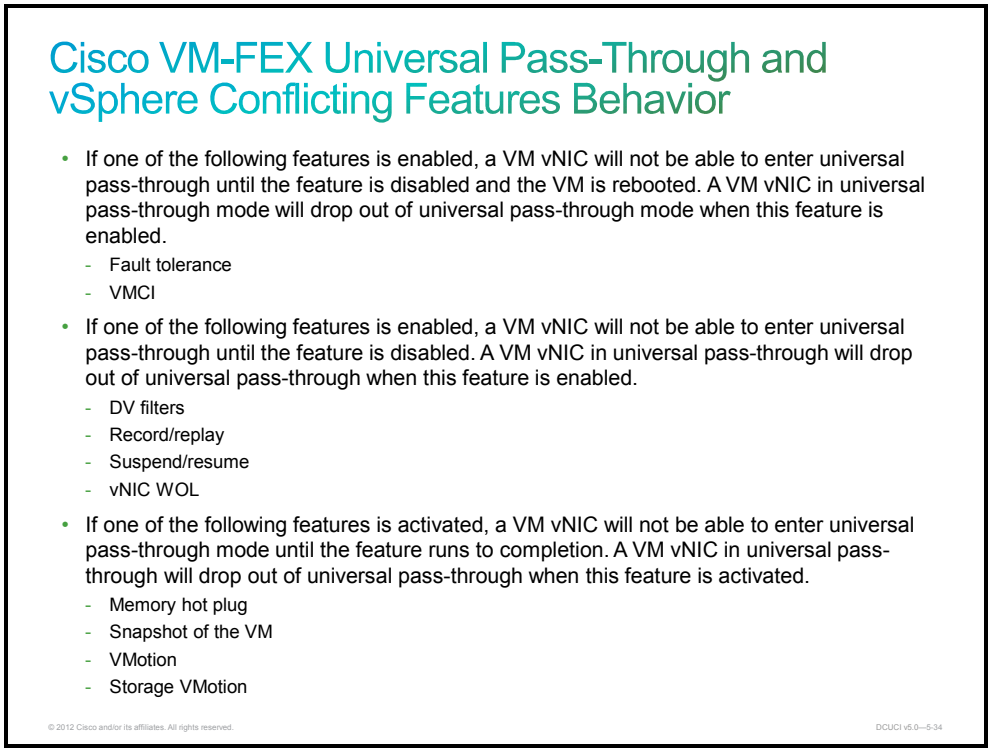
© 2012 Cisco and/or its affiliates. All rights reserved.

There are some requirements for use of Cisco VM-FEX universal pass-through mode:

- Supported guest operating systems include the following:
  - Windows 2008 Service Pack 2
  - Windows 2008 R2
  - Red Hat Enterprise Linux 6.0
  - SUSE Linux Enterprise Server 11, SUSE Linux Enterprise Server 11 Service Pack 1
- The VM vNIC must be of type VMXNET3 and the guest operating system must be running the supported universal pass-through VMXNET3 driver.
- All memory of the VM must be reserved.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets



There are some vCenter features that conflict with universal pass-through mode. When these features are enabled or activated, the behavior will be as follows:

- If one of the following features is enabled, a VM vNIC will not be able to enter universal pass-through until the feature is disabled and the VM is rebooted. A VM vNIC in universal pass-through will drop out of universal pass-through when this feature is enabled.
  - Fault tolerance
  - Virtual Machine Communication Interface (VMCI)
- If one of the following features is enabled, a VM vNIC will not be able to enter universal pass-through until the feature is disabled. A VM vNIC in universal pass-through will drop out of universal pass-through when this feature is enabled.
  - DV filters
  - Record/replay
  - Suspend/resume
  - vNIC Wake on LAN (WOL)
- If one of the following features is activated, a VM vNIC will not be able to enter universal pass-through mode until the feature runs to completion. A VM vNIC in universal pass-through will drop out of universal pass-through when this feature is activated.
  - Memory hot plug
  - Snapshot of the VM
  - VMotion
  - Storage VMotion

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.

Summary

- VM traffic is managed by software switches, such as VMware vSwitch and vDS.
- Cisco Nexus 1000V is the first third-party software DVS.
- Cisco VM-FEX extends the physical switch port to the VM vNIC, collapsing layers. It substitutes the software switches. All VM traffic switching is performed on the fabric interconnects.
- Cisco VM-FEX universal pass-through is a mode of Cisco VM-FEX in which the VM vNIC is directly connected to the PCIe device on the Cisco VIC. The VM traffic does not go through the PTS module. Only during VMotion will the VM be switched to standard Cisco VM-FEX mode.

© 2012 Cisco and/or its affiliates. All rights reserved.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 2

Provisioning Cisco VM-FEX

Overview

The Cisco Virtual Machine Fabric Extender (VM-FEX) allows virtual machine (VM) network adapters to be connected to dynamic virtual network interface cards (vNICs) that are created in the hardware of Cisco virtual interface cards (VICs). There is no software switch, and network configuration and management is performed from Cisco Unified Computing System (UCS) Manager. Cisco UCS Manager must be integrated with VMware vCenter Server and certain policies must be provisioned in the service profiles for the ESXi hosts.

Objectives

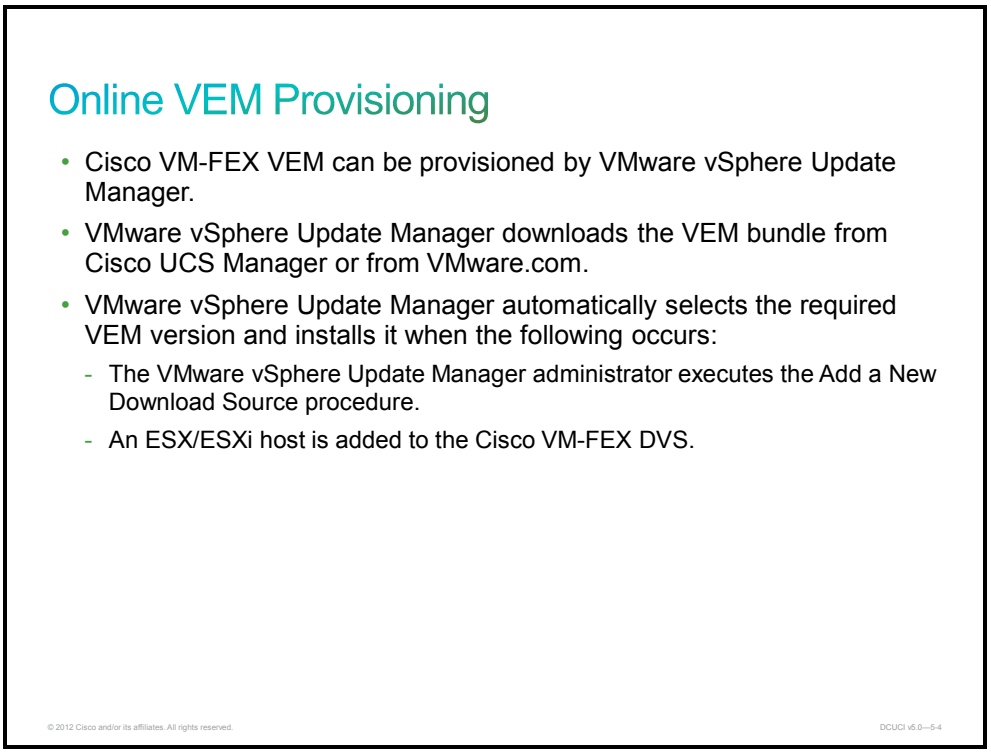
Upon completing this lesson, you will be able to provision Cisco VM-FEX in Cisco UCS Manager and VMware vCenter Server. This ability includes being able to meet these objectives:

- Provision VMware ESXi servers with a Cisco VEM
- Provision the secure connection from Cisco UCS Manager to VMware vCenter Server
- Provision port profiles and push to vCenter as port groups
- Provision a dynamic vNIC connection policy and BIOS policy for Cisco VM-FEX
- Join ESXi hosts to the DVS
- Provision VMs to consume port groups on the DVS

https://t.me/learningnets

Provision VMware ESXi Servers with a Cisco VEM

This topic describes the methods to provision a Cisco VM-FEX Virtual Ethernet Module (VEM) on ESXi hosts.



You must install the Cisco VM-FEX VEM on the ESXi host to use the Cisco VM-FEX technology. There are two ways to install the VEM:

- Online by using the VMware vCenter Update Manager
- Offline by manually installing the VEM on the ESXi host

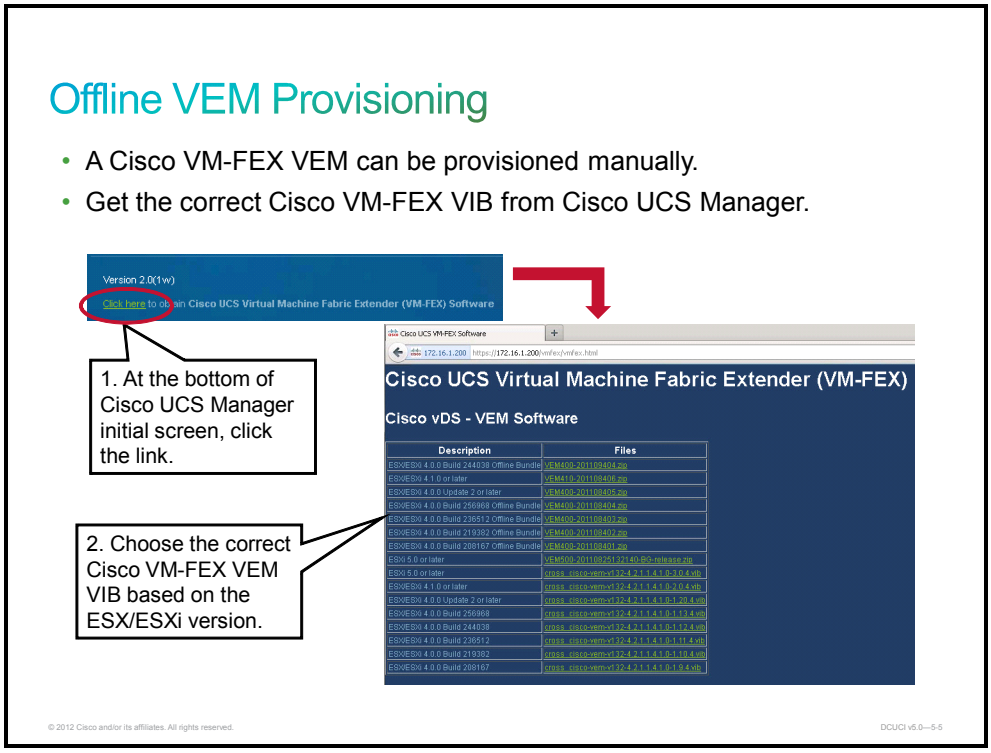
For online installation, you need to install VMware vCenter Update Manager on vCenter Server. After you have installed the VMware vCenter Update Manager, check the VMware vCenter Update Manager configuration to ensure that the correct URL is specified for downloading any needed patches. Usually, the custom update type is specified, which points to the VMware site. With the custom update, all required third-party patches will be downloaded from VMware. The other option is to manually add a download source, where you must specify the Cisco UCS Manager URL.

When the VMware vCenter Update Manager is used for the VEM installation, there are two instances in which the VEM will be installed:

- When the VMware vCenter Update Manager administrator executes the Add a New Download Source procedure
- When an ESXi host is added to the distributed virtual switch (DVS)

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



For the offline installation, you must execute several steps:

Step 1 Obtain the correct version of the Cisco VM-FEX VEM vSphere Installation Bundle (VIB) and open the Cisco UCS Manager initial screen.

Step 2 At the bottom of the screen, choose the link **Click Here to Obtain Cisco UCS Virtual Machine Fabric Extender (VM-FEX) Software**.

Step 3 A new screen will open that lists all of the VEM VIBs. Choose the correct file based on your ESX/ESXi version and store the file locally.

Note It is important to validate that the selected VEM version is compatible with your hypervisor version. Please refer to the *Cisco Nexus 1000V Series Switches Compatibility Information* page at Cisco.com.
http://www.cisco.com/en/US/products/ps9902/products_device_support_tables_list.html

---

https://t.me/learningnets

ESXi VEM Installation

- Upload the VEM VIB to the ESXi host.
- To install the VEM VIB, manually use the following command:

esxcli software vib install -v /*path_to_vib/vib_name*-maintenance-mode

Example:

esxcli software vib install -v /tmp/cross_cisco-vem-v132-4.2.1.1.4.1.0-3.0.4.vib -maintenance-mode

- Use the command text in the following example to verify the installation:

```
~ # esxcli software vib list | grep cisco
cisco-vem-v132-esx    4.2.1.1.4.1.0-3.0.4              Cisco   PartnerSupported  2012-05-04
~ # vmkload_mod -l | grep pts
mptsas                  1    260
vem-v132-pts            0    144
~ #
```

© 2012 Cisco and/or its affiliates. All rights reserved.

Step 4 Upload the VEM VIB file manually on the ESXi host.

Step 5 Access the CLI of the ESXi host and execute the following command to install the software:

```
esxcli software vib install -v /path_to_VIB/name_of_VIB_file
-maintenance-mode
```

Note Using the **–maintenance-mode** keyword at the end of the command allows the installation to proceed without putting the ESXi host in maintenance mode. The command simulates maintenance mode. The ESXi will provide you with information for the successful installation.

Step 6 To verify that the VIB is installed and loaded, execute the following commands:

```
esxcli software vib list | grep cisco
vmkload_mod -l | grep pts.
```

 © 2012 Cisco Systems, Inc.

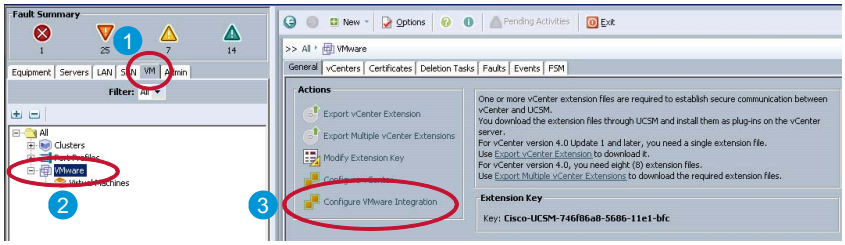
https://t.me/learningnets

Cisco UCS Manager with VMware Integration

This topic describes how to use the VMware integration wizard in Cisco UCS Manager.

Start VMware Integration Wizard

- Start the wizard to provision the integration between Cisco UCS Manager and vCenter, going through the following steps:
  - Install the Cisco UCS Manager plug-in in vCenter.
  - Define the VMware DVS.
  - Define the VM port profiles.
  - Apply port profiles to a DVS.



© 2012 Cisco and/or its affiliates. All rights reserved.

After you have enabled the use of the VMware vCenter Update Manager or you have manually installed the VEM, the next step is to provision Cisco UCS Manager. You may provision Cisco UCS Manager with or without the wizard. The steps are the same, but when the wizard is used, there is step-by-step guidance. This lesson describes the wizard-based approach.

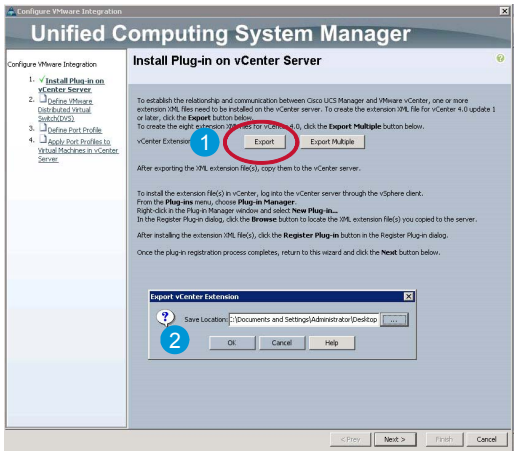
To start the wizard, choose the VM tab in Cisco UCS Manager. Choose **VMware** in the navigation pane and choose **Configure VMware Integration** in the content pane. This selection starts the wizard that will guide you through the following actions:

- Install Cisco UCS Manager extensions as plug-ins in vCenter
- Define the VMware DVS
- Define VM port profiles
- Apply port profiles to a DVS

https://t.me/learningnets

Export Cisco UCS Manager Plug-In

- Save the Cisco UCS Manager plug-in locally.
- Only one plug-in is required for vCenter 4.0 update 1.



© 2012 Cisco and/or its affiliates. All rights reserved.

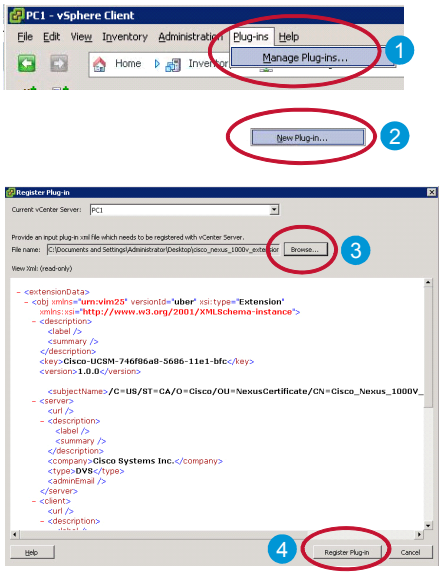
In the first step, export and locally store the Cisco UCS Manager extension. This extension is actually a Cisco UCS Manager certificate that will be installed as a plug-in in vCenter and will protect communication between vCenter and Cisco UCS Manager. If you use ESX version 4.0, you will need multiple extensions. If you use ESX/ESXi version 4 update 1 or later, you will need only one extension.

Click **Export**, specify where you want the extension to be stored, and then click **OK**.

https://t.me/learningnets

Install Plug-In in vCenter

- The Cisco UCS Manager extension is installed as a new plug-in in vCenter.
- Navigate to **Plug-ins** and select **Manage Plug-ins**.
- Right-click and select **New Plug-in**.
- Browse for the Cisco UCS Manager extension, select it, and click **Register Plug-in**.



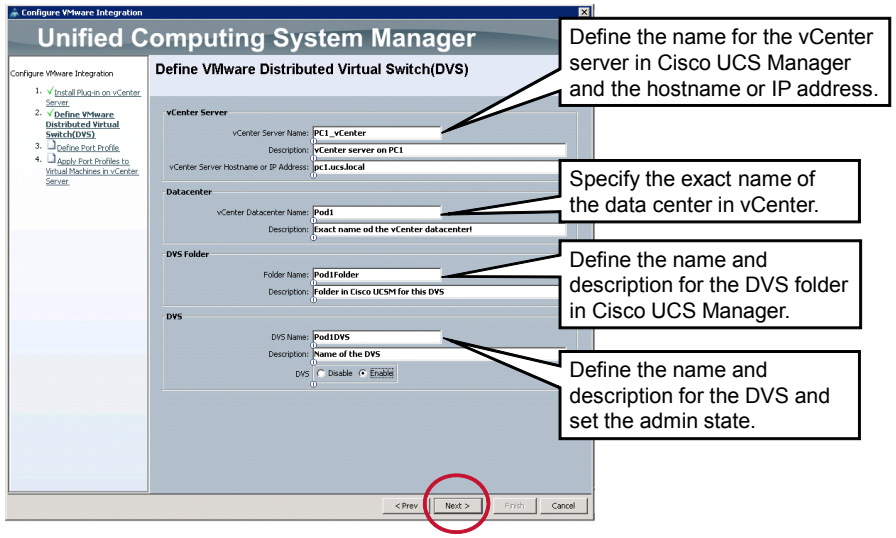
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, install the Cisco UCS Manager extension as a plug-in in vCenter. To perform this step, leave the VMware integration wizard in Cisco UCS Manager and switch temporarily to the vCenter Server. vCenter is accessed using the vSphere Client. Choose **Plug-Ins** from the menu bar and click **Manage Plug-Ins**. In the Plug-Ins Manager window, right-click in the white space and choose the only available option, **New Plug-In**.

Browse for the Cisco UCS Manager extension file, select it, and click **Register Plug-In**. The vCenter Server will return a message confirming the successful registration of the plug-in.

https://t.me/learningnets

Define VMware DVS in Cisco UCS Manager



In Cisco UCS Manager VMware Integration wizard, the next step is to define the needed components in Cisco UCS Manager. In vCenter, the logical components are organized in data centers and folders. In Cisco UCS Manager, there is a similar organization. Each vCenter Server is defined, and for each vCenter Server, a folder is created to contain the DVS. There is also an option to create additional folders to store additional components. Additionally, there is a separate folder to store and create port profiles. The port profiles are also visible under the DVS to which they are assigned.

At this stage, the wizard helps you avoid confusion by defining everything that is needed to deploy the DVS:

Step 1 Define the vCenter Server. Specify a name (this name is used only internally by the Cisco UCS Manager) and define the vCenter IP address or hostname.

Step 2 Define the vCenter data center. As mentioned, the ESXi hosts are grouped in logical data centers in vCenter. Specify the exact name of the vCenter data center where the DVS will appear.

Step 3 Define the name and description of the DVS folder. Specify the name of the folder that Cisco UCS Manager will create under the specified vCenter to store the DVS.

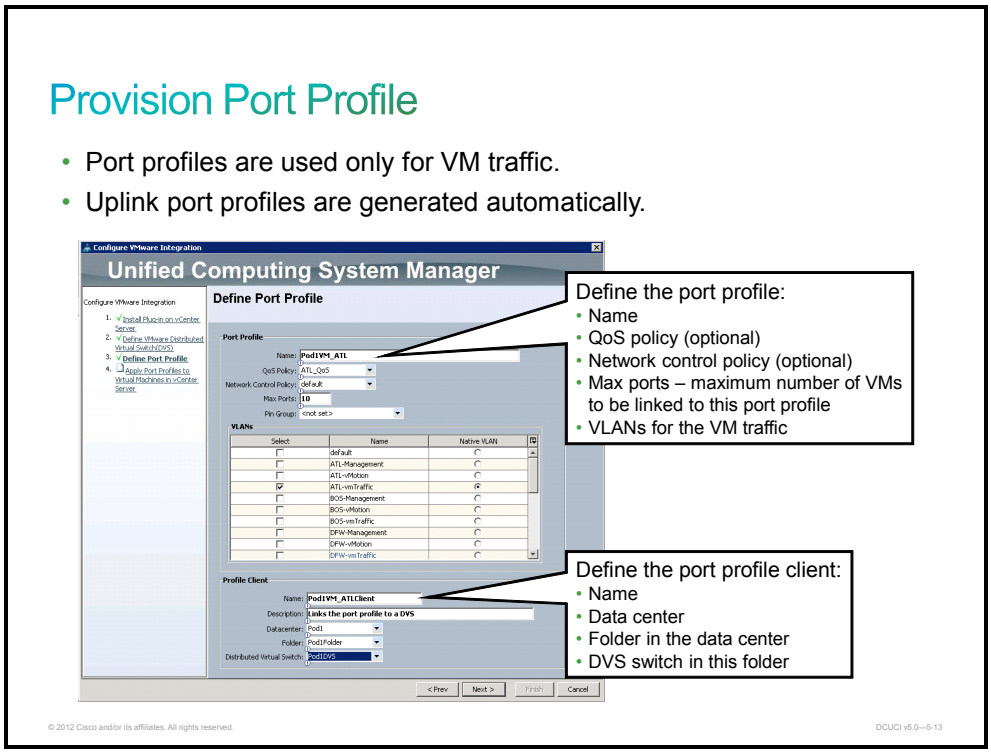
Step 4 Define the DVS name and admin state.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision Port Profiles

This topic describes how to provision port profiles and assign them to a DVS with port profile clients.



The third step of the wizard defines port profiles. When you finish the wizard, the port profile will be communicated to vCenter, where it will be converted into a port group and used for VM traffic.

In the Port Profile section of the wizard, specify the following:

- **Name:** Enter a port profile name.
- **QoS Policy:** Specify a QoS policy if needed.
- **Network Control Policy:** Optionally, specify any network control policy to be associated.
- **Max Ports:** Define the maximum number of ports that can be associated with this port profile. The default value is 64. The maximum number of ports per DVS is 4096. If only one port profile is used, then you can configure it for up to 4096 ports. If more than one port profile is used, then the total number of ports for all of the port profiles must not exceed 4096.
- **Pin Group:** If needed, choose a static pin group.
- **VLANs:** Select the VLAN or VLANs that you want to use for VM traffic. Also, if you select multiple VLANs, do not forget to specify which will be the native VLAN.

https://t.me/learningnets

If you need to provision more port profiles in the future, you can do so from the Port Profiles section of the VM tab. Remember that the port profile must be associated with a DVS because, as you can have multiple DVSs. To perform the association, you have to provision a port profile client. In the wizard, after you have provisioned a port profile, the next step allows you to provision a port profile client. Define the following:

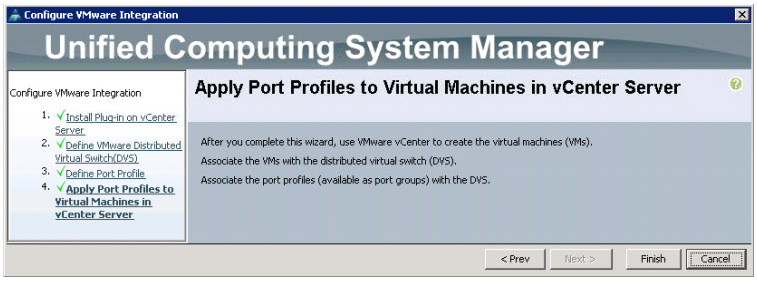
- **Name:** Enter a port profile client name.
- **Data center:** Specify the vCenter data center.
- **Folder:** Specify the folder where the DVS is located.
- **DVS:** Specify the DVS to which the port profile will be associated.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Finish the Wizard

- Next steps:
  - Prepare servers with service profiles, and a specific BIOS policy and Dynamic vNIC connection policy.
  - After ESXi installation, add the host to vCenter and create VMs.
  - Associate the ESXi host to DVS.
  - Link the VM vNIC with the correct port group.

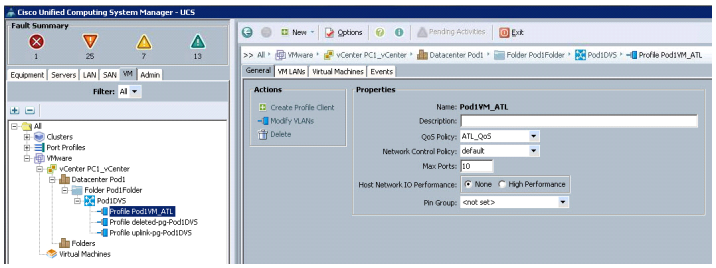


© 2012 Cisco and/or its affiliates. All rights reserved.

The final step of the wizard is named Apply Port Profiles to Virtual Machines in vCenter Server. This step provides additional information about steps to complete after you finish the wizard. You do not have to provision anything here. End the wizard by clicking **Finish**.

Verify DVS in Cisco UCS Manager

- After the wizard finishes, the DVS will appear in the VM tab.



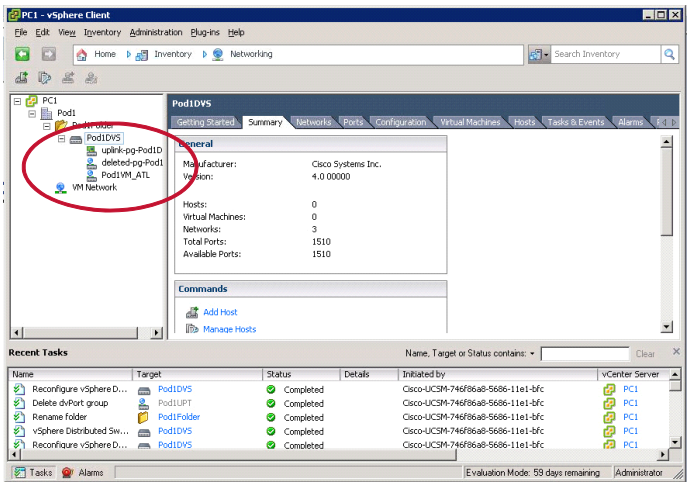
© 2012 Cisco and/or its affiliates. All rights reserved.

When you finish the wizard, you will see that the vCenter is created in the VM tab of Cisco UCS Manager. You will also see the data center, the folder, and the DVS with the created port profile.

https://t.me/learningnets

Verify DVS in vCenter

- The DVS information will be pushed immediately to vCenter.
- A new DVS will be created in vCenter.



© 2012 Cisco and/or its affiliates. All rights reserved.

In vCenter, you will observe that a new DVS has been created and that the port profile appears as a port group. Next, you have to add ESXi hosts to the DVS and migrate the VM networking.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision Service Profile Components for Cisco VM-FEX

This topic describes how to provision the required service profile components for Cisco VM-FEX.

Dynamic vNIC Connection Policy

- Determines connectivity between VMs and dynamic vNICs
- Required component used in service profile
- Defines the Ethernet adapter policy and number of dynamic vNICs to be created

Number of IOM Links	6120/6140 Discreet Mode	6248/6296 Discreet Mode	6248/6296 Port-Channel Mode
1	13 (Cisco VM-FEX dynamic vNICs: 9)	60 (Cisco VM-FEX dynamic vNICs: 56)	60 (Cisco VM-FEX dynamic vNICs: 56)
2	28 (Cisco VM-FEX dynamic vNICs: 24)	116 (Cisco VM-FEX dynamic vNICs: 112)	116 (Cisco VM-FEX dynamic vNICs: 112)
4	58 (Cisco VM-FEX dynamic vNICs: 54)	116 (Cisco VM-FEX dynamic vNICs: 112)	116 (Cisco VM-FEX dynamic vNICs: 112)
8 (using 2208)	116 (Cisco VM-FEX dynamic vNICs: 112)	116 (Cisco VM-FEX dynamic vNICs: 112)	116 (Cisco VM-FEX dynamic vNICs: 112)

© 2012 Cisco and/or its affiliates. All rights reserved.

You have provisioned integration between Cisco UCS Manager and vCenter Server. The DVS was created and is available. To use the Cisco VM-FEX, however, the service profile that is used to prepare the ESXi host must use specific components. These components will configure the hardware accordingly and allow dynamic vNICs to be created in the Cisco VIC hardware.

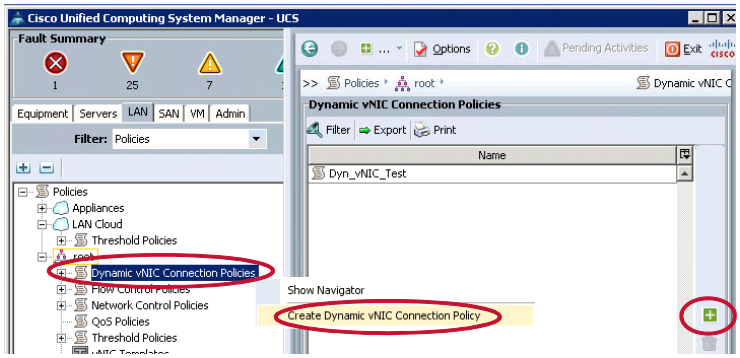
The first component is the Dynamic vNIC Connection Policy. That policy defines the connectivity between VM network adapters and dynamic vNICs. The Dynamic vNIC Connection Policy is a required component and it defines the Ethernet adapter policy and the number of dynamic vNICs that will be created.

The number of dynamic vNICs that can be created depends on the hardware that is used and on the number of uplinks between the I/O module (IOM) and the fabric interconnect.

https://t.me/learningnets

Create Dynamic vNIC Connection Policy

- From the LAN tab, navigate to **Policies > Dynamic vNIC Connection Policies**.
- Right-click **Dynamic vNIC Connection Policies** or click the plus sign (+) to start.



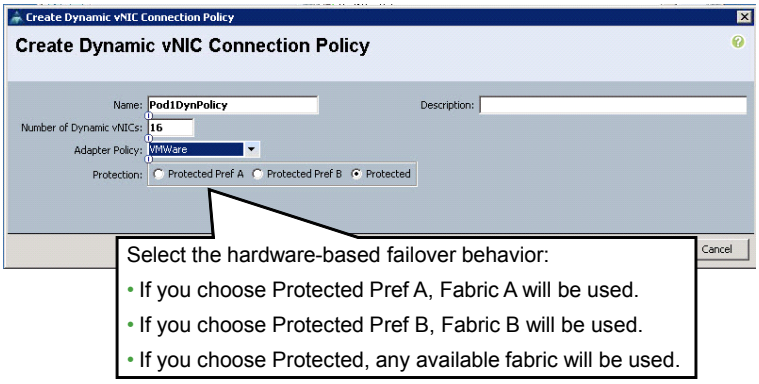
© 2012 Cisco and/or its affiliates. All rights reserved.

From the LAN tab, navigate to **Policies > Dynamic vNIC Connection Policies**. Right-click **Dynamic vNIC Connection Polices** and choose **Create Dynamic vNIC Connection Policy** from the pop-up menu or click the plus sign (+).

https://t.me/learningnets

Provision Dynamic vNIC Connection Policy

- Cisco VM-FEX in standard mode uses the VMware adapter policy.
- Specify the maximum number of dynamic vNICs to be created.



© 2012 Cisco and/or its affiliates. All rights reserved.

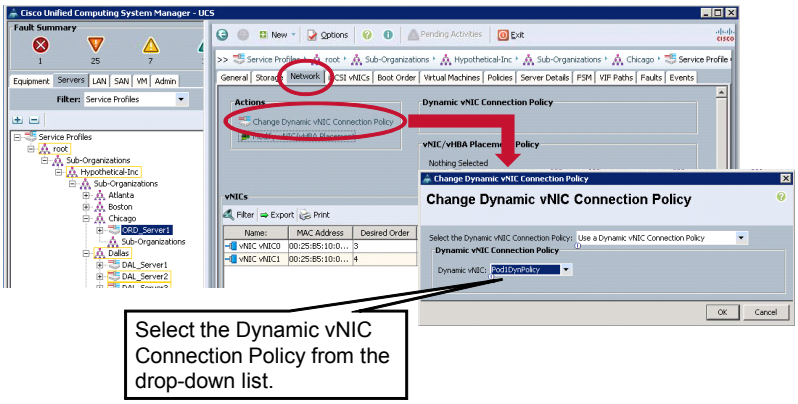
In the new window, specify the following:

- **Name:** Specify a name for this policy.
- **Number of Dynamic vNICs:** Enter the number of dynamic vNICs that will be created. The default value is 54. The value can be between 0 and 256. If there is no hardware capacity, the system will warn you.
- **Adapter Policy:** Specify the adapter policy. When you provision Cisco VM-FEX in standard mode, you have to use the VMware adapter policy.
- **Protection:** Specify the hardware-based failover behavior:
  - If you choose Protected Pref A, Cisco UCS Manager will prefer to use Fabric A if it is available. If necessary, it will fail to Fabric B.
  - If you choose Protected Pref B, Cisco UCS Manager will prefer to use Fabric B if it is available. If necessary, it will fail to Fabric A.
  - If you choose Protected, Cisco UCS Manager will use any available fabric.

https://t.me/learningnets

Associate Dynamic vNIC Policy with Service Profile

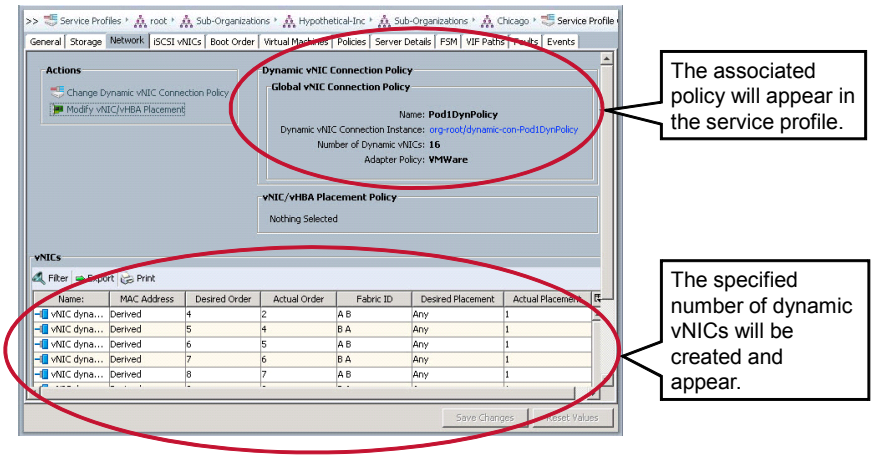
- Navigate to the service profile and select the **Network** tab in the content pane.
- Select **Change Dynamic vNIC Connection Policy**.



© 2012 Cisco and/or its affiliates. All rights reserved.

The dynamic vNIC connection policy must be associated with a service profile. To perform this association, navigate to the service profile and choose the **Network** tab. Choose **Change Dynamic vNIC Connection Policy**. In the new window, choose **Use a Dynamic vNIC Connection Policy**. From the drop-down list, choose the dynamic vNIC connection policy.

Verify Association



© 2012 Cisco and/or its affiliates. All rights reserved.

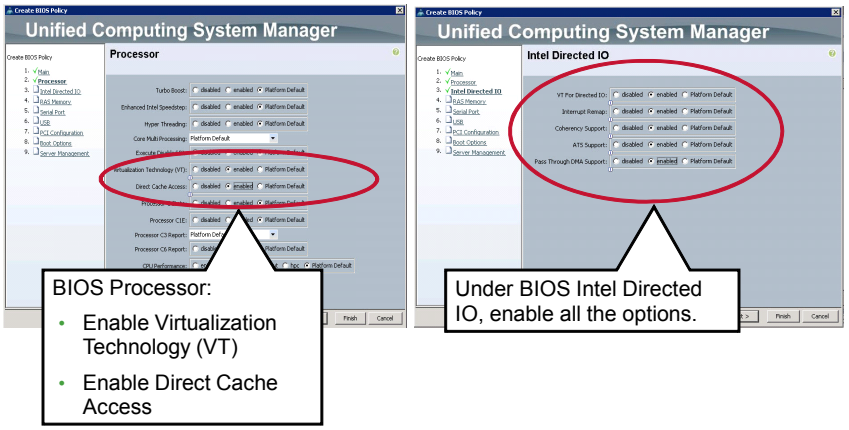
You will see that the dynamic vNIC connection policy is associated with the service profile and that the dynamic vNICs will appear.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Create BIOS Policy

- A special BIOS policy is needed for Cisco VM-FEX.
- Associate the BIOS policy with the service profile.



© 2012 Cisco and/or its affiliates. All rights reserved.

The other component that is required to use Cisco VM-FEX is a VMware-specific BIOS policy. Start the BIOS policy creation wizard at the Server tab, under Policies.

The following are required settings:

- BIOS Processor:
  - Enable Virtualization Technology (VT)
  - Enable Direct Cache Access
- BIOS Intel Directed IO:
  - Enable VT for Directed IO
  - Enable Interrupt Remap
  - Enable Coherency Support
  - Enable ATS Support
  - Enable Pass Through DMA Support

When the BIOS policy is ready, associate it with the service profile.

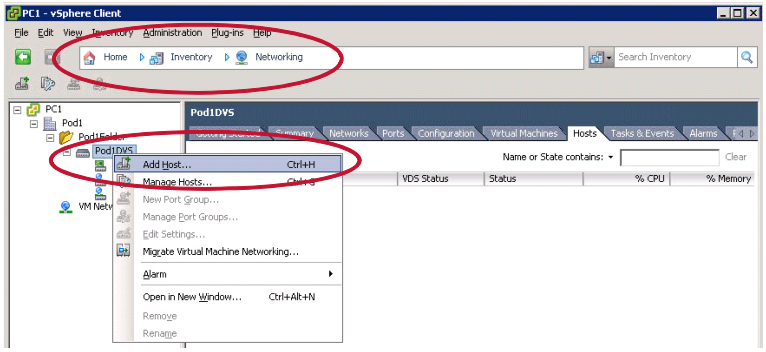
https://t.me/learningnets

Add ESXi Hosts to the DVS

This topic describes how to add ESXi hosts to the DVS.

Join ESXi Host to DVS in vCenter

- To join a host to DVS in vCenter, navigate to **Home > Inventory > Networks**.
- Right-click the DVS and select **Add Host**.

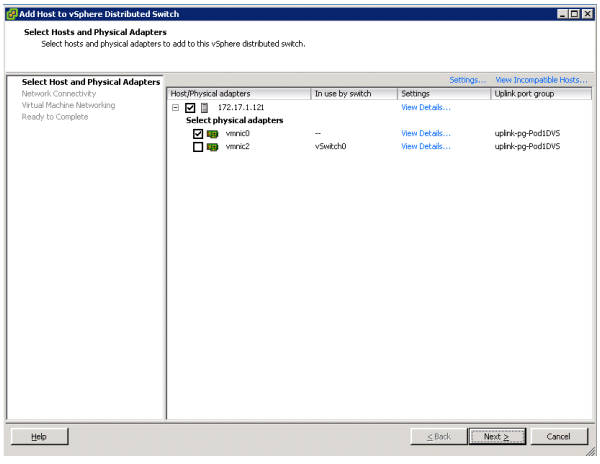


© 2012 Cisco and/or its affiliates. All rights reserved.

The ESXi hosts are added to the DVS with a wizard in vCenter. Navigate to **Home > Inventory > Networking**. To start the wizard, right-click the DVS and choose **Add Host**.

Add Host Wizard

- Select the ESXi host.
- Select which vmNICs will be added to the DVS.



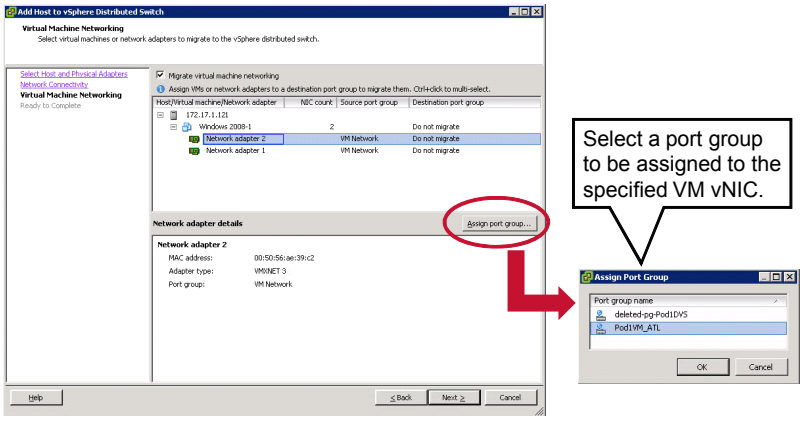
© 2012 Cisco and/or its affiliates. All rights reserved.

In the first step of the wizard, you will be provided with a list of the ESXi hosts in the data center. Choose the ESXi hosts and which of their vmNICs to add to the DVS.

https://t.me/learningnets

Migrate VM

- Skip the network connectivity step. Uplink port profiles are automatically applied to the selected vmNICs.
- Select the VM to be migrated to the DVS.



© 2012 Cisco and/or its affiliates. All rights reserved.

Skip the second step of the wizard, Network Connectivity. This step allows you to specify uplink port profiles, but with Cisco VM-FEX, uplink port profiles are applied automatically.

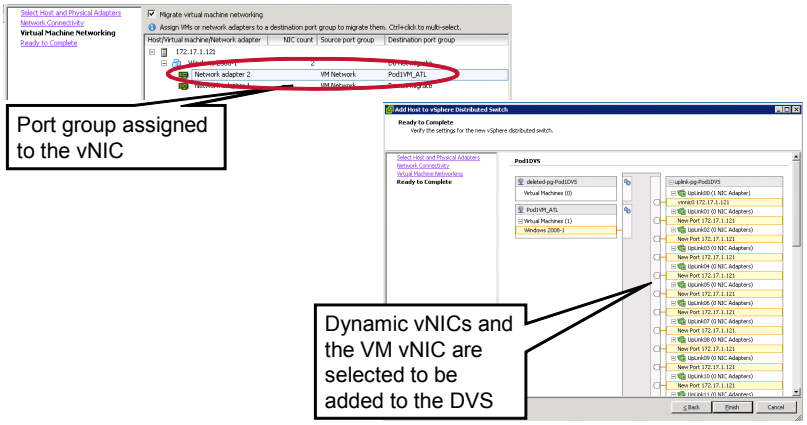
Proceed to the next step, which allows you to choose which VMs to migrate. This step is optional. You can always migrate VMs later.

If you choose to migrate a VM, select the VM, then choose a vNIC. After the vNIC is chosen, click **Assign Port Group** to link the VM vNIC to a port group. The new window will provide a list of available port groups for the DVS. Choose a port group and click **OK**.

https://t.me/learningnets

Add Host Wizard Verification

- Verify that the correct port group is selected.
- Verify that the ports appear at DVS.



© 2012 Cisco and/or its affiliates. All rights reserved.

You will see that the port group is linked with the VM vNIC.

The next step provides information about the dynamic vNICs and the VM vNIC that will be connected to the DVS.

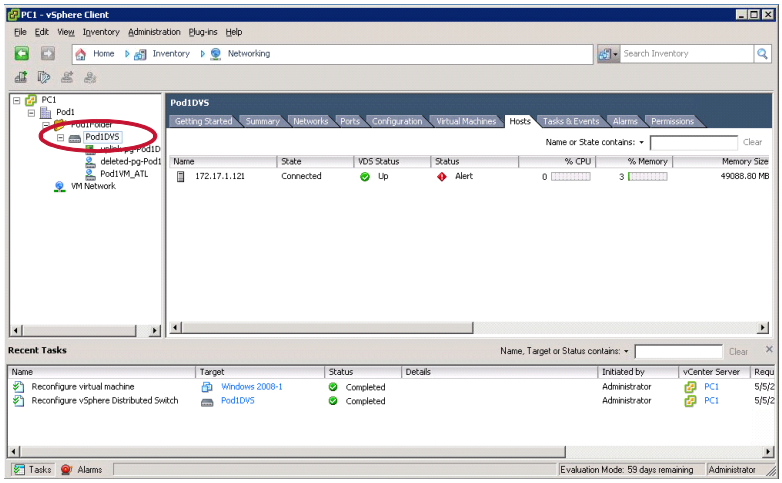
Click **Finish** to end the wizard.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

DVS Hosts Tab

- The host will appear in the DVS at the Hosts tab.



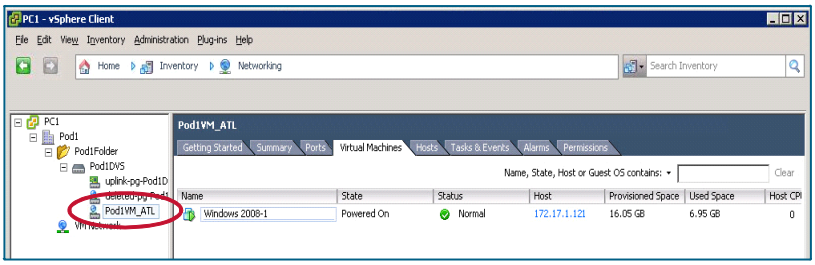
© 2012 Cisco and/or its affiliates. All rights reserved.

After you finish the wizard, the VMware vCenter Update Manager, if enabled and used, will access the ESXi host and install the VEM.

The ESXi host will be available in the Hosts tab of the DVS.

DVS Virtual Machine Tab

- The VM will appear in DVS in the Virtual Machines tab.



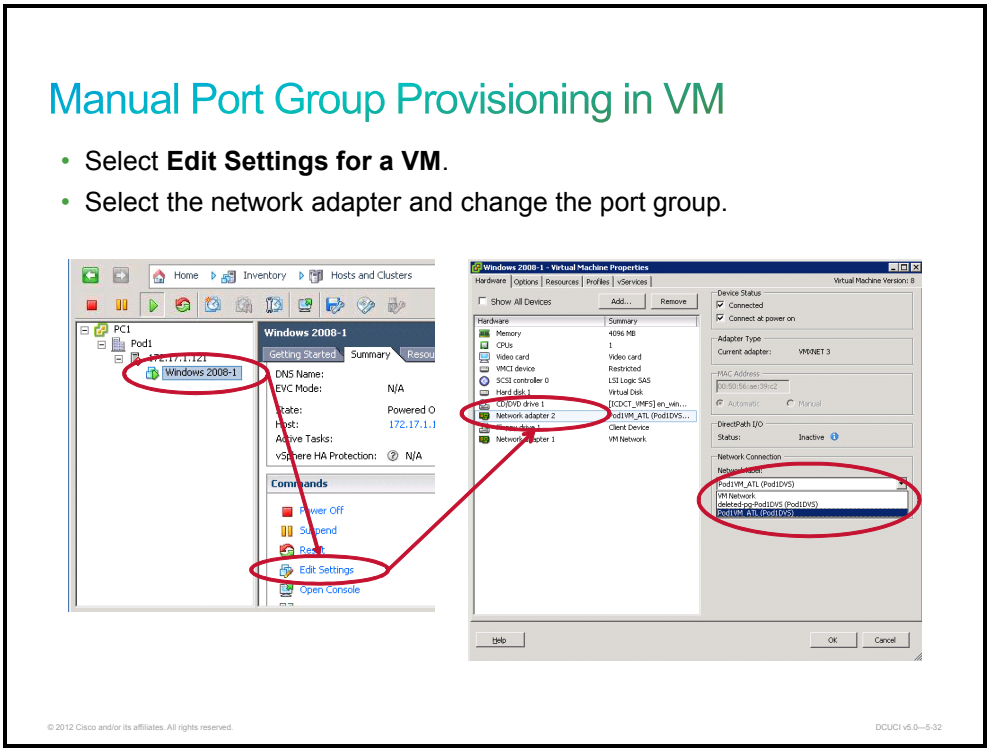
© 2012 Cisco and/or its affiliates. All rights reserved.

Available VMs will display in the Virtual Machine tab.

https://t.me/learningnets

Link a VM to a Port Group

This topic describes how to manually link a VM to a port group.



To manually link a VM vNIC to a port group, navigate to **Home > Inventory > Hosts and Clusters** and choose the VM. From the Summary tab, choose **Edit Settings**.

In the Settings window, choose the network adapter. On the right, in the Network Connection section, choose the port group from the Network Label drop-down menu.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.

Summary

- The ESXi host can be automatically provisioned with Cisco VM-FEX VEM using the VMware vSphere Update Manager or it can be manually provisioned.
- Start the VMware integration wizard to guide you through the provisioning of the vCenter communication and DVS.
- Use the wizard to provision port profiles and port profile clients.
- Provision the dynamic vNIC connection policy, BIOS policy, and use the correct Ethernet adapter policy. Associate the policies in the service profile for your ESXi host.
- Add hosts to the DVS in vCenter using the wizard. With the wizard, you can also migrate VMs at the same time.
- You can manually change the VM vNIC port group from the VM settings.

© 2012 Cisco and/or its affiliates. All rights reserved.

https://t.me/learningnets

© 2012 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 3

Provisioning Cisco VM-FEX Universal Pass-Through

Overview

Cisco Virtual Machine Fabric Extender (VM-FEX) universal pass-through mode uses the VMware DirectPath technology to bypass the hypervisor. The technology links virtual machines (VMs) directly to Peripheral Component Interconnect Express (PCIe) devices on Cisco virtual interface cards (VIC) (the dynamic virtual network interface cards [vNICs]). This technology allows for incredible performance.

Objectives

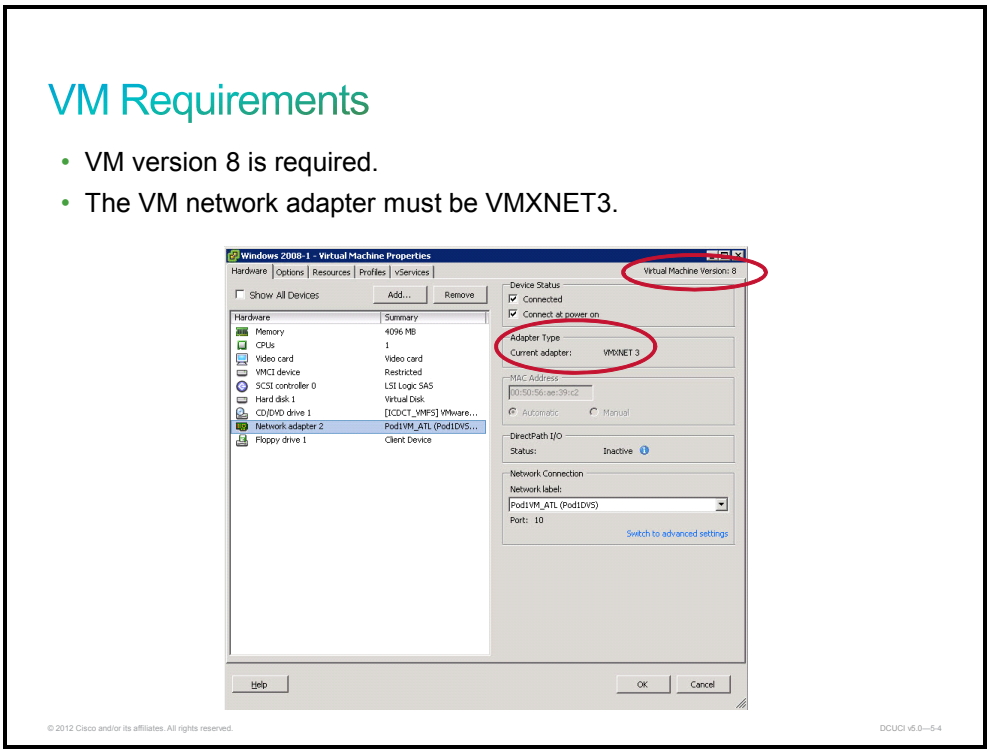
Upon completing this lesson, you will be able to provision Cisco VM-FEX universal pass-through mode in Cisco UCS Manager and VMware vCenter Server. This ability includes being able to meet these objectives:

- Describe VMware requirements for universal pass-through mode
- Provision a dynamic vNIC connection policy for Cisco VM-FEX universal pass-through
- Provision a BIOS policy for Cisco VM-FEX universal pass-through
- Associate universal pass-through policies to a service profile
- Provision a port profile for universal pass-through mode
- Provision VMs to connect to DirectPath I/O interfaces
- Verify universal pass-through mode

https://t.me/learningnets

VMware Requirements for Universal Pass-Through Mode

This topic describes specific VMware requirements for Cisco VM-FEX universal pass-through mode.



To enable Cisco VM-FEX in universal pass-through mode, there are certain requirements for the VMs:

- The VM must be version 8.
- The VM network adapter must be of the type VMXNET3.

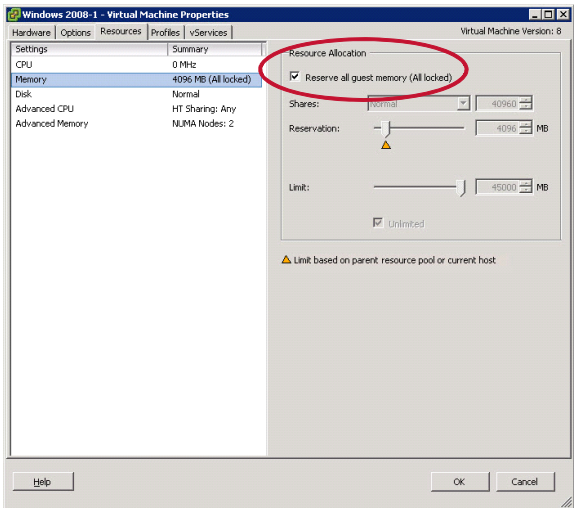
The latter requirement also means that the Vmxnet3 adapter must be recognized and installed as a network adapter in the guest operating system. For the installation to happen, you also have to install VMware tools in the guest operating system on the VM.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

VM Memory Reservation

- VM memory must be reserved.



© 2012 Cisco and/or its affiliates. All rights reserved.

Another important requirement for the VM is that its memory must be reserved. If the memory is not reserved, the DirectPath I/O remains inactive.

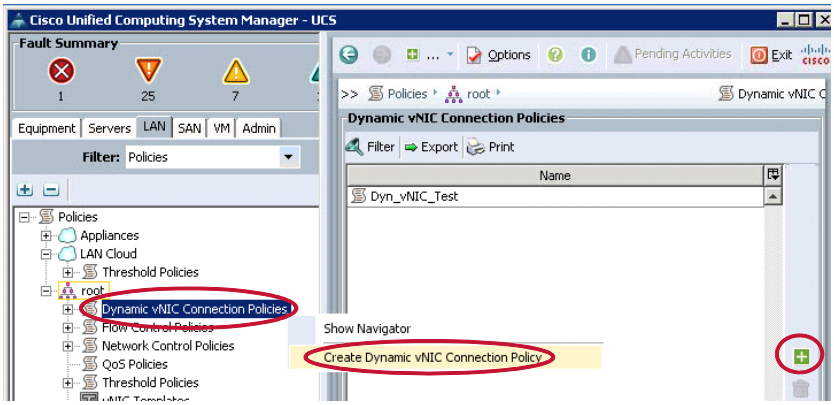
https://t.me/learningnets

Provision a Dynamic vNIC Connection Policy for Universal Pass-Through Mode

This topic describes how to provision a dynamic vNIC connection policy to support universal pass-through mode.

Create Dynamic vNIC Connection Policy

- From the LAN tab, navigate to **Policies > Dynamic vNIC Connection Policies**.
- Right-click **Dynamic vNIC Connection Policies** or click the plus sign (+) to start.



Cisco VM-FEX universal pass-through mode is another mode of operation of the Cisco VM-FEX. With this mode, you do not have to set up a new distributed virtual switch (DVS) or perform a new integration between Cisco UCS Manager and vCenter Server. Some components must be configured differently for the universal pass-through mode to be supported.

The dynamic vNIC connection policy, as discussed in the previous lesson, defines the Ethernet adapter policy that will be used on the Cisco VIC when dynamic vNICs are created.

It is important to specify the VMWarePassThru Ethernet adapter policy if you plan to use Cisco VM-FEX in universal pass-through mode.

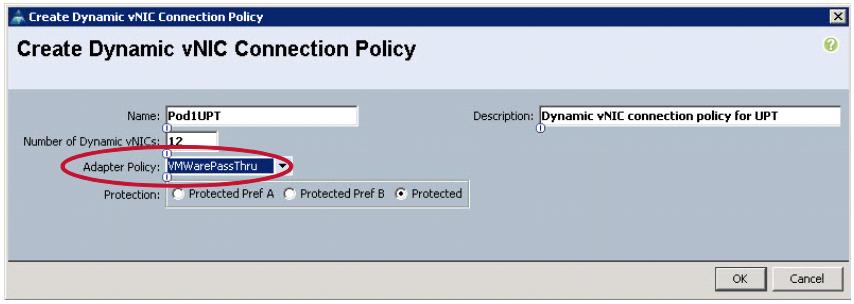
From the **LAN** tab, navigate to **Policies > Dynamic vNIC Connection Policies**. Right-click **Dynamic vNIC Connection Policies** or click the plus sign (+) to start.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision Universal Pass-Through Dynamic vNIC Connection Policy

- For Cisco VM-FEX in universal pass-through mode, use the VMWarePassThru adapter policy.
- Specify the maximum number of dynamic vNICs to be created.



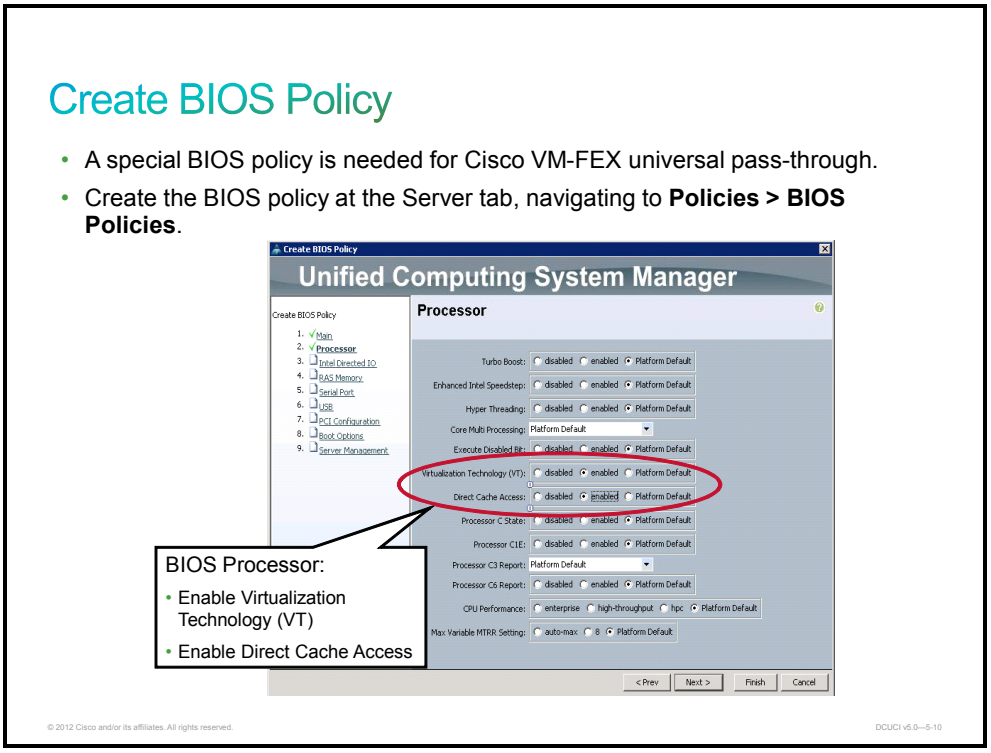
© 2012 Cisco and/or its affiliates. All rights reserved.

The Ethernet adapter policy must be VMWarePassThru.

https://t.me/learningnets

Provision BIOS Policy for Universal Pass-Through Mode

This topic describes the BIOS policy for universal pass-through mode.



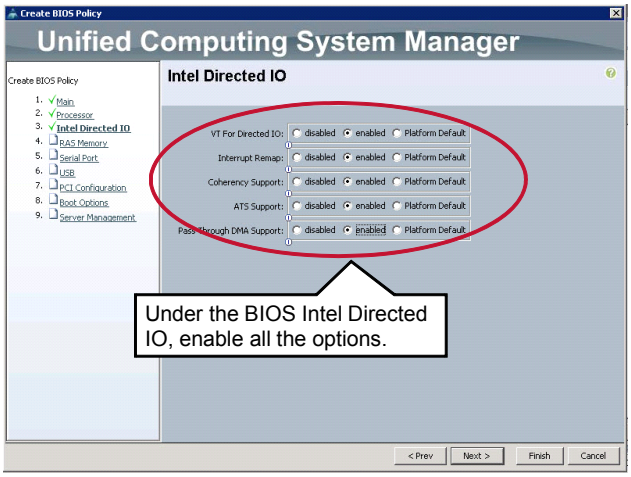
The BIOS policy that is required to support Cisco VM-FEX in universal pass-through mode must be provisioned with specific features enabled:

- BIOS Processor:
  - Enable Virtualization Technology (VT)
  - Enable Direct Cache Access

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Enable Intel Directed I/O in BIOS Policy



© 2012 Cisco and/or its affiliates. All rights reserved.

Enable all of the BIOS Intel Directed IO features:

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

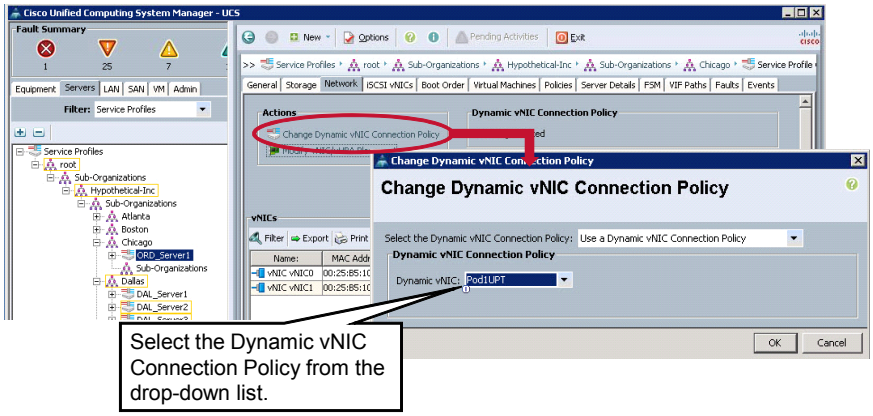
https://t.me/learningnets

Associate Universal Pass-Through Policies to a Service Profile

This topic describes the steps to associate universal pass-through-related policies to a service profile.

Associate Dynamic vNIC Policy with Service Profile

- Navigate to the service profile and select the **Network** tab.
- Select **Change Dynamic vNIC Connection Policy**.



© 2012 Cisco and/or its affiliates. All rights reserved.

Once you have created the BIOS policy and the dynamic vNIC connection policy, they must be associated with the service profile that will be used for the ESXi host.

To associate the dynamic vNIC connection policy, navigate to and select the service profile in the **Server** tab. In the content pane, choose the **Network** tab.

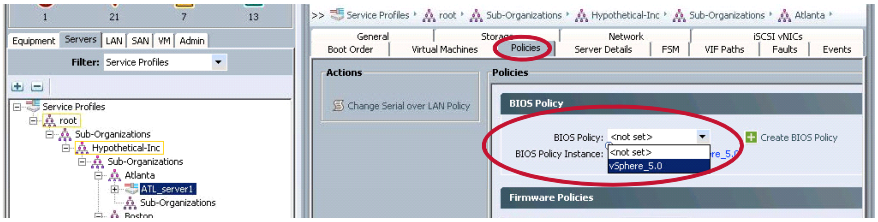
Click **Change Dynamic vNIC Connection Policy**. In the new window, select your policy from the drop-down list.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Associate BIOS Policy to Service Profile

- Navigate to **Service Profiles** under the **Servers** tab.
- Select the service profile. From **Policies**, select the correct BIOS policy.



© 2012 Cisco and/or its affiliates. All rights reserved.

To associate the BIOS policy, choose the **Policies** tab in the service profile. Expand the **BIOS** section. From the drop-down list, choose the BIOS policy.

Adding these two policies in your service profile will not result in server reboot.

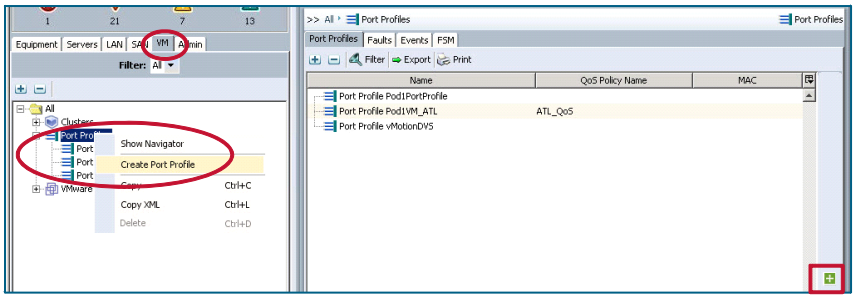
https://t.me/learningnets

Provision a Port Profile for Universal Pass-Through Mode

This topic describes the steps to provision a port profile for universal pass-through mode.

Create Universal Pass-Through Port Profile

- Navigate to **Port Profiles** under the **VM** tab.
- Right-click **Port Profiles** and select **Create Port Profile** or click the plus sign (+).



© 2012 Cisco and/or its affiliates. All rights reserved.

Universal pass-through mode is enabled and disabled for each port profile in the DVS. You can have port profiles in standard mode and port profiles in universal pass-through mode.

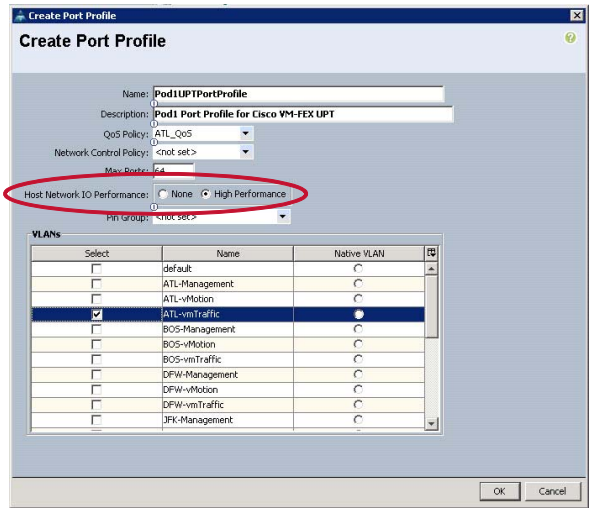
The port profile is created in the Port Profile section of the VM tab in Cisco UCS Manager.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Port Profile Settings

- Select **High Performance** to enable universal pass-through mode.



© 2012 Cisco and/or its affiliates. All rights reserved.

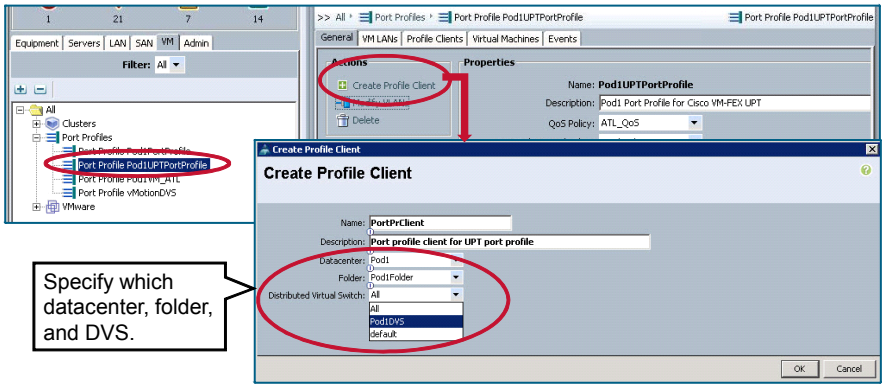
When you create the port profile for universal pass-through mode, all of the settings are similar to a port profile for standard mode. The exception is Host Network IO Performance, which must be set to High Performance.

Note	This option is not available when you create a port profile in the VMware Integration wizard. After a port profile is created, you can always choose the profile and this option will be available.

https://t.me/learningnets

Associate Universal Pass-Through Port Profile to DVS

- Create a port profile client to associate the universal pass-through port profile to a DVS.
- Select the newly created port profile and click **Create Profile Client**.



© 2012 Cisco and/or its affiliates. All rights reserved.

After the port profile is created, it must be associated with a DVS. For this association, you have to create a port profile client.

To create a port profile client, select the port profile and click **Create Profile Client**.

In the new window, specify the following:

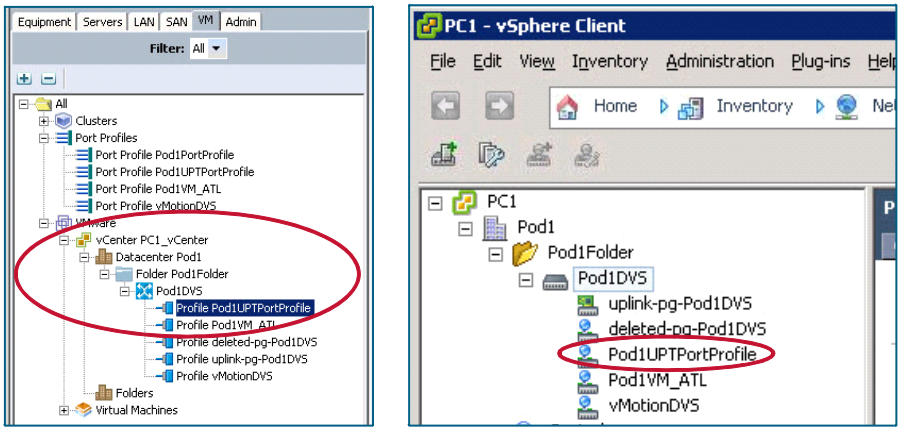
- **Datacenter:** Specify the data center in which the DVS is located for the port profile that will be associated to it.
- **Folder:** Specify the folder in the data center.
- **DVS:** Specify the DVS to which the port profile will be associated.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Verify Universal Pass-Through Port Profile

- Navigate to the DVS. The new universal pass-through port profile is there.
- In vCenter, a new port group was created.



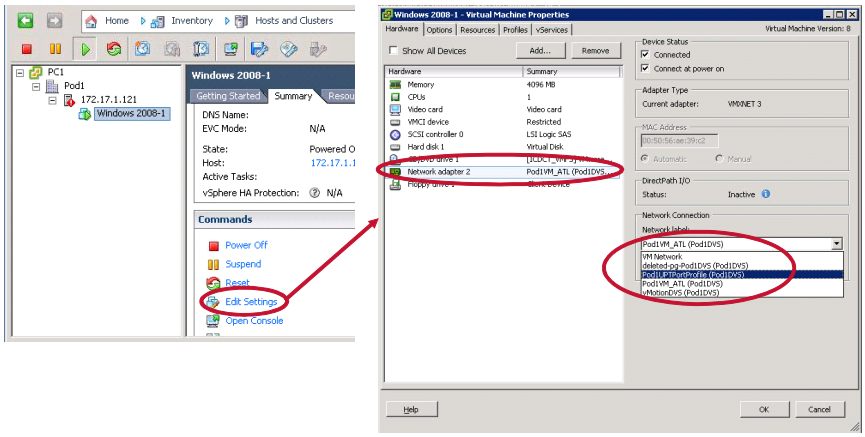
Immediately, the port profile will appear under the DVS that is specified in the port profile client. The port profile configuration will also be communicated to vCenter. You can observe that a new group appears under the DVS in vCenter.

https://t.me/learningnets

Provision VMs to Connect to DirectPath I/O Interfaces

Manual Port Group Provisioning in VM

- Select **Edit Settings** for a VM.
- Select the network adapter and change the port group.



© 2012 Cisco and/or its affiliates. All rights reserved.

All of the requirements are met and the components have been created. You now have a port group to which to link your VM. To link the VM, choose **Edit Settings**.

Choose the network adapter, which must be of type VMXNET3. From **Network Label**, choose the universal pass-through port group from the drop-down list.

 © 2012 Cisco Systems, Inc.

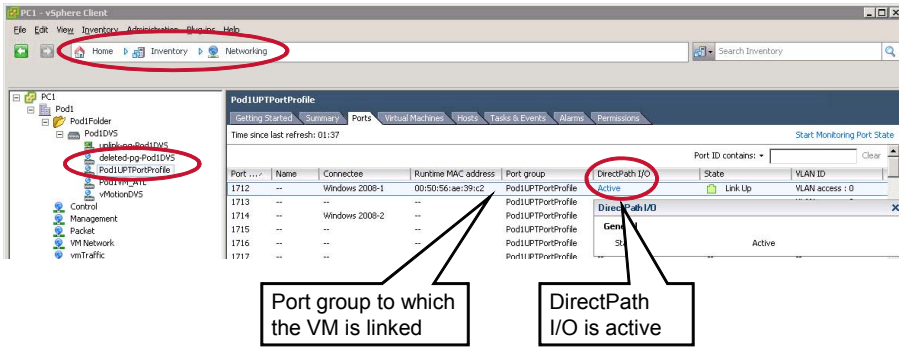
https://t.me/learningnets

Verify Universal Pass-Through Mode

This topic describes how to verify that Cisco VM-FEX runs in universal pass-through mode.

Verify DirectPath I/O in vCenter

- Navigate to **Home > Inventory > Networking**.
- At DVS, select the port group and select the **Ports** tab.



© 2012 Cisco and/or its affiliates. All rights reserved.

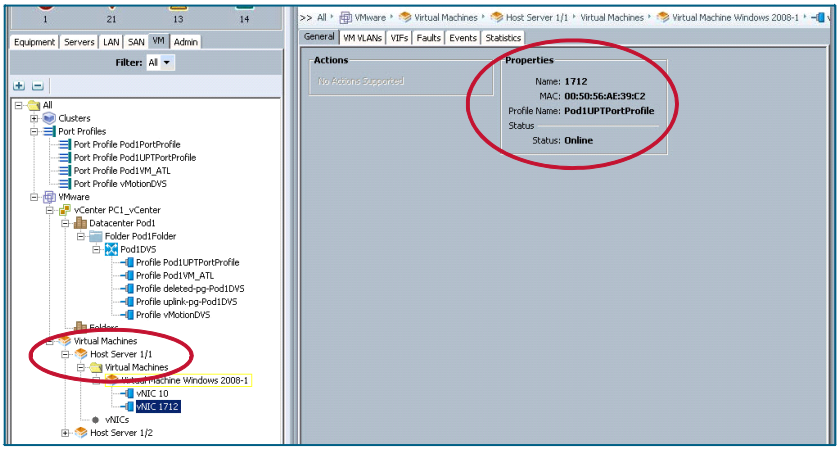
To verify that the VM network adapter is linked and operates in universal pass-through mode, go to **Networking** in vCenter server. Choose the DVS and choose the universal pass-through port group.

Go to the **Ports** tab. You will see the VM to which the dvPort is connected and if the DirectPath I/O is active. If the Direct Path I/O is active, this means that Cisco VM-FEX is operating in universal pass-through mode. Click **Active**. A new window will notify you of the DirectPath status.

https://t.me/learningnets

Verify Universal Pass-Through in Cisco UCS Manager

- The VM will appear in Cisco UCS Manager.
- The vNIC name is the same as the dvPort in vCenter.



© 2012 Cisco and/or its affiliates. All rights reserved.

In Cisco UCS Manager, you can verify that the VM is connected by its appearance in the Virtual Machines section in the VM tab.

Also, when you expand the VM, a vNIC with the same name as the dvPort in vCenter will be available. When you select the VM in the content pane, you will see information on the status of the port and to which port profile it is connected.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

This topic summarizes the primary points that were discussed in this lesson.

Summary

- The VM must be version 8 and the VM network adapter must be of type VMXNET3. The VM memory must be reserved.
- The dynamic vNIC connection policy for universal pass-through requires the usage of the VMWarePassThru Ethernet adapter policy.
- For universal pass-through mode, the BIOS policy must enable VT, Direct Cache, and all Intel Directed IO options.
- Universal pass-through BIOS policy and dynamic vNIC connection policies must be associated with the service profile for the ESXi host.
- The port profile for universal pass-through mode must have the High Performance option enabled.
- From the VM settings, select the universal pass-through port group to link the VM vNIC.
- In vCenter Server, the active DirectPath I/O informs universal pass-through mode.

© 2012 Cisco and/or its affiliates. All rights reserved.

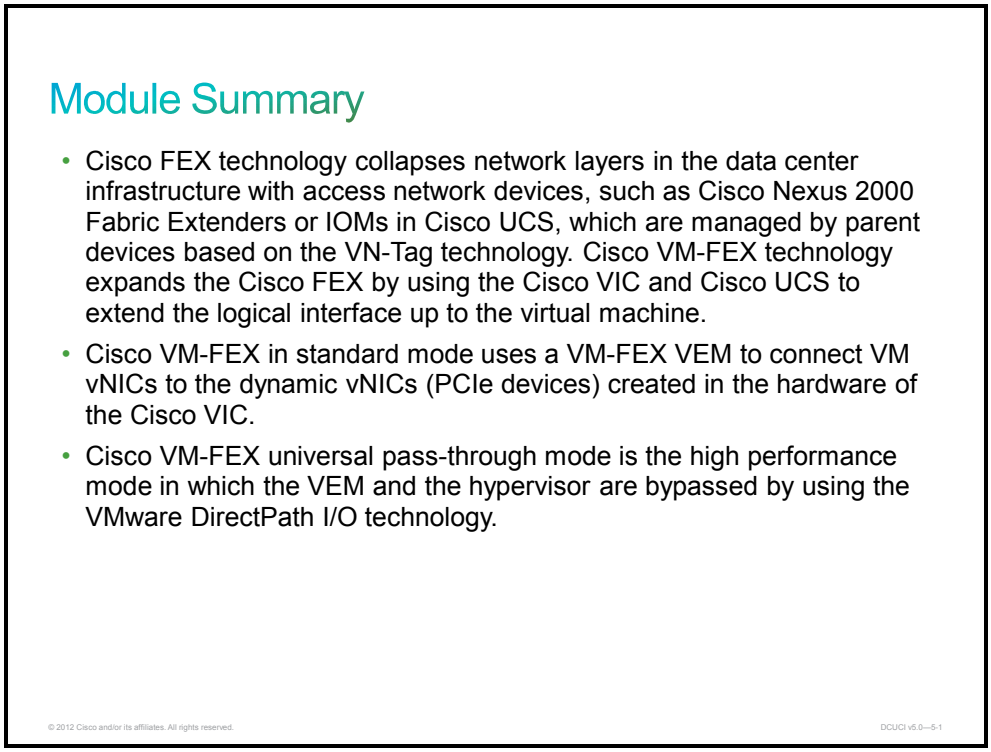
https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module Summary

This topic summarizes the primary points that were discussed in this module.



Cisco Virtual Machine Fabric Extender (VM-FEX) is an extension of Cisco Fabric Extender (FEX) technology. You must have the correct hardware, such as Cisco Unified Computing System (UCS) and Cisco virtual interface cards (VICs) installed in the servers. There are two Cisco VM-FEX modes—standard and universal pass-through. Standard mode is used in the Cisco VM-FEX Virtual Ethernet Module (VEM). Universal pass-through mode, also known as high-performance mode, is used by VMware DirectPath I/O to bypass the hypervisor.

The VMware integration wizard is a feature of Cisco UCS Manager that allows the setup of communication between Cisco UCS Manager and VMware vCenter. Port profiles are provisioned in Cisco UCS Manager and pushed to the vCenter, where they are automatically converted into port groups.

In universal pass-through mode, the port profile must be set to High Performance.

A dynamic vNIC connection policy must be provisioned in the service profile. The policy defines the number of dynamic virtual network interface cards (vNICS) (Peripheral Component Interconnect Express [PCIe] devices) that will be created in the Cisco VIC and the Ethernet adapter policy. The Ethernet adapter policy for standard mode can be VMware, but for universal pass-through mode it must be VMWarePassThru.

A special BIOS policy is required to support Cisco VM-FEX. The policy must be provisioned with specific features enabled, which includes Virtualization Technology, Direct Cache Access, and Intel Directed I/O.

To support Cisco VM-FEX universal pass-through mode, a VM must be version 8, its memory must be reserved, and network adapters must be of type VMXNET3.

https://t.me/learningnets

References

For additional information, refer to these resources:

- *Cisco UCS Manager GUI Configuration Guide*, *Release 2.0* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/2.0/b_UCSM_GUI_Configuration_Guide_2_0.html
- *Cisco UCS Manager CLI Configuration Guide*, *Release 2.0* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.0/b_UCSM_CLI_Configuration_Guide_2_0.html

© 2012 Cisco Systems, Inc.
https://t.me/learningnets

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) Which two choices are native VMware software switches? (Choose two.) (Source: Provisioning Cisco VM-FEX and Cisco VM-FEX Universal Pass-Through)

A) vSwitch
B) vDS
C) Cisco Nexus 1000V
D) Cisco Nexus 2000

Q2) Which two choices are Cisco Nexus 1000V switch components? (Choose two.) (Source: Provisioning Cisco VM-FEX and Cisco VM-FEX Universal Pass-Through)

A) VSM
B) VMA
C) VFM
D) VEM

Q3) Which technology enables Cisco FEX and Cisco VM-FEX? (Source: Provisioning Cisco VM-FEX and Cisco VM-FEX Universal Pass-Through)

A) 802.1Q VLAN tag
B) VN-Link
C) DCBX
D) VN-Tag

Q4) Which component in Cisco UCS Manager is used to create the VM network configuration? (Source: Provisioning Cisco VM-FEX and Cisco VM-FEX Universal Pass-Through)

A) port group
B) port profile
C) port policy
D) port pool

Q5) Which hardware for Cisco UCS is needed for Cisco VM-FEX? (Source: Provisioning Cisco VM-FEX and Cisco VM-FEX Universal Pass-Through)

A) Cisco IMC
B) IOM
C) LSI RAID controller
D) Cisco VIC

Q6) Which two options are ways to install Cisco VM-FEX VEM software? (Choose two.) (Source: Provisioning Cisco VM-FEX)

A) vCenter Update Manager
B) service profile
C) manual installation
D) Cisco UCS Manager software update and activate

https://t.me/learningnets

Q7) From where can you download Cisco VM-FEX VEM VIB software? (Source: Provisioning Cisco VM-FEX)

A) Apple AppStore
B) Cisco UCS Manager
C) Google Play Store
D) Microsoft.com

Q8) Which two options are methods to set up VMware integration? (Choose two.) (Source: Provisioning Cisco VM-FEX)

A) Cisco UCS service profile
B) Cisco UCS Manager VMware integration wizard
C) vCenter Server in linked mode
D) manual
E) VMware vCenter Update Manager

Q9) How many plug-ins are you required to install in vCenter 4.0 Update 1 or later? (Source: Provisioning Cisco VM-FEX)

A) 1
B) 2
C) 3
D) 4

Q10) Which two policies are required in the ESXi host service profile to use the Cisco VM-FEX? (Choose two.) (Source: Provisioning Cisco VM-FEX)

A) local storage policy
B) BIOS policy
C) dynamic vNIC connection policy
D) scrub policy

Q11) Which three requirements must be met for the VM to support Cisco VM-FEX universal pass-through mode? (Choose three.) (Source: Provisioning Cisco VM-FEX Universal Pass-Through)

A) virtual machine version 8
B) virtual machine version 6 or later
C) virtual machine memory reserved
D) virtual machine vCPU reserved
E) VMXNET3 network adapter
F) E1000 network adapter
G) VMXNET2 network adapter

Q12) Which VMware technology is used to support Cisco VM-FEX universal pass-through mode? (Source: Provisioning Cisco VM-FEX Universal Pass-Through)

A) pool reservation
B) DirectPath I/O
C) fault tolerance
D) Site Recovery Manager

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Q13) Which Ethernet adapter policy must be specified and used in the dynamic vNIC connection policy for Cisco VM-FEX universal pass-through mode? (Source: Provisioning Cisco VM-FEX Universal Pass-Through)

A) VMware
B) VMwarePassthru
C) Oracle
D) Hyper-V

Q14) Which three BIOS features must be enabled in a BIOS policy to support Cisco VM-FEX universal pass-through mode? (Choose three.) (Source: Provisioning Cisco VM-FEX Universal Pass-Through)

A) Quiet Boot
B) VT
C) Direct Cache Access
D) All Intel Directed I/O features
E) Turbo Boost
F) Hyperthreading

Q15) Which port profile setting enables universal pass-through mode? (Source: Provisioning Cisco VM-FEX Universal Pass-Through)

A) Specify QoS Policy.
B) Set the Host Network IO Performance to High Performance.
C) Set the Max Ports to 32.
D) Set a Pin Group.

https://t.me/learningnets

Module Self-Check Answer Key

Q1) A, B

Q2) A, D

Q3) D

Q4) B

Q5) D

Q6) A, C

Q7) B

Q8) B, D

Q9) A

Q10) B, C

Q11) A, C, E

Q12) B

Q13) B

Q14) B, C, D

Q15) B

© 2012 Cisco Systems, Inc.

https://t.me/learningnets