DCUCI

Implementing Cisco Data Center Unified Computing

Volume 1

Version 5.0

Student Guide

Text Part Number: 97-3200-01

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

Students, this letter describes important course evaluation access information!

Welcome to Cisco Systems Learning. Through the Cisco Learning Partner Program, Cisco Systems is committed to bringing you the highest-quality training in the industry. Cisco learning products are designed to advance your professional goals and give you the expertise you need to build and maintain strategic networks.

Cisco relies on customer feedback to guide business decisions; therefore, your valuable input will help shape future Cisco course curricula, products, and training offerings. We would appreciate a few minutes of your time to complete a brief Cisco online course evaluation of your instructor and the course materials in this student kit. On the final day of class, your instructor will provide you with a URL directing you to a short post-course evaluation. If there is no Internet access in the classroom, please complete the evaluation within the next 48 hours or as soon as you can access the web.

On behalf of Cisco, thank you for choosing Cisco Learning Partners for your Internet technology training.

Sincerely,

Cisco Systems Learning

https://t.me/learningnets

https://t.me/learningnets

Table of Contents

Volume 1

Course Introduction ***1***

Overview 1
Learner Skills and Knowledge 2
Course Goal and Objectives 3
Course Flow 4
Additional References 5
Cisco Glossary of Terms 6
Training Curriculum 7
Training Curriculum for Cisco Unified Computing Support Specialist 8
Cisco Online Education Resources 9
Introductions 11

Implement Cisco UCS C-Series Rack Servers ***1-1***

Overview 1-1
Module Objectives 1-1

Implementing Cisco R-Series Rack Enclosures **1-3**

Overview 1-3
Objectives 1-3
Unpack the Cisco R42610 Rack Enclosure 1-4
Remove the Cisco R-Series Rack from the Pallet 1-10
Secure the Cisco R-Series Rack to the Floor 1-12
Join Cisco R42610 Racks into a Suite 1-13
Install a Cisco RP208-30-U-1 PDU 1-14
Remove and Install Side Panels 1-19
Remove and Install Cisco R-Series Rack Doors 1-20
Use the Cabling Portholes 1-22
Summary 1-23

Installing Cisco UCS C-Series Server Hardware **1-25**

Overview 1-25
Objectives 1-25
ESD Precautions 1-26
Opening Cisco UCS C-Series Cases 1-28
PCIe Riser Cards in Cisco UCS C-Series Models 1-33
CPU Population Rules 1-38
Color Coding of Internal Cisco UCS C-Series Components 1-40
DRAM Installation and Population Rules 1-41
Fan Replacement 1-45
Power Supply Replacement 1-50
Summary 1-51

Installing Cisco UCS C-Series Servers in a Cisco R-Series Rack Enclosure **1-53**

Overview 1-53
Objectives 1-53
Install the Slide-Rail Assembly into the Cisco R42610 Rack Enclosure 1-54
Attach the Mounting Brackets to the Server 1-57
Insert the Server into the Slide Rail 1-58
Attach the Cable Management Arm 1-59
Connect the Cisco UCS C-Series Server to the PDU 1-60
Connect Management and Data Cables 1-61
Summary 1-62

https://t.me/learningnets

Updating Cisco UCS C-Series Firmware with the Host Upgrade Utility 1-63
Overview 1-63
Objectives 1-63
Cisco UCS Host Upgrade Utility 1-64
Enable KVM and Virtual Media 1-67
Session Options in the KVM 1-69
Virtual Media and the Cisco UCS Host Upgrade Utility ISO Image 1-72
Upgrade All Components 1-75
Summary 1-79
Provisioning Monitoring and Logging on the Cisco UCS C-Series Server 1-81
Overview 1-81
Objectives 1-81
Provision SNMP 1-82
Provision Syslog Destinations 1-88
Access the System Event Log 1-89
Export Technical Support Information 1-90
Summary 1-92
Provisioning LAN and SAN Connectivity in the Cisco Integrated Management Controller 1-93
Overview 1-93
Objectives 1-93
Provision the Cisco UCS P81E VIC to Allow FCoE 1-94
Provision Locally Administered MAC Addresses on Ethernet Interfaces 1-96
Enable RSS on Ethernet Adapters 1-98
Provision Locally Administered WWNN Addresses 1-99
Provision the Fibre Channel Boot Target 1-101
Summary 1-103
References 1-103
Provisioning RAID on the Cisco UCS C-Series Server 1-105
Overview 1-105
Objectives 1-105
RAID Characteristics 1-106
Boot the Server and Access the LSI MegaRAID Interface 1-108
Add Hard Drives to a RAID 5 Array 1-111
Summary 1-117
Installing VMware ESXi on the Cisco UCS C-Series Server Local RAID Array 1-119
Overview 1-119
Objectives 1-119
Open a KVM Session 1-120
Map Virtual Media to the ESXi Installer 1-123
Install ESXi on the Local RAID Array 1-126
Boot ESXi from the Local RAID Array 1-131
Configure a Management IP Address for the ESXi Server 1-134
Connect to the ESXi Server with the VMware vSphere Client Utility 1-140
Summary 1-147
Module Summary 1-149
References 1-150
Module Self-Check 1-151
Module Self-Check Answer Key 1-158

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Manage the Cisco UCS B-Series ***2-1***

Overview 2-1
Module Objectives 2-1

Implementing RBAC **2-3**

Overview 2-3
Objectives 2-3
RBAC in the Cisco UCS B-Series 2-4
Implement Local Users, Roles, and Privileges 2-17
Implement Organizations and Locales 2-20
Effective Rights of a User as an Intersection of Roles and Locales 2-24
Implement LDAP Providers and Provider Groups 2-27
Implement LDAP and Microsoft Active Directory as an External Service 2-32
Implement Cisco UCS Role Mapping 2-34
Summary 2-36

Managing and Upgrading Cisco UCS B-Series Firmware **2-37**

Overview 2-37
Objectives 2-37
Finding Cisco UCS Firmware Packages 2-38
Update Cisco UCS Firmware 2-45
Upgrading the Mezzanine Adapter, Cisco Integrated Management Controller, and IOM Firmware 2-50
Software Updates on the Fabric Interconnect 2-54
Requirements for Firmware Updates via Host Firmware Packages 2-57
Differences in Firmware Processes 2-60
Update and Activate the Hardware Capability Catalog 2-61
Summary 2-66

Implementing Backup, Import, and Restore of the Cisco UCS Manager Database **2-67**

Overview 2-67
Objectives 2-67
Backup Types in the Cisco UCS Manager Database 2-68
Import Operation vs. a Disaster Recovery Restore Operation 2-71
Implement a Backup Job 2-73
Implement Backup Jobs to Preserve Abstracted Identities 2-74
Verify the Backup 2-75
Restore the AAA User Database with an Import Job 2-77
Verify AAA User Database Restoration 2-80
Disaster Recovery Restore on the Cisco UCS 6100/6200 Series Fabric Interconnect 2-81
Summary 2-83

Implementing Logging and Monitoring **2-85**

Overview 2-85
Objectives 2-85
Cisco UCS Manager Interfaces 2-86
Fault Management System and Fault Severity Levels 2-87
Track Administrative Changes in the Cisco UCS Manager Audit Log 2-92
Cisco UCS Manager Operations Subject to FSM Validation 2-95
Implement Logging Options 2-99
System Event Log and Log Policies 2-100
Implement the Smart Call Home Feature 2-102
Validate the Smart Call Home Feature 2-107
Configure Settings for Logs, Events, and Faults 2-108
Configure SPAN for Protocol Analysis 2-109
Summary 2-113

https://t.me/learningnets

Implementing High Availability 2-115
Overview 2-115
Objectives 2-115
High-Availability Cluster Connection Requirements 2-116
Intercluster Communications and Cisco UCS Manager Database Synchronization 2-119
Partition-in-Time and Partition-in-Space Split-Brain Conditions 2-125
Resolving a Split-Brain Issue in the High-Availability Cluster 2-127
Modifying Cluster IP Addressing 2-128
Summary 2-129
Module Summary 2-131
References 2-132
Module Self-Check 2-133
Module Self-Check Answer Key 2-137

Implement Cisco UCS B-Series Connectivity ***3-1***

Overview 3-1
Module Objectives 3-1
Implementing Cisco UCS B-Series Physical Connectivity **3-3**
Overview 3-3
Objectives 3-3
I/O Uplinks and Bandwidth Oversubscription in Generation 2 Hardware 3-5
Cisco UCS 2204/2208XP IOM Architecture 3-11
I/O Uplinks and Bandwidth Oversubscription in Generation 1 Hardware 3-12
Cisco UCS 2104XP IOM Architecture 3-16
Cisco UCS VIC 1280 and VIC 1240 Features 3-18
Virtual Interfaces on Cisco UCS M81KR VIC and the VIC 1280 3-20
New Mezzanine Cards 3-22
Cisco Integrated Management Controller in Cisco UCS B-Series Blade Servers 3-25
Creating Port Channels with Generation 2 Hardware 3-26
Server and Uplink Port Personalities in the Cisco UCS Fabric Interconnect 3-28
Chassis Discovery Process 3-29
Configuring the Chassis Discovery Policy 3-31
Summary 3-33
Installing Cisco UCS B-Series Hardware **3-35**
Overview 3-35
Objectives 3-35
ESD Precautions for Installing Cisco UCS B-Series Components 3-36
Open Half- and Full-Slot Blade Server Cases 3-37
Install Rack-Mount Slides 3-41
Install and Remove CPU, RAM, and Mezzanine Cards 3-45
Install and Remove Local Hard Drives 3-50
Install Half- and Full-Slot Blade Servers 3-53
Install IOMs and Power Supplies 3-57
Install and Remove Fan Units 3-59
Install and Remove SFP+ Copper Twinax and Optical Modules 3-61
Summary 3-66

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Implementing Cisco UCS B-Series LAN Connectivity 3-67
Overview 3-67
Objectives 3-67
Uplink, Server, Appliance, FCoE Storage, and Monitoring Ethernet Port Personalities 3-68
Requirements and Configuration of Uplink Port Channels 3-74
Importance of End-Host Mode in Maintaining a Loop-Free Topology 3-75
End-Host Mode vs. Switching Mode 3-78
Configuring VLANs in Cisco UCS Manager 3-79
Role of vNICs 3-81
Automatic Pinning and Recovery from Failure 3-83
Configuring Manual Pinning and Recovery from Failure 3-86
Configuring Disjoint Layer 2 Domains 3-88
Summary 3-92
Implementing Cisco UCS B-Series SAN Connectivity 3-93
Overview 3-93
Objectives 3-93
Fibre Channel Switching 3-94
NPV Mode 3-96
Fibre Channel Uplink, Storage, and Monitoring Port Personalities 3-99
Benefits and Drawbacks of Fibre Channel Switching and NPV 3-103
N-Port ID Virtualization 3-104
VSAN Support in Cisco UCS Manager 3-105
Role of vHBAs 3-108
Automatic Pinning and Recovery from Failure 3-110
Configuring Manual Pinning and Recovery from Failure 3-115
Ethernet Failover and Fibre Channel Multipath I/O Recovery 3-118
Summary 3-119
Module Summary 3-121
References 3-122
Module Self-Check 3-123
Module Self-Check Answer Key 3-127

https://t.me/learningnets

https://t.me/learningnets

DCUCI

Course Introduction

Overview

This intensive five-day, hands-on course focuses on deployment and operations of the Cisco Unified Computing System (UCS) B-Series Blade Servers and C-Series Rack Servers. You will learn how to configure and manage Cisco UCS servers using Unified I/O networking for LAN and SAN connectivity, and how to virtualize server hardware identifiers to enable rapid recovery of server operating system images through service profile mobility.

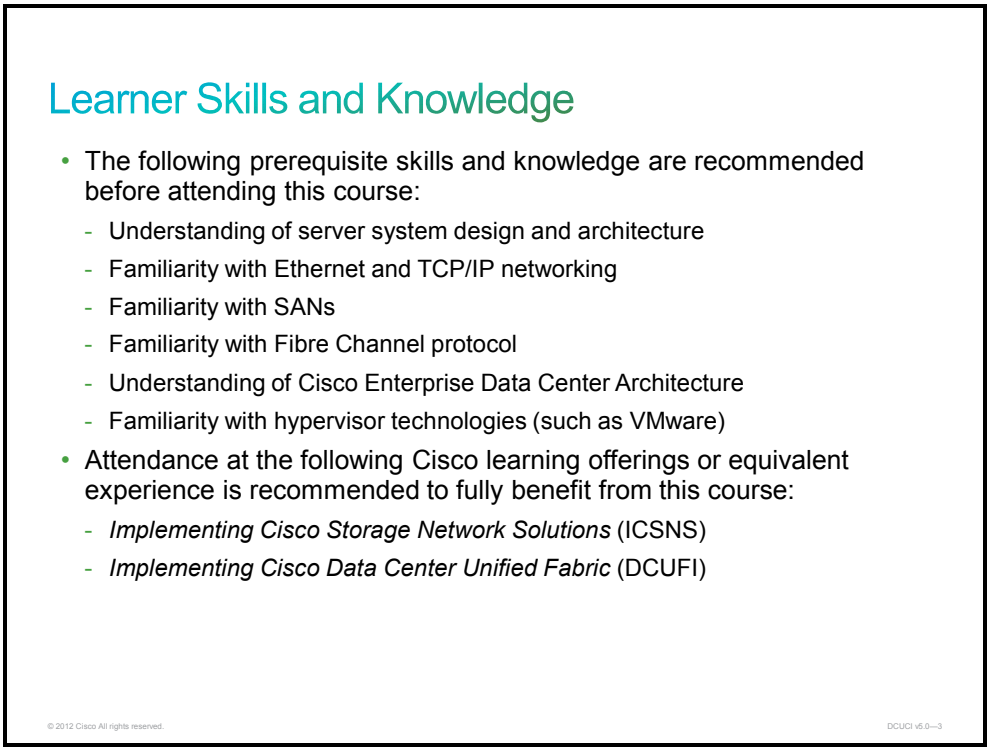
In labs, you will practice configuring fault tolerance, implementing role-based access control (RBAC), backing up and restoring system configurations, and using the monitoring and troubleshooting tools in Cisco UCS Manager and Cisco Integrated Management Controller.

You will gain hands-on experience working with Cisco C-Series servers in standalone mode, provisioning Cisco B-Series servers, installing and configuring the Cisco Virtual Interface Card (VIC) and VMware Pass-Through Switching (PTS), and leveraging VMware vSphere 4.1 on Cisco UCS B-Series and C-Series infrastructure.

https://t.me/learningnets

Learner Skills and Knowledge

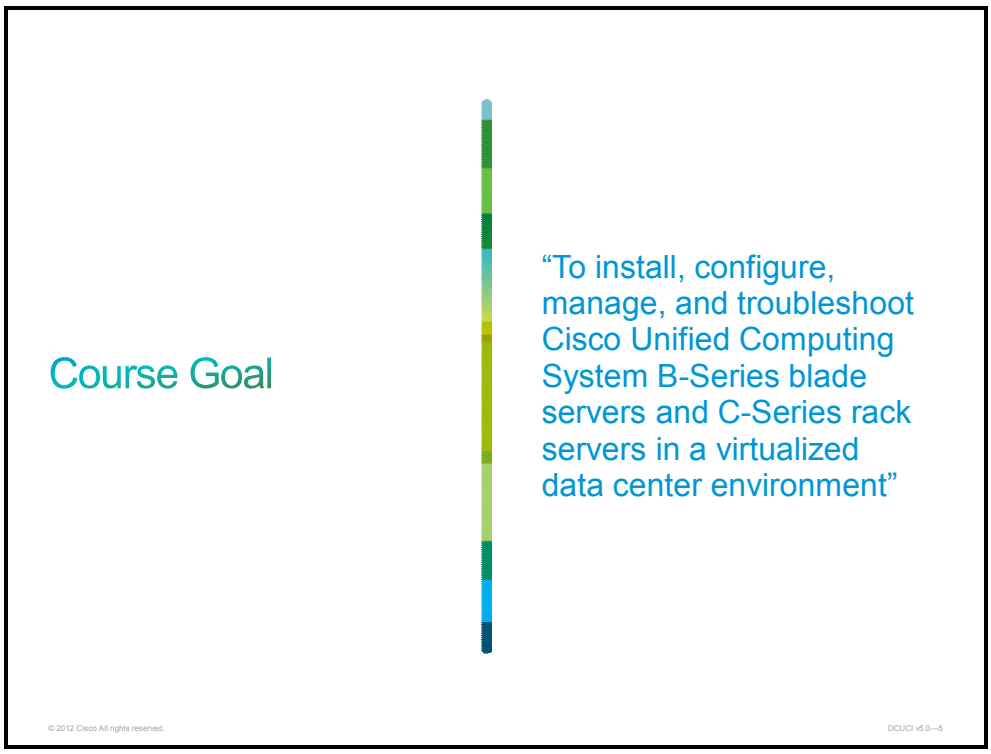
This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should first complete to benefit fully from this course.



https://t.me/learningnets

Course Goal and Objectives

This topic describes the course goal and objectives.



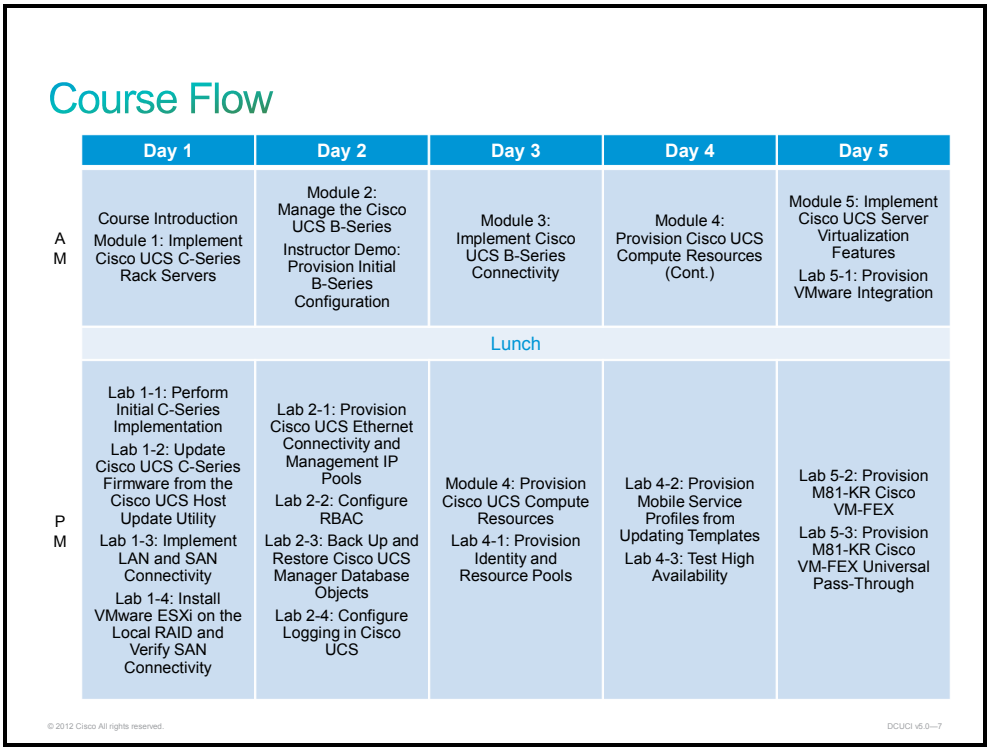
Upon completing this course, you will be able to meet these objectives:

- Install and provision Cisco UCS C-Series rack servers in standalone mode, install Cisco R-Series racks, provision the Cisco Integrated Management Controller, update the server firmware, and install operating systems like VMware ESXi
- Implement high availability, manage the Cisco UCS, provision administrator access, and maintain Cisco UCS
- Install and provision Cisco UCS B-Series blade servers in the Cisco UCS 5108 blade chassis, know the characteristics of the different models of Cisco UCS I/O modules (IOM) and how to install them, understand the different connectivity topologies and options and how the Cisco Nexus Operating System (NX-OS) treats Ethernet and Fibre Channel traffic, and be acquainted with generation 2 hardware and all the newly introduced features
- 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
- Implement virtualization features unique to Cisco UCS that improve performance and manageability

https://t.me/learningnets

Course Flow

This topic presents the suggested flow of the course materials.



The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

https://t.me/learningnets

Additional References

This topic presents the Cisco icons and symbols that are used in this course, as well as information on where to find additional technical references.

Cisco Icons and Symbols

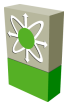
Cisco UCS 6100/6200 Series Fabric Interconnect

Cisco UCS 5108 Blade Chassis

Cisco UCS C-Series

Cisco Nexus 5000

Cisco Nexus 7000


Cisco MDS 9500 Multilayer Director

Cisco MDS 9200 Multilayer Switch

Cisco MDS 9100 Fabric Switch

© 2012 Cisco All rights reserved.

Cisco Icons and Symbols (Cont.)

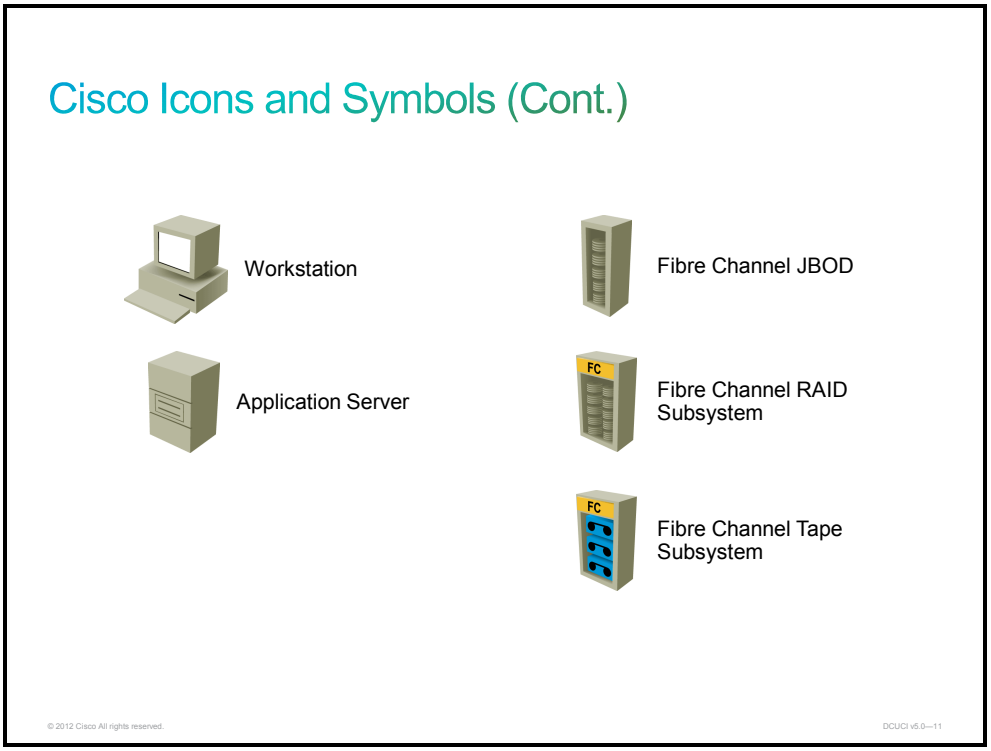
Cisco Nexus 2000 Series Fabric Extender (FEX)

Cisco Nexus 1000V Virtual Ethernet Module (VEM)

Cisco Nexus 1000V Virtual Supervisor Module (VSM)

© 2012 Cisco All rights reserved.

https://t.me/learningnets



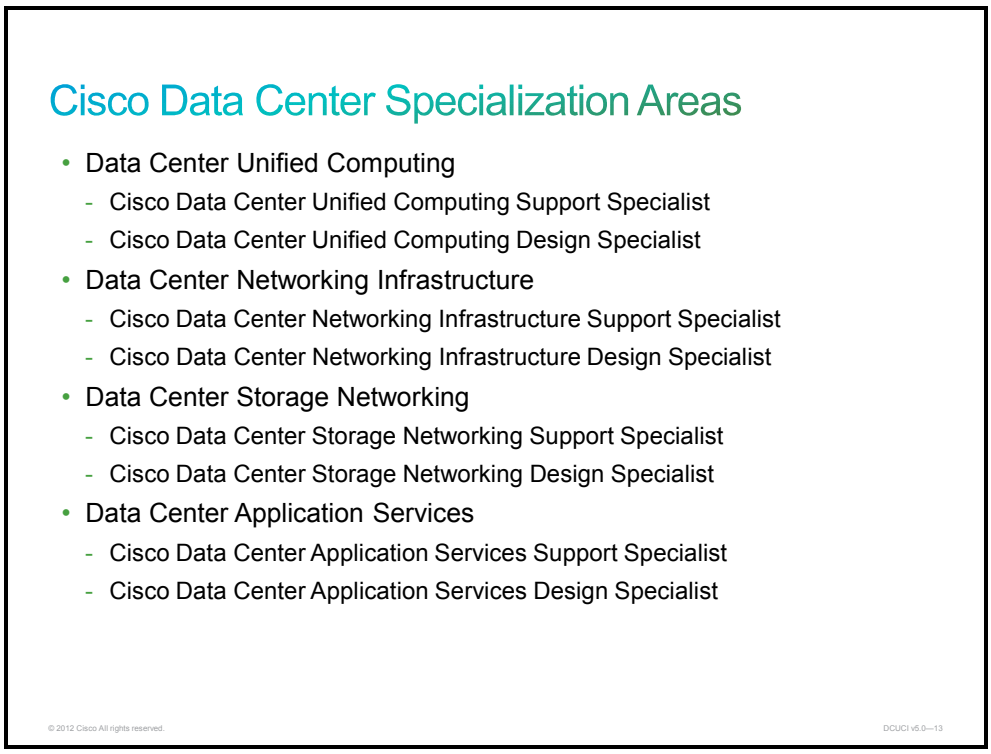
Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at http://docwiki.cisco.com/wiki/Internetworking_Terms_and_Acronyms_%28ITA%29_Guide.

https://t.me/learningnets

Training Curriculum

This topic presents Cisco data center certification options available for students to pursue.

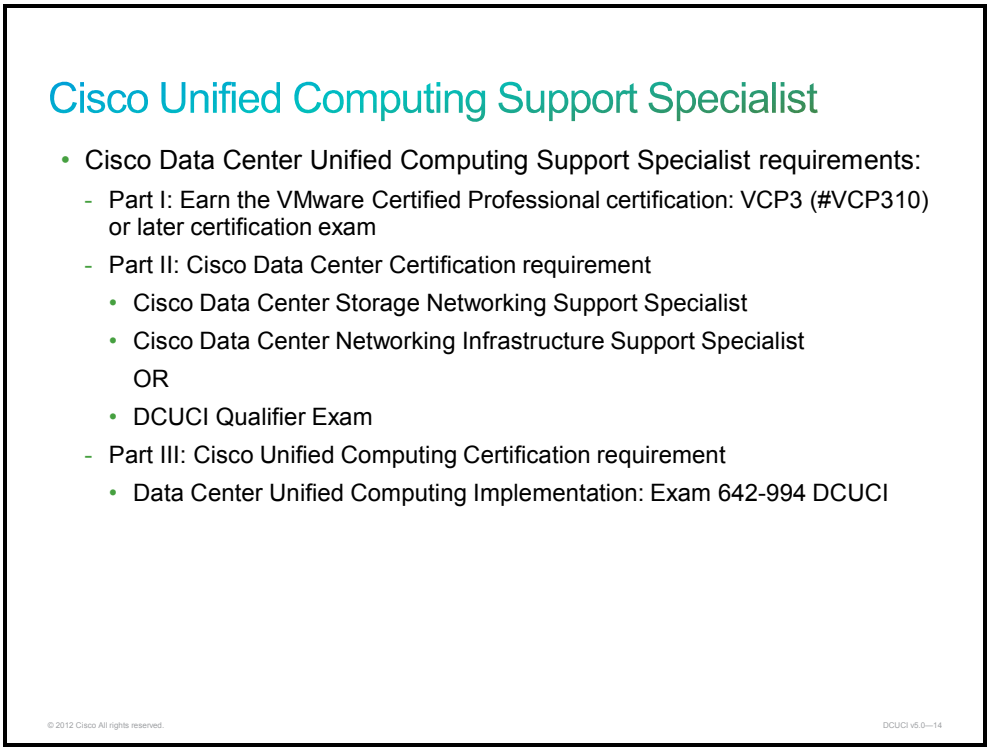


For more information on certifications, go to http://www.cisco.com/go/certifications.

https://t.me/learningnets

Training Curriculum for Cisco Unified Computing Support Specialist

This subtopic presents the exam requirements to achieve Cisco Data Center Unified Computing Support Specialist certification.



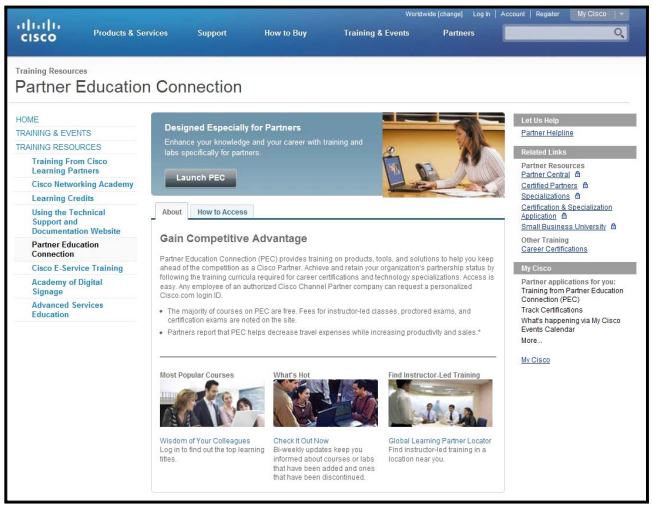
https://t.me/learningnets

Cisco Online Education Resources

This topic presents Cisco online training resources that complement this course.

Cisco Partner Education Connection

http://www.cisco.com/go/pec



© 2012 Cisco All rights reserved.

DCUCI v5.0—16

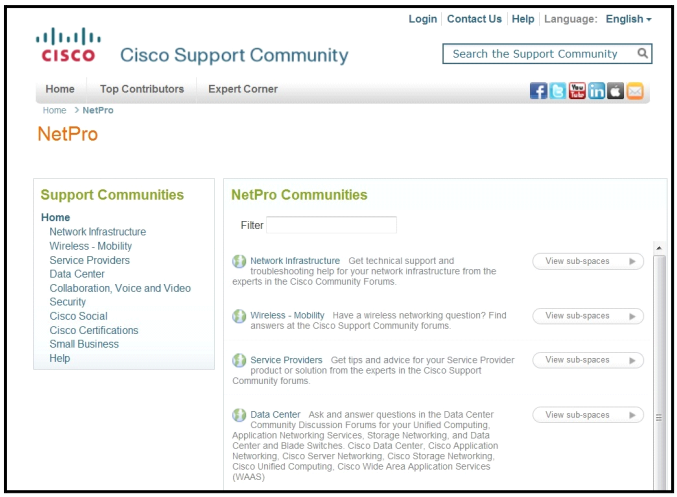
Cisco Partner Education Connection provides training on products, tools, and solutions to help you keep ahead of the competition as a Cisco Partner. Achieve and advance your partnership status for your organization by following the training curriculum that is required for career certifications and technology specializations. Access is easy. Any employee of an authorized Cisco Channel Partner company can request a personalized Cisco.com login ID.

- Most courses on Cisco Partner Education Connection are free. Fees for instructor-led classes, proctored exams, and certification exams are noted on the site.
- Partners report that Cisco Partner Education Connection helps decrease travel expenses while increasing productivity and sales.

https://t.me/learningnets

Cisco NetPro Forums

https://supportforums.cisco.com/community/netpro



© 2012 Cisco All rights reserved.

Cisco NetPro forums are part of the online Cisco Support Community. Cisco NetPro forums are designed to share configurations, issues, and solutions among a community of experts. The forums are conveniently arranged into distinct categories to make finding or supplying solutions a simple process.

Cisco Learning Network

http://www.cisco.com/go/learnnetspace

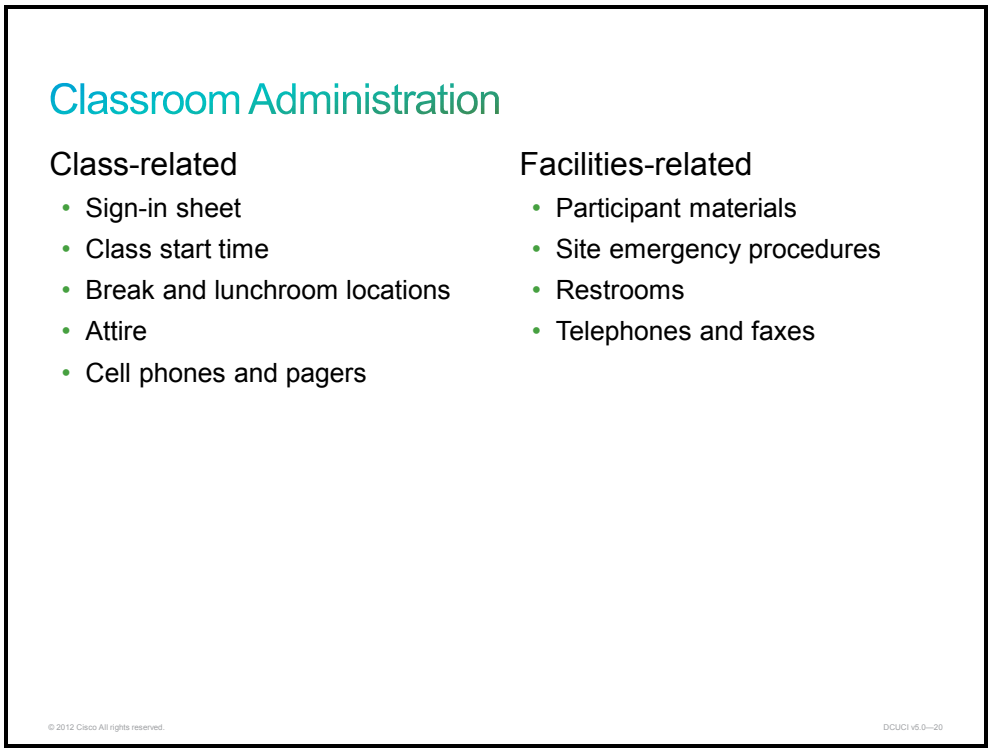
© 2012 Cisco All rights reserved.

The Cisco Learning Network is a repository where certification seekers can find the latest information on certification requirements, study resources, and discuss certification with others. Whether you are working toward certification at the Associate, Professional, or Expert level, the Cisco Learning Network is always available to assist with reaching your certification goals.

https://t.me/learningnets

Introductions

This topic presents the general administration of the course and an opportunity for student introductions.



The instructor will brief students on specific site requirements and the location of restrooms, break rooms, and emergency procedures.

https://t.me/learningnets

Introductions

- Your name
- Your company
- Prerequisite skills
- Brief history
- Objective

© 2012 Cisco All rights reserved.

The instructor encourages students to introduce themselves to the class to learn about their experience, environment, and specific learning goals for the course.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module 1

Implement Cisco UCS C-Series Rack Servers

Overview

This module describes installation and configuration of the Cisco Unified Computing System (UCS) C-Series rack-mount servers.

Module Objectives

Upon completing this module, you will be able to install and provision Cisco UCS C-Series Rack Servers in standalone mode, install Cisco R-Series Racks, provision the Cisco Integrated Management Controller, update the server firmware, and install operating systems like VMware ESXi.

This ability includes being able to meet these objectives:

- Implement Cisco R-Series rack enclosures
- Install Cisco UCS C-Series servers
- Install Cisco UCS C-Series servers in a Cisco R-Series rack enclosure
- Update Cisco C-Series firmware with the host upgrade utility
- Provision monitoring and logging on the Cisco C-Series server
- Provision LAN and SAN connectivity in Cisco Integrated Management Controller
- Provision RAID on the Cisco C-Series server
- Install VMware ESXi on the Cisco C-Series server local RAID array

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 1

Implementing Cisco R-Series Rack Enclosures

Overview

Servers in data centers are physically installed in racks. In this lesson, you will become familiar with the Cisco R Series rack enclosure.

Objectives

Upon completing this lesson, you will be able to install Cisco R-Series rack enclosures in the data center. This ability includes being able to meet these objectives:

- Unpack the Cisco R42610 rack enclosure
- Remove the Cisco R-Series rack from the pallet
- Secure the Cisco R-Series rack to the floor
- Join Cisco R42610 racks into a suite
- Install a Cisco RP208-30-U-1 PDU
- Remove and install side panels
- Remove and install Cisco R-Series rack doors
- Use cabling portholes

https://t.me/learningnets

Unpack the Cisco R42610 Rack Enclosure

This topic describes how to unpack the Cisco R-Series rack.

Cisco R42610 Rack Enclosure

- 42 RU, industry-standard EIA-310-D racks
- Standard and expansion racks
- Perforated front and rear walls for better ventilation
- Ventilated top panel
- Optimized for Cisco UCS and C-Series servers
- Tool-less door removal
- PDU trays for quick, tool-less PDU installation

PDU = power distribution unit

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

Cisco introduced the R42610 rack enclosure, which is optimized for the Cisco Unified Computing System (UCS) and C-Series servers. R42610 enclosures are standard EIA-310-D 42-rack unit (RU) racks. The standard and expansion racks can be used in single-rack or multiple-rack deployments.

Cisco R42610 racks are designed to provide the most effective airflow because the front and rear doors are perforated at 80 percent. The top panel of the rack is ventilated and has four cabling portholes for better cable management.

The front and rear doors are equipped with locks for better security and provide for tool-less removal and installation. The front door can be reversed, in case you need it to open the door in the opposite direction. There are two rear doors, thus requiring less space clearance.

The side panels are formed by an upper and lower piece and are equipped with locks. This configuration provides for easier removal and installation.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

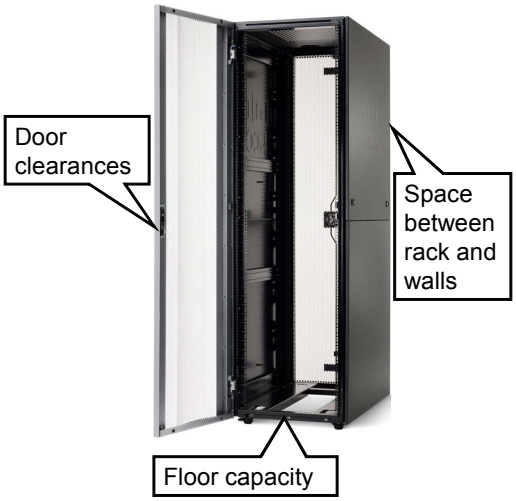
Cisco R42610 Rack Standard and Expansion Features

Feature	Standard	Expansion
Dimensions (H x W x D)	78.74 x 24 x 43.38 in. (2000 x 610 x 1102 mm)	78.74 x 23.58 x 43.38 in. (2000 x 599 x 1102 mm)
Dimensions (H x W x D) with packaging	89 x 33 x 47 in. (2261 x 838 x 1194 mm)	89 x 33 x 47 in. (2261 x 838 x 1194 mm)
Weight with packaging	354 lb (161 kg)	284 lb (129 kg)
Side panels included	Yes	No
Equipment mounting capacity	42 RU	42 RU
Static load capacity	2100 lb (954 kg)	2100 lb (954 kg)
Dynamic load capacity	Not applicable	Not applicable

https://t.me/learningnets

Site Considerations

- Space and clearances
- Tools and documentation
- Safety and ESD considerations
- Power sources and grounding
- Floor loading
  - Empty standard rack weight is 354 lb (161 kg)
  - Empty expansion rack weight is 284 lb (129 kg)
  - Load capacity maximum is 2100 lb (954 kg)



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

When you prepare to deploy Cisco R42610 racks, first make sure that the site is prepared and all precautions have been taken.

The following are important considerations:

- Read the documentation and note all requirements, recommendations, and warnings.
- Be sure that the site is prepared for the rack deployment, which includes ensuring the following:
  - Floor capacity is sufficient.
  - There is enough space for the rack deployment.
  - There will be enough clearance for the rack doors to open.
  - There will be enough space for the correct airflow.
  - All safety recommendations are in place.
  - There are adequate power sources on site and those sources have the correct grounding.
- Follow all recommendations for avoiding ESD risks. Use antistatic sprays, ESD pads, and ESD wrist straps.

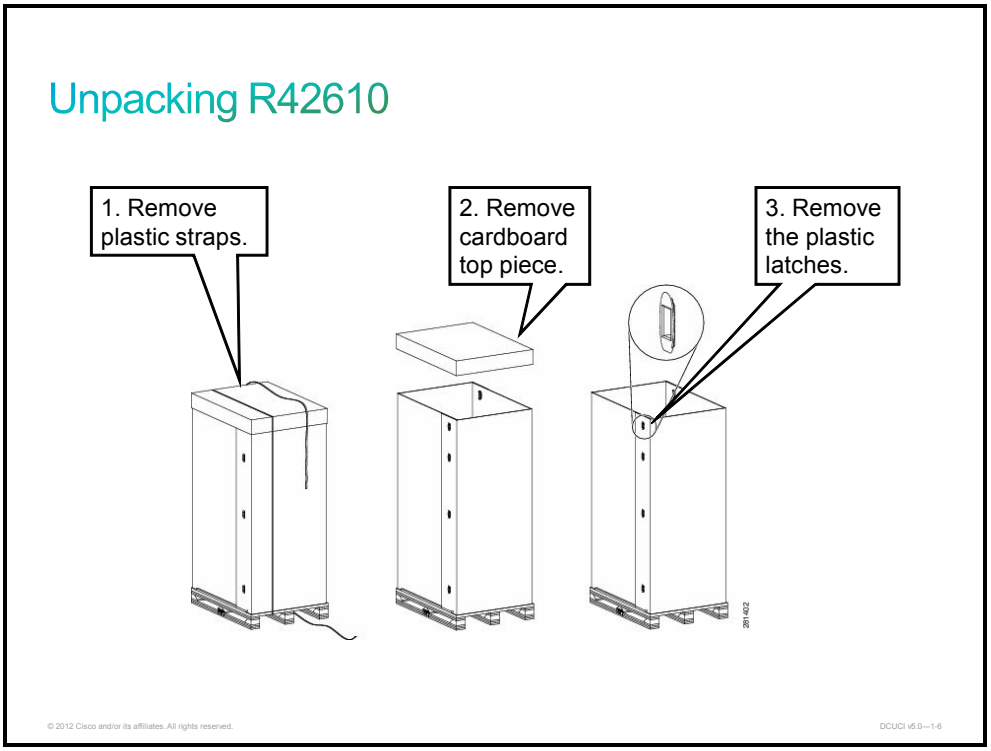
https://t.me/learningnets

- Prepare the needed tools for the rack deployment:
  - Phillips head screwdriver (#2)
  - 4-mm hex driver
  - Pozidriv screwdriver (#3)
  - 3/8-inch or ½-inch flat-head screwdriver (to lower and raise stabilizers)
  - Adjustable wrench (for unbolting system)
  - Allen wrench (to disassemble caster assembly after unit is sited)
  - Standard clippers or knife (to cut packaging binding)
  - Tape measure
  - Level
  - Anchoring bolts
  - Rotary hammer drill
  - Forklift
  - Chain hoist

Because not every precaution can be listed here, it is a best practice to create and work with a checklist. A sample site preparation checklist can be found in the document *Cisco R Series Rack and RP Series PDU Installation Guide* at

http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/rack_power/installation/guide/Rack_PDU.html

https://t.me/learningnets



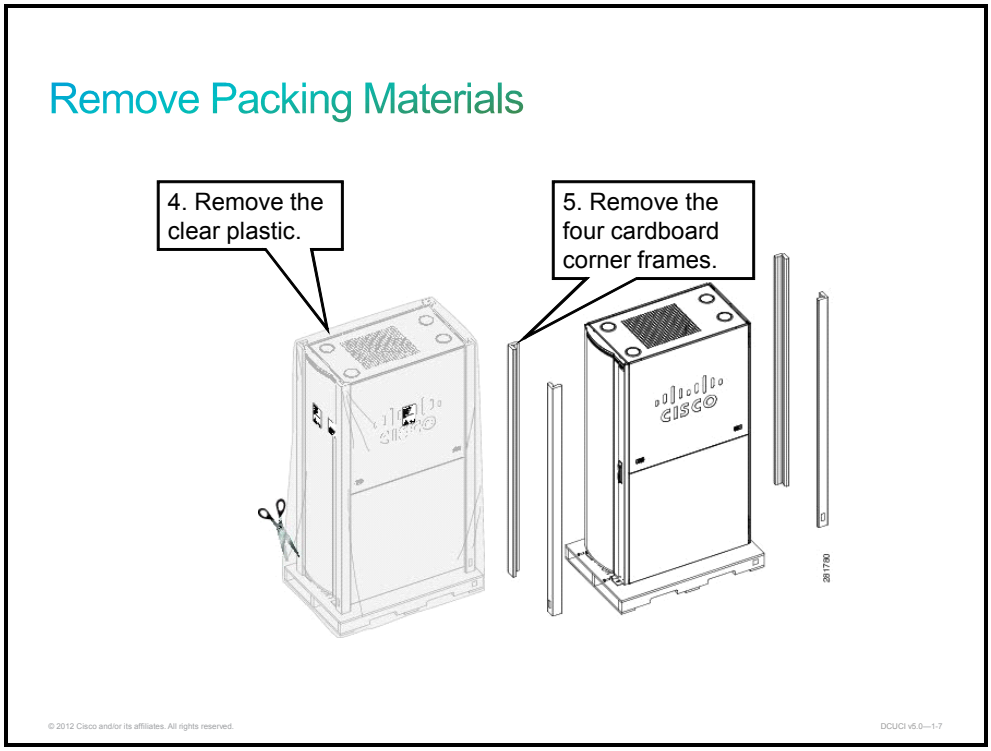
When you receive the Cisco R42610 rack, it will be installed on a pallet and packed. Your first task will be to remove the packing. Follow these steps:

Step 1 Cut and remove the plastic straps.

Step 2 Remove the top cardboard piece.

Step 3 Remove the plastic latches to remove the cardboard packing.

https://t.me/learningnets



Once you have removed the cardboard packing, you have to remove the rest of the rack packing. To do so, follow these steps:

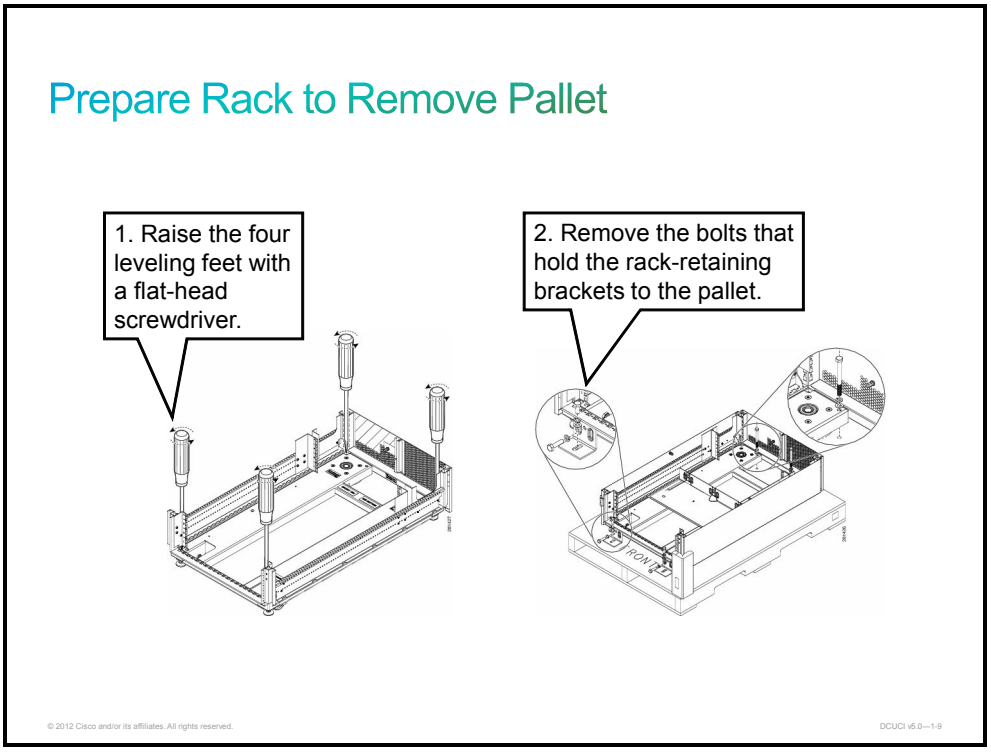
Step 4 Remove the clear plastic by cutting it with scissors or a knife.

Step 5 Remove the four cardboard corner frames.

https://t.me/learningnets

Remove the Cisco R-Series Rack from the Pallet

This topic describes the steps to remove the R42610 rack from the pallet.



After you have removed all of the packing, remove the pallet on which the R42610 rack is installed.

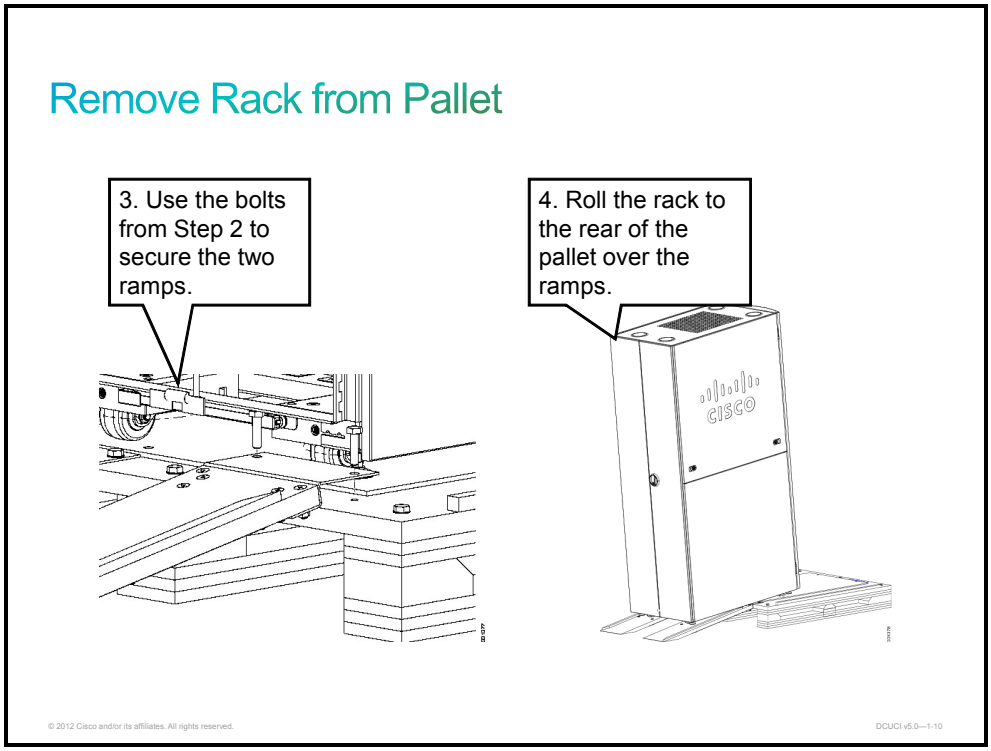
To remove the pallet, follow these steps:

Step 1 Raise the four leveling feet using a flat-head screwdriver.

Step 2 Remove the bolts that hold the rack to the pallet.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



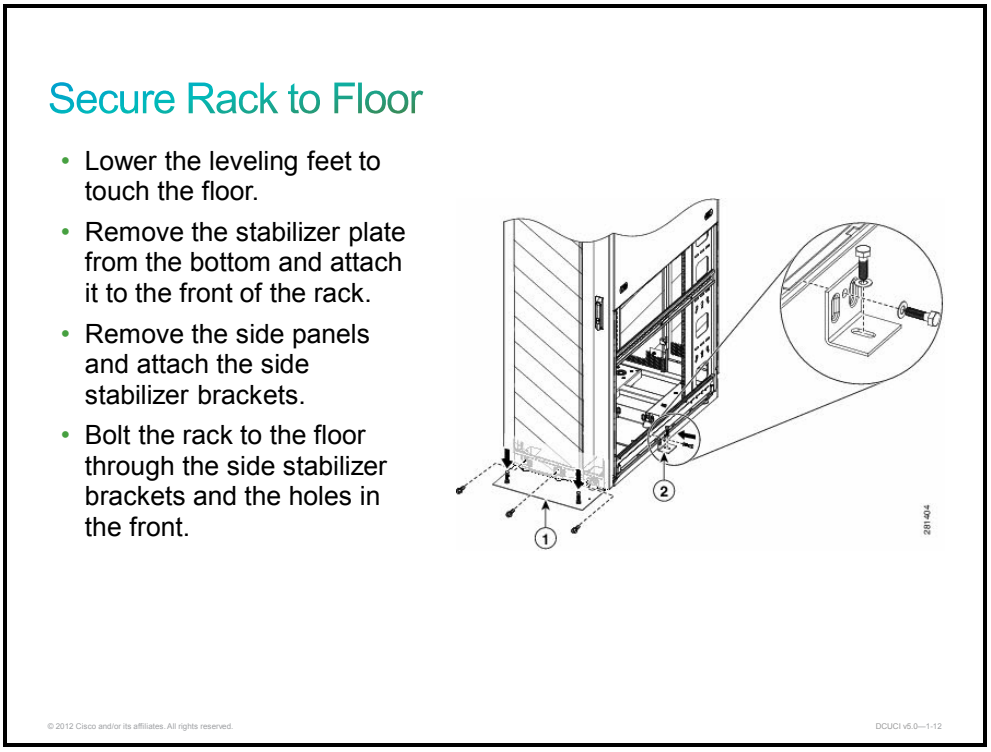
Step 3 Install the two ramps using the bolts from the previous step.

Step 4 Roll the rack off the pallet over the ramps.

https://t.me/learningnets

Secure the Cisco R-Series Rack to the Floor

This topic describes the steps to secure the Cisco R42610 rack to the floor.



When the rack is in its intended location, secure it to the floor. This step avoids the risk of the rack falling under the weight of the equipment that will be installed.

To secure the rack to the floor, follow these steps:

Step 1 Lower the four leveling feet to touch the floor.

Step 2 The front stabilizer plate is installed on the bottom of the rack. Remove the plate from there and attach it to the front of the rack.

Step 3 Attach the side stabilizers. To mount them, you have to remove the side walls.

Step 4 Bolt the rack to the floor through the holes in the side stabilizers and in the front stabilizer plate.

© 2012 Cisco Systems, Inc.

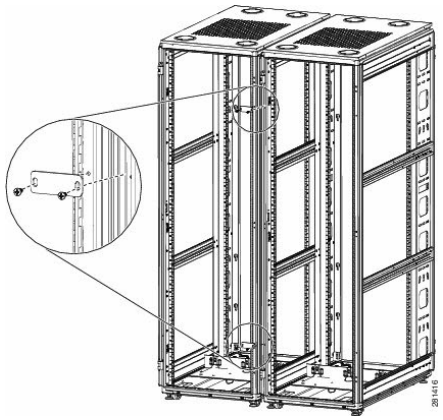
https://t.me/learningnets

Join Cisco R42610 Racks into a Suite

This topic describes how to join Cisco R42610 racks into a suite.

Joining R42610 Racks into a Suite

- You will need the optional rack joining kit (RACK-JOIN-001).
- Install and secure the first rack from the row.
- Remove all doors.
- Use two brackets in the front and two in the rear to join the racks.
- Install the front stabilizer plate to the second rack.
- Join more racks.



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

If you need to install multiple Cisco R42610 racks, you can join them into a suite. To join the racks, you need to have the optional rack-joining kit (RACK-JOIN-001). First, you have to install and secure the first rack from the row. After that, you can join additional racks to it. The procedure to create a suite of racks includes these steps:

Step 1 Install and secure the first rack.

Step 2 Remove all doors.

Step 3 Use two brackets in front to join the second rack.

Step 4 Use two brackets at the rear to join the second rack.

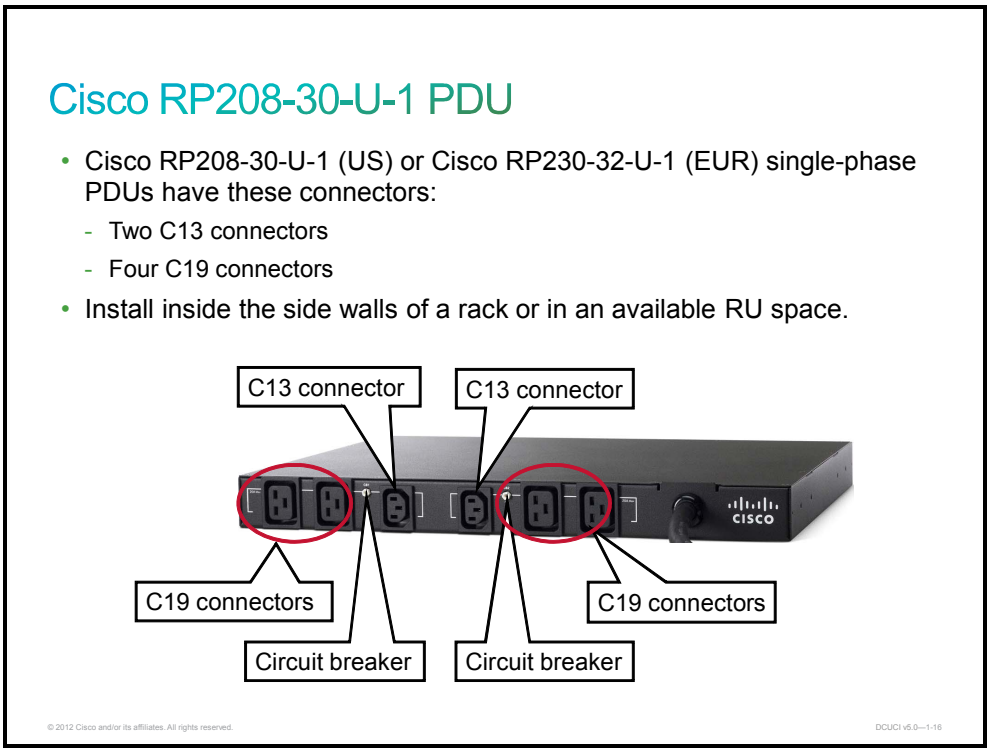
Step 5 Install the front stabilizer plate of the second rack.

Step 6 If you need to attach another rack, repeat the procedure.

https://t.me/learningnets

Install a Cisco RP208-30-U-1 PDU

This topic describes how to install a Cisco RP208-30-U-1 power distribution unit (PDU) in a Cisco R42610 rack.



Cisco has created PDUs for use with the Cisco R42610 racks. The Cisco RP208-30-U-1 (US) and RP230-32-U-1 (EUR) are a single-phase, 1-RU PDUs. The PDU is equipped with two C13 connectors and four C19 connectors. The connectors differ in the cord that is used to plug into facility power. Cisco RP208-30-U-1 PDUs are equipped with two circuit breakers.

These PDUs can be installed in a tower configuration or in 1-RU configuration. When installed in a tower configuration, the PDUs do not occupy server RUs. When installed in 1-RU configuration, each PDU occupies 1 RU.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

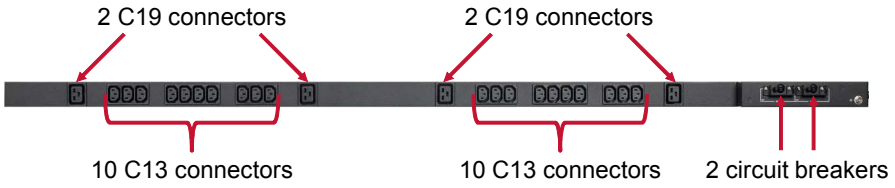
Cisco RP208-30-1P-U-1 Characteristics

Description	1-RU PDU, 2 C13 and 4 C19, Single-Phase, NA, 30 A, Fixed 3M L6-30P
Cisco option part number	RP208-30-1P-U-1
RU size	0/1
Input voltage	200 to 240 VAC ±10%
Frequency	50 to 60 Hz
Amperage	30 A
UL rating	24 A
Input plug	NEMA L6-30P
Cord length	3 m
Output voltage	200 to 240 VAC
Receptacles	▪ 2 IEC 320 C13 ▪ 4 IEC 320 C19
Circuit breakers	2 two-pole 20 A (UL 489)

https://t.me/learningnets

Cisco RP208-30-1P-U-2 PDU

- Cisco RP208-30-1P-U-2 (US) or Cisco RP230-32-1P-U-2 (EUR) single phase PDUs have these connectors:
  - 20 C13 connectors
  - 4 C19 connectors
- This PDU is a zero-RU PDU, meaning it is installed to the plates on the rear of the Cisco R-Series rack. It does not occupy RUs.



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

The Cisco RP208-30-1P-U-2 (US) or RP230-32-1P-U-2 (EUR) are single-phase, zero-RU PDUs. These PDUs are equipped with 20 C13 and four C19 connectors. The PDUs also feature two circuit breakers.

These PDUs are called zero-RU PDUs because they do not consume server RUs when installed in the rack. You can install up to six zero-RU PDUs in a Cisco R42610 rack.

RP208-30-U-2 Characteristics

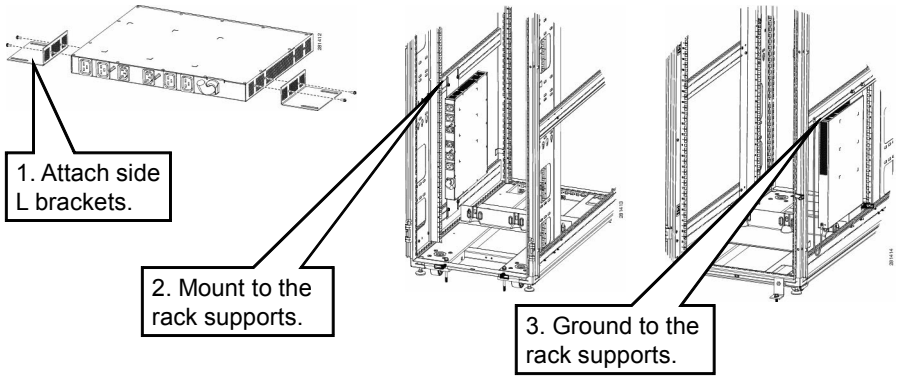
Description	Zero-RU Strip PDU, 20 C13 and 4 C19, Single-Phase, NA, 30 A, Fixed 3M L6-30P
Cisco option part number	RP208-30-1P-U-2
RU size	0
Input voltage	200 to 240 VAC ±10%
Frequency	50 to 60 Hz
Amperage	30 A
UL rating	24 A
Input plug	NEMA L6-30P
Cord length	3 m
Output voltage	200 to 240 VAC
Receptacles	▪ 20 IEC 320 C13 ▪ 4 IEC 320 C19
Circuit breakers	2 two-pole 20 A (UL 489)

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Tower Mount of RP208-30-U-1

- Tower mount configuration does not occupy RU.
- Use the rack-mount kit.



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

For tower mount configuration, follow these steps:

Step 1 Remove the L brackets from the mounting kit.

Step 2 Attach the L brackets on the two sides of the Cisco RP208-30-U-1 PDU.

Step 3 Mount the PDU to the rack supports.

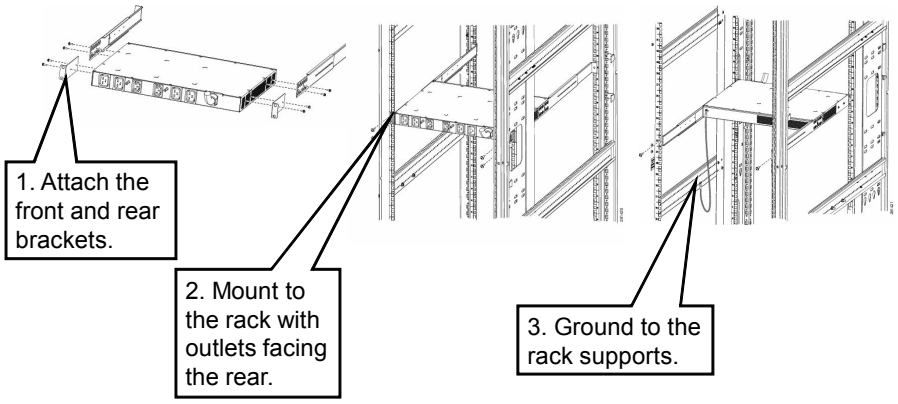
Step 4 Ground the PDU to the rack support by using a no. 12 self-tapping screw.

Step 5 Connect the PDU to the AC power source.

https://t.me/learningnets

1 RU Mount of RP208-30-U-1

- 1 RU mount configuration occupies RU
- Requires square rack holes



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

For the 1-RU mount configuration, follow these steps:

Step 1 Attach the left and right L brackets using eight M4 Phillips-head screws.

Step 2 Slide the rear L bracket onto the rear bracket.

Step 3 Install eight cage nuts in the rack square holes.

Step 4 Install the PDU with the outlets facing the rear.

Step 5 Ground the PDU to the rack supports.

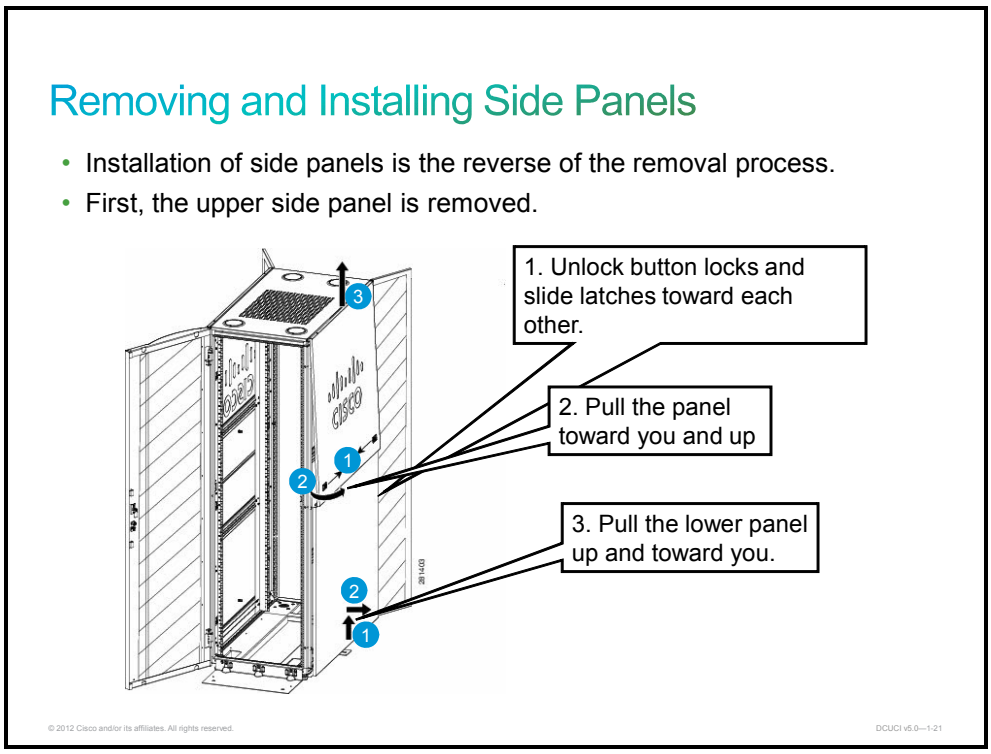
Step 6 Connect the PDU to the AC power source.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Remove and Install Side Panels

This topic describes how to remove and install side panels.



The Cisco R42610 rack side-panel installation process is the reverse of the removal process.

The side panels are formed by two parts. When you remove the side panels, first remove the upper panel and then remove the lower panel. When you install the side panels, first install the lower panel and then the upper panel.

The steps are as follows:

Step 1 Unlock the button locks and slide the latches toward each other on the upper side panel.

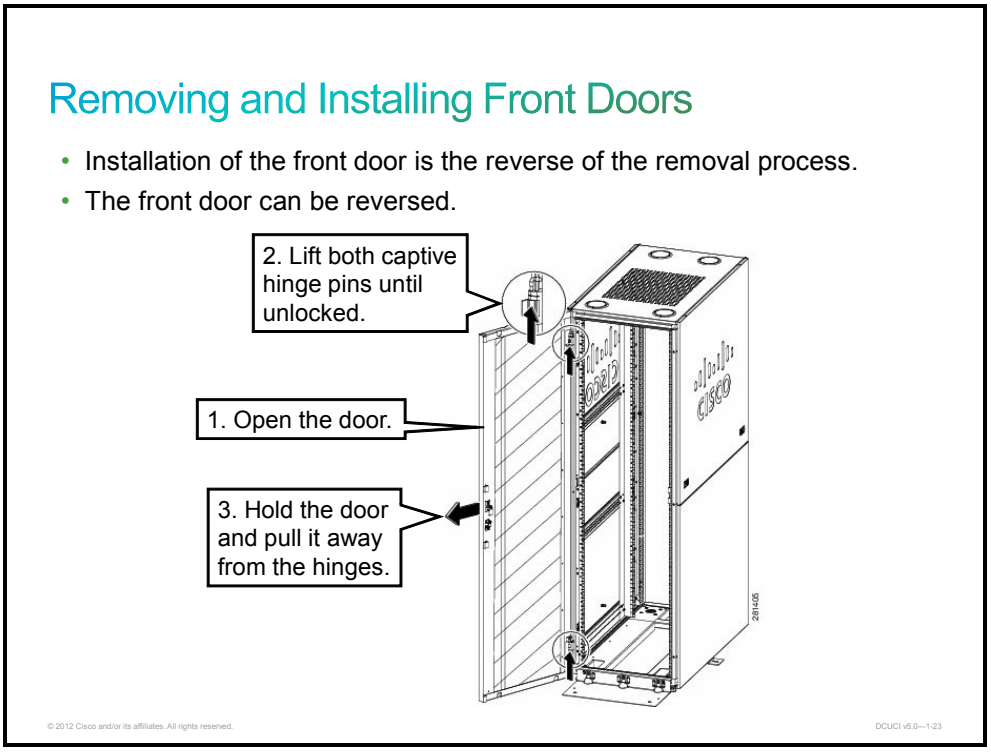
Step 2 Pull the upper side panel toward you and up to remove it.

Step 3 Pull the lower panel up and toward you to remove it.

https://t.me/learningnets

Remove and Install Cisco R-Series Rack Doors

This topic shows how to remove Cisco R-Series rack doors.



To remove the front door of the Cisco R42610 rack, follow these steps:

Step 1 Open the front door.

Step 2 Unlock both captive hinge pins by lifting them.

Step 3 Hold and pull the door away from the hinges.

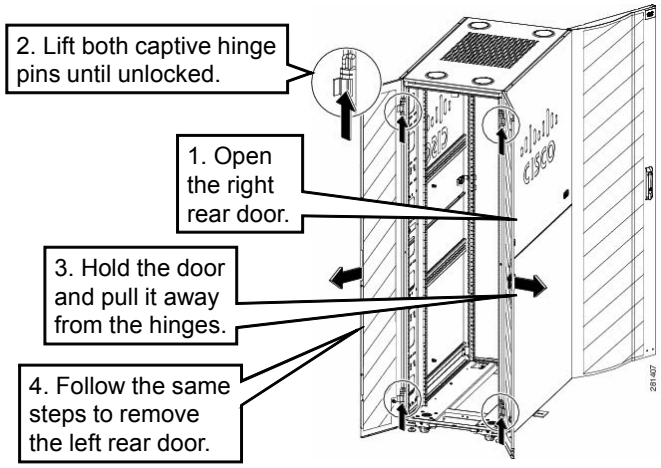
The installation process follows the reverse order of these steps.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Removing and Installing Rear Doors

- Installation of rear doors is the reverse of the removal process.
- First, the right rear door must be removed.



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

To remove the rear doors, follow these steps:

Step 1 Open the right rear door.

Step 2 Unlock the captive hinge pins by lifting them.

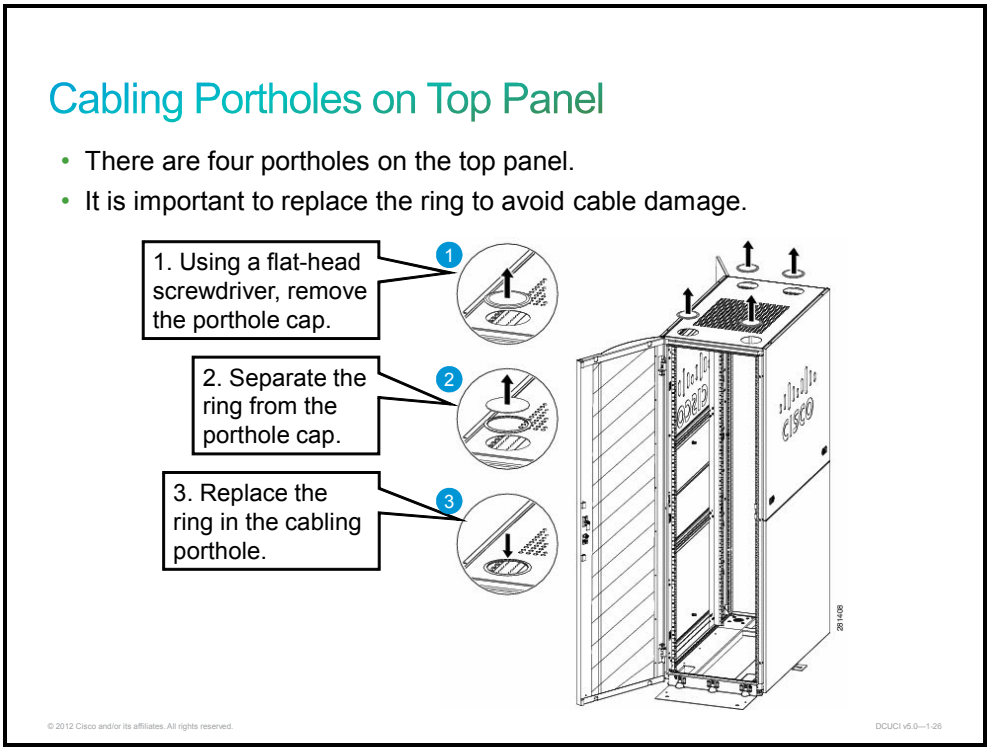
Step 3 Hold the door and pull it away from the hinges.

Step 4 Follow the same steps to remove the left rear door.

https://t.me/learningnets

Use the Cabling Portholes

This topic describes how to use cabling portholes on the top panel of the rack.



There are four cabling portholes on the top panel of the rack. You can run cables through these portholes. To prepare the portholes, follow these steps:

Step 1 With a flat-head screwdriver, remove the porthole caps.

Step 2 Remove the center from the cap, but preserve the ring.

Step 3 Place the ring in the porthole to avoid cable damage.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

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

Summary

- To unpack the R42610 rack, remove the plastic straps, the cardboard top, the plastic latches, the clear plastic cover, and the cardboard corner frames.
- To remove the Cisco R-Series rack from the pallet, raise the leveling feet, remove the bolts that hold the rack to the pallet, install the ramps, and roll the rack off the pallet.
- To secure the Cisco R-Series rack to the floor, lower the leveling feet, attach the side stabilizer brackets and the stabilizer plate, and secure them to the floor with the provided bolts.
- To join Cisco R42610 racks into a suite, use the rack-joining kit and remove the doors. Install and secure the first rack and join the second by using two brackets at the front and two at the rear.
- Cisco RP208-30-U-1 PDUs can be installed in a tower configuration that does not occupy RUs, or in a 1-RU configuration.
- To remove the side panels, first remove the upper panel and then the lower panel.
- To remove the front door, open it, release the hinge pins, and pull it. To release the rear doors, first remove the rear right door and then the rear left door. The installation process is the reverse of the removal process.
- To use the cabling portholes, remove the caps and replace the rings back in the holes to avoid cable damage.

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

https://t.me/learningnets

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

Lesson 2

Installing Cisco UCS C-Series Server Hardware

Overview

Cisco Unified Computing System (UCS) C-Series servers contain components that can be replaced or added, such as power supply units, fan modules, Peripheral Component Interconnect Express (PCIe) cards, and memory modules. This lesson describes which components can be replaced and shows the steps that are needed to accomplish installation and replacement tasks.

Objectives

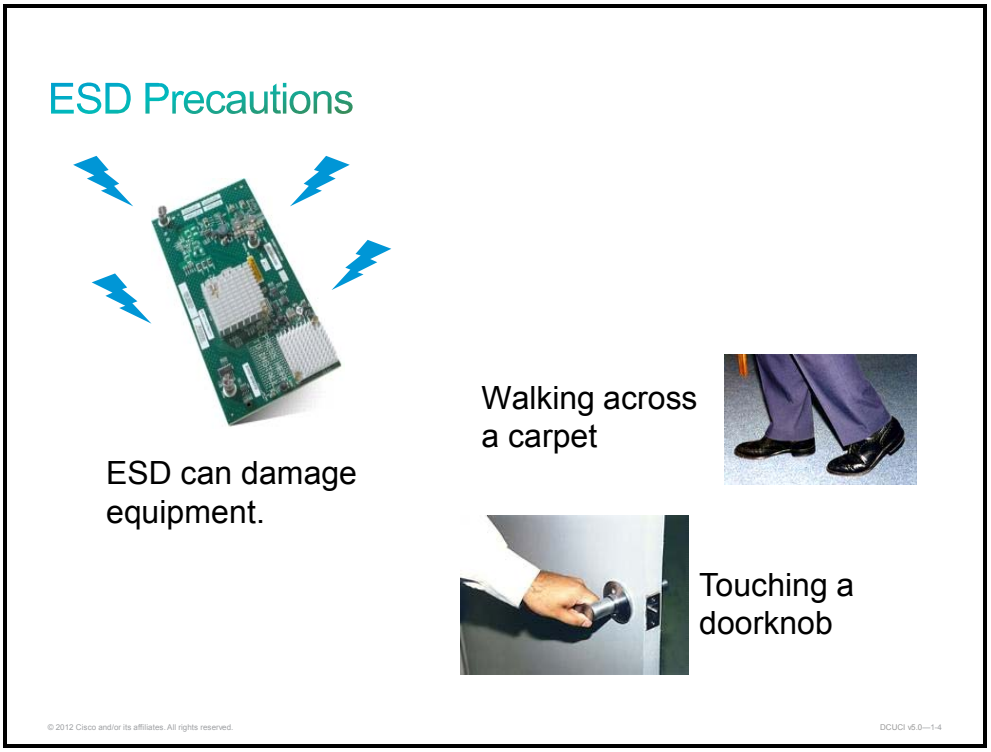
Upon completing this lesson, you will be able to install components in the Cisco UCS C-Series rack server before rack mounting. This ability includes being able to meet these objectives:

- Review ESD precautions
- Review how to open Cisco UCS C-Series cases
- Compare PCIe riser cards across Cisco UCS C-Series models
- Describe CPU population rules for dual- and quad-socket servers
- Describe the importance of color coding internal Cisco UCS C-Series components
- Describe DRAM installation and population rules
- Describe fan replacement
- Describe power supply replacement

https://t.me/learningnets

ESD Precautions

This topic explains ESD-related risks and precautions that can be taken to prevent those risks.



ESD can cause serious damage to electronic equipment. It is estimated that ESD damage costs U.S. industry approximately $5 billion each year.

ESD is the rapid movement of an electric charge from one object to another object. As you walk across the carpet, you may not realize that you are generating several thousand volts of electricity. When your finger comes close to a doorknob or your computer screen, you may feel a slight shock. That shock can cause severe damage to electronic components or entire circuit card assemblies. This shock, or release of energy, is known as an ESD event. Sometimes the results of an ESD event will not show up in electrical components for weeks or even months.

Every time that you touch an electronic piece of equipment, you may feel nothing, but a sensitive electronic component could either be destroyed or become unstable.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

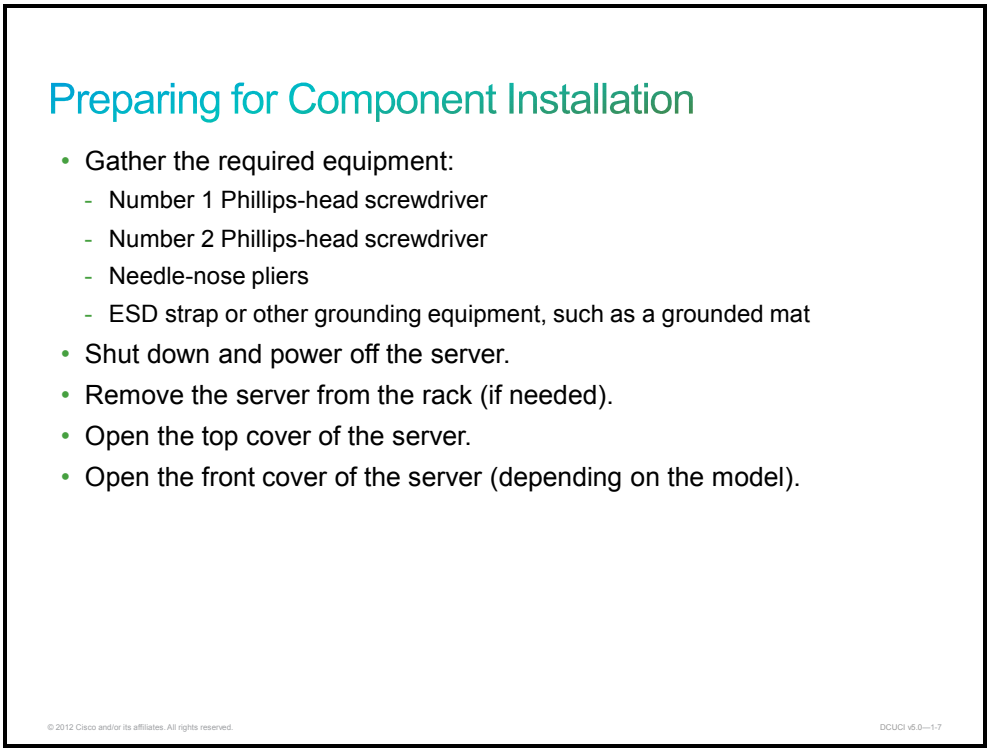
The following practices can help to control and eliminate the effects of ESD:

- Remove unneeded static objects from your workstation, and keep objects that you need a safe distance away from any sensitive components and assemblies.
- Use an antistatic spray, if possible, to eliminate static buildup on objects that are necessary to do your job.
- Minimize movement and friction.
- Protect any sensitive parts from the charges around them by using ESD protective packaging.
- Place components and assemblies only on a dissipative mat or dissipative work surface.
- Ensure that all personnel, surfaces, and equipment are grounded in order to drain off any charges that are created.
- Keep all of your work surfaces clean and free of dirt buildup.
- Store static-generating objects within ESD control containers.

https://t.me/learningnets

Opening Cisco UCS C-Series Cases

This topic describes how to open C-Series server covers.



Before installing or removing any components of C-Series servers, you must first prepare the server. Begin by shutting down and powering off the server. Of course, to minimize the loss of data or damage to the operating system, you should perform a graceful shutdown. To perform a graceful shutdown, press and release the power button. However, to perform an emergency shutdown, press and hold the power button for 4 seconds to force the main power off and immediately enter standby mode.

Next, make sure that you have the required tools to remove and replace the enclosure and any other component. Using the wrong tools may damage the server. The tools that you will need when working with C-Series servers are number 1 and 2 Phillips-head screwdrivers, needle-nose pliers, and an ESD strap. When managing electronic components, you should always take the appropriate steps to minimize any damage that is caused by ESD.

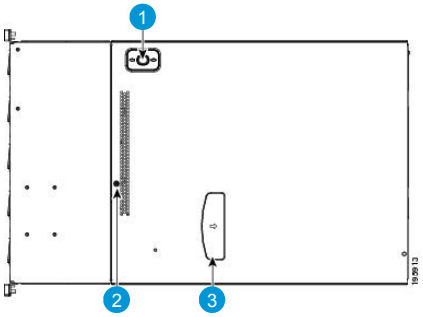
Next, remove the server from the rack if it is mounted. With the server removed from the rack, you can now open the cover to install or replace a component.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Open the Cisco UCS C200 M2/C210 M2 Server Enclosure Top Cover

1. Press the release button.
2. Push the cover toward the rear about 1 inch.
3. Lift the cover to remove it.



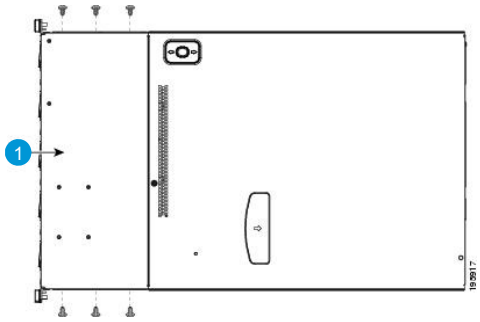
© 2012 Cisco and/or its affiliates. All rights reserved.

To install components into the Cisco UCS C210 M2 General-Purpose Rack Server or the Cisco UCS C200 M2 High-Density Rack Server, you must first remove the top cover. To remove the top cover, press down on the release button (item 1 in the figure). Use the nonslip pad (item 3) to push the cover toward the rear about 1 inch, until you feel it stop sliding. Finally, lift the cover from the server and set it aside.

https://t.me/learningnets

Open the Cisco UCS C200 M2/C210 M2 Server Enclosure Front Cover

- The front cover has six screws on the top surface and three screws on each side.

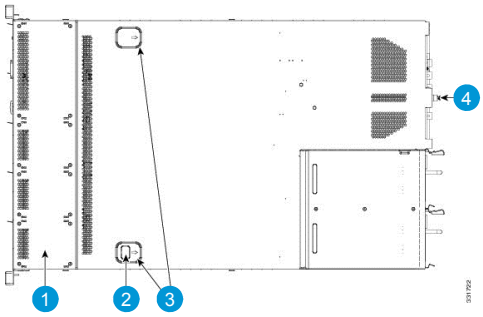


© 2012 Cisco and/or its affiliates. All rights reserved.

To remove the front cover, follow these steps. First, remove the server top cover by using the procedure that was described previously. Then, using a number 1 Phillips-head screwdriver, remove the 12 screws that secure the front cover. There are six screws on the upper surface and three screws on each side of the front cover. Finally, lift the front cover straight up off the chassis.

Open the Cisco UCS C220 M2 Server Enclosure Top Cover

1. Release the thumbscrews (4).
2. Press the release button (2).
3. Push to the rear and lift the cover.



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

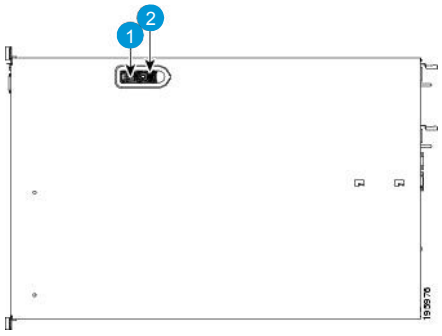
To install components into the Cisco UCS C220 M3 Rack Server, you must first remove the top cover. Removing the top cover is simple and only requires that you press the release button, push the cover to the rear, and lift it.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Open the Cisco UCS C250 M2 Server Enclosure Top Cover (Cont.)

1. Release the latch.
2. Lock the screw.



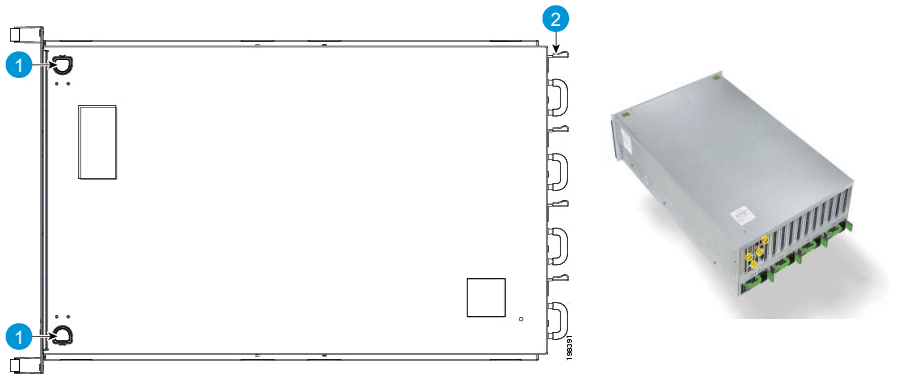
© 2012 Cisco and/or its affiliates. All rights reserved.

To install components into the Cisco UCS C250 M2 Extended Memory Rack Server, you must first remove the top cover. Removing the top cover is simple and only requires a number 2 Phillips-head screwdriver. To begin, first unlock the screw. Next, lift the release latch (item 1 in the figure) and push the cover toward the rear about 1 inch, until it stops sliding. Finally, lift the cover from the server and set the cover aside.

https://t.me/learningnets

Open the Cisco UCS C460 M2 Server Enclosure Top Cover

1. Press the green release buttons.
2. Push the cover toward the server rear about 3 inches, until it stops.
3. Then lift the cover straight up from the server and set the cover aside.



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

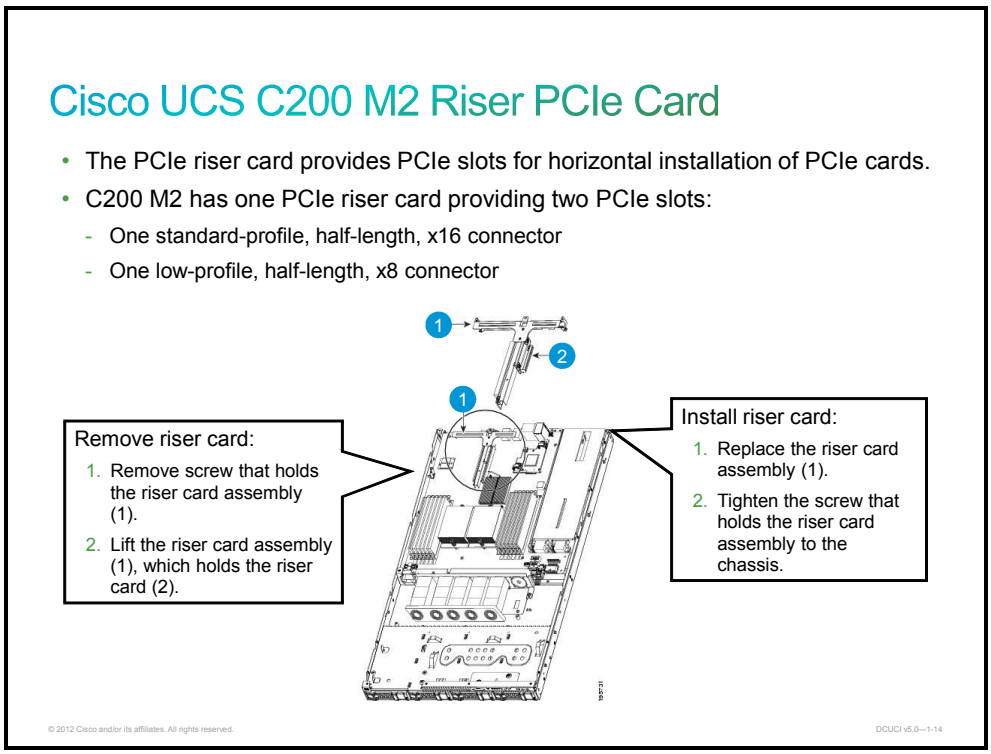
To install components in the Cisco UCS C460 M2 High-Performance Rack Server, you must first remove the front cover. To begin, simultaneously press the two green release buttons (item 1 in the figure). Next, push the cover toward the back of the server about 3 inches, until it stops. Then, lift the cover straight up from the server and set the cover aside.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

PCIe Riser Cards in Cisco UCS C-Series Models

This topic describes the available PCIe riser cards for Cisco UCS C-Series servers.



The PCIe riser card is a small adapter on which there are PCIe slots. The riser card is connected to a slot on the motherboard and allows for the horizontal installation of PCIe cards in the server.

The Cisco C200 M2 server has one PCIe riser card, which provides two PCIe slots:

- One standard-profile, half-length, x16 connector
- One low-profile, half-length, x8 connector

To replace a riser card, first you have to turn off the server, remove the server from the rack, and open the cover.

The riser card is part of the riser card assembly. The riser card assembly is designed differently in the different models of the C-Series servers and allows for riser card mounting.

To remove a riser card from a C200 M2 server, follow these steps:

Step 1 Remove the screw that holds the riser card assembly to the chassis.

Step 2 With both hands, carefully lift the riser card assembly, together with the installed PCIe cards.

Step 3 Remove the PCIe cards.

To install a riser card, follow these steps:

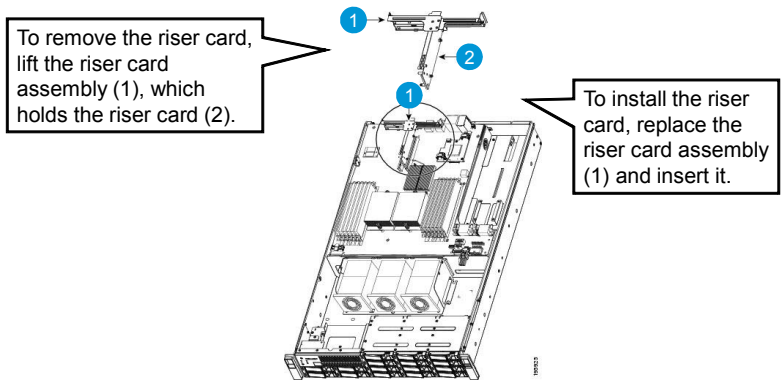
Step 1 Replace the riser card assembly.

Step 2 Tighten the holding screw.

https://t.me/learningnets

Cisco UCS C210 M2 Riser PCIe Card

- C210 M2 has one PCIe riser card providing five PCIe slots:
  - Two standard-profile, full-length, x16 connector
  - Three low-profile, half-length, x16 connector



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

The C210 M2 server has one riser card, which provides the following PCIe slots:

- Two standard-profile, full-length, x16 connector
- Three low-profile, half-length, x16 connector

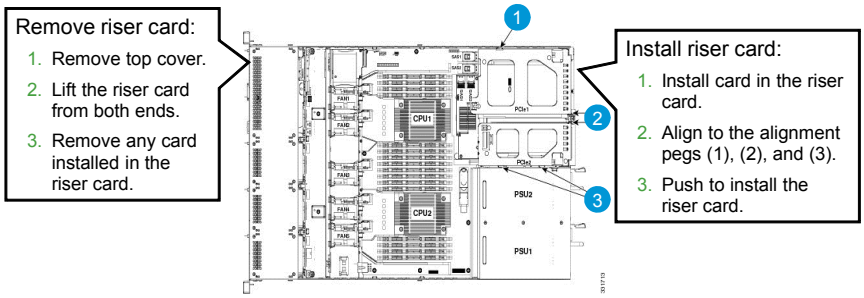
The procedure for removal and installation of the riser card is the same as the procedure for the C200 M2 server.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS C220 M3 Riser PCIe Card

- C220 M3 has two tool-less PCIe riser cards providing five PCIe slots:



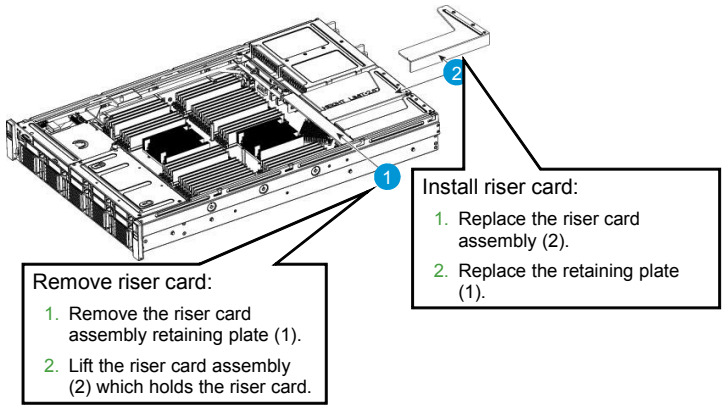
© 2012 Cisco and/or its affiliates. All rights reserved.

The C220 M3 server has two tool-less PCIe riser cards. The top cover of the server must be removed for any riser card to be installed or removed. If a card is to be installed in a riser card, it must be installed before the installation of the riser card.

https://t.me/learningnets

Cisco UCS C250 M2 Riser PCIe Card

- C250 M2 has one PCIe riser card providing five PCIe slots:
  - Two standard-profile, half-length
  - Three low-profile, half-length



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

The C250 M2 server has one riser card, which provides the following PCIe slots:

- Two standard-profile, half-length
- Three low-profile, half-length

To remove a riser card from a C250 M2 server, follow these steps:

Step 1 Remove the riser card assembly retaining plate.

Step 2 With both hands, carefully lift the riser card assembly, together with the installed PCIe cards.

Step 3 Remove the PCIe cards.

To install a riser card, follow these steps:

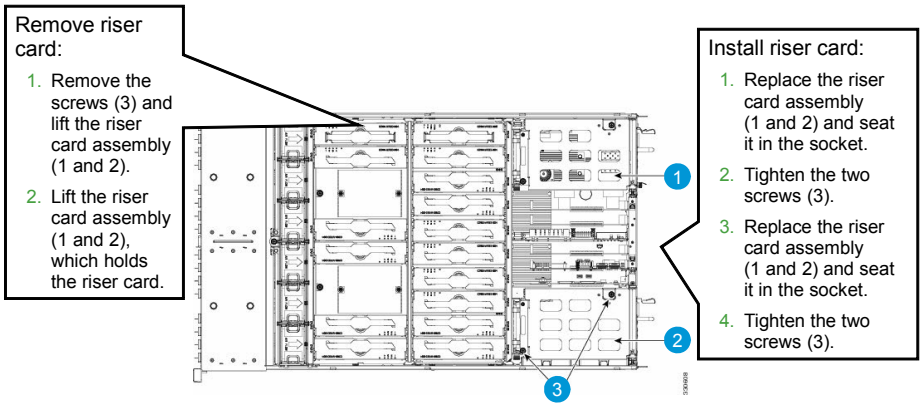
Step 1 Replace the riser card assembly.

Step 2 Replace the retaining plate.

https://t.me/learningnets

Cisco UCS C260 M2 Riser PCIe Card

- C260 M2 has two PCIe riser cards, each providing one standard-profile, half-length PCIe slot.
- Riser cards are installed in PCIe slots 1 and 7 on the motherboard.
- There are five PCIe low-profile slots on motherboard.



The C260 M2 server has two PCIe riser cards, each providing one standard-profile, half-length PCIe slot.

The C260 M2 server has seven PCIe slots on the motherboard. To directly install a PCIe card, you can use slots 2 to 5.

The two riser cards occupy PCIe slots 1 and 7 on the motherboard. They are positioned around the power supply bays.

To remove any of the riser cards, follow these steps:

Step 1 Remove the two captive screws from the riser card assembly.

Step 2 Pull out the riser card assembly.

To install a riser card, follow these steps:

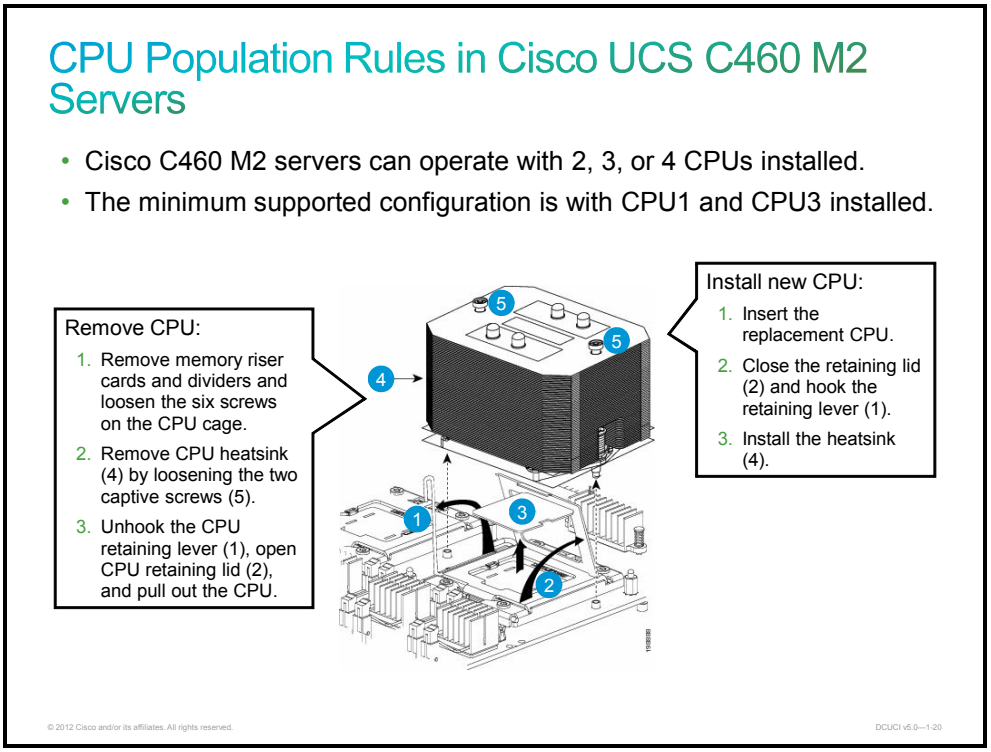
Step 1 Replace the riser card assembly as you seat it correctly in the socket.

Step 2 Tighten the two captive screws.

https://t.me/learningnets

CPU Population Rules

This topic describes the CPU population rules for dual-core and quad-core servers.



The C460 M2 server has four CPU sockets. It can operate with two, three, or four CPUs installed. The minimum supported configuration is to have CPUs in sockets 1 and 3.

To remove a CPU from the C460 server, follow these steps:

Step 1 Remove the memory riser and dividers.

Step 2 Loosen the six screws on the CPU cage.

Step 3 Loosen the two captive screws of the CPU heatsink and remove the heatsink.

Step 4 Unhook the CPU retaining lever and open the CPU retaining lid.

Step 5 Pull out the CPU from the socket.

To install a CPU, follow these steps:

Step 1 Carefully insert the new CPU in the socket.

Step 2 Close the retaining lid.

Step 3 Hook the retaining lever.

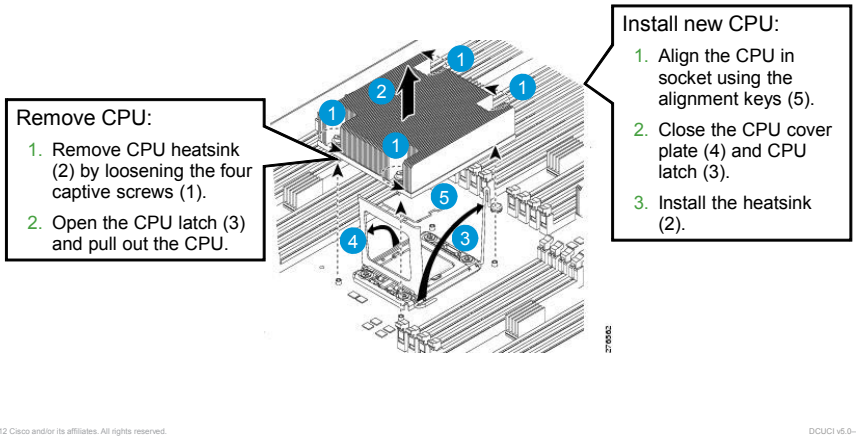
Step 4 Install the CPU heatsink.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

CPU Population Rules in Cisco UCS C250 M2 Servers

- All Generation M2 servers require two CPUs to support the DIMM configurations.
- CPU sockets are fragile. Approach with caution.



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

The Generation M2 dual CPU servers require two CPUs to support the DIMM configurations.

To remove a CPU in a C250 M2 server, follow these steps:

Step 1 Loosen the four captive screws of the CPU heatsink.

Step 2 Remove the heatsink.

Step 3 Open the CPU latch.

Step 4 Pull out the CPU.

To install a CPU in a C250 M2 server, follow these steps:

Step 1 Align the CPU to the CPU socket using the alignment keys.

Step 2 Carefully install the CPU in the socket.

Step 3 Close the CPU cover plate and latch the plate.

Step 4 Install the heatsink.

https://t.me/learningnets

Color Coding of Internal Cisco UCS C-Series Components

This topic describes the color-coded touch points on Cisco UCS C260 M2 Rack Servers.

Color-Coded Touch Points

- Color coding provides a quick and efficient way to immediately know which components are hot-swappable and which are only replaceable.
- Color coding was implemented first in the C260 M3.
- Color coding will be used in M3 and later generations.
- Hot-swappable components have green plastic touch points:
  - Internal cooling fans
  - Power supplies
- Replaceable, but non-hot-swappable components have light-blue plastic touch points:
  - Memory risers
  - PCIe risers
  - PCIe slots
  - Fan trays

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

When you replace components on your server, you must check if the components are hot-swappable or you must take the server from the rack and perform the procedure with a powered-down server. That process is disruptive. Also, if you try to replace a non-hot-swappable component, you may damage the server.

Starting with the C260 M3 servers, Cisco implemented a color coding system that indicates if a component is hot-swappable.

Color coding will be used in servers of generation 3 and later.

The color-coded touch-point system provides the following information:

- Green plastic touch points are hot-swappable components, which include the following:
  - Internal cooling fans
  - Power supplies
- Light-blue plastic touch points are non-hot-swappable components, which include the following:
  - Memory risers
  - PCIe risers
  - PCIe slots
  - Fan trays

 © 2012 Cisco Systems, Inc.

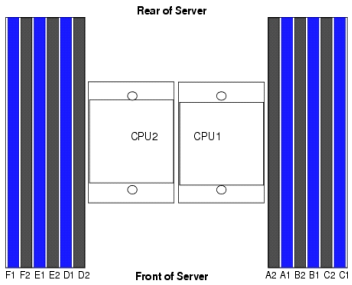
https://t.me/learningnets

DRAM Installation and Population Rules

This topic describes the DRAM installation and population rules.

Cisco UCS C210 M2 Memory Population Rules

- DIMMs within the server should all be the same type, speed, and size.
- Do not mix different-sized DIMMs.
- Do not mix DIMMs with different clock rates in the same server.
- DIMMs can be used either in a one-DIMM-per-channel (1DPC) configuration or in a two DIMMs-per-channel (2DPC) configuration.
- There are blue and black DIMM slots. Populate the blue slots in a bank first.



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

The C210 server has two CPU sockets and 12 DIMM slots, supporting a maximum of 96 GB of memory.

Each CPU supports three memory channels, which are identified by letters. The memory channels for CPU1 are A, B, and C. The memory channels for CPU2 are D, E, and F. For each CPU, there are two banks, which are identified by numbers. In this way, the DIMM slots for Bank 1 for CPU1 will be A1, B1, and C1. The DIMM slots for Bank 2 will be A2, B2, and C2. In the same manner, for CPU2 the DIMM slots for Bank 1 will be D1, E1, and F1, and the DIMM slots for Bank 2 will be D2, E2, and F2.

The slots belonging to Bank 1 are blue, while the slots for Bank 2 are black.

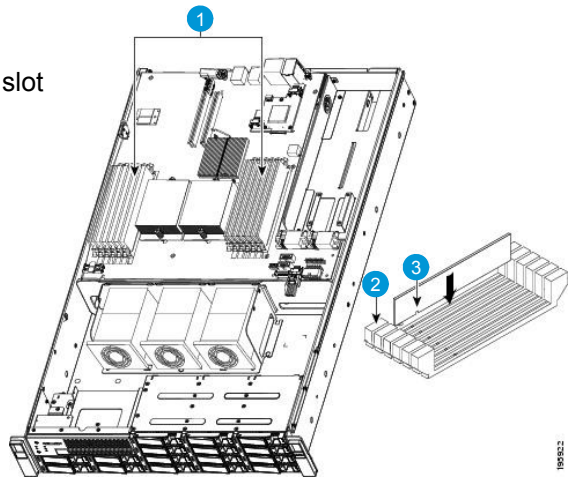
The following are rules for memory population:

- DIMMs within the server should all be the same type, speed, and size.
- Do not mix different-sized DIMMs.
- Do not mix DIMMs with different clock rates in the same server.
- DIMMs can be used either in a one-DIMM-per-channel (1DPC) configuration or in a two-DIMMs-per-channel (2DPC) configuration.
- There are blue and black DIMM slots. Populate the blue slots in a bank first.

https://t.me/learningnets

Install a DIMM

1. DIMM slots (12)
2. DIMM slot ejector lever (two on each slot)
3. Alignment key in DIMM slot



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

To install DIMM modules in a C210 server, follow these steps:

Step 1 Power down the server, unplug it, and remove it from the rack.

Step 2 Open the server cover.

Step 3 Locate the DIMM slots next to the CPUs.

Step 4 Align the DIMM module.

Step 5 Press the DIMM module until it is seated properly and you hear the locking sound.

To remove a DIMM module, follow these steps:

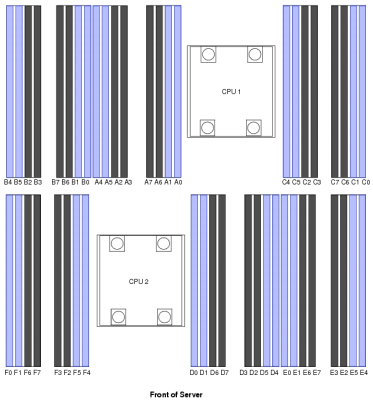
Step 1 Press the DIMM slot ejector levers to release the module.

Step 2 Pull out the DIMM module.

https://t.me/learningnets

Cisco UCS C250 M2 Memory Population Rules

- DIMMs within the server should all be the same type, speed, and size.
- Do not mix different-sized DIMMS or DIMMs with different clock rates.
- DIMM configurations and population information is provided in tables in the installation and upgrade guide.
- DIMMs are populated in pairs.
- DIMM pairs are installed side-by-side under the same CPU in the same color slots.
- There are blue and black DIMM slots. Populate the blue slots in a bank first.



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

The C250 server supports two CPUs and 48 DIMM slots, providing for up to 384 GB of double data rate (DDR3) memory.

Each CPU supports three memory channels, which are identified by letters. Again, A, B, and C are used by CPU1 and D, E, and F by CPU2. Each channel supports eight DIMM slots, marked with numbers from 0 to 7. The memory banks are identified in the same manner. Bank 1 has slots A1, B1, and C1, and Bank 2 has slots A2, B2, and C2.

Supported DIMM configurations and DIMM module population information is provided in tables in the *Cisco UCS C250 Installation and Service Guide* at

http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C250M1/install/c250M1.html

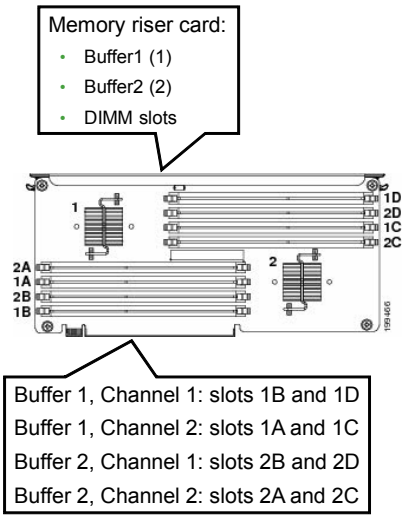
The following rules apply:

- DIMMs within the server should all be the same type, speed, and size.
- Do not mix different-sized DIMMs or DIMMs with different clock rates.
- DIMM configurations and population information is provided in tables in the installation and upgrade guide.
- DIMMs are populated in pairs.
- DIMMs pairs are installed side-by-side under the same CPU in the same color slots.
- There are blue and black DIMM slots. Populate the blue slots in a bank first.

https://t.me/learningnets

Cisco UCS C460 M2 Memory Population Rules

- Each CPU supports two memory risers.
- Each memory riser contains two memory buffers.
- Each memory buffer has two memory channels.
- Each memory channel contains a pair of DIMM slots.
- At least one DIMM pair must be installed for CPU1 or CPU2.
- All four CPUs can run from a single DIMM pair.
- DIMMs must be identical.
- A DIMM pair in the riser card of an empty CPU socket is not accessible.
- DIMMs are populated starting from the farthest slots.



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

The Cisco UCS C460 server supports four CPUs and 64 DIMM slots with up to 512 GB of DDR3 memory. The DIMM slots are located on eight memory risers.

Each memory riser is connected to the motherboard and provides eight DIMM slots. The memory risers are hot-swappable.

Each CPU supports two memory risers. CPU1 supports risers 1 and 2, CPU2 supports risers 3 and 4, CPU3 supports risers 5 and 6, and CPU4 supports risers 7 and 8. The numbers of the memory riser are shown on the CPU cage.

Each memory riser contains two memory buffers that are connected to the CPU based on the serial memory interface. Each memory buffer has two memory channels. Each memory channel has two DIMM slots, forming a pair.

The buffers and channels distribution is as follows:

- **Buffer 1, Channel 1:** Slots 1B and 1D
- **Buffer 1, Channel 2:** Slots 1A and 1C
- **Buffer 2, Channel 1:** Slots 2B and 2D
- **Buffer 2, Channel 2:** Slots 2A and 2C

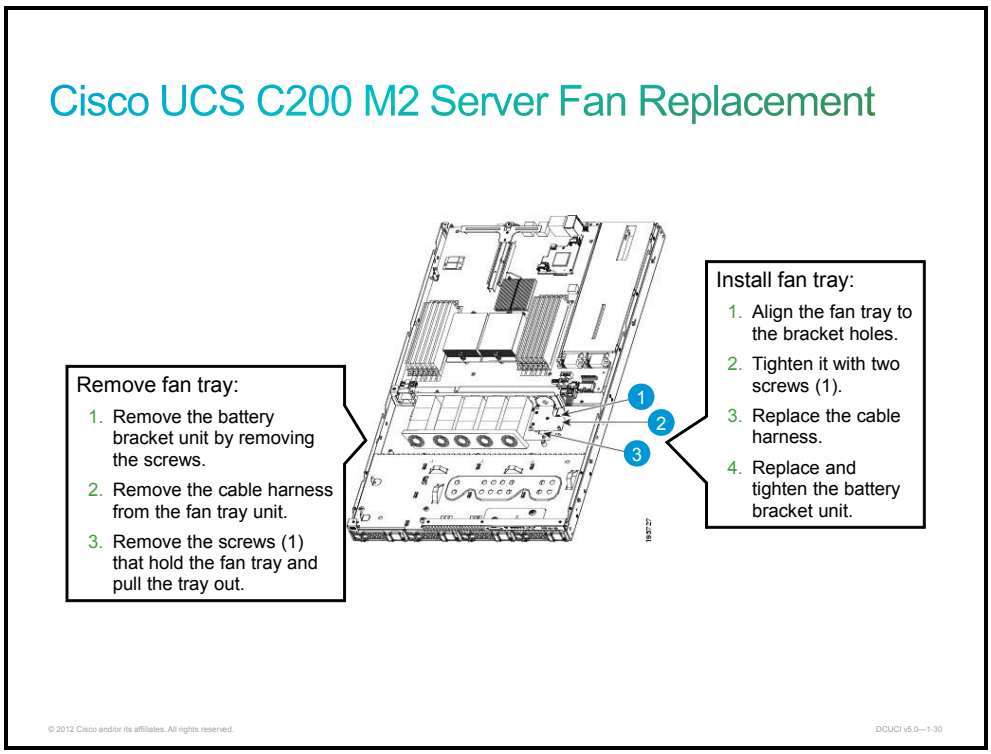
The memory population rules are as follows:

- At least one DIMM pair must be installed for CPU1 or CPU2.
- All four CPUs can run from a single DIMM pair.
- DIMMs must be identical.
- A DIMM pair in the riser card of an empty CPU socket is not accessible.
- DIMMs are populated starting from the farthest slots.

https://t.me/learningnets

Fan Replacement

This topic describes the steps to replace fans in Cisco UCS C-Series servers.



To remove a fan tray from a C200 server, follow these steps:

Step 1 Remove the battery bracket unit by removing the screws.

Step 2 Remove the cable harness from the fan tray unit.

Step 3 Remove the screws that hold the fan tray and pull out the fan tray.

To install a fan tray, follow these steps:

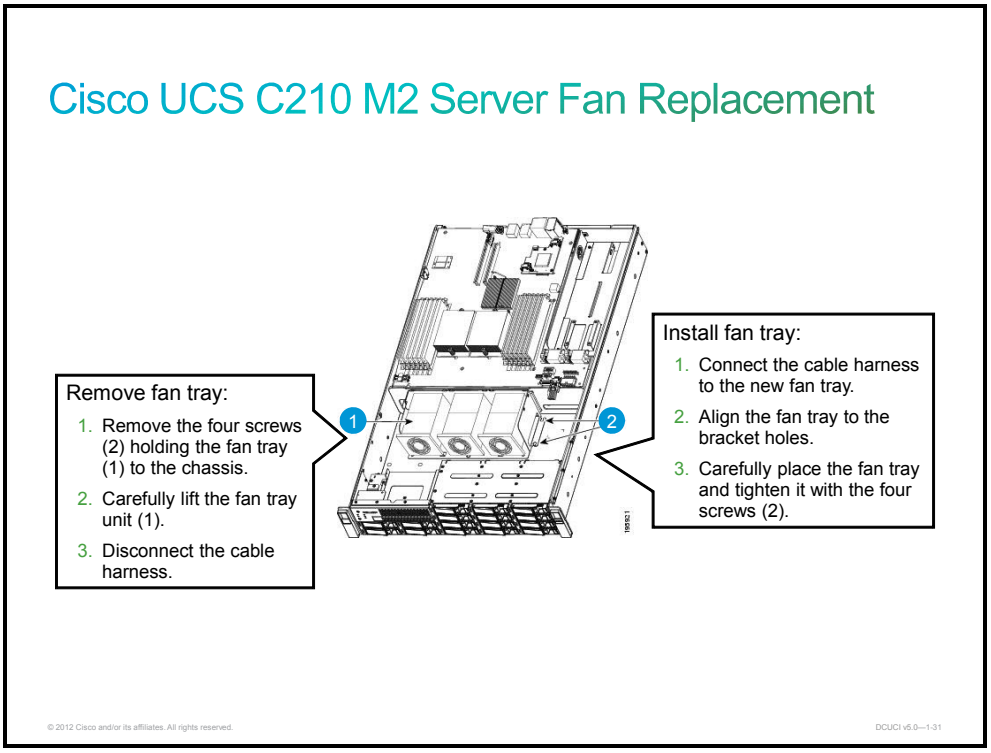
Step 1 Align the fan tray to the bracket holes.

Step 2 Tighten the fan tray with two screws.

Step 3 Replace the cable harness.

Step 4 Replace and tighten the battery bracket unit.

https://t.me/learningnets



To remove the C250 server fan tray, follow these steps:

Step 1 Remove the four screws holding the fan tray to the chassis.

Step 2 Carefully lift the fan tray unit.

Step 3 Disconnect the cable harness.

To install the fan tray, follow these steps:

Step 1 Connect the cable harness to the new fan tray.

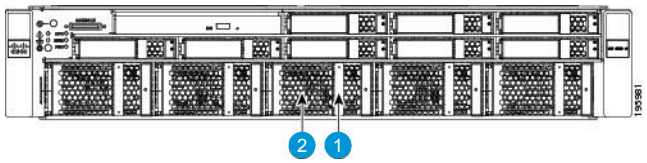
Step 2 Align the fan tray to the bracket holes.

Step 3 Carefully place the fan try and tighten the fan tray with the four screws.

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

Cisco UCS C250 M2 Server Fan Replacement

- Remove fan module:
  1. Press the release button (1) to access the ejector lever (2).
  2. Pull the ejector lever (2) to remove the fan module.
- Install fan module:
  1. Open the ejector lever (2) and slide the fan module into the bay.
  2. Close the ejector lever (2).



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

The fan modules of C250 servers are accessible from the front of the server. The fan modules are hot-pluggable, so you do not have to power down and remove the server to replace them.

To remove a fan module from the C250 server, follow these steps:

Step 1 Press the release button to access the ejector lever.

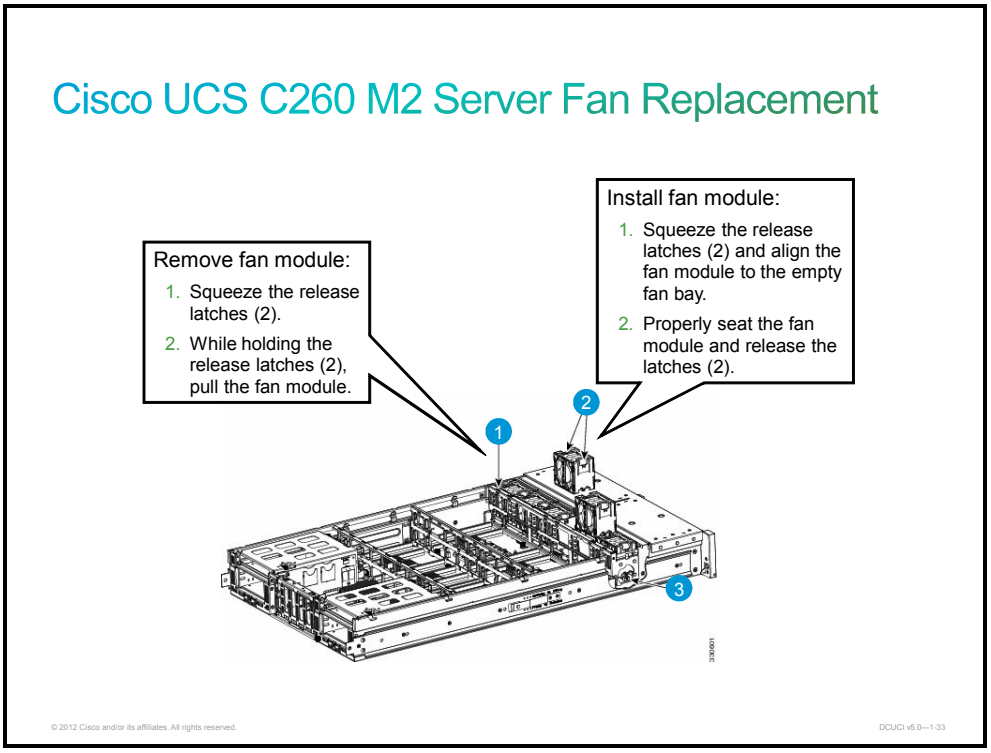
Step 2 Pull the ejector lever to remove the fan module.

To install a fan module, follow these steps:

Step 1 Open the ejector lever and slide the fan module into the bay.

Step 2 Close the ejector lever.

https://t.me/learningnets



The fan modules of C260 servers are organized in a fan tray. Each of the fan modules can be separately replaced. The fan modules are hot-pluggable.

Each fan module has a status LED. An LED color of amber indicates failure in the fan module.

To remove a fan module, follow these steps:

Step 1 Squeeze the release latches.

Step 2 While holding the release latches, pull out the fan module.

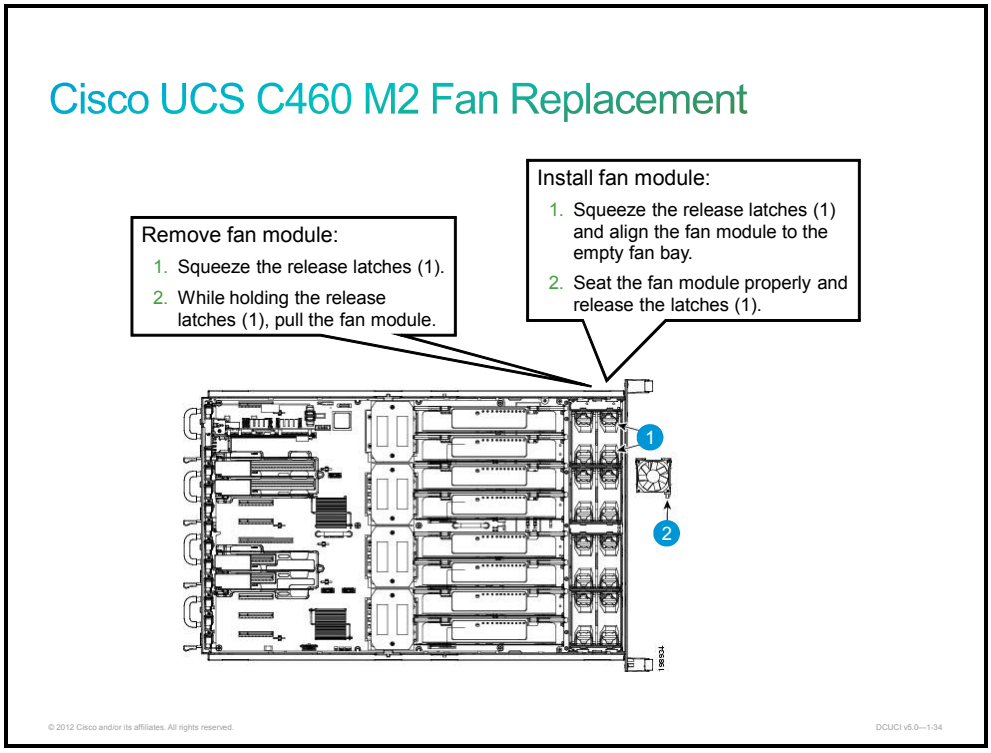
To install a fan module, follow these steps:

Step 1 Squeeze the release latches and align the fan module to the empty fan bay.

Step 2 Properly seat the fan module and release the latches.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



C460 servers have eight hot-pluggable fan modules. Each fan module has a fault LED.

To remove a fan module, follow these steps:

Step 1 Squeeze the release latches.

Step 2 While holding the release latches, pull out the fan module.

To install a fan module, follow these steps:

Step 1 Squeeze the release latches and align the fan module to the empty fan bay.

Step 2 Properly seat the fan module and release the latches.

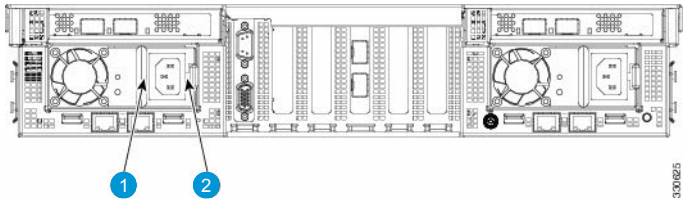
https://t.me/learningnets

Power Supply Replacement

This topic describes the power supply replacement procedure.

Cisco UCS C-Series Server Power Supply Replacement

- The procedure for installing and removing power supply units is the same for all of the C-Series servers.
- Press the release button (2) and pull the power supply unit to remove it.
- To install a power supply unit, slide it until it is seated in the bay and the release lever (2) locks.



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

The procedures for removing or installing power supplies in the C-Series servers are the same.

To remove a power supply, press the release button or lever and pull out the power supply unit.

To install a power supply unit, slide the unit into the bay until it is seated properly and you hear the release button lever locking sound.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

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

Summary

- ESD can cause severe damage to your equipment. Use antistatic sprays, ESD protective packaging, and antistatic wrist straps and pads.
- To open the covers of the C-Series servers, use the appropriate equipment. Power off the server, unplug it, and remove it from the rack. Then proceed according to the instructions in the installation and upgrade guides.
- The C-Series servers are equipped with PCIe riser cards, providing PCIe slots for the installation of PCIe cards.
- The quad CPU servers must be populated with CPU1 and CPU3 as a minimum supported configuration. The dual CPU servers from generation M2 must have two CPUs to support all of the DIMM configurations.
- Color-coded touch points provide information about which components are hot-swappable. Hot-swappable components are marked with green plastic touch points. Non-hot-swappable components are marked with light-blue plastic touch points.
- DIMM population rules differ for the different C-Series server models. Consult the installation and upgrade guide for your model for the supported DIMM configurations and population. As a general rule, try to use the same type of DIMM modules.
- Cisco C250, C260, and C460 servers have hot-pluggable fan modules. To replace the fan tray for C200 and C210, you have to power down the server.
- Power supply units are hot-pluggable. To replace power supply units without shutting down the server, your server must have redundant power supplies.

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

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 3

Installing Cisco UCS C-Series Servers in a Cisco R-Series Rack Enclosure

Overview

The Cisco Unified Computing System (UCS) C-Series servers and components must be installed in a rack. This lesson describes the steps to install the C-Series servers in Cisco R42610 racks.

Objectives

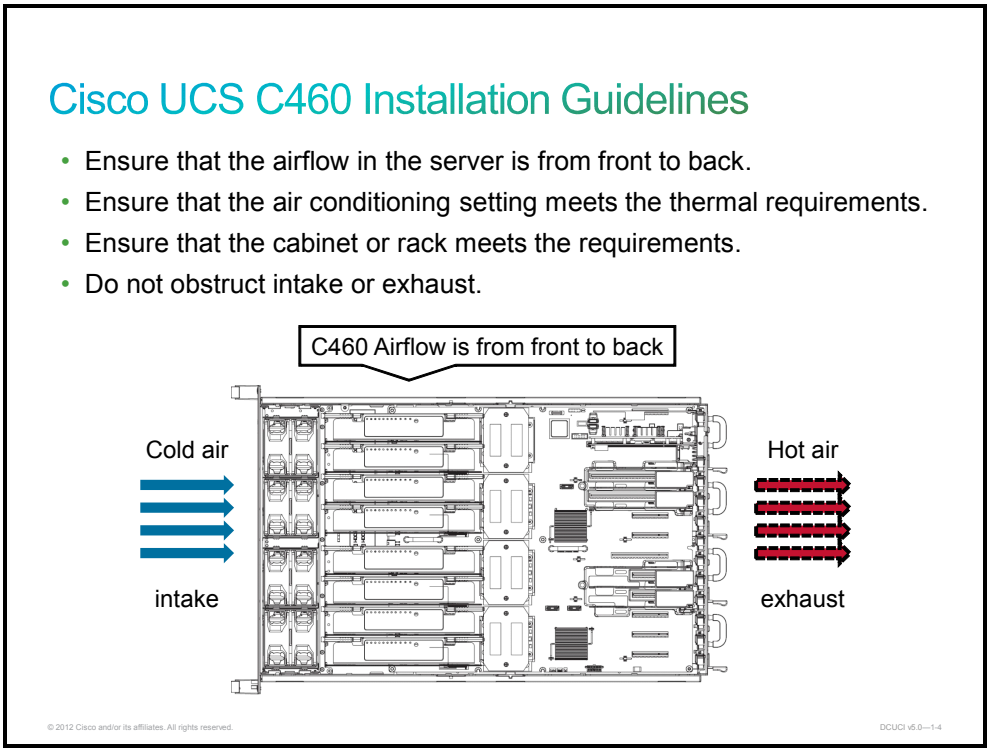
Upon completing this lesson, you will be able to install Cisco UCS C-Series rack servers in a Cisco R-Series rack. This ability includes being able to meet these objectives:

- Install the slide-rail assembly into the Cisco R42610 rack enclosure
- Attach the mounting brackets to the server
- Insert the server into the slide rail
- Attach the cable management arm
- Connect the Cisco UCS C-Series server to the PDU
- Connect management and data cables

https://t.me/learningnets

Install the Slide-Rail Assembly into the Cisco R42610 Rack Enclosure

This topic describes how to install the slide-rail assembly into a Cisco R42610 rack.



To begin the C-Series servers rack installation, you need to follow some guidelines. It is always a best practice to consult the *Cisco UCS Site Preparation Guide* (http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/site_prep/guide/ucs_site_prep.html) for the recommended site-planning tasks. Accurate planning will ensure that requirements for air conditioning, site power, and racks are met.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Rack Requirements for Cisco UCS C460

- The rack should be a standard 19-inch-wide (48.3-cm-wide), four-post EIA rack with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- The rack post holes can be square or round when you use the supplied slide rails.
- The minimum vertical rack space per server must be four RUs, equal to 7 in. (17.8 cm).
- Cisco R42610 racks and RP208-30-U-1 PDUs are designed for optimum performance for Cisco UCS products.

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

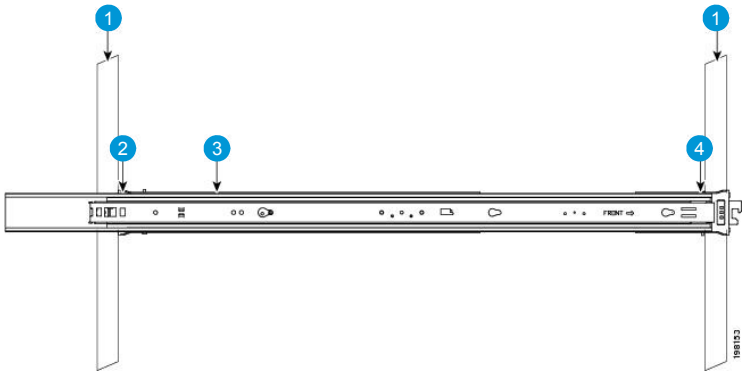
The following are the requirements for standard open racks.

- The rack must be a standard 19-inch-wide (48.3-cm-wide), four-post EIA rack with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- The rack post holes can be square or round when you use the supplied slide rails.
- The minimum vertical rack space per server must be 4 rack units (RUs), which is equal to 7 inches (17.8 cm).
- The Cisco R42610 racks and the Cisco RP208-30-U-1 power distribution units (PDUs) are designed for the optimum performance of Cisco UCS products.

https://t.me/learningnets

Install the Slide-Rail Assemblies in the R42610 Rack

1. Rack posts
2. Rear mounting pegs and locking clip
3. Slide-rail assembly
4. Front mounting pegs and locking clip



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

The following are the steps for installing the slide rail assemblies into the rack.

Step 1 Place the slide-rail assembly (item 3 in the figure) against the inside of the front and rear rack post that is represented by item 1.

Step 2 To ensure that the rear mounting pegs seat in the rear rack post hole (item 2), expand the slide-rail assembly toward the rear of the rack.

Step 3 Ensure that the slide-rail assembly is fastened into place, and then compress the slide-rail assembly until the mounting pegs are fully seated and the locking clips at both ends of the assembly are locked.

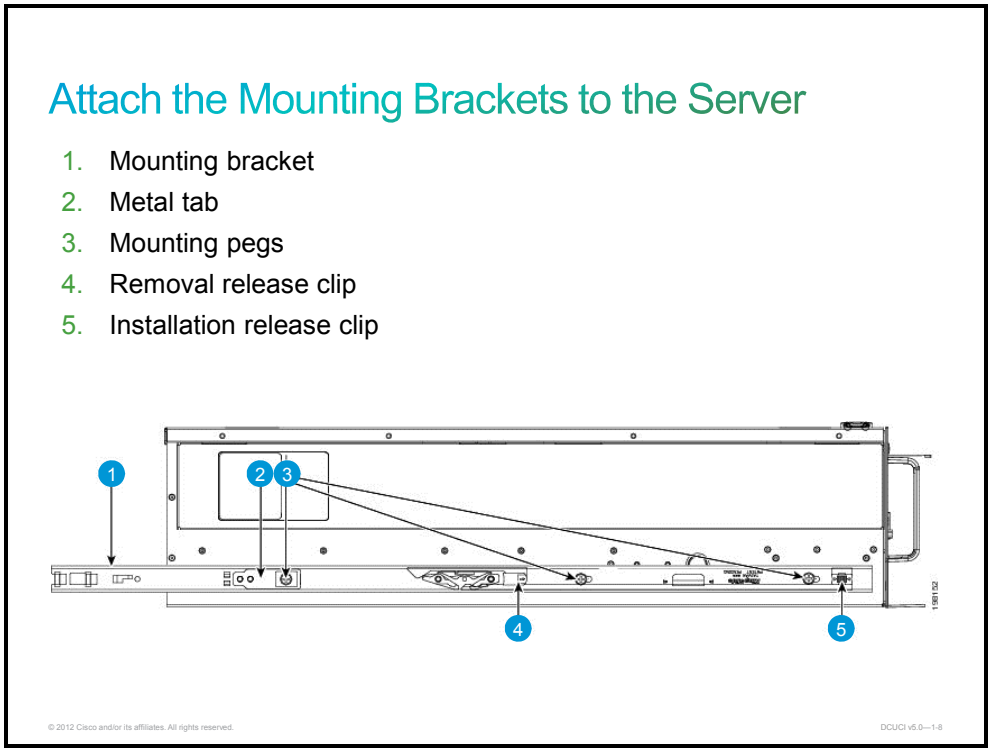
Step 4 Once you complete one side, you can attach the second slide-rail assembly to the opposite side of the rack.

Step 5 Confirm that the slide-rail assembly is level, is at the same height, and is properly locked to the rack.

https://t.me/learningnets

Attach the Mounting Brackets to the Server

This topic describes the steps to attach the mounting brackets.



The next part of the procedure is to attach the mounting bracket to the server. The mounting brackets are shown as item 1 in the figure. Follow these steps:

Step 1 Place the mounting bracket against the side of the server, with the end of the bracket marked “Front” facing toward the front of the server.

Step 2 There are three bracket mounting holes. Match these holes with the three mounting pegs (item 3 in the figure).

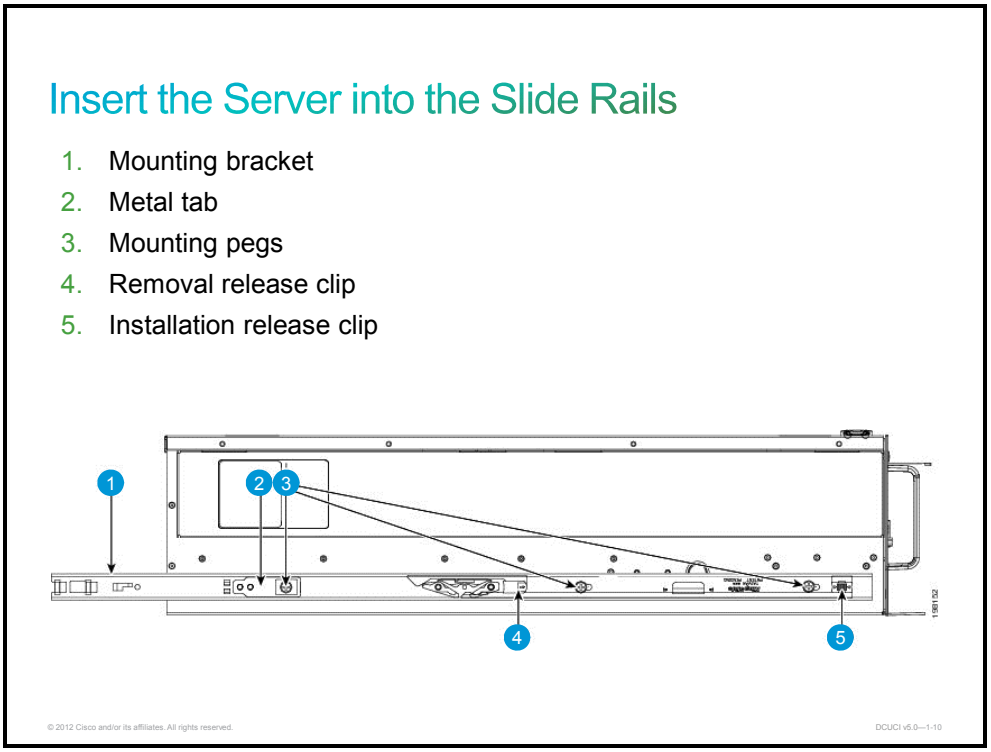
Step 3 Slide the bracket toward the rear of the server until the metal tab on the bracket (item 2 in the figure) is locked over the rear mounting peg.

Step 4 The mounting brackets should now be fastened to the server.

https://t.me/learningnets

Insert the Server into the Slide Rail

This topic describes how to insert the server into the slide rail.



When the slide-rail assembly and the mounting brackets are in place, insert the server into the slide rails.

Step 1 Align the rear of the mounting brackets with the front of the empty slide rails that you installed in the previous step.

Step 2 When the server is lined up, push the server into the slide rails until it stops at the internal stops.

Step 3 Push the plastic installation release clip on each mounting bracket toward the server rear.

Step 4 Proceed by pushing the server into the rack until its front flanges touch the rack posts and the thumb latches engage.

© 2012 Cisco Systems, Inc.

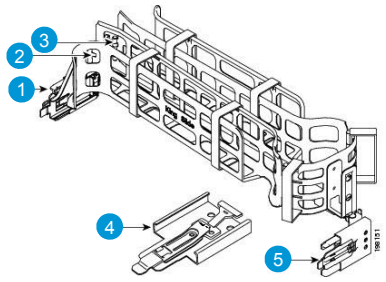
https://t.me/learningnets

Attach the Cable Management Arm

This topic describes how to attach the cable management arm.

Attach Cable Management Arm

- Attach the square metal connector with the blue tab (4) to the rear of the left slide-rail assembly. The clip must lock.
- Attach Connector B (5) to the metal connector (4).
- Attach Connector A (2) to the rear right slide rail.
- Attach the blue clip connector (3) to the right slide rail.
- Attach the metal connector (1) to the mounting bracket at the right side of the server.



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

For better cable management, it is recommended to use the optional cable management arm.

The figure describes the procedure to attach the cable management arm:

Step 1 Attach the square metal connector with the blue tab (item 4 in the figure) to the rear of the left slide-rail assembly. The clip must lock.

Step 2 Attach Connector B (item 5 in the figure) to the square metal connector (item 4 in the figure).

Step 3 Attach Connector A (item 2 in the figure) to the rear right slide-rail assembly.

Step 4 Attach the blue clip connector (item 3 in the figure) to the rear right slide-rail assembly.

Step 5 Attach the metal connector (item 1 in the figure) to the mounting bracket at the right side of the server.

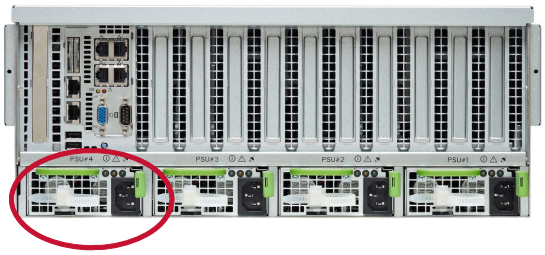
https://t.me/learningnets

Connect the Cisco UCS C-Series Server to the PDU

This topic describes what is needed to connect the C-Series server to the rack PDU.

Connect the C-Series Server to the PDU

- Each power supply has a power cord.
- Jumper power cords are designed to be used in racks.
- The optional jumper power cords have an IEC C19 connector to plug into the PDU and an IEC C20 connector to plug into the C19 connector of the server.
- Only the provided server standard and jumper power cords are approved and supported by Cisco.



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

The Cisco UCS C-Series servers are delivered with standard power cords. The standard power cords are intended to be used in standalone installations, when the server is plugged directly to a plug from the power source.

When you install the server in a rack and use a rack PDU, you must use the optional jumper power cord.

The jumper power cord has an International Electrotechnical Commission (IEC) C19 connector at the side, which is intended to be plugged in the PDU. At the other side, the jumper power cord is equipped with an IEC C20 connector to plug it into the IEC C19 connector of the server.

Only the provided server standard and jumper power cords are approved and supported by Cisco.

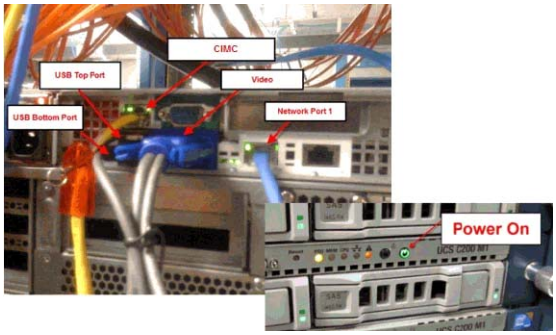
https://t.me/learningnets

Connect Management and Data Cables

This topic describes how to connect management and data cables to the server.

Keyboard, Monitor, and Network Connections

- Connect the USB keyboard and VGA monitor to the rear ports of the server.
- Connect cables to the Cisco Integrated Management Controller management port and at least one LAN on motherboard or expansion card.



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

The initial connection to your C-Series server must be made with a physical keyboard and monitor to interact with the BIOS setup. The figure illustrates a Cisco UCS C200 server that is viewed from the rear and front. Although not shown, there is a port on the front of the server to connect a keyboard, video, mouse (KVM) dongle that supplies a DB-15 Video Graphics Array (VGA) port, a two-port USB, and a DB-9 serial port. That port can also be used for initial setup.

Note	The KVM dongle has priority over the rear panel connections. The rear monitor, USB, and serial ports are disabled when the KVM dongle is attached to the front panel. After the KVM dongle is removed, control reverts to the rear panel KVM connections.

The Cisco Integrated Management Controller management port is a 10/100/1000BaseTX port and requires a Category 6 Ethernet cable to operate in a Gigabit switch port. The two LAN on motherboard (LOM) connections on the C200 M2, C210 M2, and C250 M2 servers are also 10/100/1000BaseTX and similarly require Category 6 cabling. The number and type of LOM ports vary by C-Series model.

A network connection to the Cisco Integrated Management Controller port is required to remotely access Cisco Integrated Management Controller management and monitoring services. At least one connection to a LOM or expansion card is necessary for a host operating system or hypervisor to communicate externally. Note that 10 Gigabit Ethernet ports require either copper twin-axial or optical small form-factor pluggable plus (SFP+) connections.

https://t.me/learningnets

Summary

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

Summary

- Before installing the Cisco UCS C-Series server in the Cisco R42610 rack, ensure that there is proper airflow and that you meet the rack and power requirements. Start preparing for the server installation by mounting the slide-rail assembly in the Cisco R42610 rack.
- Attach the mounting brackets to the server.
- Insert the server into the slide rail.
- For proper cable management, use the cable management arm.
- Use the jumper power cords provided with the server to connect the C-Series server to the PDU.
- Finally, connect management and at least one data cable.

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

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 4

Updating Cisco UCS C-Series Firmware with the Host Upgrade Utility

Overview

Cisco Unified Computing System (UCS) C-Series servers contain different components that run different firmware. Currently, the Cisco Host Upgrade Utility is used to upgrade the firmware of C-Series components such as the Cisco Integrated Management Controller, the server BIOS, or Redundant Array of Independent Disks (RAID) controllers. This lesson describes how to get the correct version of the Cisco Host Upgrade Utility and perform component upgrades.

Objectives

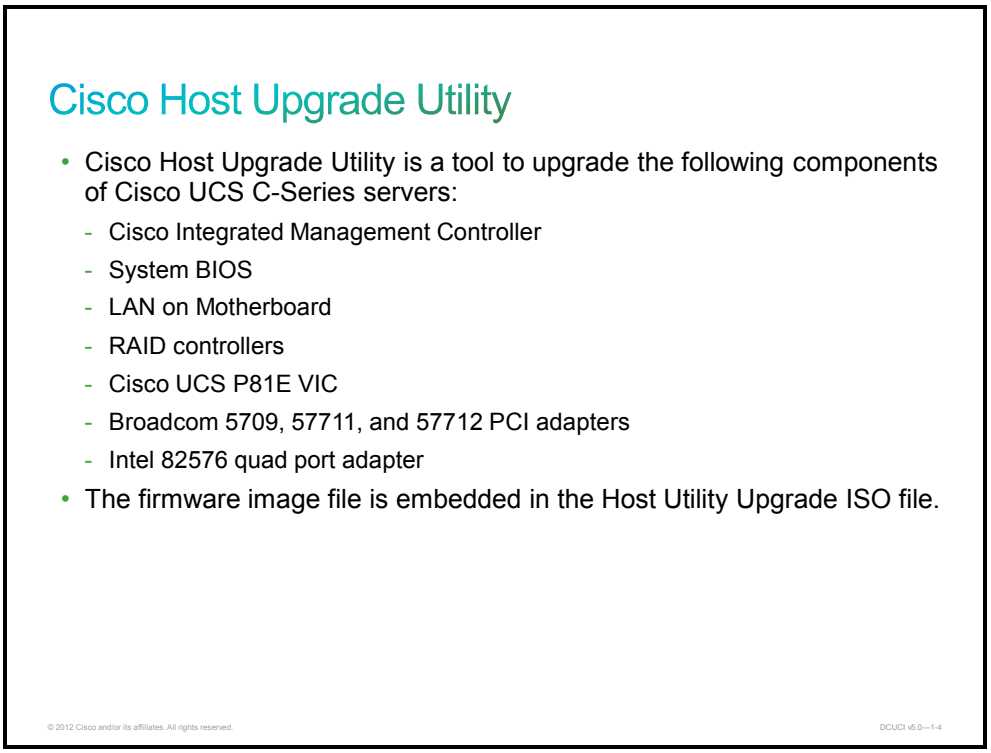
Upon completing this lesson, you will be able to use the Cisco UCS Host Upgrade Utility to upgrade or downgrade C-Series firmware to the correct version. This ability includes being able to meet these objectives:

- Download the Cisco UCS Host Upgrade Utility from Cisco.com
- Enable KVM and virtual media in Cisco Integrated Management Controller
- Describe the session options that are available in the KVM
- Launch virtual media and map the Cisco UCS Host Upgrade Utility ISO image
- Perform an upgrade of all components

https://t.me/learningnets

Cisco UCS Host Upgrade Utility

This topic describes how to download the correct version of the Cisco UCS Host Utility Upgrade.



The Cisco Host Upgrade Utility is a tool that is used in Cisco UCS C-Series servers to perform upgrades of various components.

The tool supports the upgrade of the following components:

- Cisco Integrated Management Controller
- System BIOS
- LAN on motherboard (LOM)
- RAID controllers
- Cisco UCS P81E Virtual Interface Card (VIC)
- Broadcom PCI adapters:
  - Dual and quad port 5709
  - Dual port 57711
  - Dual port 57712
- Intel 82576 quad port adapter

Starting with version 1.4, the Cisco Host Utility Upgrade also provides the following:

- Download selected platform images for the Windows operating system.
- Recover a corrupt BIOS through the Extensible Firmware Interface (EFI) shell.

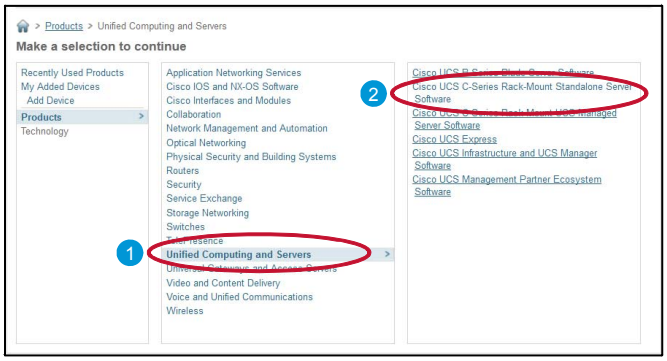
When you download the Cisco Host Utility Upgrade ISO image file, the file also contains the firmware image file.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Choose C-Series Software at Cisco.com

- Go to http://www.cisco.com/cisco/software/navigator.html.
- Choose **Unified Computing and Servers** in the middle column.
- Choose **Cisco UCS C-Series Rack-Mount Standalone Server Software** in the right column.



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

The first step is to get the Cisco Host Utility Upgrade ISO image file from Cisco.com. To retrieve the file, follow these steps:

Step 1 Go to http://www.cisco.com/cisco/software/navigator.html.

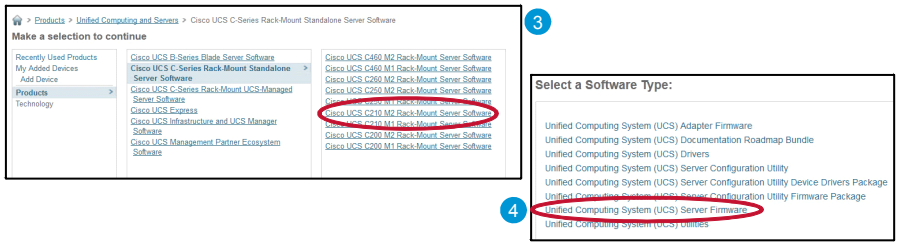
Step 2 In the middle column, choose **Unified Computing and Servers**.

Step 3 In the right column, choose **Cisco UCS C-Series Rack-Mount Standalone Server Software**.

https://t.me/learningnets

Download Host Upgrade Utility

- Choose the server model and server firmware, version 1.4, and download Host Upgrade Utility.
- Extract and use as virtual media or prepare the image on local media.



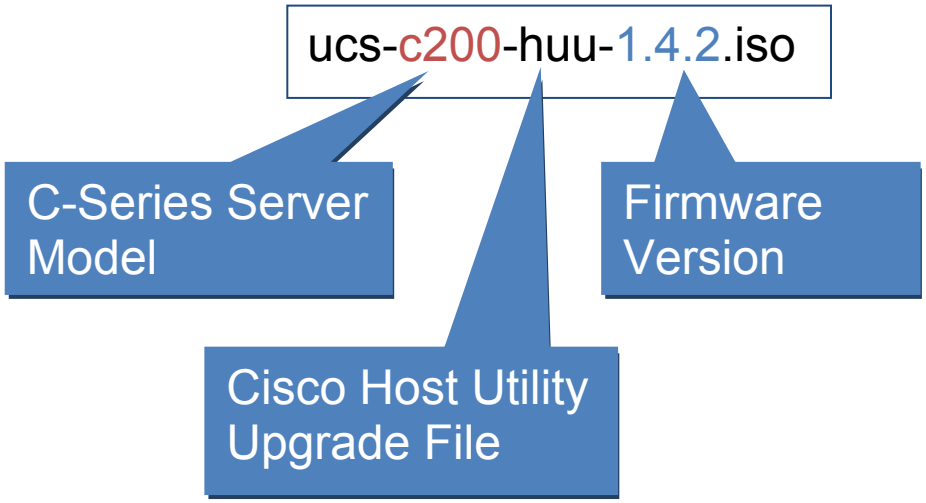
© 2012 Cisco and/or its affiliates. All rights reserved.

Step 1 From the list of servers, choose your server model.

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

Step 3 Select the correct version and download the Cisco Host Utility Upgrade image file.

The name of the Cisco Host Utility Upgrade is quite informative:



 © 2012 Cisco Systems, Inc.

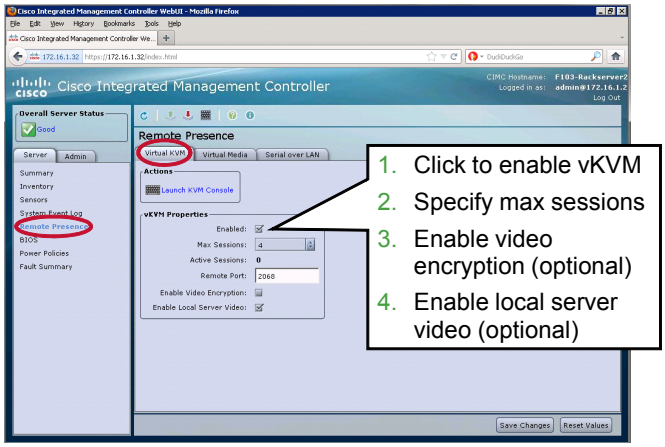
https://t.me/learningnets

Enable KVM and Virtual Media

This topic describes how to enable keyboard, video, and mouse (KVM) and virtual media.

Enable KVM from Cisco Integrated Management Controller

- From a browser, access the IP address of the Cisco UCS C-Series server Cisco Integrated Management Controller
- Navigate to **Server > Remote Presence > Virtual KVM**.



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

DCUCI v5.0—1-8

To use the remote KVM to connect to your server, first you have to enable the remote KVM in Cisco Integrated Management Controller. To enable KVM, follow these steps:

Step 1 Access the Cisco Integrated Management Controller GUI and log in.

Step 2 In the Navigation pane, choose **Remote Presence**.

Step 3 In the Content pane, choose the first tab, **Virtual KVM**.

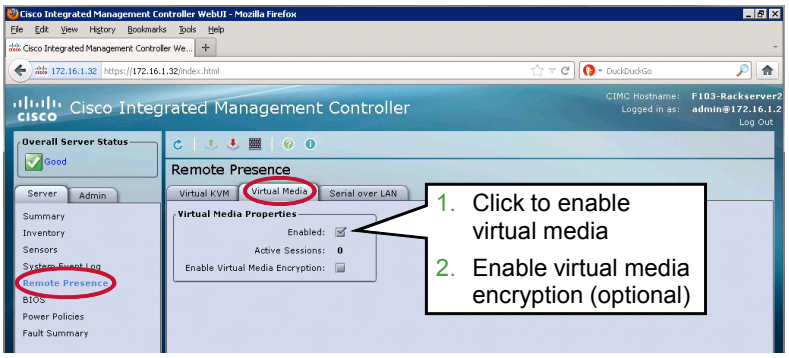
The following are available options:

- **Enable:** Enables the remote KVM.
- **Max Sessions:** Limits the maximum number of simultaneous sessions. Choose in the range from 1 to 4.
- **Active Sessions:** When enabled, you can see here the number of currently active sessions.
- **Remote Port:** You can define a custom port.
- **Enable Video Encryption:** Enables encryption of video data that is transmitted over the KVM communication session.
- **Enable Local Server Video:** Enables video output to a locally attached monitor.

https://t.me/learningnets

Enable Virtual Media from Cisco Integrated Management Controller

- Navigate to **Server > Remote Presence > Virtual Media**.



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

To use virtual media in the remote KVM console, so that you can remotely mount images for your server or use media remotely such as DVDs, you have to enable the virtual media feature.

To enable the virtual media feature, choose **Remote Presence** and in the content pane choose the **Virtual Media** tab.

The following are available options:

- **Enable:** Enables use of virtual media.
- **Active Sessions:** When enabled, you can see here the number of currently active sessions.
- **Enable Virtual Media Encryption:** Enables encryption of mapped data.

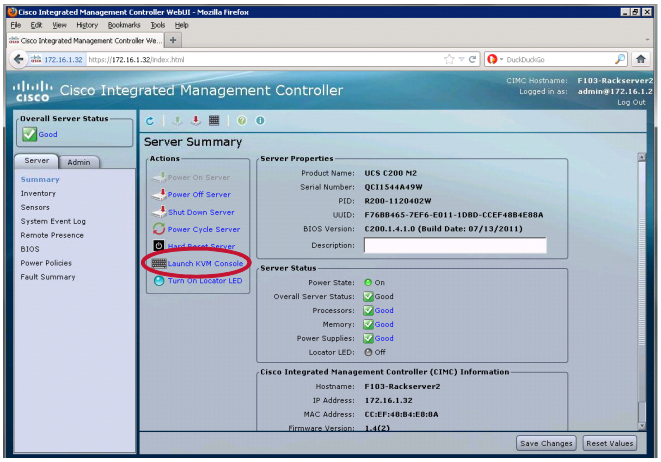
https://t.me/learningnets

Session Options in the KVM

This topic describes the settings that are available in the KVM console.

Launch KVM Console

- Access the Cisco Integrated Management Controller.
- Launch KVM.



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

DCUCI v5.0—1-11

To launch the remote KVM console, follow these steps:

Step 1 Open the GUI of Cisco Integrated Management Controller.

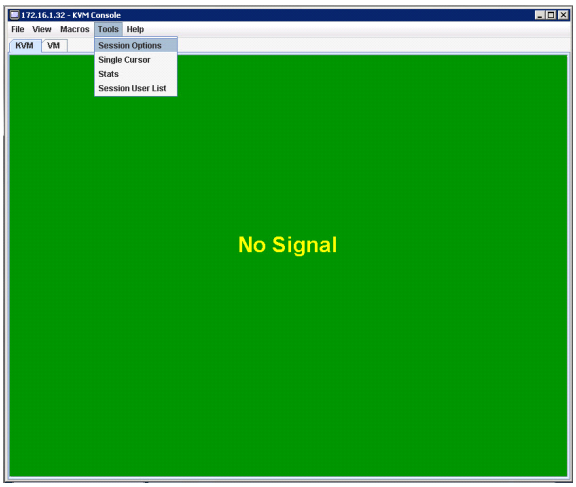
Step 2 Log in.

Step 3 From Server Summary, choose **Launch KVM Console**.

https://t.me/learningnets

KVM Tools Menu

- In the KVM window, click the **Tools** menu.
- Choose **Session Options**.



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

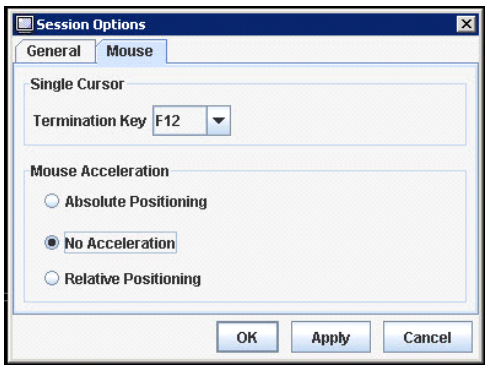
From the menu bar of the KVM console window, navigate to **Tools > Session Options** to access the available settings.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

KVM Session Options

- Under Single Cursor, F12 is the default termination key.
- Specify mouse acceleration.



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

The following are available options:

- **Termination Key:** This key is used when you enable the Single Cursor mode from Tools > Single Cursor. The single cursor mode is a feature that copes with the mouse cursor offset at some remote systems. When enabled, it will lock the mouse cursor within the KVM console window. To release the mouse cursor, press the termination key. The default is F12.
- **Mouse Acceleration:** You can choose one of the following options.
  - Absolute Positioning
  - No Acceleration
  - Relative Positioning

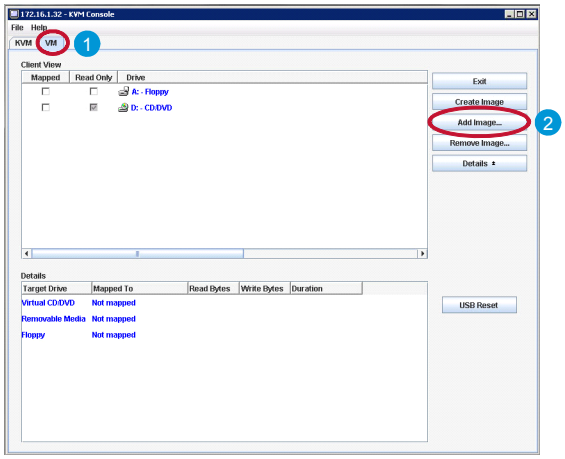
https://t.me/learningnets

Virtual Media and the Cisco UCS Host Upgrade Utility ISO Image

This topic describes the steps to launch virtual media and map the Cisco Host Utility Upgrade image.

Virtual Media Tab in KVM

- Click the **VM** tab in the KVM session window.
- Choose **Add Image**.



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

To map and use the Cisco Host Utility Upgrade image file, go to the Virtual Media tab in the KVM console window.

Note	How you access virtual media depends on the version of your KVM console. This lesson describes accessing virtual media from the VM tab in the KVM console window. If you do not see a VM tab, navigate to **Tools > Launch Virtual Media** in the menu bar.

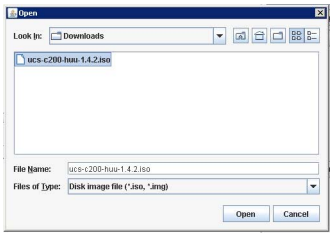
Click **Add Image** to open the browser window and select the Cisco Host Utility Upgrade ISO file.

 © 2012 Cisco Systems, Inc.

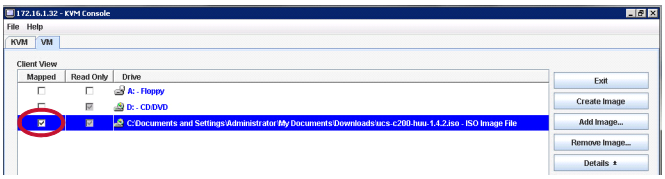
https://t.me/learningnets

Map the Host Upgrade Utility Image

- Choose the Host Upgrade Utility ISO image file.



- Check the **Mapped** check box to map the image.



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

In the new browser window, select the Cisco Host Utility Upgrade ISO image file that you downloaded earlier in this lesson.

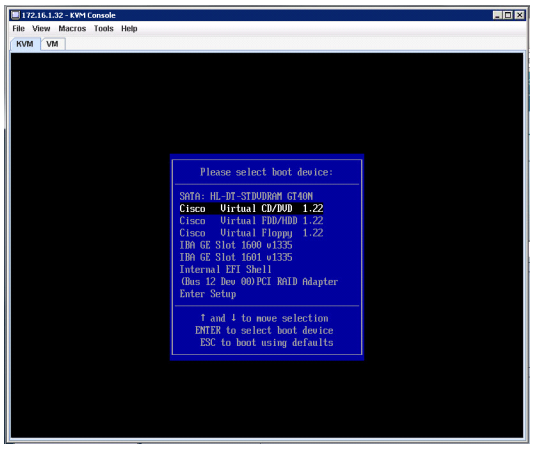
Once selected, you will see the file in the Client View window. You have selected an image, but the image is not yet mapped to the server. To map the image file, click the Mapped check box.

Note	If you do not work with the VM tab, you have to leave the VM window open. If you close the VM window, or if you close the KVM console session, the image will be unmapped and unavailable to the server.

https://t.me/learningnets

Boot from Cisco Virtual CD or DVD

- Power up the server.
- Press **F6** to choose the Cisco Virtual CD/DVD drive to boot.



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

Next, force the server to boot from the Cisco Host Utility Upgrade image file. To do so, follow these steps:

Step 1 Power up the server or reboot it.

Step 2 Press **F6** to access the boot menu.

Step 3 Choose **Cisco Virtual CD/DVD** from the available options.

 © 2012 Cisco Systems, Inc.

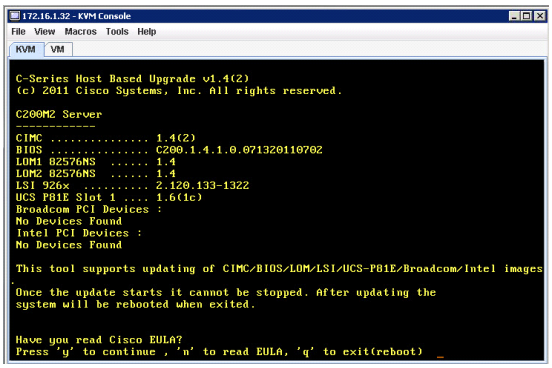
https://t.me/learningnets

Upgrade All Components

This topic describes how to perform component upgrades with the Cisco Host Utility Upgrade tool.

Agree to EULA

- The Cisco End User License Agreement appears.
- To read it, type **n**.
- To continue, type **y**.



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

When the Cisco Host Utility Upgrade loads, the first screen will ask you to accept the Cisco End User License Agreement.

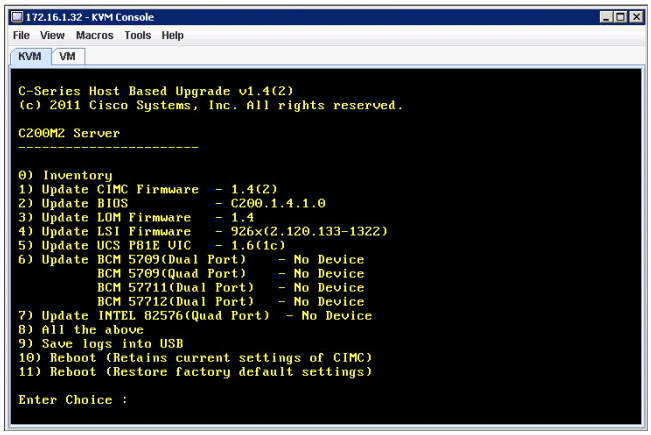
The following are the available options:

- Press the **y** key to agree and continue.
- Press the **n** key to read the Cisco end user license agreement (EULA).
- Press the **q** key to quit.

https://t.me/learningnets

Cisco Host Utility Upgrade Menu

- The Cisco Host Utility Upgrade menu provides choices.
- To upgrade all components, choose option 8 – All the Above.



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

Once you have agreed to the Cisco EULA, you will see the Cisco Host Utility Upgrade menu.

You will see a list of choices with corresponding numbers. To choose an option, type its number and press **Enter**.

Information for the current version of the firmware will be provided next to each component.

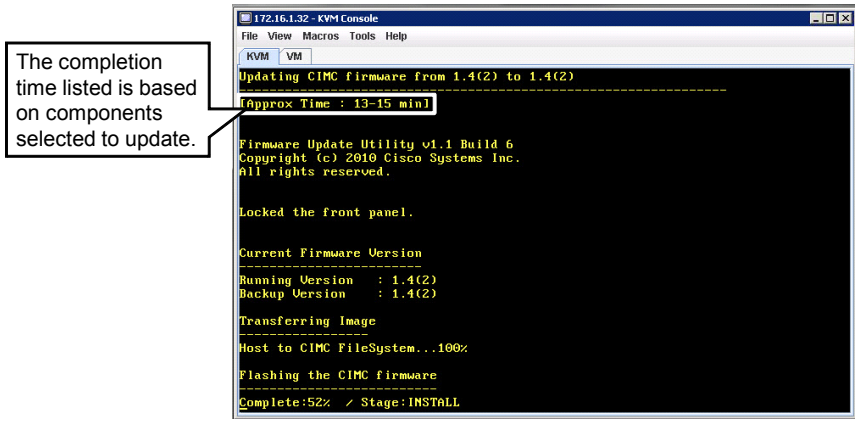
To upgrade all components, choose **8) All the Above**.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Upgrade Progress

- The Cisco Host Utility Upgrade provides information for the following:
  - Status of the upgrade progress
  - Currently upgraded components



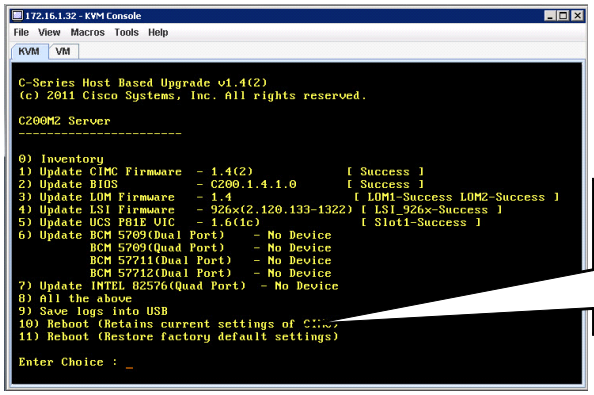
© 2012 Cisco and/or its affiliates. All rights reserved.

During the upgrade, the Cisco Host Utility Upgrade will provide information about the overall upgrade progress, estimated upgrade time, and the component currently being upgraded.

https://t.me/learningnets

Finalize Upgrade

- Wait to see confirmation of a successful upgrade.
- To finalize the upgrade process, choose one of the following:
  - 10) Reboot (Retains current settings of CIMC)
  - 11) Reboot (Restore factory default settings)



During Cisco Integrated Management Controller reboot, the connection with the server will be lost.

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

After the upgrade has completed, the Cisco Host Utility Upgrade indicates the successful end of the process.

The last step is to reboot the Cisco Integrated Management Controller. You can choose from two options:

- Reboot Cisco Integrated Management Controller and preserve current settings.
- Reboot Cisco Integrated Management Controller and reset it to the factory default settings.

Note When you reboot the Cisco Integrated Management Controller, you will lose connectivity. The reboot will reset your KVM console session and your session to the Cisco Integrated Management Controller.

https://t.me/learningnets

Summary

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

Summary

- Before you can upgrade the components of your Cisco UCS C-Series server, you must download the Cisco UCS Host Upgrade Utility from Cisco.com.
- To perform upgrades with the Host Upgrade Utility, you need the KVM console and virtual media. Enable these features from the Cisco Integrated Management Controller settings.
- By navigating to Tools > Session Options in the KVM session window, you can set the termination key and mouse acceleration.
- From the Virtual Media tab, mount the Cisco UCS Host Upgrade Utility ISO image, reboot the server, and choose Cisco Virtual CD/DVD from the boot menu.
- Perform an upgrade of all components by selecting option 8 – All the Above.

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

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 5

Provisioning Monitoring and Logging on the Cisco UCS C-Series Server

Overview

The Cisco Unified Computing System (UCS) C-Series servers support Simple Network Management Protocol (SNMP) versions 1, 2c, and 3, and syslog to export server-related information. Locally, Cisco Integrated Management Controller gathers system-generated logs and can export remotely the tech support file of the server. This lesson describes how to provision these features and know their limits.

Objectives

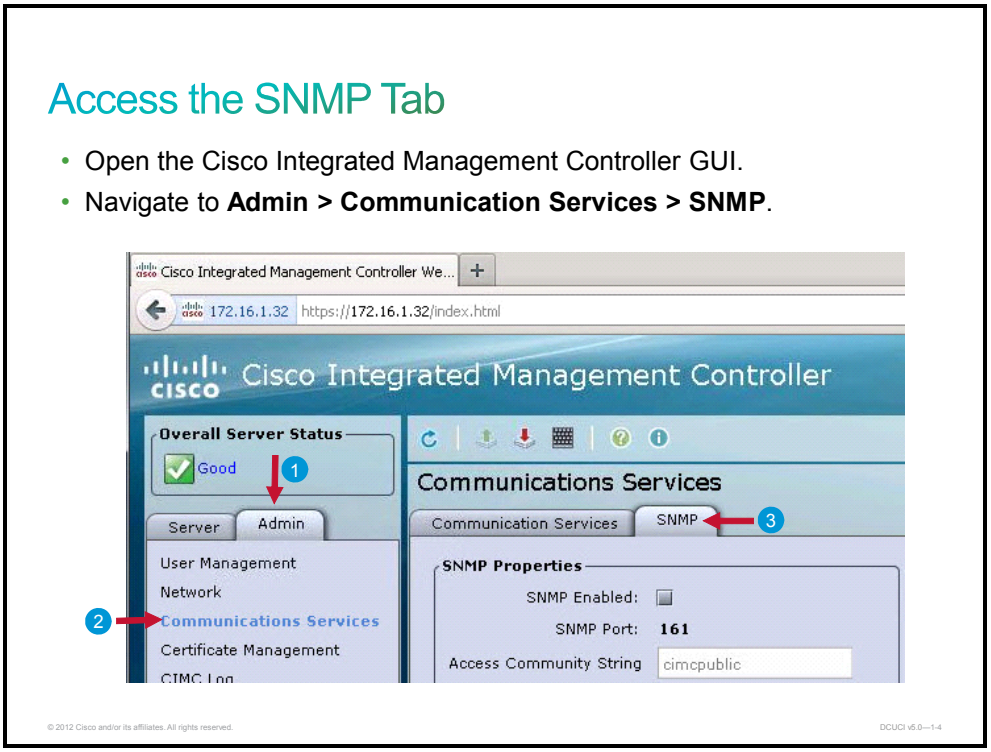
Upon completing this lesson, you will be able to provision SNMP and syslog, and use C-Series monitoring tools. This ability includes being able to meet these objectives:

- Provision SNMP
- Provision syslog destinations for server logging data
- Access data from the system event log
- Export technical support information

https://t.me/learningnets

Provision SNMP

This topic describes the steps to provision SNMP.



Cisco UCS C-Series servers support SNMP versions 1, 2c, and 3. SNMPv3 provides enhanced security features, such as message integrity, authentication, and encryption of messages.

To provision SNMP on C-Series servers, you have to access the Cisco Integrated Management Controller GUI.

Step 1 Select the **Admin** tab.

Step 2 Select **Communication Services** in the **Navigation** pane.

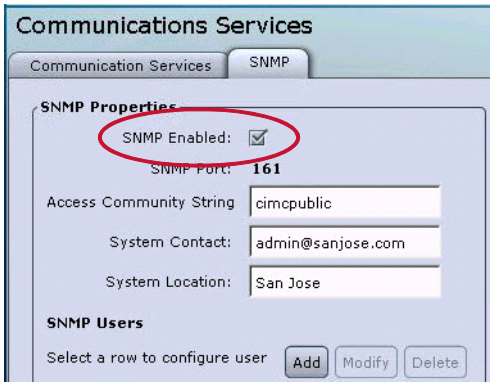
Step 3 Select the **SNMP** tab in the **Content** pane.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Enable SNMP

- Enable SNMP.
- Provision general SNMP settings.



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

SNMP provisioning is a multistep process. In the first step, enable the SNMP feature and specify the general settings. The following are the available options:

- **SNMP Enabled:** Click this check box to enable SNMP.
- **SNMP Port:** This value indicates the SNMP server port that is used for communication. This value cannot be changed.
- **Access Community String:** This string is the default community name or username that will be included in SNMP messages.
- **System Contact:** This option is the email address of the person who is responsible for the system.
- **System Location:** This option is the physical location of the system.

https://t.me/learningnets

Provision Trap Settings

- Specify the SNMP community string.
- Specify SNMP version v1, v2, or v3.
- Choose **Trap** or **Inform**.

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

The next step is to provision SNMP trap settings. The following are the available options:

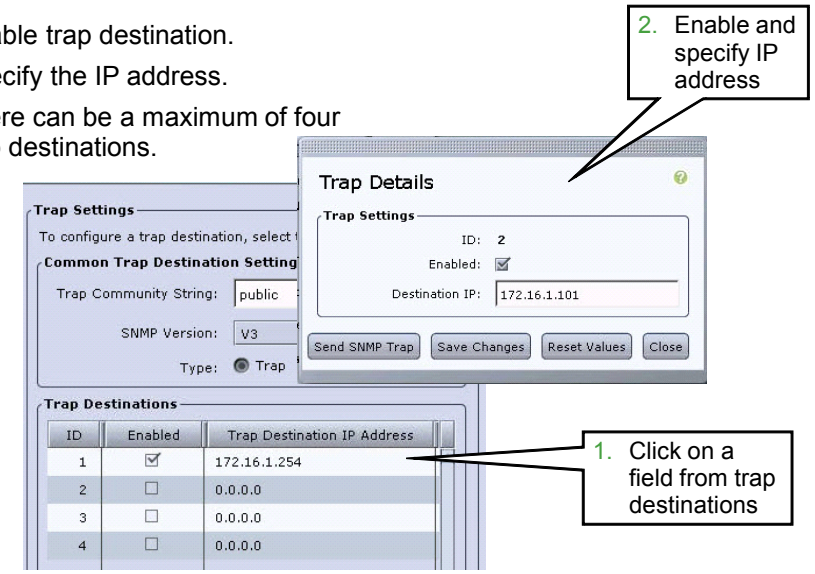
- **Trap Community String:** This setting is the SNMP community group.
- **SNMP Version:** The available options are v1, v2, or v3.
- **Type:** Specify that the SNMP messages are traps or informs.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision Trap Destinations

- Enable trap destination.
- Specify the IP address.
- There can be a maximum of four trap destinations.



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

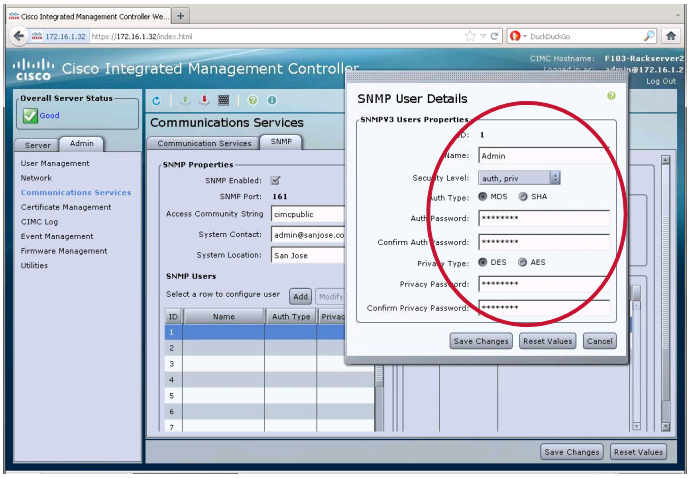
Provision the SNMP servers that will receive the SNMP messages. Click a row and a new window will open. The following are the available options:

- **ID:** The trap destination ID is a value that cannot be changed.
- **Enabled:** Check this check box to enable the trap destination.
- **Trap Destination IP Address:** Specify the IP address of the SNMP server.

https://t.me/learningnets

Provision SNMP v3 Users

- Select a user field and click **Add**.
- In the new window, specify properties for users.



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

SNMP security is based on a combination of security models and security levels. The security models specify the authentication for the SNMP users and to which groups they belong. The security levels specify the security privilege within the security model.

The security in SNMPv3 results in the following options:

- Authentication that is based on username, without encryption of SNMP messages, is also referred to as noAuthNoPriv.
- Authentication that is based on Message Digest 5 (MD5) or Secure Hash Algorithms (SHA), without encryption or authNoPriv.
- Authentication that is based on MD5 or Secure Hash Algorithm (SHA) and Data Encryption Standard (DES) 56-bit-based encryption of SNMP packets or authPriv.

To use SNMPv3 in the Cisco UCS C-Series servers, you have to specify the SNMP users and their attributes to define the security strategy. To do so, click one of the fields in the SNMP Users section and click **Add**.

A new window opens displaying the following options:

- **ID:** This value is not changeable.
- **Name:** The name is the SNMP username.
- **Security Level:** This option defines the security strategy that will be used with this user:
  - **no auth, no priv:** The user will be authenticated only based on the username. No password will be required, and no encryption will be performed.
  - **auth, no priv:** The user will be authenticated and authorized based on username and password, using the Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms. The communication will not be permitted.
  - **auth, priv:** The same authentication and authorization mechanism as auth, no priv. The communication will be encrypted based on DES or the Advanced Encryption Standard (AES) algorithm. For this encryption, you have to specify the encryption key, which is called the Privacy Password.

https://t.me/learningnets

- **Auth Type:** Choose MD5 or SHA.
- **Auth Password:** Specify the password that is used for user authentication and authorization.
- **Confirm Auth Password:** Retype the password.
- **Privacy Type:** Choose the encryption algorithm DES or AES.
- **Privacy Password:** Specify the encryption key.
- **Confirm Privacy Password:** Retype the password.

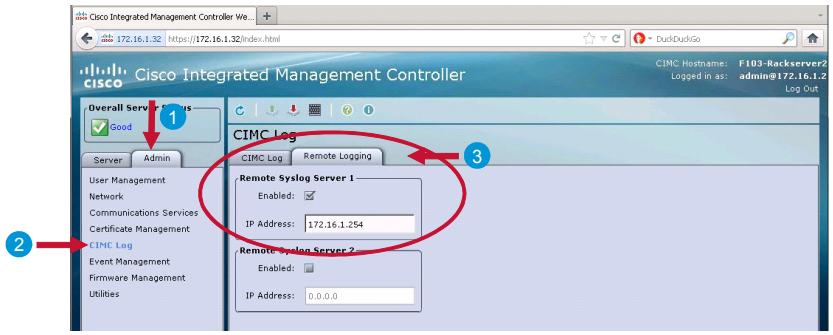
https://t.me/learningnets

Provision Syslog Destinations

This topic describes the steps to provision remote syslog servers.

Provision Remote Syslog Servers

- Navigate to **Admin > CIMC Log > Remote Logging**.
- Enable a remote syslog server and specify an IP address.
- There can be a maximum of two remote syslog servers.



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

DCUCI v5.0—1-10

To specify remote syslog servers, perform the following steps:

Step 1 Select the **Admin** tab.

Step 2 Choose **CIMC Log**.

Step 3 Choose the **Remote Logging** tab in the **Content** pane.

You can provision up to two remote syslog servers. Follow these steps:

Step 1 Enable the server by clicking the Enabled check box.

Step 2 Specify the IP address of the server.

 © 2012 Cisco Systems, Inc.

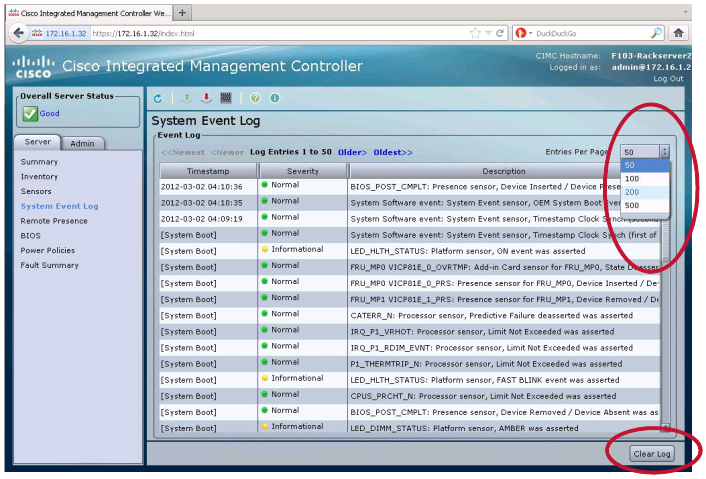
https://t.me/learningnets

Access the System Event Log

This topic describes how to access the system event logs.

System Event Log

- From the Server tab, choose **System Event Log**.
- The available options include Entries Per Page and Clear Log.



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

The server-generated logs can be found in the System Event Log section in the Server tab of the Cisco Integrated Management Controller GUI.

When you choose this option, the content pane will show a list of the logs that are generated by the server. These log messages are related only to the server.

The Cisco Integrated Management Controller-generated logs can be found by choosing CIMC Log from the Admin tab.

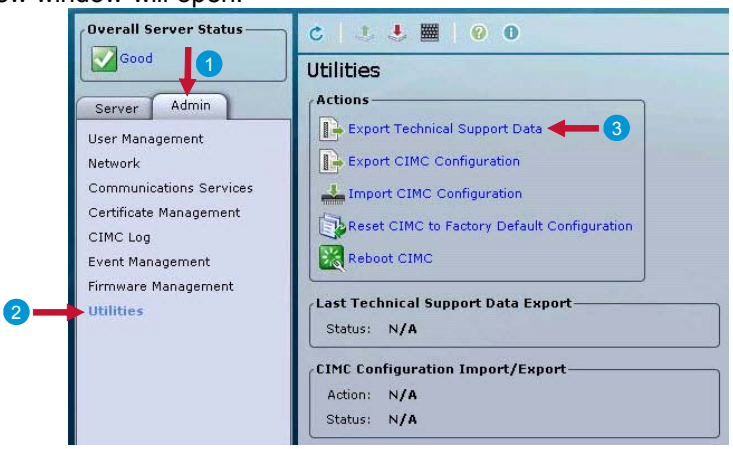
https://t.me/learningnets

Export Technical Support Information

This topic describes the steps to export the C-Series server tech support file.

Export Tech Support Data

- Navigate to **Admin > Utilities > Actions > Export Technical Support Data**.
- A new window will open.



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

Just like any device that is created by Cisco, C-Series servers can generate and export tech support files. This export can be useful during troubleshooting and is always required when you open a case at the Cisco Technical Assistance Center (TAC).

To generate and export the tech support file:

Step 1 Select the **Admin** tab.

Step 2 Select **Utilities** in the **Content** pane.

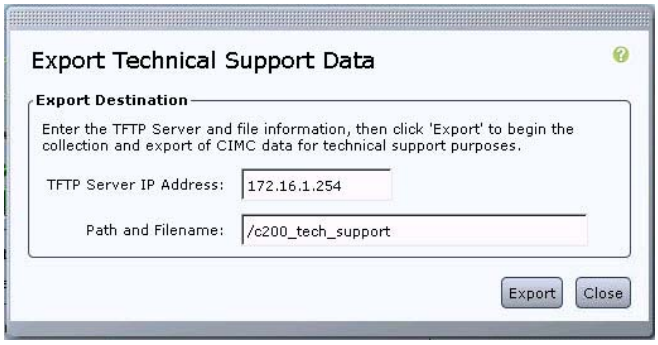
Step 3 Click **Export Technical Support Data**.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Specify Remote TFTP Server

- Specify the remote TFTP server IP address.
- Specify the remote relative path and filename.
- Click **Export** to start the tech support export.



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

When the tech support file is generated, the file will be exported and stored to a remote server, using the TFTP protocol. In the new window that opens, you have to specify the following information:

- **TFTP Server IP Address**
- **Path and Filename:** The relative path on the remote server and the filename for the stored tech support file

When you are ready, click Export and the tech support file will be prepared and sent to the remote server.

https://t.me/learningnets

Summary

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

Summary

- SNMP v1, v2, and v3 are supported. You have to enable SNMP, specify a version and community string, and choose trap or inform messages. If you use SNMPv3, you also have to specify users.
- Logs to remote syslog servers can be exported. A maximum of two remote syslog servers are supported.
- System event logs are the logs generated by the server. You can access these logs by choosing System Event Log from the Server tab.
- Cisco UCS C-Series servers can generate and export a tech support file to a remote TFTP server.

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

https://t.me/learningnets

Lesson 6

Provisioning LAN and SAN Connectivity in the Cisco Integrated Management Controller

Overview

The Cisco Unified Computing System (UCS) C-Series Integrated Management Controller allows you to access and provision your server. From the GUI of the Cisco Integrated Management Controller, you can access and provision the Cisco UCS P81E Virtual Interface Card (VIC). You can add or remove virtual Ethernet and virtual host bus adapters (vHBAs). You can change the MAC and world wide name (WWN) addresses. You can enable and disable functionality such as receive-side scaling (RSS) and Fibre Channel SAN boot.

Objectives

Upon completing this lesson, you will be able to use the Cisco Integrated Management Controller to provision LAN and SAN connectivity for the C-Series server. This ability includes being able to meet these objectives:

- Provision the Cisco UCS P81E VIC to allow FCoE
- Provision a locally administered MAC address for the A- and B-side 10 Gigabit Ethernet interfaces
- Enable RSS on Ethernet adapters
- Provision locally administered addresses for the Fibre Channel interface WWPN and WWNN
- Provision the Fibre Channel boot target for the A- and B-side Fibre Channel interfaces

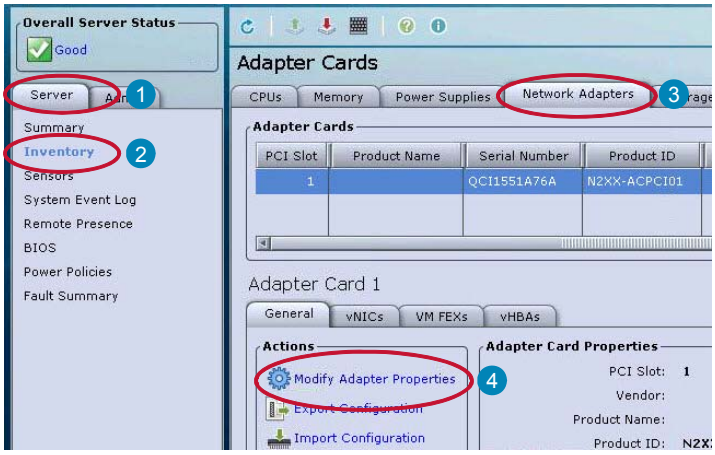
https://t.me/learningnets

Provision the Cisco UCS P81E VIC to Allow FCoE

This topic shows how to enable Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP).

Access Network Adapter Properties

- Navigate to **Server > Inventory > Network Adapters**.
- Click **Modify Adapter Properties**.



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

The Cisco UCS P81E VIC can be installed in the C-Series servers to provide I/O consolidation and virtualization. The card is equipped with two 10-Gb/s physical Ethernet interfaces that support FCoE, to connect to the upstream fabric interconnects or Cisco Nexus switches. At the server side, the card uses a Peripheral Component Interconnect Express (PCIe) interface to connect to the server.

The architecture of the Cisco UCS P81E card allows up to 16 virtual Fibre Channel and 16 virtual Ethernet adapters to be provisioned and presented to the operating system of the server.

The hardware of the C-Series servers in standalone mode is managed and provisioned through the Cisco Integrated Management Controller. Follow these steps to access and change the settings for the Cisco P81E VIC:

Step 1 Select the **Server** tab.

Step 2 Choose **Inventory** in the **Content** pane.

Step 3 Select the **Network Adapters** tab in the **Navigation** pane.

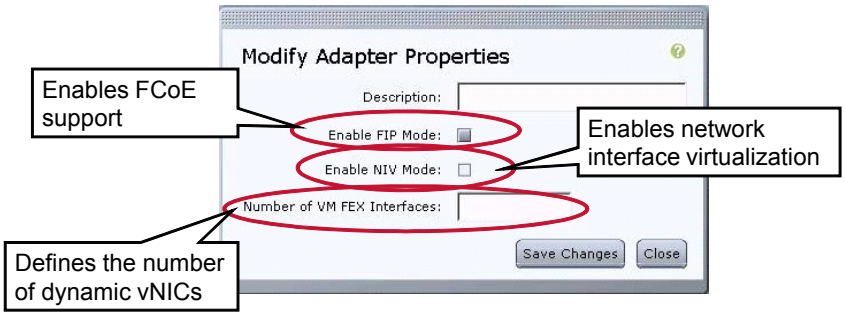
Step 4 Click **Modify Adapter Properties**.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Enable FIP and NIV Modes

- FIP is needed for FCoE support.
- NIV enables the Cisco Adapter FEX technology.



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

To enable support for the FCoE protocol, you must enable FIP.

To enable FIP, click **Modify Adapter Properties**.

In the new window, the following are the available options:

- **Description:** Enter a description of the adapter.
- **Enable FIP Mode:** When this check box is clicked, FIP is enabled.
- **Enable NIV Mode:** Check this box to enable network interface virtualization (NIV) mode. This mode is the adapter fabric extender mode. In this mode, you can do the following:
  - Assign virtual network interface cards (vNICs) and vHBAs to specific port channels.
  - Associate vNICs and vHBAs to a port profile.
  - Enable vNIC failover.
- **Number of VM-FEX Interfaces:** If NIV mode is enabled, you can specify how many dynamic vNICs the Cisco Integrated Management Controller will provision. The value is an integer in the range 0 to 112.

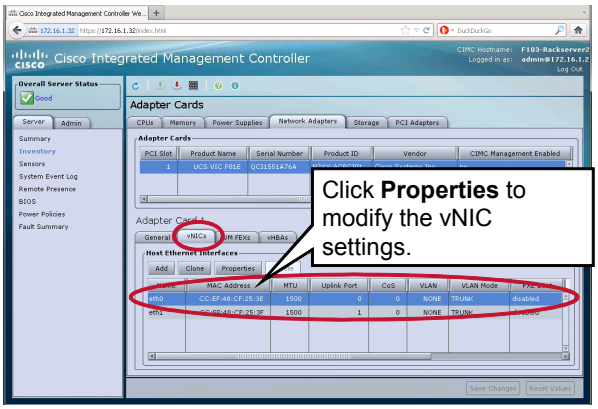
https://t.me/learningnets

Provision Locally Administered MAC Addresses on Ethernet Interfaces

This topic describes how to provision a MAC address for virtual Ethernet adapters.

Choose vNIC

- By default, there are two vNICs:
  - Eth0, connected to uplink port 0 (side A)
  - Eth1, connected to uplink port 1 (side B)
- Choose vNIC to provision MAC address.



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

By default, the Cisco UCS P81E VIC card provides two virtual Ethernet adapters, which are named eth0 and eth1. Eth0 communicates through uplink port 0, which can be assumed to be data path A, and eth1 communicates through uplink port 1, which provides data path B.

The Cisco UCS P81E VIC provides MAC addresses for the virtual Ethernet adapters. You can manually provision specific MAC addresses. To do so, follow these steps:

Step 1 Open the Cisco Integrated Management Controller and log in.

Step 2 Navigate to **Server > Inventory > Network Adapters**.

Step 3 Choose the **vNICs** tab.

Step 4 Select **eth0** or **eth1**.

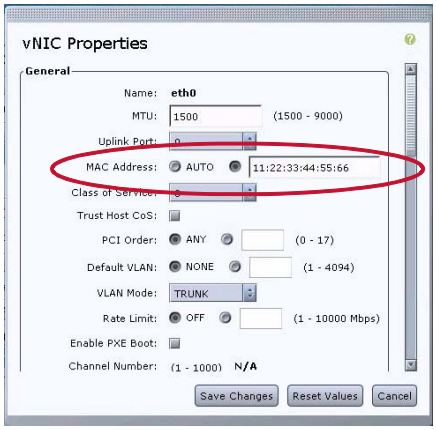
Step 5 Click **Properties**.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Modify MAC Address

- The P81E VIC comes with predefined MAC addresses.
- To provision a specific MAC address, change the setting from AUTO.



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

In the new window, you will be provided with all of the options that can be tuned for the virtual Ethernet adapter.

The MAC address option, by default, is set to auto. This setting means that the server will use the MAC address that is provisioned by the Cisco UCS P81E card. To specify a different MAC address manually, click the other radio button and, in the MAC address field, input the new address.

Click Save Changes to finish.

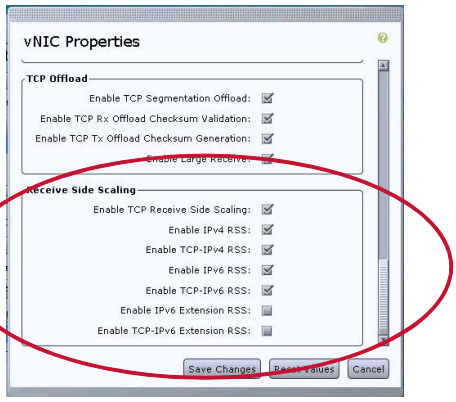
https://t.me/learningnets

Enable RSS on Ethernet Adapters

This topic describes how to enable RSS.

Enable RSS

- RSS distributes the receive network processing load among multiple CPUs and cores.
- RSS has no effect if only one single-core CPU is present.



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

RSS is a feature that allows you to utilize multiple CPUs and multiple cores per CPU to process the receiving network load. Without RSS, all of the receive network traffic is processed by one CPU and by only one core of the CPU. RSS distributes receive processing to all of the CPUs and all of their cores.

Note	RSS does not use hyperthreaded processors because hyperthreaded CPUs share the same execution engine.
Note	RSS is required if you want to use Intel I/O Acceleration Technology.

The Cisco UCS P81E card allows the RSS feature to be enabled and the following are available options:

- **Enable TCP Receive Side Scaling:** Click this check box to enable RSS.
- **Enable IPv4 RSS:** Click to enable RSS on IPv4 networks.
- **Enable TCP-IPv4 RSS:** Enable RSS for TCP transmissions on IPv4 networks.
- **Enable IPv6 RSS:** Enable RSS on IPv6 networks.
- **Enable TCP-IPv6 RSS:** Enable RSS for TCP transmissions on IPv6 networks.
- **Enable IPv6 Extension RSS:** Enable RSS for IPv6 extensions.
- **Enable TCP-IPv6 Extension RSS:** Enable RSS for TCP transmissions on IPv6 networks.

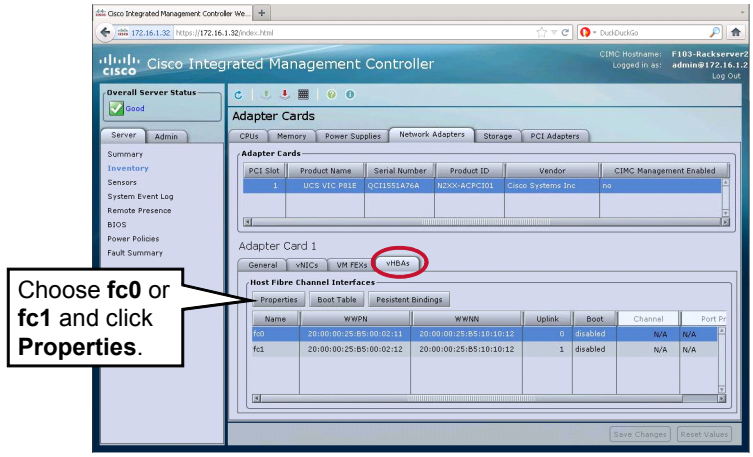
https://t.me/learningnets

Provision Locally Administered WWNN Addresses

This topic describes how to provision world wide node name (WWNN) and world wide port name (WWPN) addresses.

Choose vHBA

The P81E VIC provides two vHBAs.



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

By default, the Cisco UCS P81E card provides two vHBAs:

- fc0 communicates through uplink port 0
- fc1 communicates through uplink port 1

Because the uplink ports are Ethernet ports, the vHBA communication with storage systems is based on the FCoE protocol.

To provision the WWNN and WWPN addresses, follow these steps:

Step 1 Navigate to **Server > Inventory > Network Adapters**.

Step 2 Choose the **vHBAs** tab.

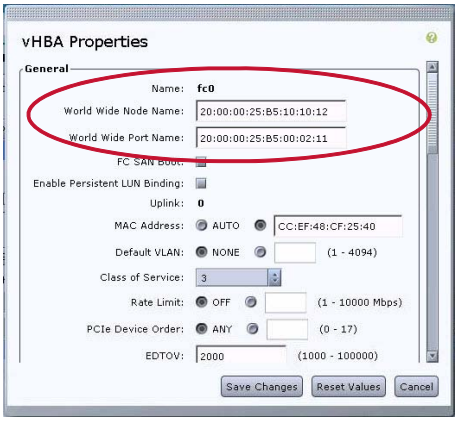
Step 3 Select **fc0** or **fc1**.

Step 4 Click **Properties**.

https://t.me/learningnets

Modify WWN Addresses

- WWNN and WWPN addresses can be locally administered.
- The server must be rebooted for the settings to take effect.



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

In the vHBA properties window, you can modify the WWNN and WWPN addresses.

To finish, click Save Changes.

Note	For the changes to be applied, you have to reboot the server.

© 2012 Cisco Systems, Inc.

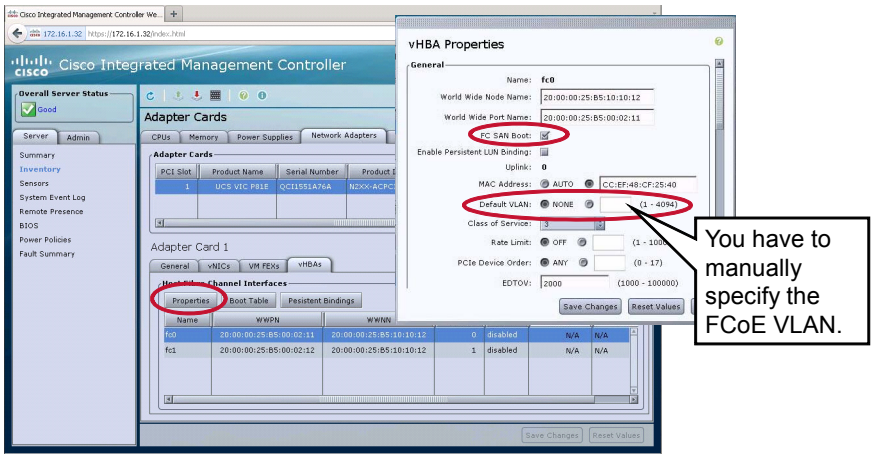
https://t.me/learningnets

Provision the Fibre Channel Boot Target

This topic describes how to provision the Fibre Channel SAN boot target.

Enable FC SAN Boot

- In vHBA properties, enable **FC SAN Boot**.
- Cisco UCS C-series servers cannot find the FCoE VLAN. It must be specified manually.

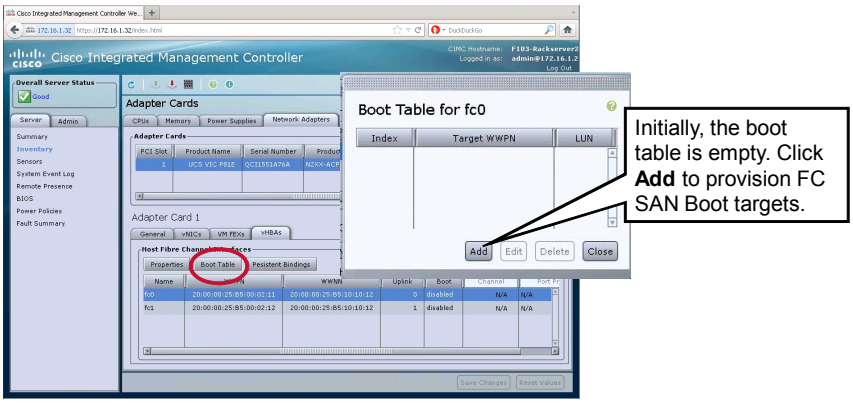


© 2012 Cisco and/or its affiliates. All rights reserved.

If you need your C-Series server to boot from a storage system in your SAN infrastructure, you have to specify an FC SAN Boot target. The first step is to enable the FC SAN Boot functionality, which is done in the vHBA properties window. Check the FC SAN Boot check box.

Access Boot Table

- SAN boot targets are provisioned in the boot table.
- From the Server tab, navigate to **Inventory > Network Adapters > vHBAs** and click the **Boot Table** tab.



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

https://t.me/learningnets

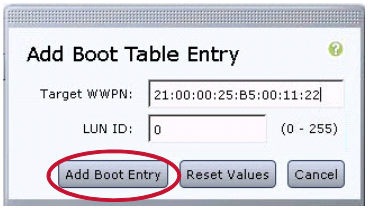
The next step is to provision the SAN boot target itself. SAN boot targets are provisioned in the boot table.

To access the boot table, click **Boot Table** in the **vHBAs** tab. A new window will open that lists the entries in the boot table. Initially, there will be no entries.

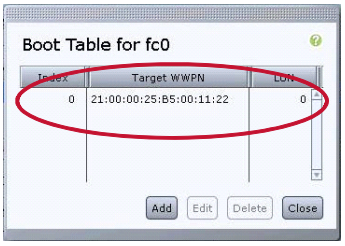
Click **Add** to create a SAN boot target.

Provision SAN Boot Target

- Specify the WWPN and LUN ID of the SAN boot target.



- Verify that the boot target is present in the boot table.



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

In the Add Boot Table Entry window, you have to specify the following:

- **Target WWPN:** The WWPN address of the SAN boot target
- **LUN ID:** The logical unit number (LUN) ID, values in the range 0 to 255

To finish, click **Add Boot Entry**.

The new FC SAN Boot target will appear in the boot table immediately.

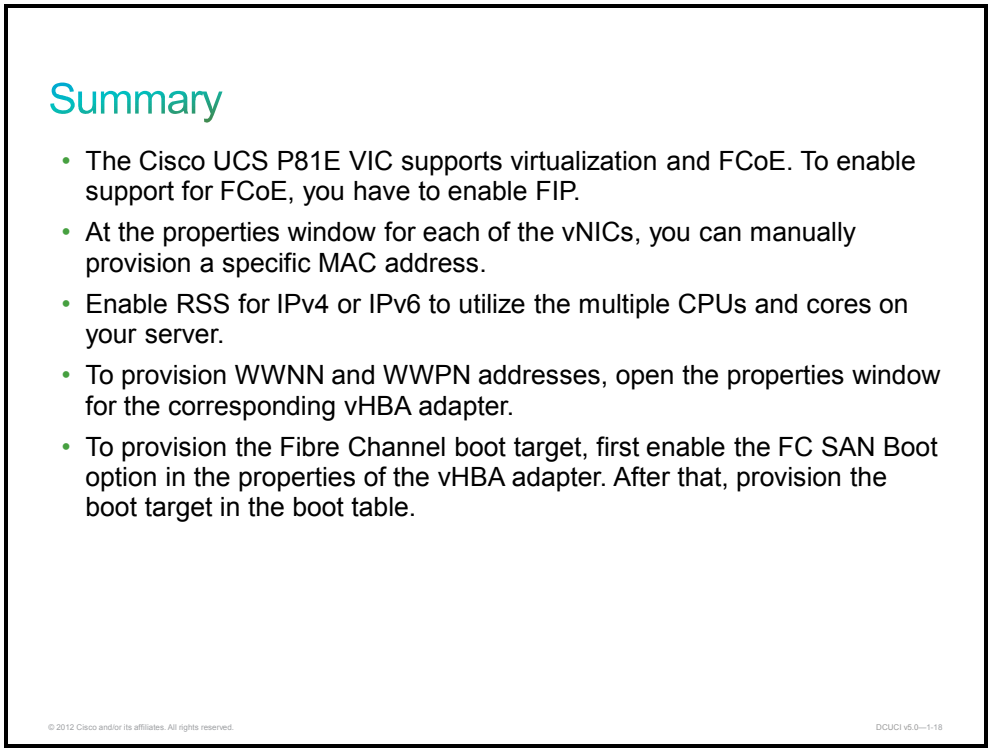
Note	Most operating systems and hypervisors require a LUN ID of 0 or 1 as a boot LUN.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

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



References

For additional information, refer to this resource:

- Cisco Systems, Inc. *Cisco UCS Site Preparation Guide* http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/site_prep/guide/ucs_site_prep.html

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 7

Provisioning RAID on the Cisco UCS C-Series Server

Overview

The Cisco Unified Computing System (UCS) C-Series server features different Redundant Array of Independent Disks (RAID) controllers for hard drive control and management. RAID controllers allow different modes of operation, which provide for fault tolerance and different levels of performance from various drives. This lesson discusses the different RAID levels and how to configure them.

Objectives

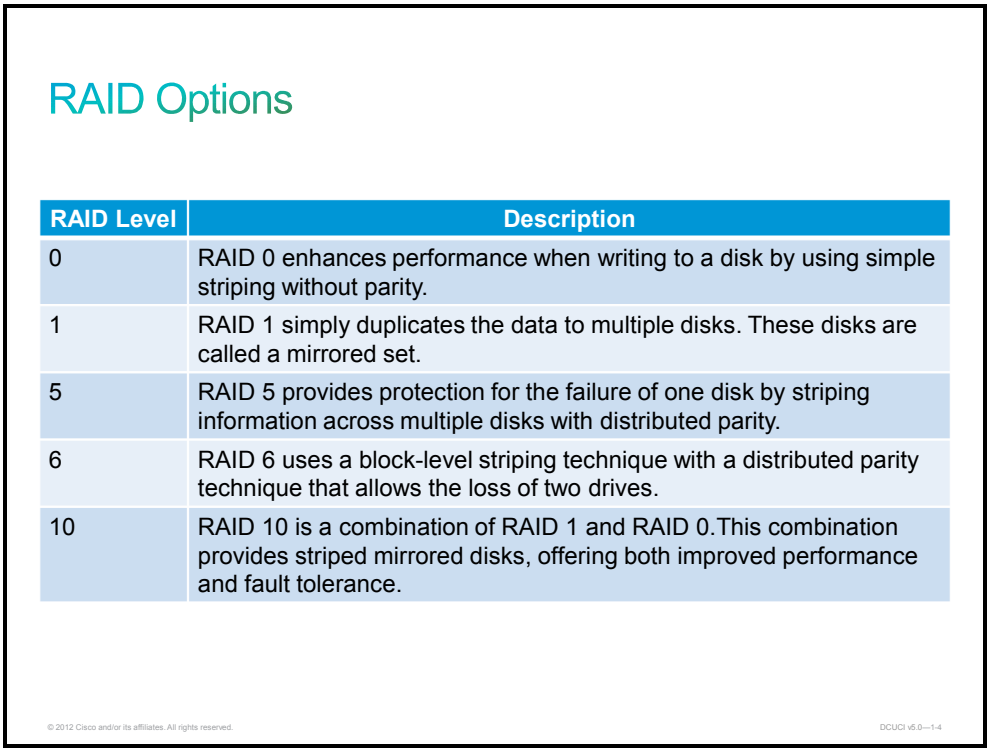
Upon completing this lesson, you will be able to use the LSI MegaRAID web user interface to provision local hard drives into a RAID 5 array. This ability includes being able to meet these objectives:

- Describe the characteristics of RAID levels 0, 1, 5, 6, and 10
- Boot the server in the KVM and access the LSI MegaRAID web user interface
- Add all local hard drives to a RAID 5 array and save the configuration

https://t.me/learningnets

RAID Characteristics

This topic describes the various RAID modes.



The table describes different RAID levels and provides a brief description of each. (A complete discussion of RAID technology is out of the scope of this class.)

RAID 0 enhances performance when writing to a disk. By using simple striping without parity, data can be simultaneously written across several disks. This process increases bandwidth, which ultimately improves performance. However, RAID 0 provides no redundancy.

Unlike RAID 0, RAID 1 provides fault tolerance. In short, RAID 1 simply duplicates the data to multiple disks. These disks are called a mirrored set. If a disk failure occurs, the remaining mirrored drives can continue operations. RAID 1 does not perform striping, which is why there is no performance improvement.

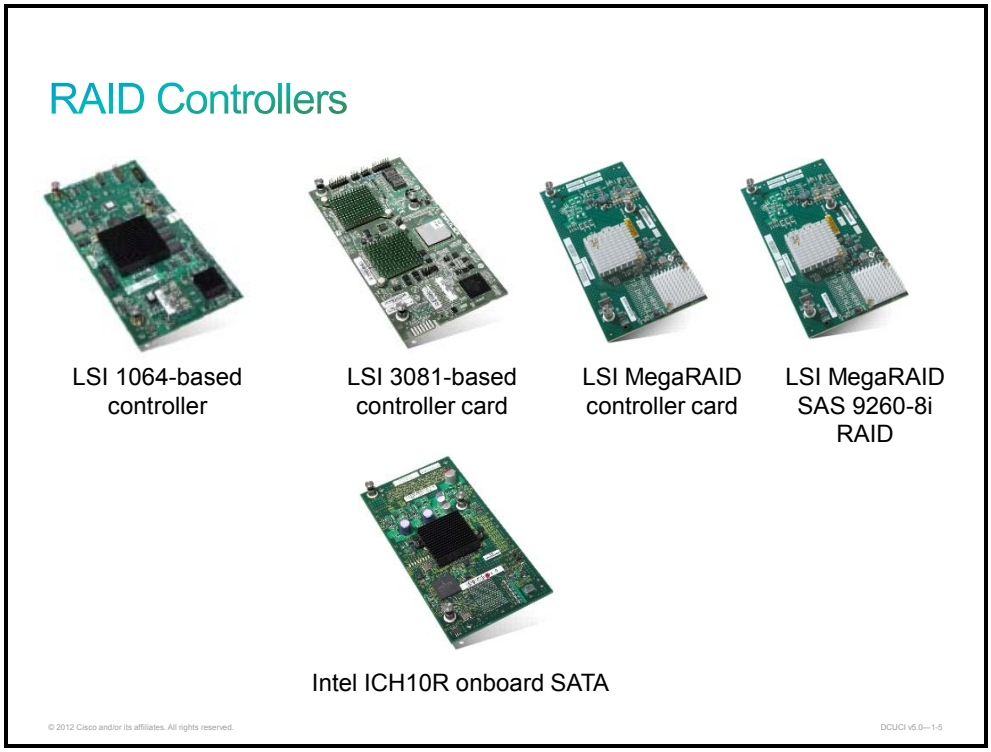
RAID 5 provides fault tolerance and improved performance. RAID 5 provides protection for the failure of one disk by striping information across multiple disks with distributed parity. If one drive fails, the remaining drives can continue operations. The replacement drive will be rebuilt to participate in the RAID process.

RAID 6 is very similar to RAID 5 in that it provides fault tolerance and improves performance. RAID 6 uses a block-level striping technique with distributed parity that allows the loss of two drives.

RAID 10 is a combination of RAID 1 and RAID 0. This combination provides striped mirrored disks, offering both improved performance and fault tolerance.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



Different controllers are available on the Cisco C-Series servers. Some of the models, like the C200 and C210, have onboard, integrated RAID controllers. However, all the C-Series models support various RAID controllers that can be added to the chassis. The controllers that are shown in the figure give you an idea of some of the available adapters that can be used in the C-Series servers.

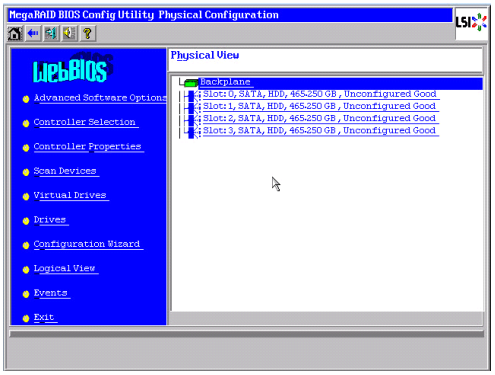
https://t.me/learningnets

Boot the Server and Access the LSI MegaRAID Interface

This topic describes how to access the LSI WebBIOS Configuration Utility.

LSI MegaRAID WebBIOS Configuration Utility

- The WebBIOS Configuration Utility is embedded in the BIOS of the LSI controller.
- The utility allows for provisioning, managing, and troubleshooting the LSI MegaRAID controller.



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

To configure and manage the LSI MegaRAID controllers, there are two options:

- Use the MegaRAID Storage Manager software.
- Use the WebBIOS Configuration Utility.

The WebBIOS Configuration Utility is software that is embedded in the BIOS of the LSI MegaRAID controller.

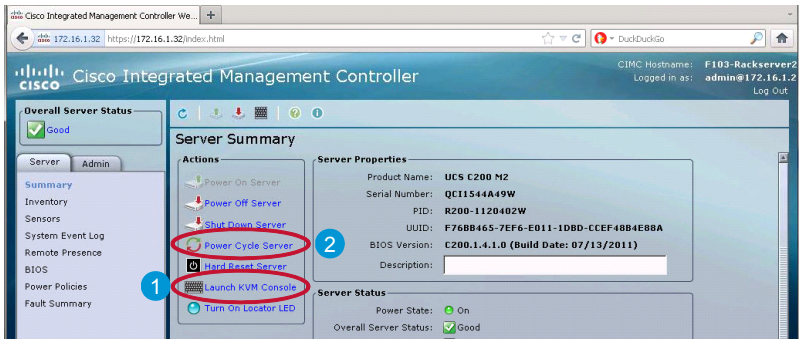
The WebBIOS Configuration Utility allows you to do the following:

- Create drive groups and virtual drives for storage configurations.
- Display controller, virtual drive, drive, and battery backup unit properties, and change parameters.
- Delete virtual drives.
- Migrate a storage configuration to a different RAID level.
- Detect configuration mismatches.
- Import a foreign configuration.
- Scan devices that are connected to the controller.
- Initialize virtual drives.
- Check configurations for data consistency.

https://t.me/learningnets

Launch KVM and Reboot Server

- To access the LSI WebBIOS Configuration Utility, do the following:
  - Open a KVM session to the server.
  - Power cycle the server.



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

To start the WebBIOS Configuration Utility, follow these steps:

Step 1 From Cisco Integrated Management Controller, launch the keyboard, video, mouse (KVM) console.

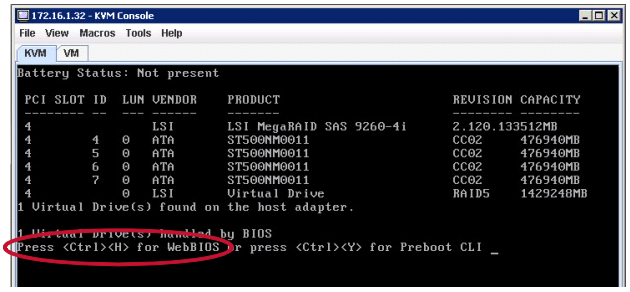
Step 2 From the Cisco Integrated Management Controller, power cycle the server while the KVM console is open.

Step 3 Monitor the boot process in the KVM window.

https://t.me/learningnets

Access LSI WebBIOS Configuration Utility

- Monitor the boot process in KVM.
- Press **Ctrl+H** to start the LSI WebBIOS Configuration Utility.



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

Step 4 Press the **Esc** key to disable the quiet boot and to be able to observe the messages.

Step 5 During the LSI MegaRAID controller initialization, a message will display listing the available options. Press **Ctrl-H** to access the WebBIOS Configuration Utility.

 © 2012 Cisco Systems, Inc.

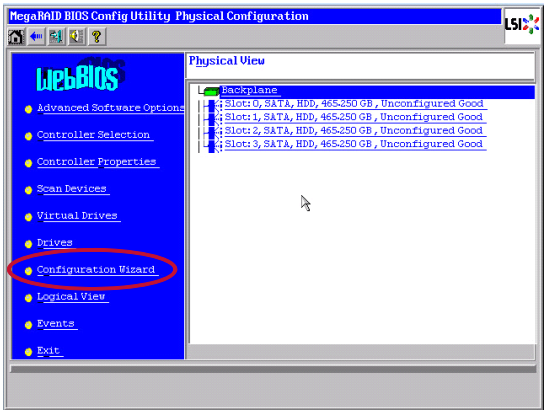
https://t.me/learningnets

Add Hard Drives to a RAID 5 Array

This topic describes the steps to create a RAID 5 drive group and a virtual drive.

Start Configuration Wizard

- To create drive groups and virtual drives, use the configuration wizard.
- Start the wizard from the home screen of the LSI WebBIOS Configuration Utility.

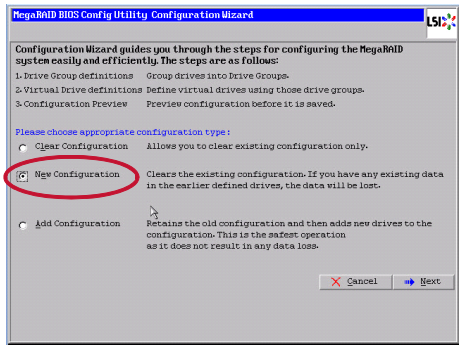


© 2012 Cisco and/or its affiliates. All rights reserved.

In the WebBIOS Configuration Utility, use the configuration wizard to create a drive group and a virtual drive or drives. The wizard is started from the WebBIOS Configuration Utility home screen.

Types of Configuration

- Choosing New Configuration erases the old configuration and creates a new one.
- Choosing Clear Configuration clears the present configuration.
- Choosing Add Configuration preserves the present configuration and adds a new one.



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

https://t.me/learningnets

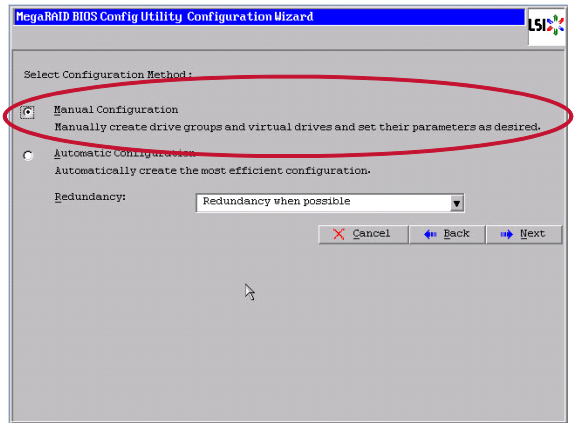
In the wizard, the first step is to specify what configuration will be created:

- Clear Configuration removes any current configuration.
- New Configuration removes the current configuration and creates a new one.
- Add Configuration preserves the current drive group configuration and adds a new one.

Choose **New Configuration** and click **Next** to continue.

Type of RAID Configuration

- Select the manual RAID configuration method.



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

The next screen provides two options:

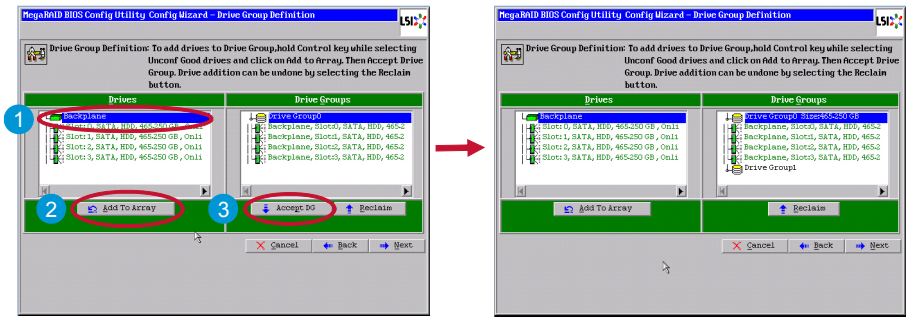
- **Manual Configuration:** With this option, you control which drives will participate in the drive group, the RAID level, and the number and size of the virtual drives created.
- **Automatic Configuration:** This option creates the optimal configuration that is based on the present hardware and the two redundancy options:
  - **No Redundancy:** The system will create a RAID 0 drive group.
  - **Redundancy:** Available drives determine how this option is configured:
    - **Two available drives:** A RAID 1 configuration will be created.
    - **Three or more available drives:** A RAID 5 configuration will be created.
    - **Three or more drives available and RAID 6 option enabled:** A RAID 6 configuration will be created.

Choose **Manual Configuration** and click **Next** to continue.

https://t.me/learningnets

Add Drives to the Drive Group

- Select drives to be added to the drive group.
- Select each of the drives and click **Add to Array**.
- Finally, click **Accept DG**.



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

In the Drive Group Definition screen, choose the physical drives that will form the drive group. Perform these steps to choose drives and add them to the drive group:

Step 1 Choose a drive from the list at the left.

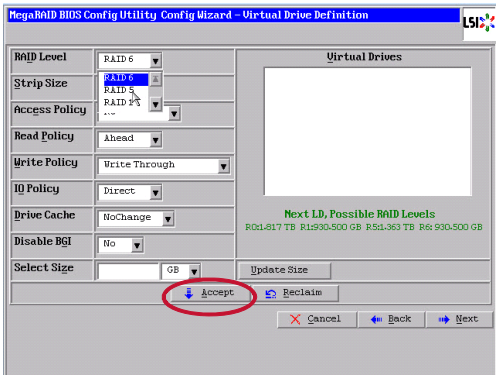
Step 2 Click **Add to Tray**.

Step 3 When finished with the selection, click **Accept DG** and click **Next** to continue.

https://t.me/learningnets

RAID Attributes

- Choose **RAID 5** as the Strip Size.
- Specify the virtual drive size or click **Update Size** to use the available space.



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

The figure shows the Virtual Drive Definition screen. The following options are available:

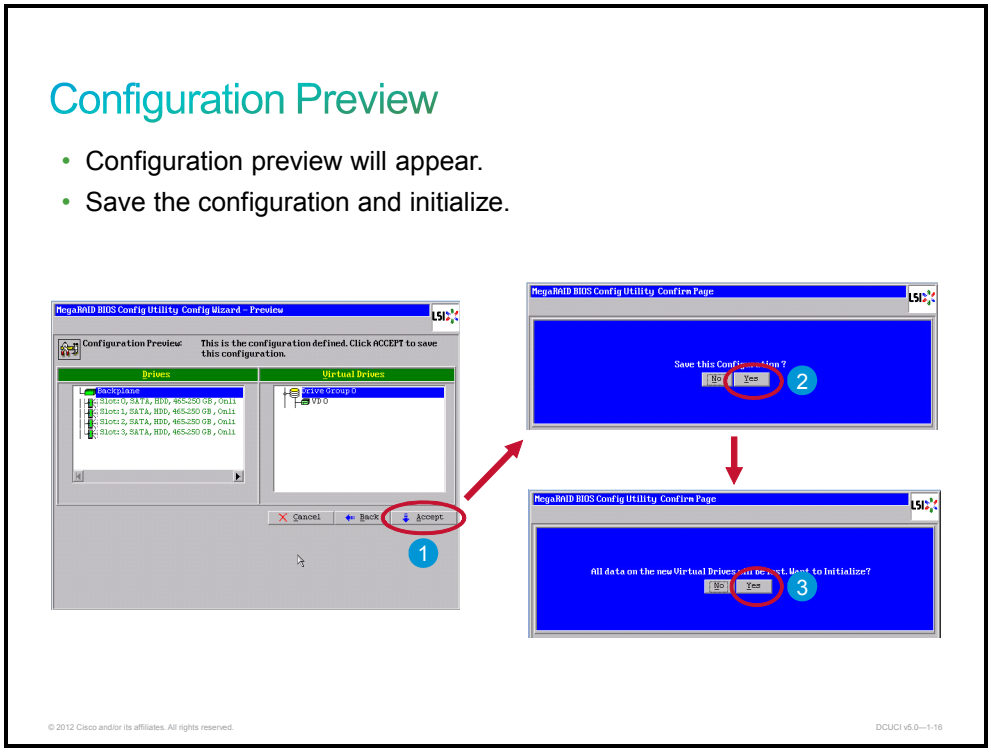
- **RAID Level:** A drop-down menu lists the available RAID levels. Select RAID 5.
- **Strip Size:** This field indicates the size of a stripe on a single drive in a drive group. The available sizes are 8, 16, 32, 64, 128, 256, 512, and 1024 KB. The default size is 64 KB.
- **Access Policy:** This field indicates the type of data access to the virtual drive:
  - **RW:** Read/write
  - **Read Only**
  - **Blocked:** Do not allow access
- **Read Policy:** This field indicates the read policy for the virtual drive:
  - **Normal:** Disables the read ahead capability. This setting is the default.
  - **Ahead:** Enables the read ahead capability.
- **Write Policy:** Use this field to specify the write policy for the virtual drive:
  - Write Back is the write-back mode. In this mode, the controller will send a data transfer completion signal to the host when all of the data is received in the cache of the controller.
  - Write Through is the write-through mode. In this mode, the data transfer completion signal will be sent when all of the data is received in the drive subsystem. This mode is the default.
  - Bad BBU is the mode to select if you want to use write-back mode without a battery backup unit.
- **IO Policy**
  - **Direct:** Reads are not buffered in the cache memory. This mode is the default.
  - **Cached:** All reads are buffered in the cache memory.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

- **Drive Policy:** Enable or disable the drive cache.
- **Disable BGI:** The default setting is NO. This setting will leave the background initialization (BGI) enabled.
- **Select Size:** Specify the size of the virtual drive. For a RAID 5 configuration, normally this size will be the full size.

Click **Accept** and **Next** to continue.



The next screen is the Configuration Preview. Check your configuration and click **Accept** to finish the configuration.

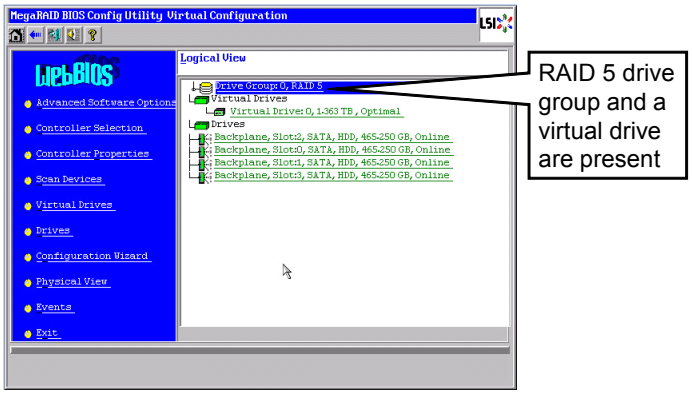
The WebBIOS will ask you to save the configuration. Choose **Yes** to continue.

Finally, the system will warn you that all of the data on the new virtual drive will be lost during the drive initialization. Choose **Yes** to continue.

https://t.me/learningnets

RAID 5 Drive Group Verification

- Click **Home**.
- Verify the RAID group.
- Exit the WebBIOS Configuration Utility and reboot the server.



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

Click **Home** to return to the initial WebBIOS screen. The new drive group will be listed with the drives that form it, the virtual drive, and the RAID level.

Follow these steps to apply the configuration:

Step 1 Exit the WebBIOS Configuration Utility.

Step 2 Power cycle the server.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

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

Summary

- RAID levels 0, 1, 5, 6, and 10 provide for different levels of fault tolerance and performance for the drives.
- To access the LSI MegaRAID WebBIOS Configuration Utility, launch the KVM console, reboot the server, and press Ctrl+H.
- Use the configuration wizard with manual configuration to create a RAID 5 drive group and a virtual drive.

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

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 8

Installing VMware ESXi on the Cisco UCS C-Series Server Local RAID Array

Overview

This lesson describes the procedure to install the VMware ESXi operating system on a Cisco Unified Computing System (UCS) C-Series server.

Objectives

Upon completing this lesson, you will be able to install VMware ESXi in the Cisco UCS C-Series server local hard drives. This ability includes being able to meet these objectives:

- Open a KVM session to the Cisco UCS C-Series server
- Map virtual media to the ESXi installer ISO image
- Install ESXi on the local RAID array
- Boot ESXi from the local RAID array
- Configure a management IP address for the ESXi server
- Connect to the ESXi server with the VMware vSphere Client utility and connect to the VMware File System shared storage LUN on the Fibre Channel storage system

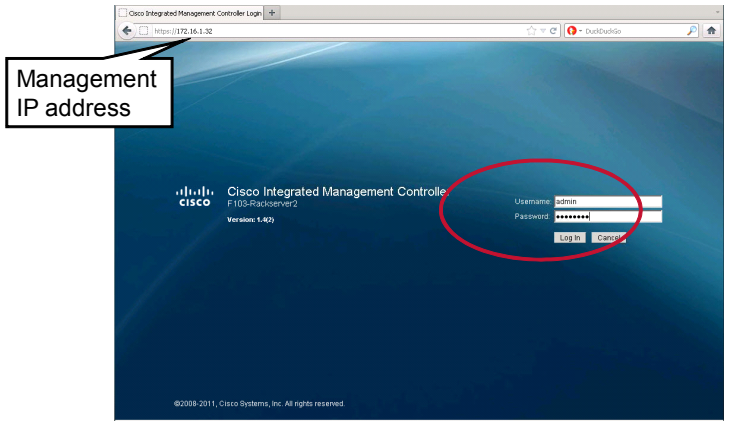
https://t.me/learningnets

Open a KVM Session

This topic describes how to launch the keyboard, video, mouse (KVM) console.

Open Cisco Integrated Management Controller

- Use a browser to open Cisco Integrated Management Controller.
- Provide username and password.



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

To launch the remote KVM console, you have to access the Cisco Integrated Management Controller GUI. To do so, open a browser and enter the management IP address of the server.

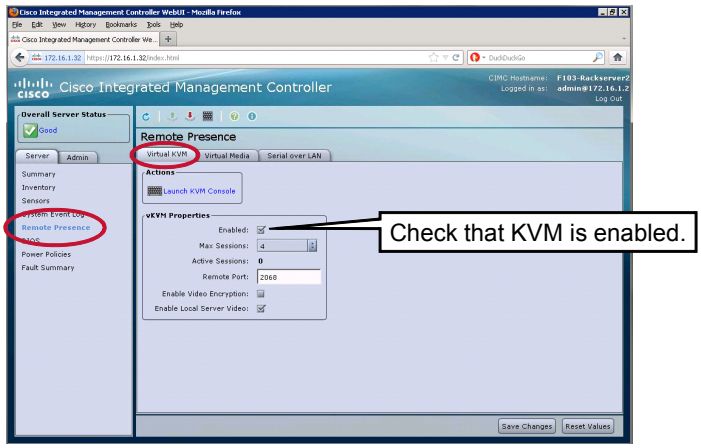
Provide the credentials of the administrator to log into the Cisco Integrated Management Controller.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Check KVM Settings

- Navigate to **Server > Remote Presence > Virtual KVM**.
- Ensure that KVM is enabled.



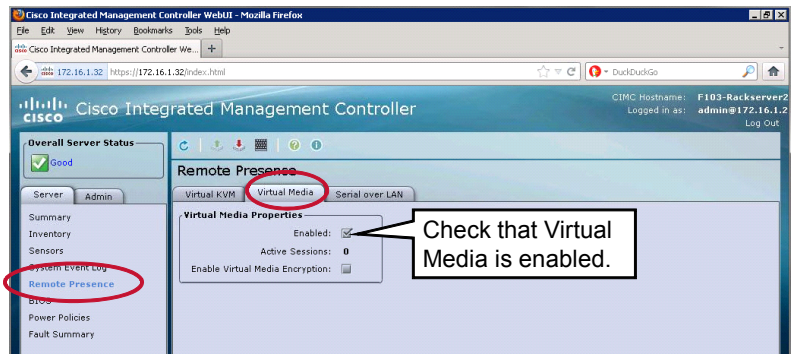
© 2012 Cisco and/or its affiliates. All rights reserved.

The KVM feature must be enabled for you to launch the remote KVM console.

Navigate to **Server > Remote Presence > Virtual KVM** to confirm that the feature is enabled and configured correctly.

Check Virtual Media Settings

- Navigate to **Server > Remote Presence > Virtual Media**.
- Ensure that Virtual Media is enabled.



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

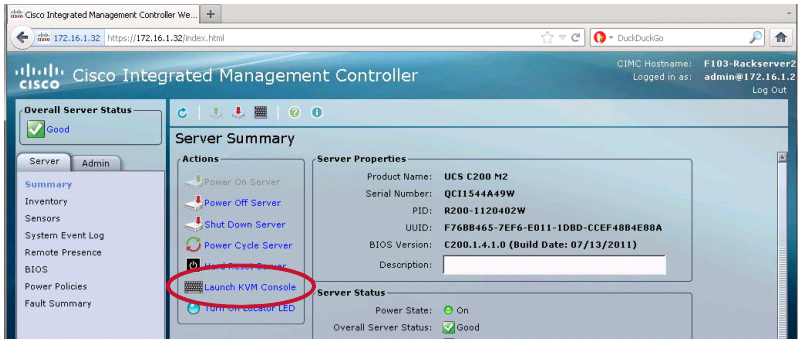
For the installation of the VMware ESXi system, you will use an image file. You have to map the image file using the Virtual Media feature.

Navigate to **Server > Remote Presence > Virtual Media** to confirm that the feature is enabled.

https://t.me/learningnets

Launch KVM

- Navigate to **Server > Summary**.
- Click **Launch KVM Console**.



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

Navigate to **Server > Summary**. In the **Actions** section, click **Launch KVM Console**.

The KVM console will open in a new window.

The KVM console can also be opened from any screen in the Cisco Integrated Management Controller interface by clicking the keyboard icon that is highlighted in the figure.

 © 2012 Cisco Systems, Inc.

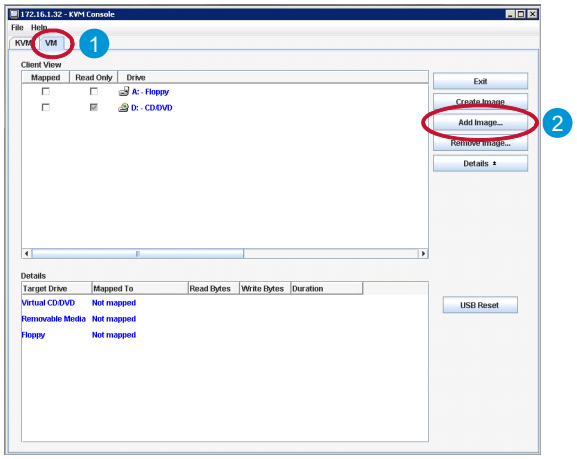
https://t.me/learningnets

Map Virtual Media to the ESXi Installer

This topic describes how to map the ESXi image file.

Virtual Media Tab in KVM

- Click the **VM** tab in the KVM session window.
- Click **Add Image**.



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

You have two options to install the VMware ESXi operating system:

- Burn the install image on a DVD and perform the installation. This option requires that you have physical access to the server to load the installation DVD.
- Map the image using Virtual Media.

This lesson describes the second option of mapping the image.

To map the ESXi installation ISO image file in Virtual Media, go to the VM tab in the KVM window.

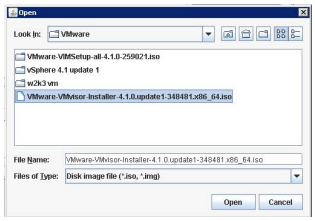
Click **Add Image…** to open a browser window.

Note	If you do not see a VM tab in the KVM window, navigate to **Tools** in the menu bar and click **Launch Virtual Media**. A new window will open.

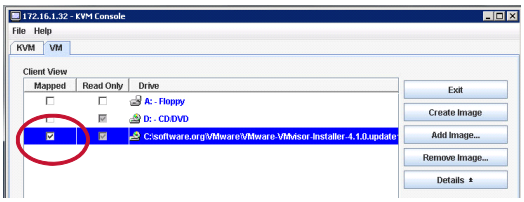
https://t.me/learningnets

Map the VMware ESXi Image

- Choose the VMware ESXi image file.



- Check the **Mapped** check box to map it.



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

Browse for the installation image file and select it. Click **Open**.

The image file will appear in the Client View area in the VM tab.

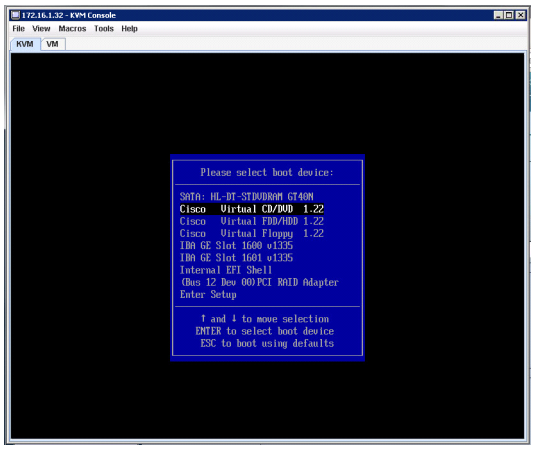
For the image to become visible to the server, you have to map the image. Click the **Mapped** check box.

Note	If you use a separate Virtual Media window, leave it open. If you close the window, the image will be unmapped.

https://t.me/learningnets

Boot from Cisco Virtual CD/DVD

- Power up or power cycle the server.
- Press **F6** to select Cisco Virtual CD/DVD drive to boot.



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

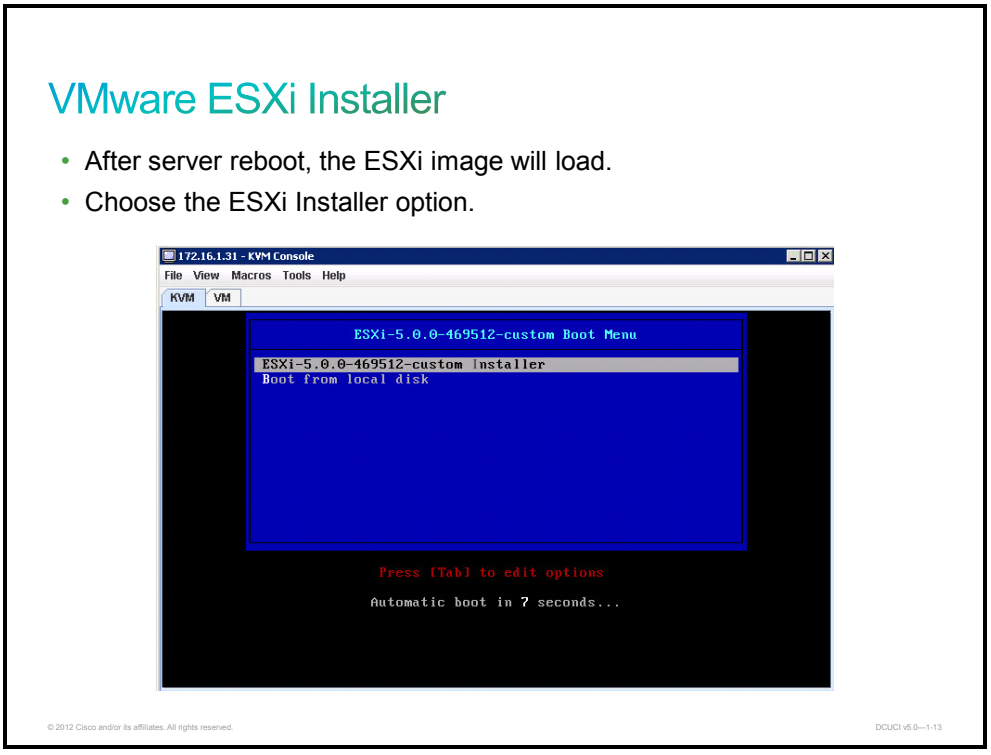
With the image mapped, you can now start the installation process. Power up the server or power cycle the server, depending on the initial power state.

During boot, press **F2** to open the Boot Options menu. From the menu, select **Cisco Virtual CD/DVD**. This option instructs the server to boot from the image file.

https://t.me/learningnets

Install ESXi on the Local RAID Array

This topic describes the steps of the ESXi installation process.



Once the server is rebooted and you have selected the Cisco Virtual CD/DVD option, the ESXi installer will load.

The first screen provides two options:

- ESXi Installer
- Boot from local disk

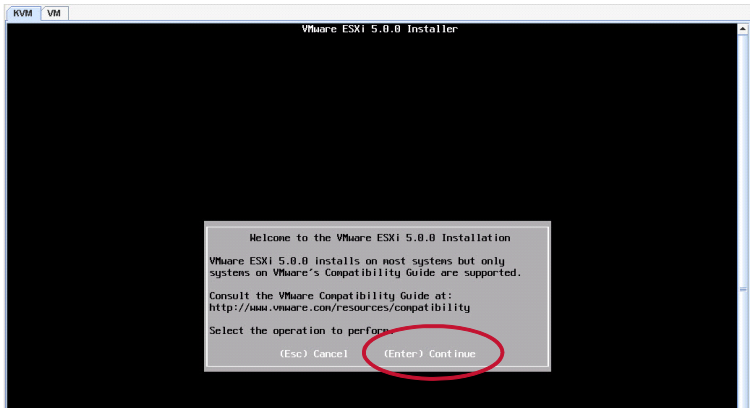
Choose **ESXi Installer** to start the installation process.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Start VMware ESXi Installation

- Available options are Cancel, Repair, or Install.
- Press **Enter** to start the installation.



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

The installation process is organized in a series of steps. The first steps will ask you to choose the needed installation options.

The first screen provides three options:

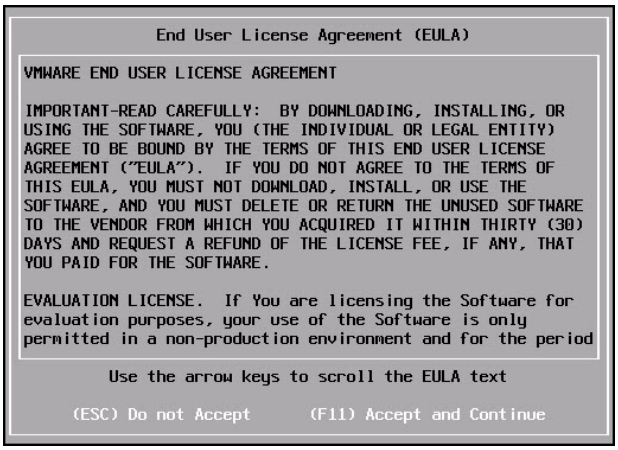
- **Cancel:** This option stops the ESXi installer.
- **Repair:** This option attempts to repair a bad installation.
- **Install:** This option starts a fresh installation.

Press **Enter** to start the installation.

https://t.me/learningnets

VMware End User License Agreement

- The VMware End User License Agreement is displayed.
- Press **F11** to accept and continue.

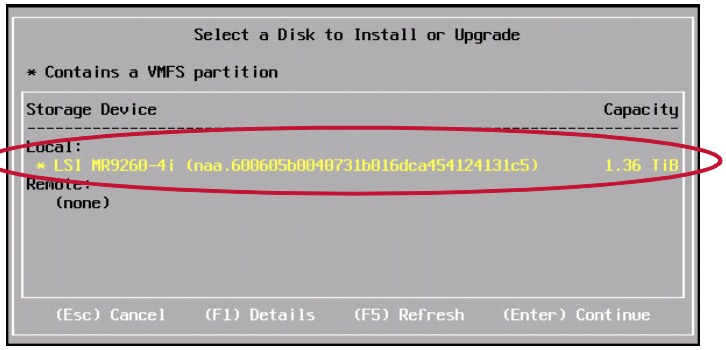


© 2012 Cisco and/or its affiliates. All rights reserved.

The figure shows the VMware End User License Agreement (EULA). Press **F11** to accept it and to continue with the installation.

Installation Target Drive

- Specify the installation target drive.
- Navigate to the LSI RAID drive group and press **Enter** to select it.



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

The next choice that you have to make is the target drive on which to install the ESXi operating system.

Navigate with the arrow keys to the LSI RAID option to choose the RAID drive group.

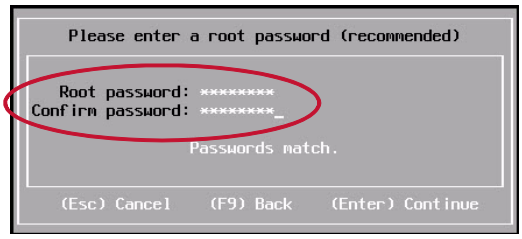
Press **Enter** to continue.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Create Root Password

- Create the password for the root user.

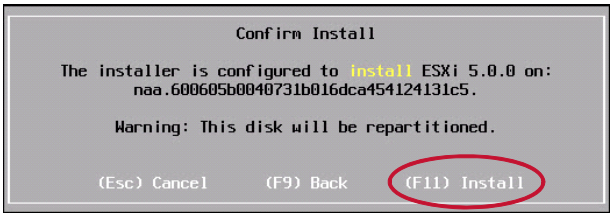


© 2012 Cisco and/or its affiliates. All rights reserved.

The next step will require you to create a password for the root user.

Install Confirmation

- Press **F11** to confirm the start of the install process.



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

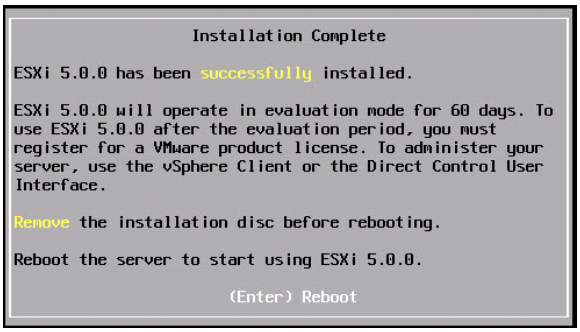
In this step, you are asked to confirm the installation. The installer notifies you that it is ready to start the installation.

Press **F11** to start the installation.

https://t.me/learningnets

VMware ESXi Installation End

- Unmap the install image in the VM tab.
- Return to the KVM tab and press **Enter** to reboot.



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

After the installation completes, a screen notifies you of the successful installation of the ESXi operating system. The last step is to press **Enter** to reboot the server.

Note	During server reboot, make sure that the image in the VM tab is unmapped. If you use the Virtual Media window, close the window.

© 2012 Cisco Systems, Inc.

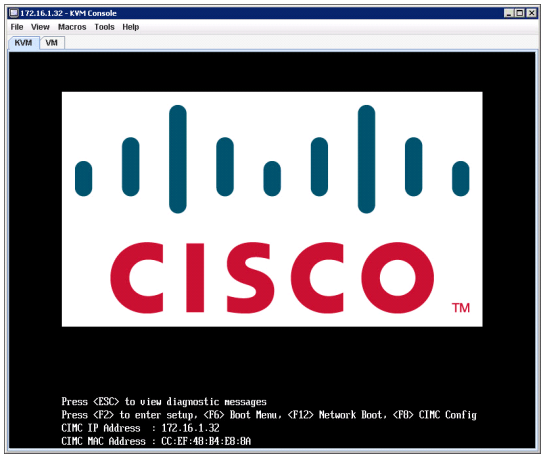
https://t.me/learningnets

Boot ESXi from the Local RAID Array

This topic describes the steps to boot the server from the RAID drive group.

Access BIOS

- Provision boot order from the BIOS of the server.
- During boot, select **F2** to access the BIOS.



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

You have successfully installed the VMware ESXi operating system. The last stage of the installation process is to reboot the server. Configure the boot option in the BIOS of the server for the server to boot from the RAID drive group where the ESXi system was installed.

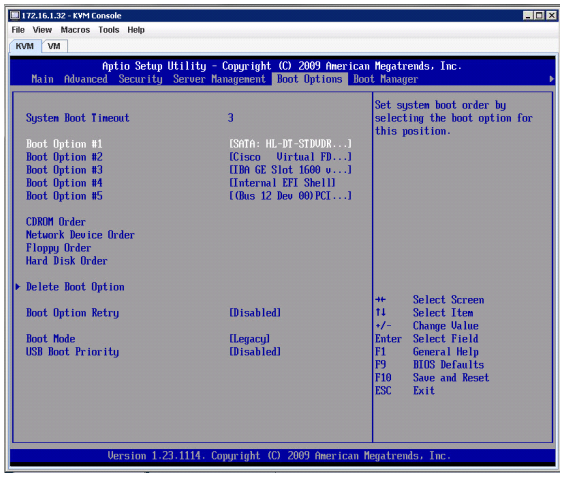
To access the BIOS of the server during boot, observe the screen that provides information about F-keys that can be used to access the BIOS, the Cisco Integrated Management Controller, the boot menu, and so on.

Press **F2** to access the BIOS of the server.

https://t.me/learningnets

BIOS Boot Options

- Use arrow keys to navigate to the **Boot Options** menu.
- Go to **Boot Option #1** and press **Enter**.



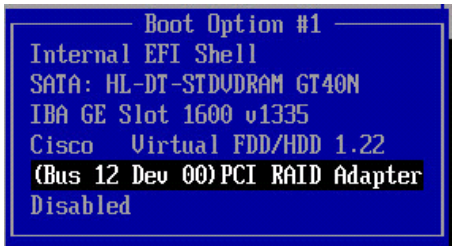
© 2012 Cisco and/or its affiliates. All rights reserved.

In the BIOS of the server, use the arrow keys to navigate to the Boot Options tab.

Navigate to **Boot Option #1** and press **Enter** to choose a boot target.

Select Boot Device

- Select **PCI RAID Adapter**.
- Press **Enter** to accept the choice.



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

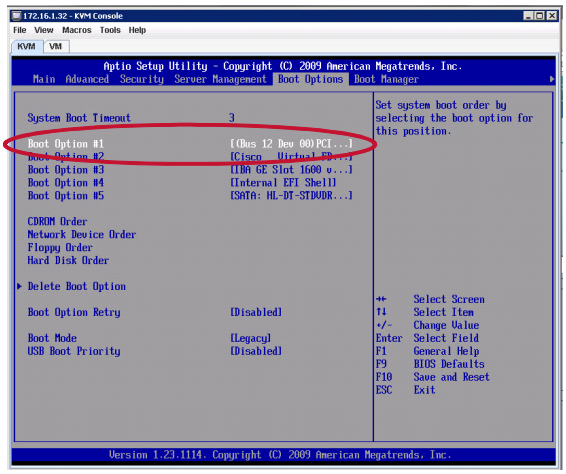
From the list of available boot targets, choose **PCI RAID Adapter**. Press **Enter** to choose it and continue.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Boot Option Verification

- Verify that the RAID group is the first boot option.
- Press **F10** to save and exit the BIOS.



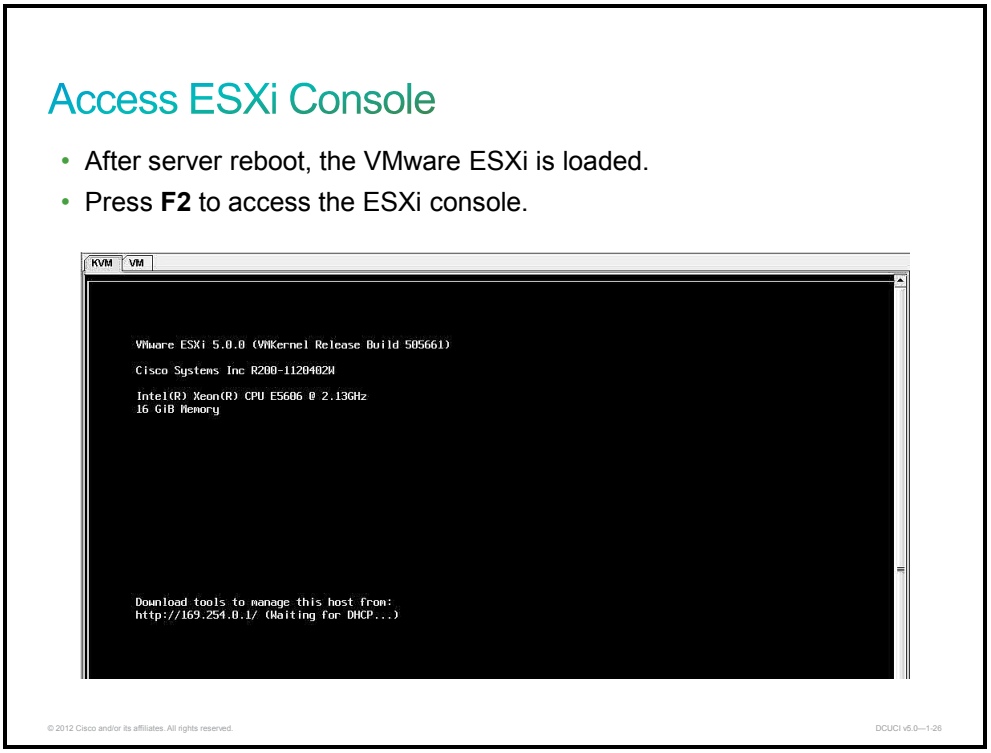
© 2012 Cisco and/or its affiliates. All rights reserved.

Verify that Boot Option #1 changed to the PCI RAID Adapter option. Press **F10** to save the changes and exit the BIOS of the server.

https://t.me/learningnets

Configure a Management IP Address for the ESXi Server

This topic describes how to provision management network settings for the ESXi server.



The VMware ESXi operating system is now installed on the server. To access, configure, and manage the ESXi system, a management IP address must be specified, along with additional needed network configuration.

Initially, you will be able to access the ESXi console only using the KVM console or, if you are attached directly to the server, you can access the console using a monitor and a keyboard.

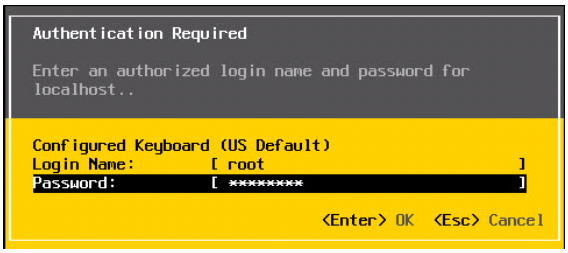
In the KVM window, you will see that the ESXi system is loaded. To access the ESXi console, press **F2**.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Initial Authentication

- The Authentication window will appear.
- Type in the password created during the installation.
- The default user is root.

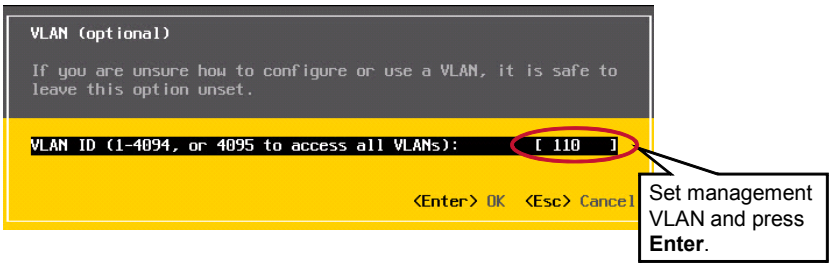


© 2012 Cisco and/or its affiliates. All rights reserved.

You will be asked to provide authentication credentials. Provide the password that you created during the installation.

Provision Management VLAN

- Select **Configure Management Network**.
- Click **VLAN**.



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

To configure the management network, select **Configure Management Network** from the ESXi console main menu.

Next, specify the management VLAN. Select **VLAN (optional)** and, in the new window, specify the management VLAN.

Press **Enter** to confirm and continue.

https://t.me/learningnets

Provision IP Address

- Select IP Configuration.

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

Select **IP Configuration**. In the new window, specify the following:

- IP address
- Subnet mask
- Default gateway

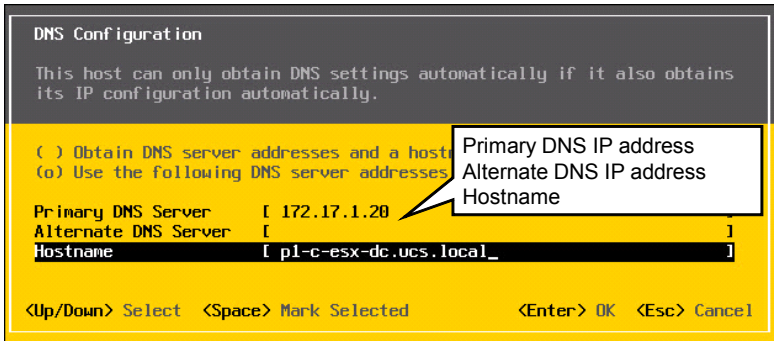
Press **Enter** to continue.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Provision DNS

- Select **DNS Configuration**.
- Provision DNS.



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

Select **DNS Configuration**. In the new window, specify the following:

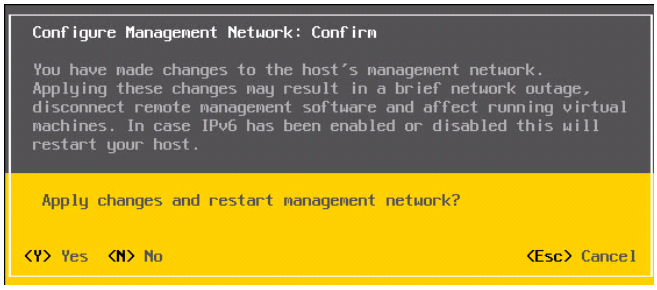
- IP address of the primary Domain Name System (DNS) server
- IP address of the alternate DNS server, if available
- Hostname

Press **Enter** to continue.

https://t.me/learningnets

Save Network Configuration

- Press **Esc** to exit the Configuration Management Network.
- Press **Y** to save the configuration.



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

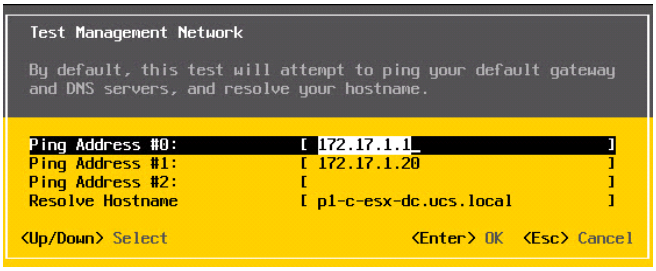
At this point, the management network configuration is ready. Press **Esc** to exit the Configuration Management Network option. The system will ask you to save the configuration. Press **Y**.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Test Management Network Configuration

- Select **Test Management Network**.
- Press **Enter** to start the tests.



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

To verify network settings for management access, select **Test Management Network**. In the new window, you will see the IP addresses of the default gateway and the DNS servers. The system will try to ping these servers to confirm connectivity. The system will also try to resolve the hostname of the server to confirm that the DNS service is operational.

Press **Enter** to start the tests.

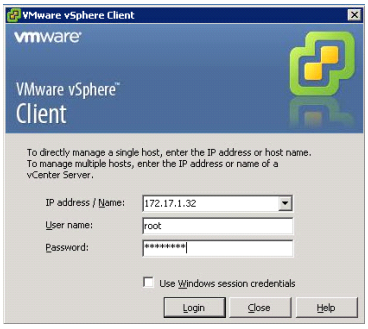
https://t.me/learningnets

Connect to the ESXi Server with the VMware vSphere Client Utility

This topic describes how to access the ESXi server using the VMware vSphere Client. You will also learn how to connect to the VMware File System shared storage logical unit number (LUN) on the Fibre Channel storage system.

Start VMware vSphere Client

- Specify the IP address.
- Input login credentials.



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

The VMware ESXi host can be managed directly by using the VMware vSphere Client utility, or it can be managed by the VMware vCenter Server. The VMware vCenter Server is used to manage multiple ESXi hosts, while the vSphere utility is used to connect to only one ESXi server.

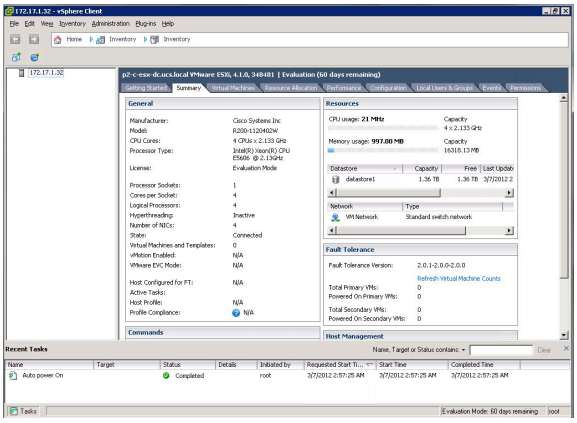
To access the ESXi server using the vSphere Client utility, start the utility and enter the IP address of the ESXi server, username, and password for the user.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

VMware vSphere Client

- Tabs provide different information.
- The Summary tab provides general information for the ESXi host.



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

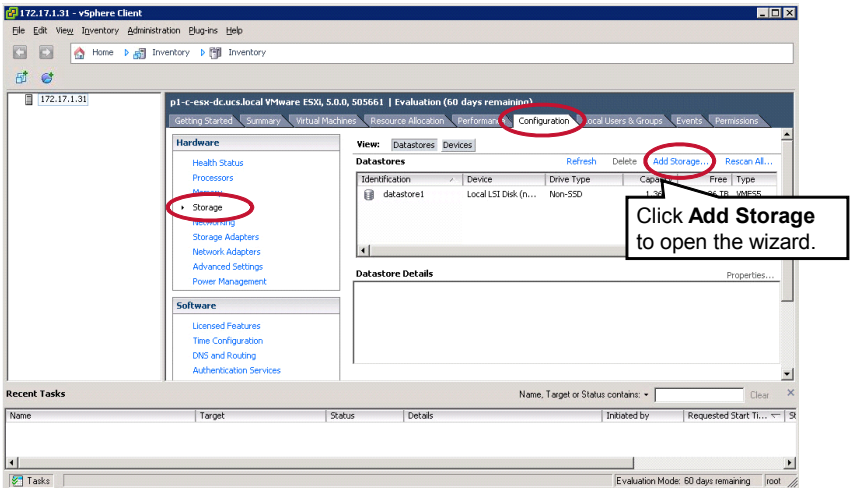
In the vSphere Client Utility window, there are multiple tabs that provide different information for the ESXi server.

Choose the **Summary** tab for general information that is related to the server.

https://t.me/learningnets

Storage Configuration

- Navigate to **Configuration > Storage** to see the storage.



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

To start the storage-related configuration, perform the following steps:

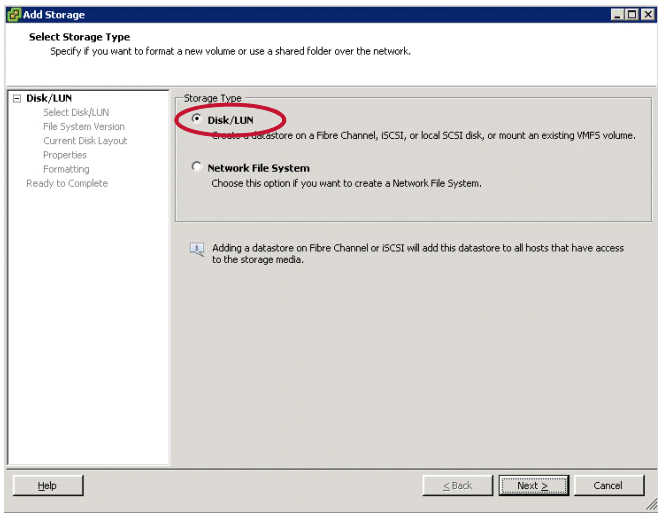
Step 1 Select the **Configuration** tab.

Step 2 Select **Storage**.

Step 3 Click **Add Storage**.

Add Storage Wizard

- In the first step, select the Storage Type.



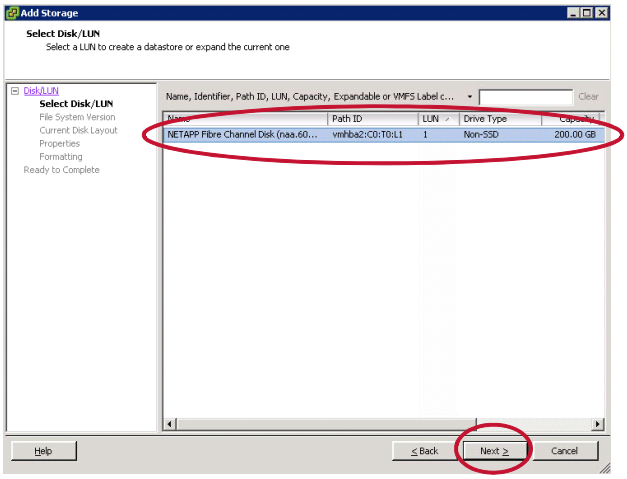
© 2012 Cisco and/or its affiliates. All rights reserved.

In the first step of the wizard, you have to select the storage type. Click **Next** to continue.

https://t.me/learningnets

Select Disk/LUN

- Select the disk/LUN from the list.
- Click **Next** to continue.

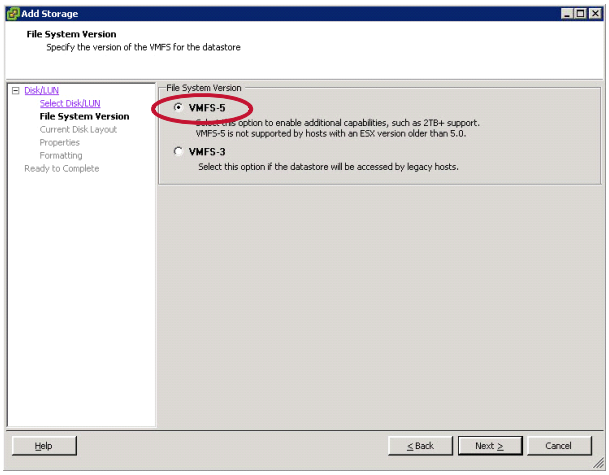


© 2012 Cisco and/or its affiliates. All rights reserved.

In the second step of the wizard, you have to select the Disk/LUN on which the new datastore will be created. Click **Next** to continue.

File System

- Select the file system version.
- Click **Next** to continue.



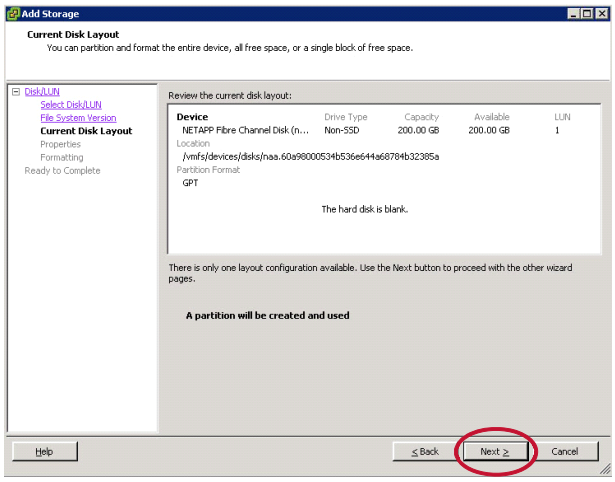
© 2012 Cisco and/or its affiliates. All rights reserved.

In the third step of the wizard, you have to select the file system of the new datastore. Click **Next** to continue.

https://t.me/learningnets

Disk Layout

- In this step, you will be provided with the current disk layout.
- Click **Next** to continue.

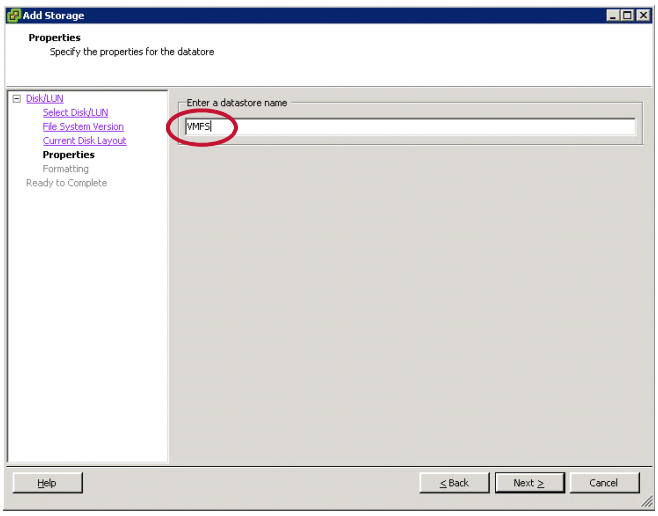


© 2012 Cisco and/or its affiliates. All rights reserved.

In the fourth step of the wizard, you will be provided with the disk layout. Click **Next** to continue.

Datastore Name

- Specify a name for the new datastore.



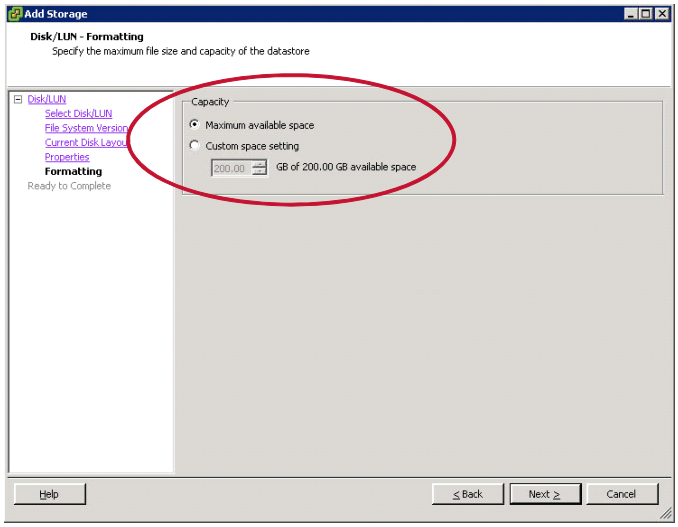
© 2012 Cisco and/or its affiliates. All rights reserved.

In the fifth step of the wizard, you will be asked to provision a name for the new datastore. Click **Next** to continue.

https://t.me/learningnets

Disk/LUN Formatting

- Specify the new disk capacity.

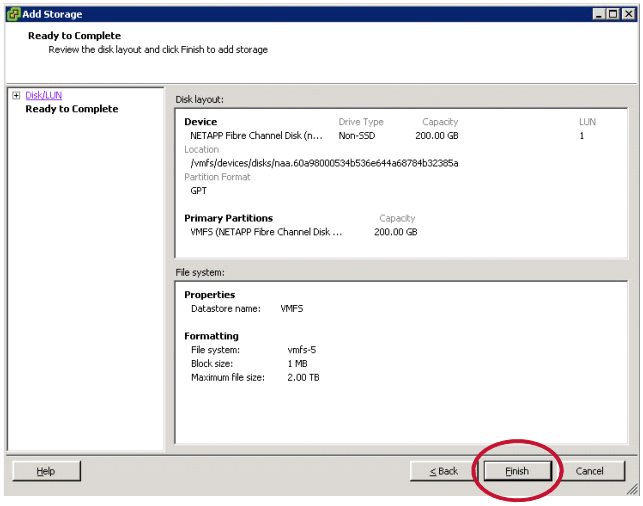


© 2012 Cisco and/or its affiliates. All rights reserved.

In the sixth step of the wizard, you have to specify the capacity of the new datastore. Click **Next** to continue.

Datastore Overview

- The final step of the wizard provides an overview of the new datastore.



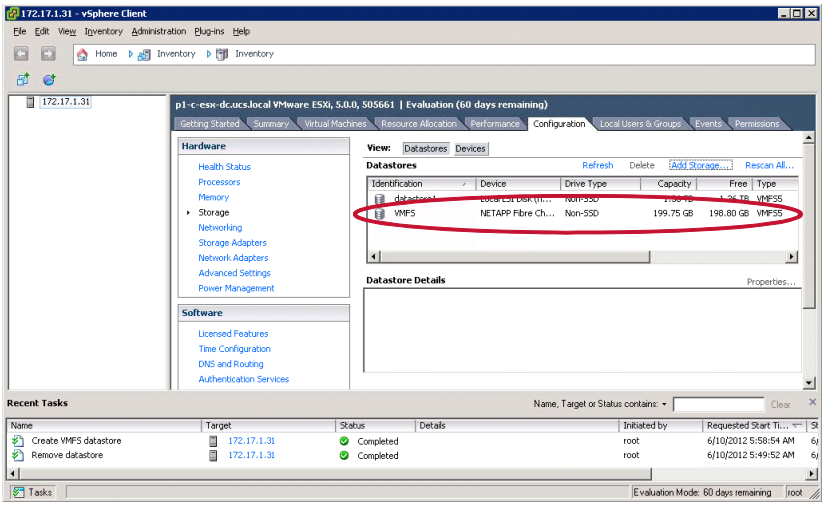
© 2012 Cisco and/or its affiliates. All rights reserved.

In the final step of the wizard, you will be provided with an overview of the new datastore. Click **Finish** for the system to create the new datastore.

https://t.me/learningnets

Verify Datastore

- The new datastore will be visible after it is created.



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

To verify that the new datastore is created and available, check in the storage configuration of the ESXi host. The new datastore will be listed under Datastores.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

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

Summary

- Check that KVM and Virtual Media are enabled and launch the KVM console.
- In the VM tab, browse for the VMware ESXi image file and map it.
- During the installation process, select the local RAID drive group.
- After installation, change the boot options in the BIOS of the server to boot from the RAID drive group.
- Using the KVM console, access the ESXi console to provision the password for the user root and to configure management network settings.
- Use the VMware vSphere client to connect to the ESXi host and manage it.

© 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.

Module Summary

- Cisco R42610 racks and Cisco RP208-30-U-1 PDUs are optimized for use with Cisco UCS products, and provide for optimal airflow and space usage.
- Before installing the Cisco UCS C-Series servers in the Cisco R42610 rack, you can install or replace components. For DRAM population, follow the rules specified in the installation and upgrade guides. New color coding helps you immediately identify hot-swappable components.
- Use the provided rack mounting kit to install the Cisco UCS C-Series server in the Cisco R42610 rack.
- Cisco UCS Host Upgrade Utility is a tool that allows upgrades and downgrades of server firmware components.
- From Cisco Integrated Management Controller, you can provision SNMP monitoring of the server to access the server event logs and to provision remote syslog servers. SNMP v1, v2c, and v3 are supported.

© 2011 Cisco and/or its affiliates. All rights reserved.

Module Summary

- You can provision Cisco P81E VICs from Cisco Integrated Management Controller.
- To provision the RAID controller, during boot, press Ctrl+H to access the LSI MegaRAID WebBIOS Configuration Utility.
- To install the VMware ESXi operating system, map the image file in virtual media and boot the server from the image file.

© 2011 Cisco and/or its affiliates. All rights reserved.

https://t.me/learningnets

References

For additional information, refer to these resources:

- *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.4* at http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.4.1/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_141.html
- *Cisco UCS C200 Installation and Service Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C200M1/install/c200M1.html
- *Cisco UCS C210 Installation and Service Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C210M1/install/C210M1.html
- *Cisco UCS C250 Server Installation and Service Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C250M1/install/c250M1.html
- *Cisco UCS C460 Server Installation and Service Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C460/install/C460.html
- *Cisco R Series Rack and RP Series PDU Installation Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/rack_power/installation/guide/Rack_PDU.html
- *Cisco Host Upgrade Utility Release 1.4(x) Quick Start Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/lomug/1.4.x/install/b_HUUUG_1_4.html
- LSI Corporation, *MegaRAID SAS Software User Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/3rd-party/lsi/mrsas/userguide/LSI_MR_SAS_SW_UG.pdf
- *Cisco UCS C-Series Servers VMware Installation Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/os/vmware/install/vmware_install_c.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 RUs can be contained in a Cisco R42610 rack? (Source: Implementing Cisco R Series Rack Enclosures)

A) 38 RU
B) 40 RU
C) 42 RU
D) 44 RU

Q2) Which two rack deployment models are supported by Cisco R42610 racks? (Choose two.) (Source: Implementing Cisco R Series Rack Enclosures)

A) single-rack deployment
B) partial-rack deployment
C) multiple-rack deployment
D) vertical-rack deployment

Q3) Which four items must be checked before the installation of Cisco R42610 racks? (Choose four.) (Source: Implementing Cisco R Series Rack Enclosures)

A) floor weight capacity
B) adequate installation space
C) building roof capacity
D) adequate airflow clearance
E) presence of armed guards
F) power sources
G) staff protective equipment

Q4) How many circuit breakers are available on Cisco RP208-30-U-1 PDUs? (Source: Implementing Cisco R Series Rack Enclosures)

A) 0
B) 1
C) 2
D) 3

Q5) Which installation configuration of RP208-30-U-1 PDUs does not consume RUs? (Source: Implementing Cisco R-Series Rack Enclosures)

A) single configuration
B) tower configuration
C) 1-RU configuration
D) front configuration
E) bottom configuration

Q6) Which four ESD precaution measures are recommended? (Choose four.) (Source: Installing Cisco UCS C-Series Server Hardware)

A) antistatic spray
B) hold a colleague
C) ESD wrist-strap
D) ESD tie
E) ESD pads
F) ESD packaging
G) ESD pants

https://t.me/learningnets

Q7) How many riser cards and PCIe slots per riser card are provided by the C200 server? (Source: Installing Cisco UCS C-Series Server Hardware)

A) one riser card with one standard-profile and one low-profile PCIe slot
B) two riser cards with one standard PCIe slot on each
C) one riser card with one low-profile PCIe slot
D) one riser card with two standard-profile PCIe slots

Q8) On which PCIe slots are the two riser cards of the C260 server installed? (Source: Installing Cisco UCS C-Series Server Hardware)

A) PCIe slots 2 and 6
B) PCIe slots 3 and 5
C) PCIe slots 4 and 8
D) PCIe slots 1 and 7

Q9) What is the minimum CPU configuration that is supported for C460 servers? (Source: Installing Cisco UCS C-Series Server Hardware)

A) CPU1 and CPU2 installed
B) CPU2 and CPU3 installed
C) CPU1 and CPU3 installed
D) CPU3 and CPU4 installed

Q10) Which color code indicates hot-swappable Cisco components? (Source: Installing Cisco UCS C-Series Server Hardware)

A) yellow plastic touch points
B) green plastic touch points
C) black plastic touch points
D) orange plastic touch points
E) light-blue plastic touch points

Q11) What is the airflow direction of Cisco UCS C-Series servers? (Source: Installing Cisco UCS C-Series Servers in a Cisco R-Series Rack Enclosure)

A) bottom to top
B) back to front
C) front to back
D) side to side

Q12) In RUs, what is the minimal server rack space? (Source: Installing Cisco UCS C-Series Servers in a Cisco R Series Rack Enclosure)

A) 3 RU
B) 4 RU
C) 6 RU
D) 7 RU

Q13) Which power cord type must be used to connect the server to the PDU? (Source: Installing Cisco UCS C-Series Servers in a Cisco R Series Rack Enclosure)

A) standard power cords
B) jumper power cords
C) crossed power cords
D) electric company-provided power cords

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Q14) Which connector type is needed for the power cord to connect to the C19 connector of the server? (Source: Installing Cisco UCS C-Series Servers in a Cisco R-Series Rack Enclosure)

A) C13
B) C18
C) C20
D) C17

Q15) To perform initial configuration, which two items must be connected directly to the server? (Choose two.) (Source: Installing Cisco UCS C-Series Servers in a Cisco R-Series Rack Enclosure)

A) USB mouse
B) USB keyboard
C) VGA monitor
D) USB flash drive
E) USB Bluetooth extender
F) USB monitor

Q16) Which seven actions can be taken using the Cisco UCS Host Upgrade Utility? (Choose seven.) (Source: Updating Cisco UCS C-Series Firmware with the Host Upgrade Utility)

A) upgrade Cisco Integrated Management Controller firmware
B) upgrade BIOS firmware
C) upgrade RAID controllers
D) upgrade LOM
E) upgrade Cisco UCS P81E
F) upgrade Broadcom 5709, 57711, and 57712 adapters
G) upgrade Intel 82576 adapter
H) upgrade operating system drivers
I) apply operating system patches

Q17) From where do you download the Cisco UCS Host Upgrade Utility? (Source: Updating Cisco UCS C-Series Firmware with the Host Upgrade Utility)

A) www.intel.com
B) www.microsoft.com
C) www.cisco.com
D) Torrent tracker
E) Apple Appstore

Q18) Which two features must be enabled in the Cisco Integrated Management Controller to use the Cisco Host Upgrade Utility? (Choose two.) (Source: Updating Cisco UCS C-Series Firmware with the Host Upgrade Utility)

A) remote syslog servers
B) KVM
C) SNMPv3
D) virtual media
E) SoL

https://t.me/learningnets

Q19) What is the default single-cursor termination key in the KVM console? (Source: Updating Cisco UCS C-Series Firmware with the Host Upgrade Utility)

A) F11
B) F12
C) F9
D) F7
E) F6

Q20) Which connection with the server will be lost during Cisco Integrated Management Controller reboot? (Source: Updating Cisco UCS C-Series Firmware with the Host Upgrade Utility)

A) data interface connection
B) Cisco Integrated Management Controller connection
C) Internet connection
D) Cisco.com connection

Q21) Which three versions of SNMP are supported in the Cisco Integrated Management Controller? (Choose three.) (Source: Provisioning Monitoring and Logging on the Cisco UCS C-Series Server)

A) v1
B) v4
C) v2c
D) v3
E) v5
F) v6a

Q22) How many SNMP servers can be provisioned in Cisco Integrated Management Controller? (Source: Provisioning Monitoring and Logging on the Cisco UCS C-Series Server)

A) 1
B) 2
C) 3
D) 4
E) 5

Q23) Which two encryption algorithms are supported for SNMP message encryption in Cisco Integrated Management Controller? (Choose two.) (Source: Provisioning Monitoring and Logging on the Cisco UCS C-Series Server)

A) DES
B) AES
C) 3DES
D) AES256
E) SHA
F) MD5

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Q24) How many remote syslog servers can be provisioned in Cisco Integrated Management Controller? (Source: Provisioning Monitoring and Logging on the Cisco UCS C-Series Server)

A) 1
B) 2
C) 3
D) 4
E) 5

Q25) Which protocol is used to export the tech support file in Cisco Integrated Management Controller? (Source: Provisioning Monitoring and Logging on the Cisco UCS C-Series Server)

A) FTP
B) SFTP
C) TFTP
D) SCP
E) HTTP

Q26) Which mode must be enabled on the Cisco UCS P81E VIC in Cisco Integrated Management Controller to support FCoE? (Source: Provisioning LAN and SAN Connectivity in the Cisco Integrated Management Controller)

A) NPV
B) Fibre Channel
C) FIP
D) NIV
E) NPIV

Q27) By default, how many vNICs are present on the Cisco UCS P81E VIC? (Source: Provisioning LAN and SAN Connectivity in the Cisco Integrated Management Controller)

A) 1
B) 2
C) 3
D) 4
E) 6

Q28) What is the maximum number of vNICs that can be provisioned on the Cisco UCS P81E VIC? (Source: Provisioning LAN and SAN Connectivity in the Cisco Integrated Management Controller)

A) 8
B) 16
C) 64
D) 116
E) 128

Q29) How many vHBAs are provided by the Cisco UCS P81E VIC? (Source: Provisioning LAN and SAN Connectivity in the Cisco Integrated Management Controller)

A) 1
B) 2
C) 4
D) 16

https://t.me/learningnets

Q30) Which feature must be enabled on Cisco UCS P81E VIC to distribute the network processing load among multiple CPUs? (Source: Provisioning LAN and SAN Connectivity in the Cisco Integrated Management Controller)

A) hyperthreading
B) RSS
C) Intel direct I/O
D) TCP offload

Q31) Which RAID level uses simple striping without parity? (Source: Provisioning RAID on the Cisco UCS C-Series Server)

A) RAID 0
B) RAID 1
C) RAID 5
D) RAID 10

Q32) Which RAID level is referred to as mirroring? (Source: Provisioning RAID on the Cisco UCS C-Series Server)

A) RAID 0
B) RAID 1
C) RAID 5
D) RAID 10

Q33) Which RAID level uses striping with distributed parity? (Source: Provisioning RAID on the Cisco UCS C-Series Server)

A) RAID 0
B) RAID 1
C) RAID 5
D) RAID 10

Q34) Which embedded LSI RAID controller tool is used for configuration and monitoring? (Source: Provisioning RAID on the Cisco UCS C-Series Server)

A) WebBIOS Configuration Utility
B) LSI ConfigTool
C) MegaRAID Storage Manager
D) Cisco Integrated Management Controller RAID Configuration Utility

Q35) Which key combination must be used to access the LSI interface during server boot? (Source: Provisioning RAID on the Cisco UCS C-Series Server)

A) Ctrl-A
B) Ctrl-C
C) Ctrl-D
D) Ctrl-H
E) Ctrl-Z

Q36) What is the default user in the VMware ESXi operating system? (Source: Installing VMware ESXi on the Cisco UCS C-Series Server Local RAID Array)

A) admin
B) administrator
C) vmware-root
D) root
E) esxi-admin

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Q37) What is the default password in VMware ESXi? (Source: Installing VMware ESXi on the Cisco UCS C-Series Server Local RAID Array)

A) admin
B) root
C) none
D) vmware
E) esxi

Q38) Which key must be used to access the ESXi console? (Source: Installing VMware ESXi on the Cisco UCS C-Series Server Local RAID Array)

A) F1
B) F2
C) F6
D) F12

Q39) Which six options are available in the Configure Management Network menu in the ESXi console? (Choose six.) (Source: Installing VMware ESXi on the Cisco UCS C-Series Server Local RAID Array)

A) network adapters
B) VLAN
C) default gateway configuration
D) IP configuration
E) IPv6 configuration
F) DNS configuration
G) WWPN configuration
H) WWNN configuration
I) custom DNS suffixes

Q40) Which two applications are used to manage an ESXi host? (Choose two.) (Source: Installing VMware ESXi on the Cisco UCS C-Series Server Local RAID Array)

A) VMware vSphere Client
B) VMware vSphere Server
C) VMware vCenter Server
D) VMware Host Manager

https://t.me/learningnets

Module Self-Check Answer Key

Q1) C

Q2) A, C

Q3) A, B, D, F

Q4) C

Q5) B

Q6) A, C, E, F

Q7) A

Q8) D

Q9) C

Q10) B

Q11) C

Q12) B

Q13) B

Q14) C

Q15) B, C

Q16) A, B, C, D, E, F, G

Q17) C

Q18) B, D

Q19) B

Q20) B

Q21) A, C, D

Q22) D

Q23) A, B

Q24) B

Q25) C

Q26) C

Q27) B

Q28) B

Q29) B

Q30) B

Q31) A

Q32) B

Q33) C

Q34) A

Q35) D

Q36) D

Q37) C

Q38) B

Q39) A, B, D, E, F, I

Q40) A, C

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module 2

Manage the Cisco UCS B-Series

Overview

The Cisco Unified Computing System (UCS) provides the infrastructure for applications that are used in the data center. That application infrastructure is why high availability, user access, and Cisco UCS management are important. This module covers system management, maintenance, and high-availability services of the Cisco UCS B-Series servers.

Module Objectives

Upon completing this module, you will be able to implement high availability, manage the Cisco UCS, provision administrator access, and maintain Cisco UCS B-Series servers.

This ability includes being able to meet these objectives:

- Implement RBAC
- Manage and upgrade Cisco UCS B-Series firmware
- Implement a backup, import, and restore of the Cisco UCS Manager database
- Implement logging and monitoring
- Implement high availability

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 1

Implementing RBAC

Overview

Data center applications run on Cisco Unified Computing System (UCS). It is crucial to control the access of administrators to avoid the risks of misconfiguration, or loss of service or sensitive company data. The authentication, authorization, and accounting (AAA) model is used to control who has access to Cisco UCS and what can be accessed by different administrators. This lesson describes Cisco UCS Manager support for local and remote authentication and authorization.

Objectives

Upon completing this lesson, you will be able to implement local and remote authentication services to restrict privileges and delegate management authority in Cisco UCS Manager. This ability includes being able to meet these objectives:

- Describe the overall framework of RBAC in the Cisco UCS B-Series
- Implement local users, roles, and privileges
- Implement organizations and locales
- Describe the effective rights of a user as an intersection of roles and locales mapped to a user
- Implement LDAP providers and provider groups
- Implement LDAP (Microsoft Active Directory) as an external authentication and authorization service
- Implement Cisco UCS roles mapping to LDAP (Active Directory) attributes with LDAP provider maps

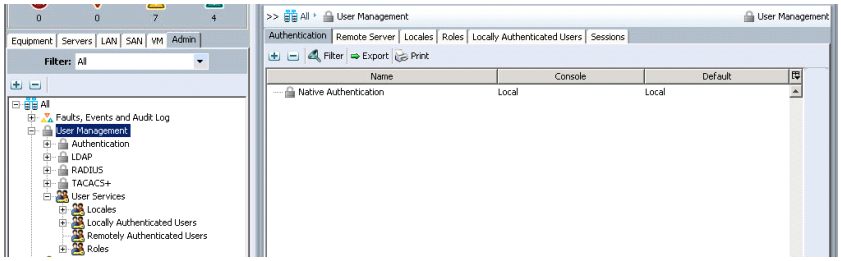
https://t.me/learningnets

RBAC in the Cisco UCS B-Series

This topic describes authentication and role-based access control (RBAC) in Cisco UCS.

Cisco UCS AAA Model

- New Cisco UCS multiauthentication model
  - True simultaneous authentication against multiple sources, including local. No limitation to choose only one authentication method of remote or local.
- Local and remote user databases
- LDAP, RADIUS, and TACACS+ remote user databases supported
- Authorization based on RBAC and locales



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

Authentication is the process in which the system identifies the user that wants access.

Authorization is the process to assign the correct privileges and resource access to the user after successful authentication.

Cisco UCS uses a multidestination authentication schema to authenticate administrator access. User credentials are checked against local user and remote user databases.

Before Cisco UCS version 1.4.1, there was a restriction. You could work with the local user database to provision remote AAA servers, but you were allowed to specify only one authentication method. This restriction meant that the user would be authenticated only to the local user database or to the remote AAA server. There was also a sequence for checking the external authentication servers, starting with the first in the list and going down to the last. This sequence was followed only when Cisco UCS Manager was not able to communicate with the first server. Finally, as a fallback solution, the system tried the local database, again only when there was no communication with any of the external servers.

Starting with Cisco UCS version 1.4.1, the sequence and fallback functionality are preserved. The change in the authentication is that you can provision multiple external AAA servers and the administrator can select the authentication server or group of servers against which the check will be performed. This functionality allows for a working multiple destination model. The external authentication servers belong to protocol realms, depending on the protocol that is used for communication between them and Cisco UCS. The supported protocols are Lightweight Directory Access Protocol (LDAP), RADIUS, and TACACS+. Groups of authentication servers can be formed within each of the protocols. Authentication domains are created based on this grouping, which will be available when the user logs in. Of course, the option to use the local user database is available, but this option is recommended for small Cisco UCS deployments because you have to maintain multiple local user databases, one for each Cisco UCS.

https://t.me/learningnets

The component that is used in the authentication and authorization processes is the user. The user can be created in the local database or can exist on external AAA servers. The user is composed of attributes, or you can refer to them as variables, which describe the user component. The user attributes that are used in the authentication process are the login ID and password. To allow access to features and resources, role and, optionally, locale attributes are configured for the user.

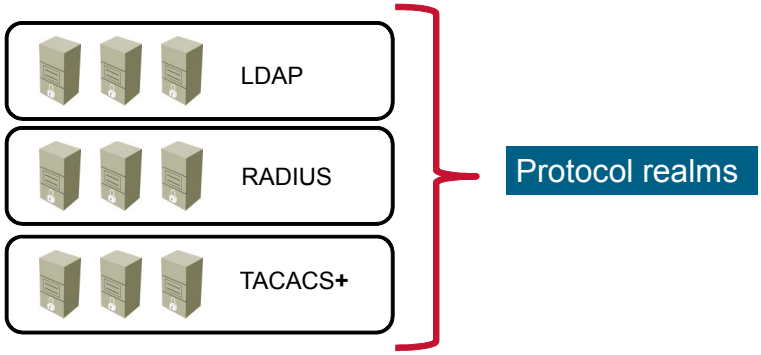
Roles and locales are the components that build RBAC. One or more roles are assigned to each user, as are one or multiple locales. The role defines which features the user can access. Locales define which logical resources the user can access.

Access will be described more in this lesson. Accounting will be reviewed in another lesson.

https://t.me/learningnets

Cisco UCS Authentication: Protocol Realms

- Protocol realms determine how the user will be authenticated:
  - Local and none: Native Cisco UCS Manager realms for local authentication
  - LDAP, RADIUS, TACACS+: Global protocol realms for remote AAA servers
- Authentication servers are put in global protocol realms when added, based on the protocol.



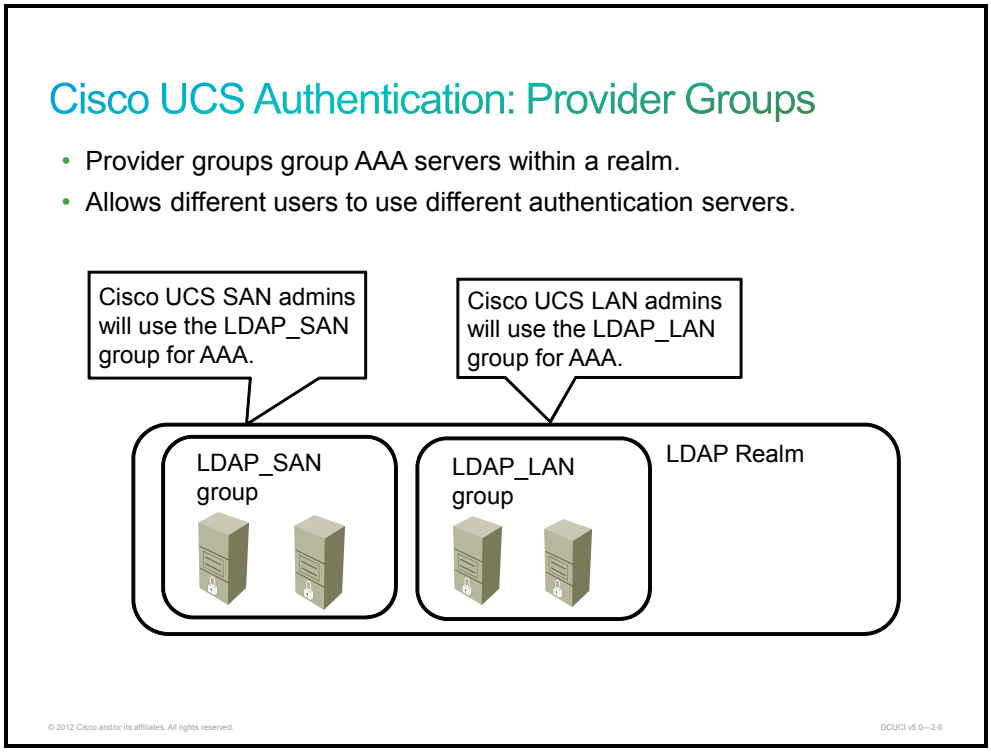
© 2012 Cisco and/or its affiliates. All rights reserved.

As mentioned previously, in Cisco UCS, local or external user databases are automatically placed in protocol realms. Using the AAA protocol, protocol realms define how the user will be authenticated. The following are available protocol realms:

- **Local or none:** These are native protocol realms, identifying the local user database in Cisco UCS.
- **LDAP, RADIUS, and TACACS+:** These protocol realms are used for external AAA servers. When you provision an external LDAP server, for example, and Microsoft Active Directory, the server will be assigned automatically to the LDAP protocol realm by the Cisco UCS Manager. In other words, authentication servers will be added to one of these global protocol realms based on the AAA protocol that you specify during the external AAA provider creation.

In this situation, all servers that are based on LDAP will be added to the LDAP realm. All servers using RADIUS will be placed in the RADIUS realm, and so on. You do not have to create any protocol realms and there is no such functionality in the Cisco UCS.

https://t.me/learningnets



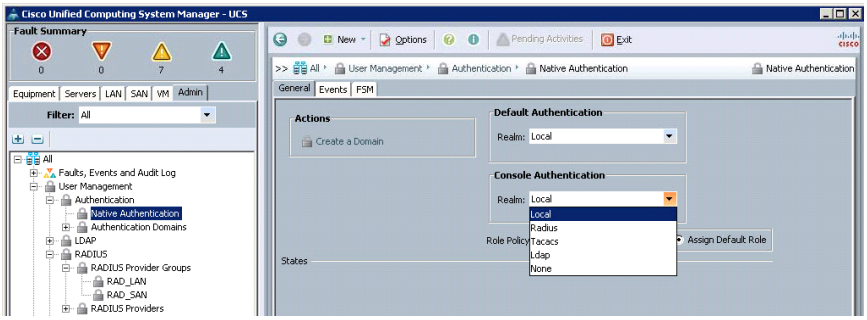
Providers are the components in Cisco UCS that are used to describe and provision the communication with an external AAA server. When a provider is created, Cisco UCS Manager automatically adds it to a realm based on the protocol that is used. This feature is how the system automatically groups external AAA servers based on authentication protocol. But if you need to use different servers for the authentication of different administrator teams, there is the option to group AAA servers, or providers, within a realm into provider groups. After the creation of provider groups, you can create the authentication domain, making the creation of provider groups mandatory in external AAA provisioning. In a provider group, you can have one or multiple AAA servers from the same protocol realm. You cannot create a provider group with servers from different protocol realms.

Cisco UCS Manager groups external servers into protocol realms, and the servers are further segmented into provider groups.

https://t.me/learningnets

Native Authentication and Authentication Domains

- Native authentication is the default authentication for the following:
  - Default access method: Remote access through Telnet, SSH, Cisco UCS Manager GUI, or XML
  - Console access method: Access through the serial console
- Authentication domains are domains for various AAA servers, based on provider groups and protocol realms.



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

After external providers are created and grouped into provider groups, you must tell the system about the authentication methods that are available, which is done in two steps:

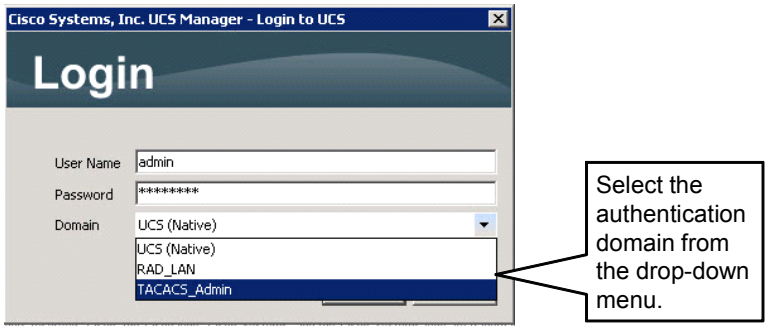
- **Native authentication:** You must specify the default authentication method for user access to the system. Like with Cisco IOS devices, you have to specify the authentication that will be used—local or external—for the two access methods:
  - **Default access method:** Access to Cisco UCS Manager through Telnet, Secure Shell (SSH), HTTP/S, or XML.
  - **Console access method:** Access the system through the console connection.
- **Authentication domains:** These domains are the available authentication options for the user to choose from based on the different provider groups and protocol realms.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS User Login

- Changed login window provides added selection for authentication domain.
- User selects the authentication domain or authentication performed based on native authentication settings.



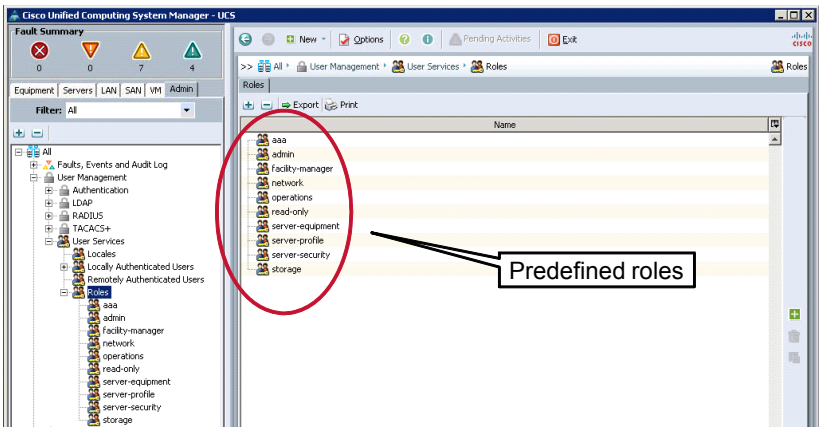
© 2012 Cisco and/or its affiliates. All rights reserved.

As already mentioned, starting with Cisco UCS version 1.4.1, the user login window has changed. The window includes an additional drop-down menu that lists available authentication domains. The user can select the authentication domain against which the authentication is performed. If no selection is made, the user will be authenticated according to the settings for native authentication.

https://t.me/learningnets

Cisco UCS Authorization: Roles

- RBAC provides role-based user authorization.
- A role defines a collection of privileges that determines which actions a user can take in Cisco UCS Manager.



In Cisco UCS, authorization is based on the RBAC model. RBAC consists of three components that are based on the access to features and resources that the user has been granted. The three components are roles, organization structure, and locales.

A role is a set of privileges. The role specifies to which Cisco UCS features the user will have access. In Cisco UCS, there are predefined roles that can be used immediately, or you can create custom roles based on different needs.

The predefined roles include the following:

- AAA administrator
- Administrator
- Facility manager
- Network administrator
- Operations
- Read-only
- Server equipment administrator
- Server profile administrator
- Server security administrator
- Storage administrator

In Cisco UCS Manager, you can have a maximum of 48 user roles including the default roles.

When the user is created, you must assign one or multiple roles. The system will authorize the user depending on the role or roles that are assigned. When there is more than one role that is assigned to the user, then the effective privileges that are granted will be the union of all privileges that are specified in the assigned roles.

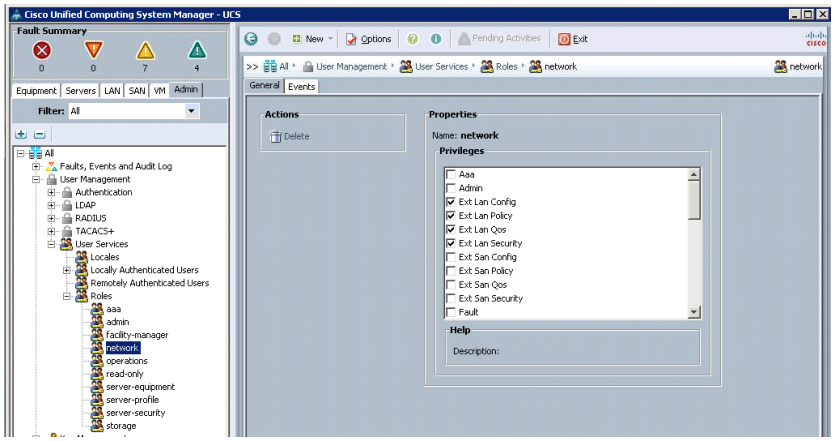
RBAC is a functionality of the Cisco Nexus Operating System (NX-OS). Authorization for all Cisco NX-OS devices—Cisco Nexus switches, Cisco MDS switches, and Cisco UCS—is performed based on RBAC.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Structure of a Role

- Select a role to view its privileges in the content pane.
- Select privileges from a list.



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

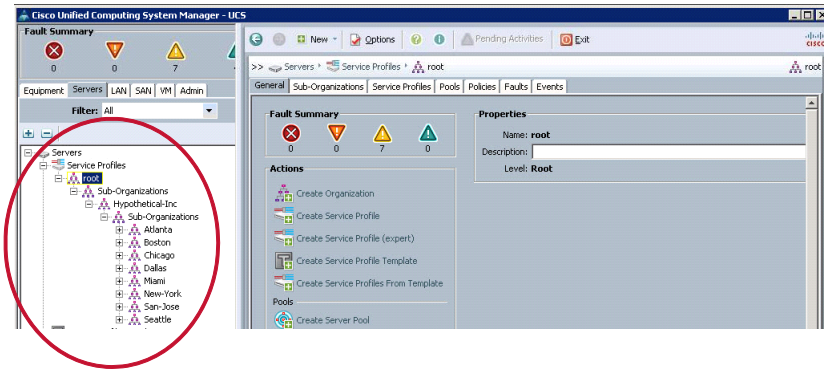
In the figure, the network role is selected. In the content pane, the privileges that define the network role are indicated by the check boxes that have been checked. There are 34 system-defined privileges. Privileges cannot be deleted and, unlike roles, new privileges cannot be created.

The creation of roles is similar to the creation of command sets in Cisco IOS devices, but it is easier because you do not have to explicitly define commands and arguments. You only have to select the areas of features that are needed—network, storage, server, or system-related.

https://t.me/learningnets

Cisco UCS Authorization: Organizations

- Organizations are used to provide an administrative hierarchy to the application of policy.



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

Organizations are created to organize logical resources, such as policies and pools, into an administrative hierarchy. Although organizations are not a mandatory component of Cisco UCS, they can greatly simplify locating the appropriate policy.

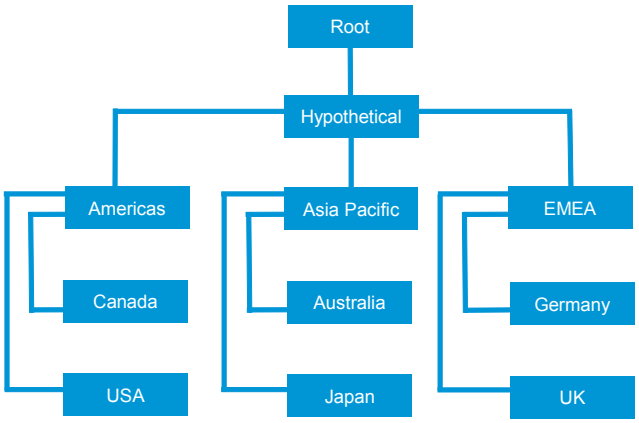
The organizations structure is needed if you want to authorize access to logical resources in Cisco UCS, because the locale component is created from organizations.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Organizational Hierarchy Example

- Root is at the top of the hierarchy.
- Root cannot be deleted. It always exists.

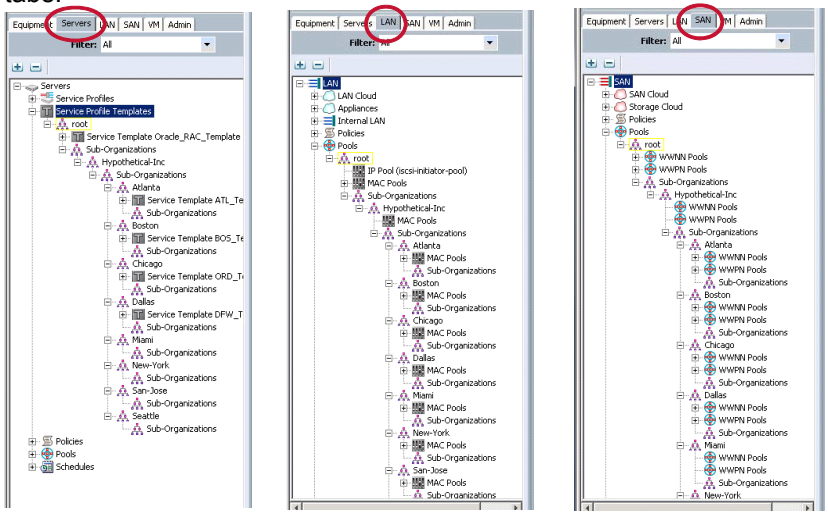


© 2012 Cisco and/or its affiliates. All rights reserved.

The example in the figure illustrates one approach to organizational hierarchy. Hypothetical Inc. is a fictional multinational company that has decided to use organizations to divide policy by geography. At the top of the hierarchy is an organization called root. Even if organizations are not created in Cisco UCS, there is always one organization—root.

Scope of Organizations

- Organizations can be created (and exist) on the servers, LAN, and SAN tabs.



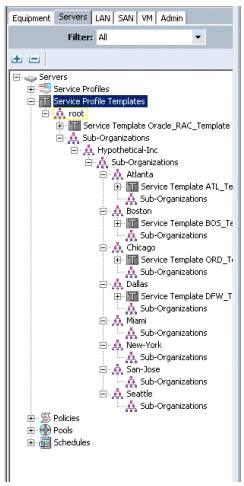
© 2012 Cisco and/or its affiliates. All rights reserved.

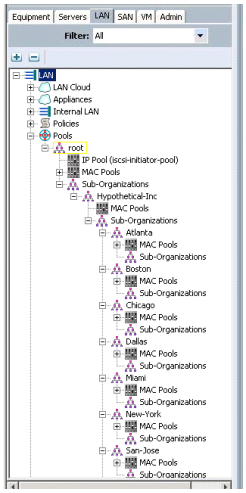
Organizations can be created in the Server, LAN, and SAN tabs of the navigation pane in Cisco UCS Manager. Each tab allows the creation of organizations to organize function-specific policy. When you create an organization in one of the tabs, it will appear automatically in the other tabs.

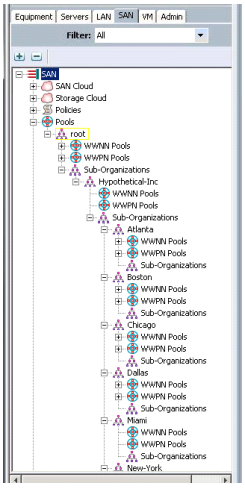
https://t.me/learningnets

What Can Be Configured in an Organization?

- You can create policies, profiles, thresholds, and pools specific to the tab context (Servers, LAN, or SAN).



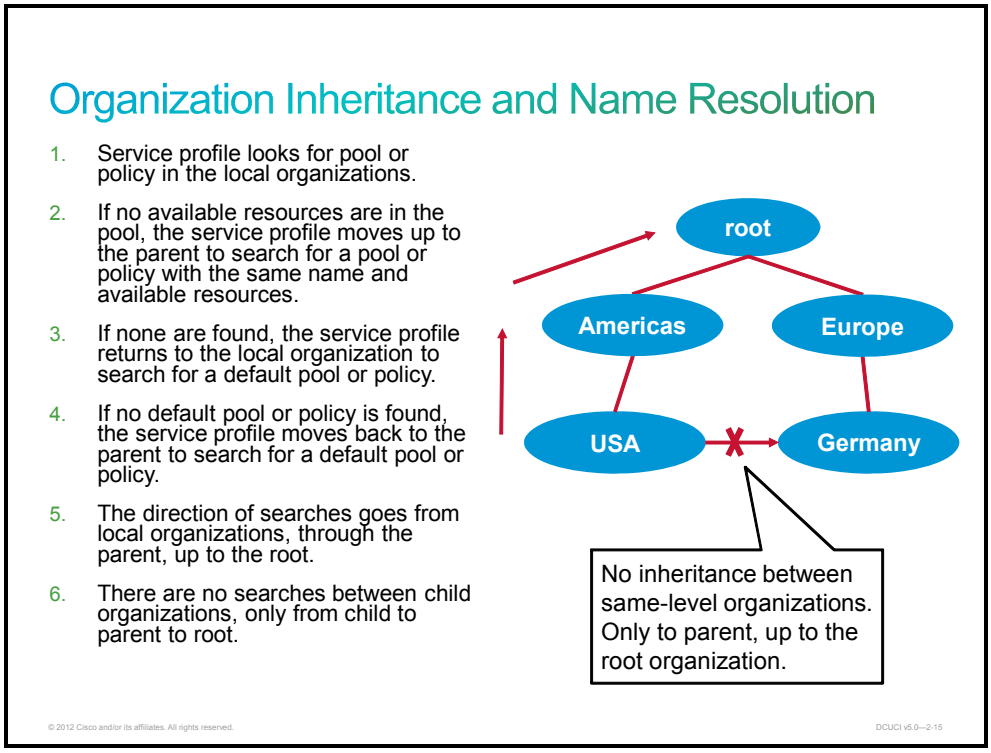




© 2012 Cisco and/or its affiliates. All rights reserved.

Depending on the tab context in Cisco UCS Manager, organizations can contain service profiles, identity pools, resource pools, policies, and thresholds.

https://t.me/learningnets



The logical resources—pools and policies—are grouped in organizations. When you create a service profile in one organization, you can use the local pools and policies. Also visible are the root pools and policies. There are some rules that are related to the availability of resources to a service profile created in an organization. The following is the order in which the service profile will search for resources:

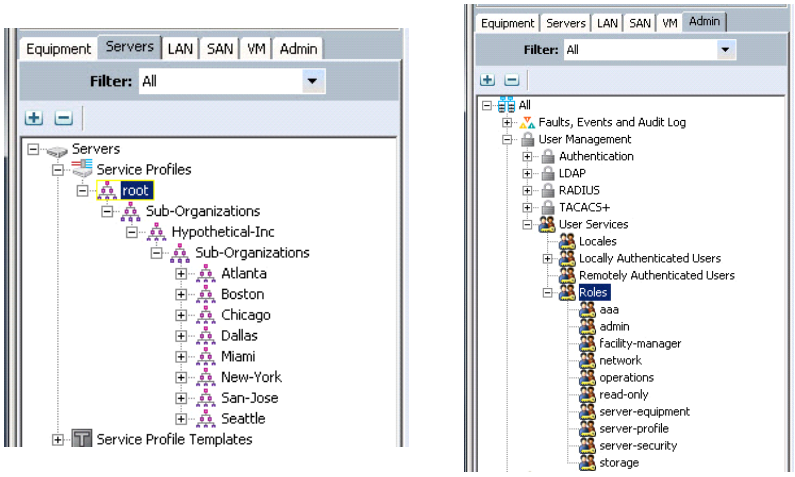
1. The service profile will look for resources in the local organization pools and policies.
2. If the service profile cannot find available resources, it will search in the parent organization for pools and resources with the same names and available resources. The service profile will look up to the root organization.
3. If no default pools and policies are found, the service profile will return to its organization and will search for default pools and policies.
4. Again, if no default pools and policies are found, the service profile will search in the parent organization. Again, it will go through all parent organizations up to the root until it finds resources.

The direction of search, or inheritance, is always from the local to the parent to the root organization. The search will never be performed against any other organization that is not a parent.

https://t.me/learningnets

RBAC and Organizations

- RBAC and organizations are complimentary constructs.
- They can be used separately or together.



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

Roles and organizations are complementary components. You can use them together or separately. If only roles are used, then the users will be controlled by the features they can configure. If you use organizations, then the users will be controlled by logical resources to which they have access.

© 2012 Cisco Systems, Inc.

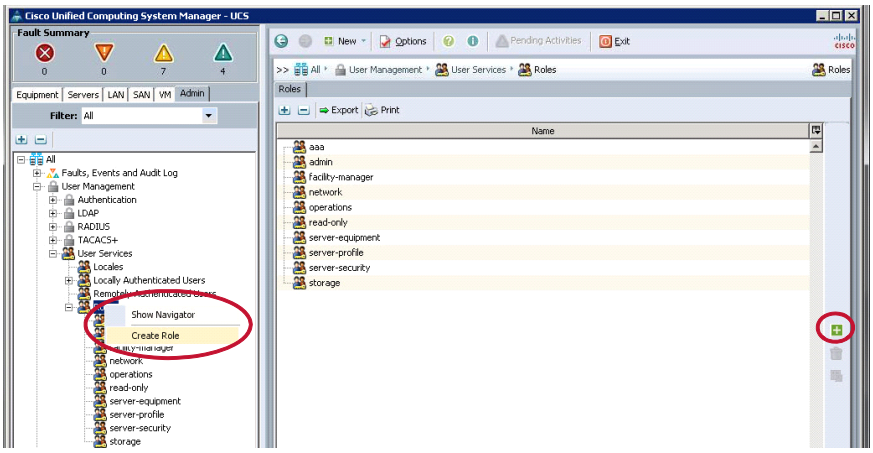
https://t.me/learningnets

Implement Local Users, Roles, and Privileges

This topic describes how to provision local users and roles.

Create a Role: Start the New Role Wizard

- To start the new role wizard, right-click **Roles** and select **Create Role**.
- You can also click the plus sign (+) in the content pane.

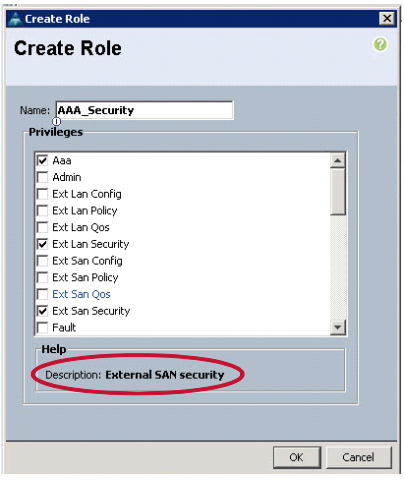


© 2012 Cisco and/or its affiliates. All rights reserved.

To start the new role wizard, right-click the role in the navigation pane or click the plus sign (+) in the content pane.

Name Role and Define Privileges

- Specify name.
- Click the text of a privilege and its description will appear in the Help section.



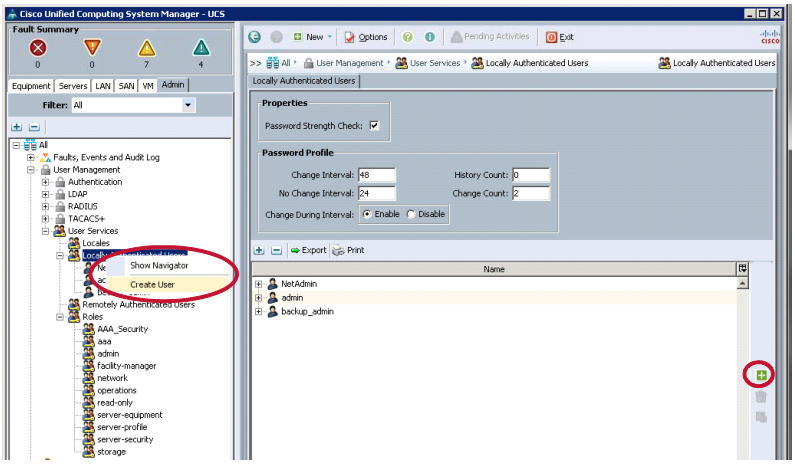
© 2012 Cisco and/or its affiliates. All rights reserved.

Define a name for the new role and select the appropriate privileges. Click **OK** to finish creating the role.

https://t.me/learningnets

Create a Local User: Start the New User Wizard

- To create a local user, right-click **Locally Authenticated Users** and select **Create User**.
- You can also click the plus sign (+) in the content pane.



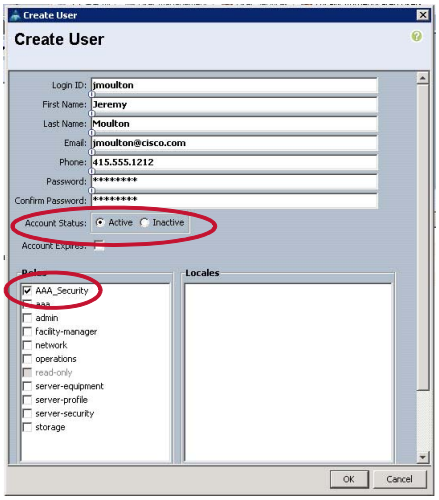
To create a new user, right-click **Locally Authenticated Users** or click the plus sign (+) in the content pane.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Create Local User with Custom Role

- Jeremy will inherit the permissions of the new AAA_Security role.



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

The figure shows the settings for the creation of user jmoulton. This user will be created with the new AAA_Security role and its inherent privileges. The only two required fields in the Create User wizard are Login ID and Password. If no role is selected, then the user is assigned read-only privileges.

The status of the user must also be set.

The Locales section is empty because no locales have been created. If a locale is created, it will appear in the Locales area.

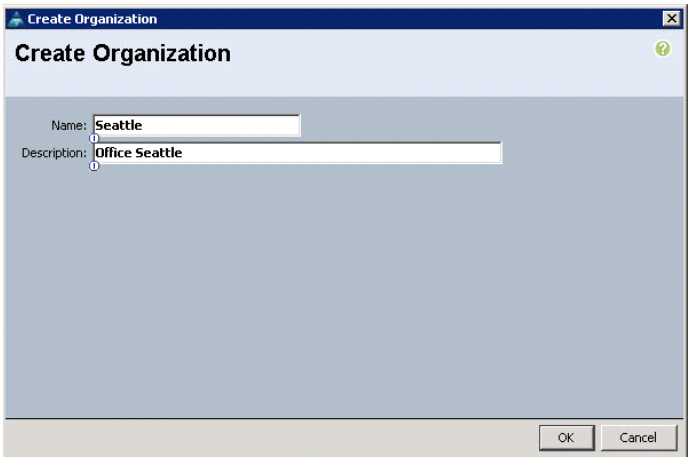
https://t.me/learningnets

Implement Organizations and Locales

This topic describes how to provision organizations and locales.

Create a New Organization

- Right-click the root or any suborganization element in the hierarchy, and then click **Create Organization**.
- The new organization will appear under the selected one.

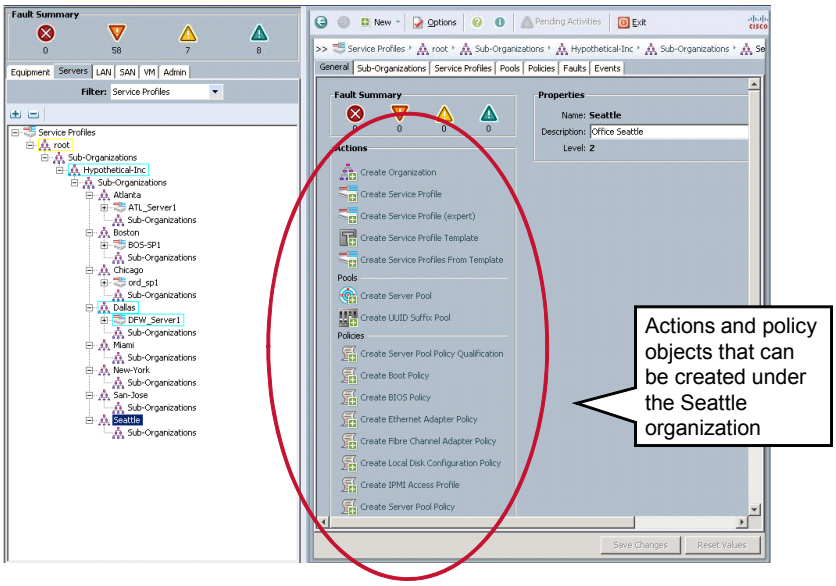


© 2012 Cisco and/or its affiliates. All rights reserved.

To create a new organization, right-click the root organization or any previously created suborganization. New organizations can be created in the Server, LAN, or SAN tabs. The new organization is propagated automatically to all three relevant tabs.

https://t.me/learningnets

Actions in New Organization

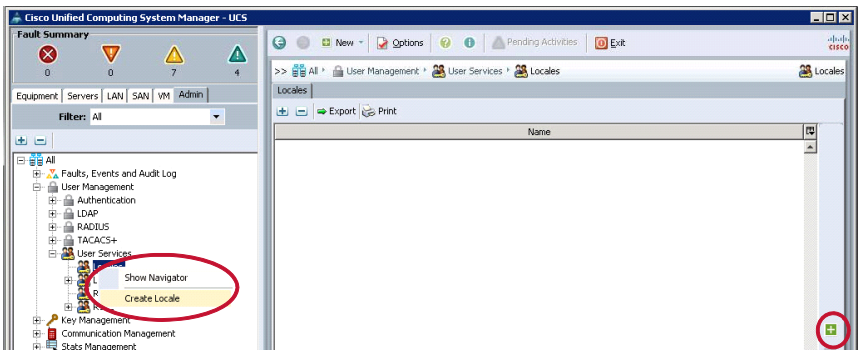


© 2012 Cisco and/or its affiliates. All rights reserved.

In the figure, a new suborganization is created for Seattle. The Seattle organization is propagated to the LAN and SAN tabs. Because the current context is the Server tab, all of the actions that are available in the Seattle organization relate to service profiles, pools, and policies that relate to blade-server definition.

Start the New Locale Wizard

- Locales are groups of organizations for authorization purposes.
- From the Admin tab, filter on User Management.
- Right-click **Locales** or click the plus sign (+) in the content pane.

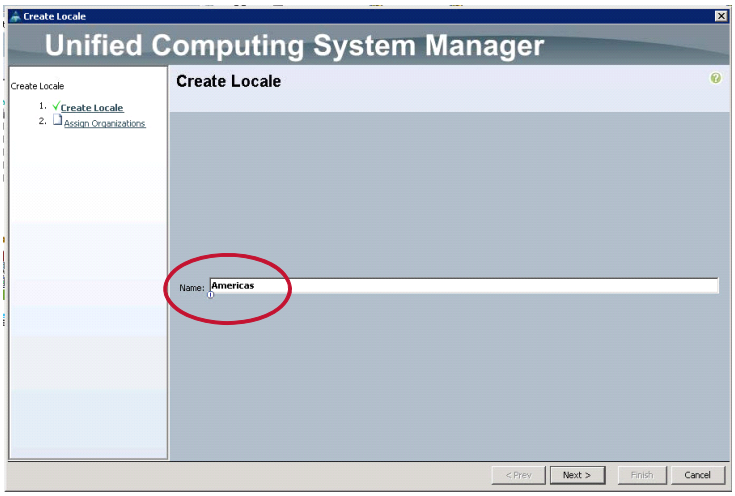


© 2012 Cisco and/or its affiliates. All rights reserved.

Unlike organizations, locales are created under the Admin tab. Set the filter to **User Management** from the drop-down list. To create a new locale, right-click **Create Locale** or click the plus sign (+) in the content pane.

https://t.me/learningnets

Name the Locale

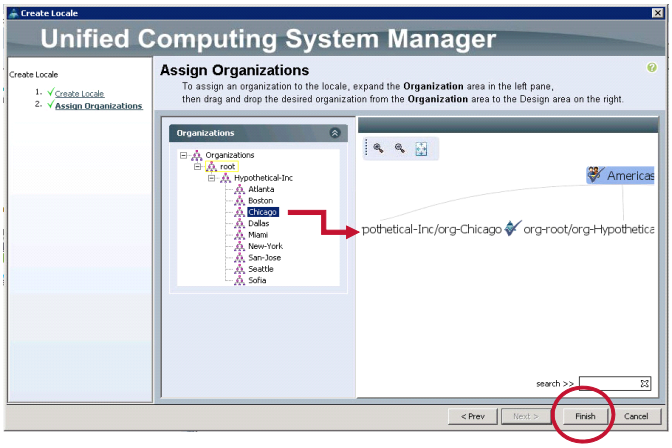


© 2012 Cisco and/or its affiliates. All rights reserved.

Provide a descriptive name for the new locale.

Drag and Drop the Organization onto the Locale Name

- Select organizations from the list.
- Drag and drop the selected organizations in the white field.



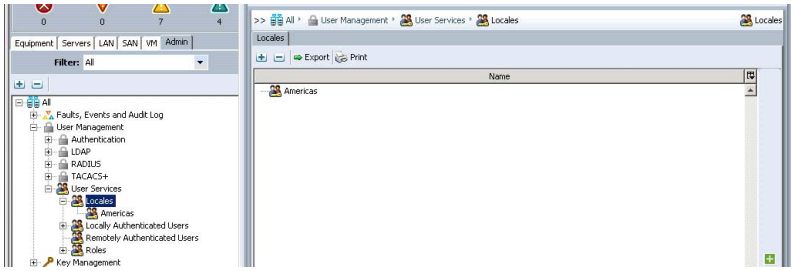
© 2012 Cisco and/or its affiliates. All rights reserved.

Click the double down-arrow icon and expand the list of organizations. Click the organization that applies to the new locale and drag it into the right-hand window, under the name of the locale. If the operation is successful, the name of the organization appears beneath the name of the locale with a check mark to the left of the organization. Click **Finish** to complete the wizard.

https://t.me/learningnets

Locale Available to Restrict User Rights

- Check the new locale by navigating to **Admin > User Management > User Services > Locales**.
- The locale can be used to authorize users.

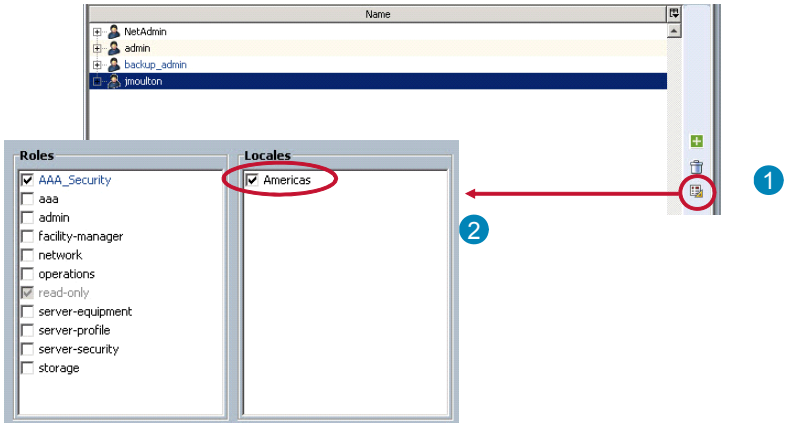


© 2012 Cisco and/or its affiliates. All rights reserved.

The purpose of creating a locale is to restrict the privileges of the user to a particular organization. Your new locale should appear in the Locales list.

Modify Local User Rights to Apply Locale

- Go to Locally Authenticated Users and select a user to modify.
- Assign roles and locales.



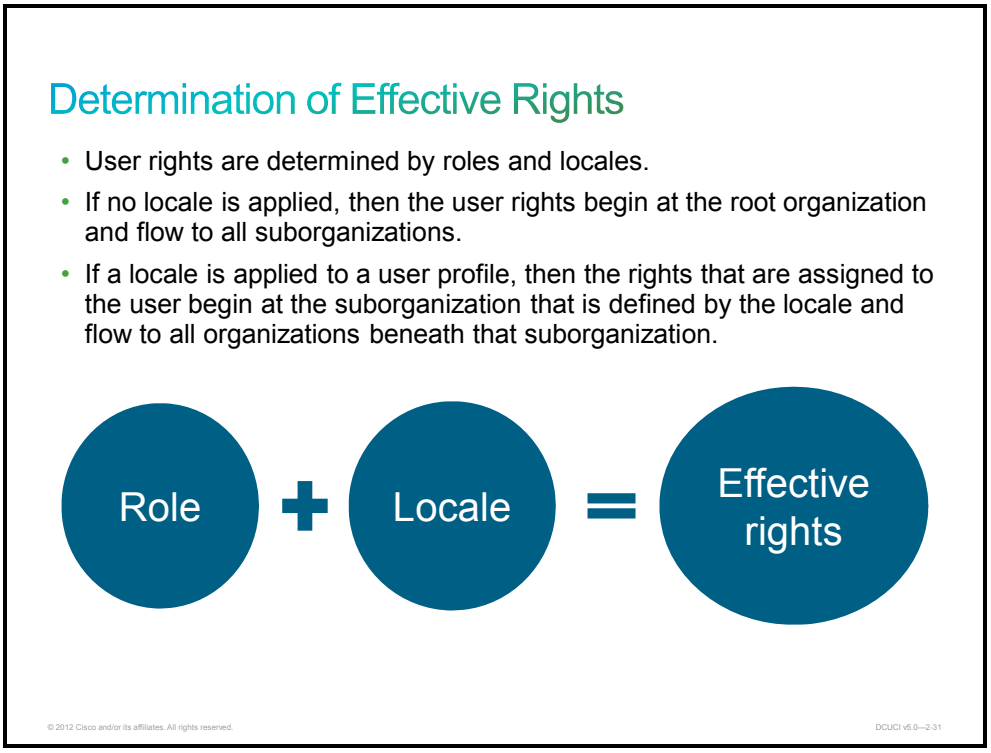
© 2012 Cisco and/or its affiliates. All rights reserved.

In the example, user jmoulton is assigned the AAA_Security role and is also now bounded by the Americas locale.

https://t.me/learningnets

Effective Rights of a User as an Intersection of Roles and Locales

This topic discusses the effective rights of users.



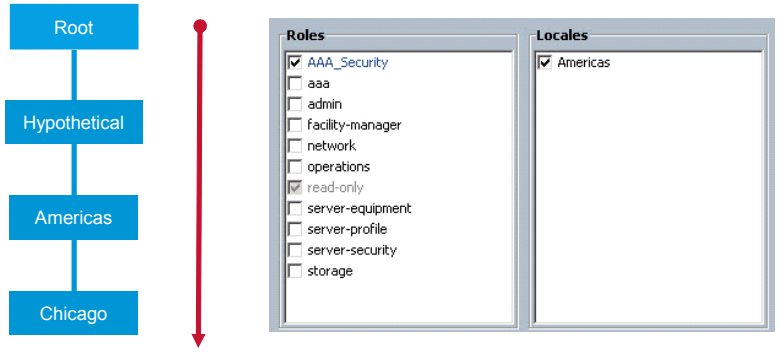
The effective rights of the user are determined by the privileges that role membership bestows and that locale restricts.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Effective User Rights for Admin

- The admin user has unrestricted privileges from the root organization down to every suborganization.
- The admin user cannot be restricted by locale.



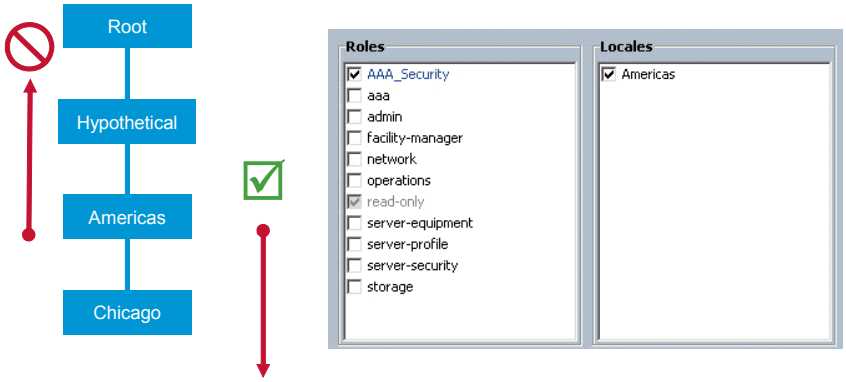
© 2012 Cisco and/or its affiliates. All rights reserved.

The built-in admin user has complete administrative privileges, from the root organization down to the lowest suborganization. The admin user and any user with the admin role cannot be assigned to a locale.

https://t.me/learningnets

Effective User Rights for jmoulton

- The effective rights for the user jmoulton are the intersection of the AAA_Security role and the Americas locale.



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

User jmoulton has privileges only in the Americas organization and suborganizations. This user has those privileges because the Americas locale is assigned to the user jmoulton and the Americas organization and its suborganizations are members of the Americas locale. Although jmoulton has read-only privileges higher up in the organizational hierarchy, this user cannot create any objects that are associated with the assigned roles that are higher than Americas in the organizational structure.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

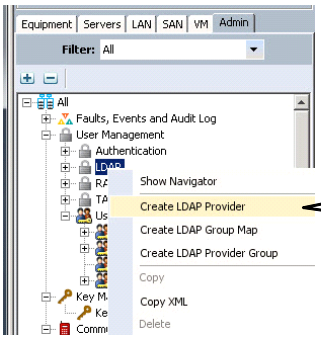
Implement LDAP Providers and Provider Groups

This topic describes how to provision LDAP providers and provider groups.

Remote User Databases

The following is the sequence for implementing remote AAA:

1. Create remote provider: LDAP, RADIUS, or TACACS+.
2. Create provider group.
3. Create authentication method.
4. Set native authentication.



1. Create a remote provider by navigating to **Admin > All > User Management**. Right-click **LDAP** to select **Create LDAP Provider** or click the plus (+) sign.

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

Starting with Cisco UCS version 1.4.1, there is a sequence of steps that is needed to provision and use an external AAA server. This section provides an example with an LDAP provider. Based on LDAP, you can provision a provider that will use Active Directory. Also, additional configuration must be performed for LDAP providers—LDAP group maps. The provisioning of RADIUS or TACACS+ providers follows the same steps, excluding the group mapping steps.

The following are the steps:

Step 1 Create a remote provider—LDAP, RADIUS, or TACACS+.

Step 2 Create a provider group.

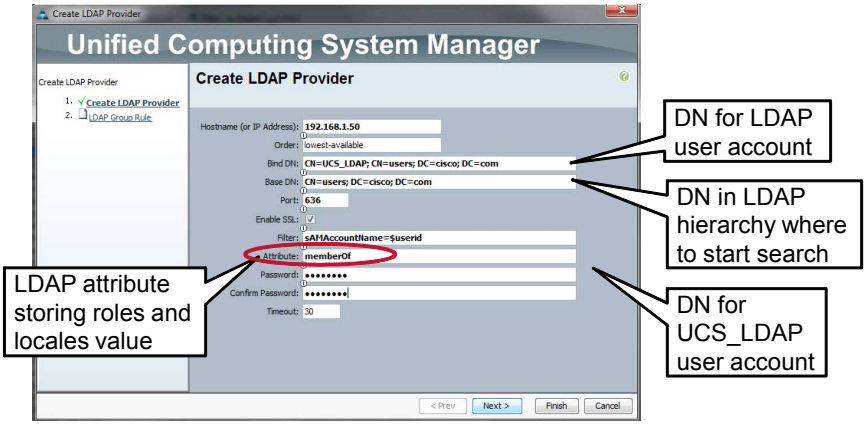
Step 3 Create an authentication method.

Step 4 Set native authentication. (This step was shown earlier.)

To start the remote provider creation wizard, navigate to **Admin > User Management** and right-click **LDAP** to select **Create LDAP Provider**.

https://t.me/learningnets

Create an LDAP and Active Directory Provider



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

In the LDAP Provider wizard, the first step will require the provisioning of the following:

- **Hostname (or IP Address):** Enter the IP address of the LDAP provider or its fully qualified domain name (FQDN).
- **Order:** Enter a number or accept the default to have Cisco UCS Manager select the lowest available number. If this is the first LDAP provider, the automatically selected number will be 1. The number indicates the order in which Cisco UCS Manager selects LDAP servers for authentication. If server 1 is unavailable or unresponsive, then Cisco UCS Manager attempts to authenticate requests with LDAP provider 2, and so on. A total of 16 LDAP servers can be configured for redundancy. At least two are recommended.
- **Bind DN:** Enter the distinguished name (DN) of the LDAP object that will perform the username and password lookup in the LDAP database. In the example, user UCS_LDAP is configured to perform the lookup. The entry "CN=UCS_LDAP; CN=users; DC=cisco; DC=com" describes the user UCS_LDAP in the users container in the domain Cisco.com. (CN is the abbreviation for common name, and DC is the abbreviation for domain component.) User UCS_LDAP does not require administrative privileges, only the rights that are required to connect to the LDAP database.
- **Base DN:** Enter the DN for the LDAP database superuser account.
- **Port and Enable SSL check box:** These two fields are related. The default port for LDAP is TCP port 389. If the default is selected, then authentication requests are processed in cleartext. A best practice is to check the Enable SSL check box and change the port to TCP port 636. Microsoft Windows servers listen for LDAP over Secure Sockets Layer (SSL) on TCP port 636.
- **Filter:** The LDAP search is restricted to those usernames that match the defined filter. This property is required. If you do not specify a filter on this tab, then you must specify one on the General tab for every LDAP provider that is defined in this Cisco UCS instance.

https://t.me/learningnets

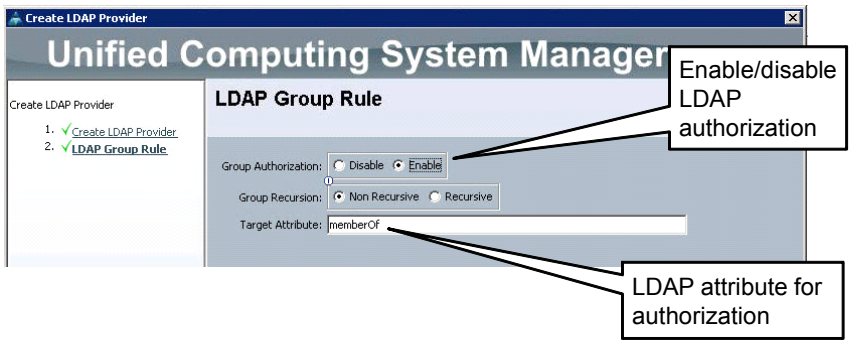
- **Attribute:** Specify the LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. If you do not want to extend your LDAP schema, you can configure an existing, unused LDAP attribute with the Cisco UCS roles and locales. Alternatively, you can create an attribute named CiscoAVPair in the remote authentication service with the attribute ID of 1.3.6.1.4.1.9.287247.1.
- **Password and Confirm Password:** Enter the password for the LDAP user (in the example, user UCS_LDAP).
- **Timeout:** The length of time in seconds that the system should spend trying to contact the LDAP database before it times out. The default value is 30 seconds. The available range is from 1 to 60 seconds.

Note	The username that is specified in the Bind DN does not need to have administrator privileges. In fact, the user only needs enough rights to read values in the Active Directory LDAP tree.

https://t.me/learningnets

LDAP Group Rule

- Enable authorization for the LDAP provider.
- Provision LDAP group map for the rule.



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

In the second step of the wizard, you have to enable or disable the authorization. You must also define two more options:

- **Group Recursion:** This option determines whether Cisco UCS will search both the mapped groups and their parent groups for the user authorization properties. The following are available options:
  - **Non Recursive:** Cisco UCS Manager will search only the mapped groups.
  - **Recursive:** The parent groups will also be searched.
- **Target Attribute:** This option is the LDAP attribute that Cisco UCS Manager uses to determine the group membership. The default string is memberOf.

The default attribute that is used in Cisco UCS Manager for RADIUS, TACACS+, and LDAP servers is the CiscoAVPair. While CiscoAVPair exists as a vendor-specific attribute in RADIUS and in the TACACS+ server, it does not exist in the LDAP schema. For the LDAP server, you must either modify the schema to include the CiscoAVPair, or use any of the available and valid attributes.

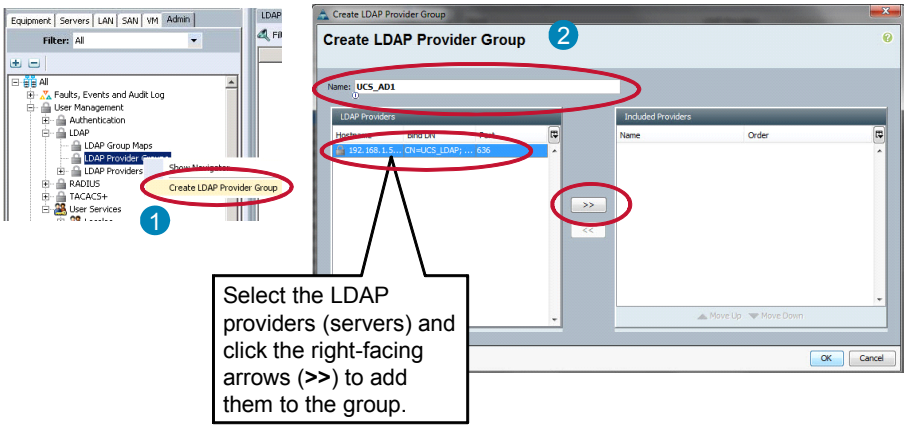
Click **Finish** to end the wizard.

Additionally, you have to provision an LDAP group map for the authorization to also work with roles and locales. The creation of an LDAP group map is discussed later in this lesson.

https://t.me/learningnets

LDAP Provider Group

- Groups LDAP providers
- Needed to create authentication domain that is based on LDAP realm



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

At this point, you have created the LDAP provider. To create an authentication domain for this provider, you have to create an LDAP provider group. To create an LDAP provider group, navigate to **Admin > User Management > LDAP** and right-click **LDAP Provider Groups** and click **Create LDAP Provider Group**.

Define a name for the group. Next, select from the available LDAP providers from the left and click the right-facing arrows (>>) to add them to the group. Click **OK** to end the creation of the group.

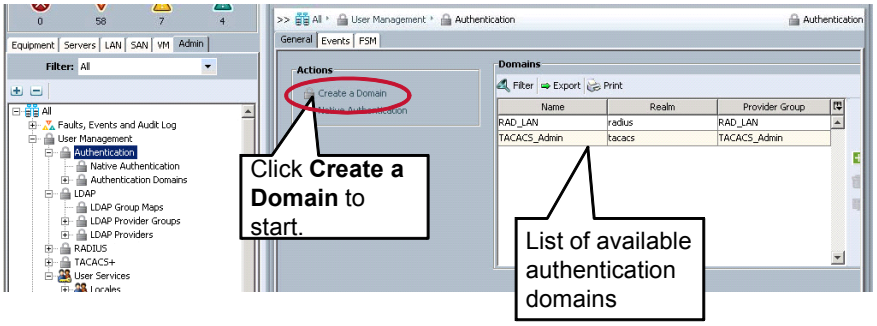
https://t.me/learningnets

Implement LDAP and Microsoft Active Directory as an External Service

This topic describes how to provision an authentication domain for the LDAP provider.

Create Authentication Method

- Create authentication domain to include the LDAP provider group in the authentication selection.
- The authentication domain will appear in the domain field in the login window.
- Navigate to **Admin > User Management > Authentication**.



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

To make the LDAP provider available in the login window selection, you have to create an authentication domain for the LDAP provider group.

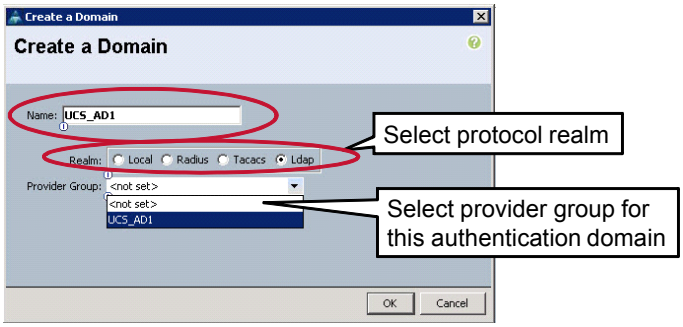
Click **Authentication** under **User Management**. In the content pane, click **Create Domain**.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Authentication Domain Settings

- Specify name.
- Specify protocol realm.
- Select from available provider groups for this protocol realm.



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

In the new window, define the following:

- **Name:** Enter a name for the authentication domain.
- **Realm:** Select the protocol realm. For this example, select **Ldap**.
- **Provider Group:** The drop-down menu will be based on the selected realm. Provider groups for the selected realm will be listed.

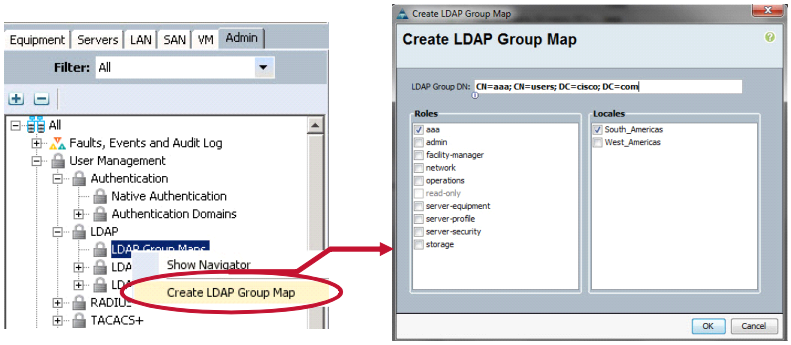
https://t.me/learningnets

Implement Cisco UCS Role Mapping

This topic describes how to create an LDAP group map.

LDAP Group Map

- LDAP Group Map: Mapping between roles and locales and LDAP groups. Link between Cisco UCS Manager and LDAP server for authorization information.
- Needed for LDAP Group Rule.
- The user is authorized for a specific LDAP group and, based on this, is assigned the roles and locales specified in the LDAP Group Map.



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

On the LDAP server, users are organized in groups that are based on their roles. For example, the administrators that are responsible for the AAA configuration will be in the aaa group on the LDAP server. The corresponding component in the Cisco UCS Manager is the aaa role. Also on the LDAP server, authorization properties for users are defined, but roles and locales are components that are specific to the Cisco NX-OS. On the external AAA server, you do not have the functionality to create roles and locales. For authorization to work, an attribute is used to carry authorization information between Cisco UCS Manager and the LDAP server. You enabled the authorization and defined the attribute that is used for this purpose in the second step of the LDAP provider creation wizard. With the LDAP group map, you map roles and locales to the user group in the LDAP server. Thus, when group membership information is provided to Cisco UCS Manager, the system will know which roles and locales to apply to the user.

To create the LDAP group map, right-click **LDAP Group Maps**, select **Create LDAP Group Map**, and define the following:

- **LDAP Group DN:** The distinguished name for the LDAP group.
- **Roles:** Select the roles to be mapped to this group.
- **Locales:** Select the locales to be mapped to this group.

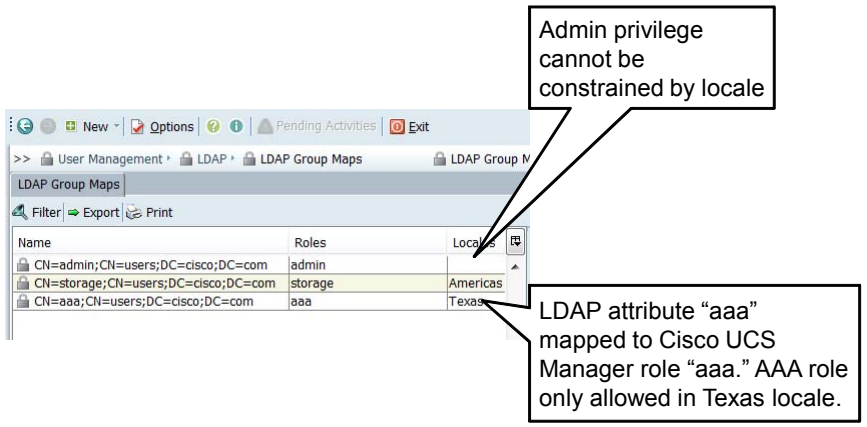
Click **OK** to finish.

The creation of the LDAP group map is needed for the LDAP group rule to be operational.

https://t.me/learningnets

LDAP Group Mappings

- Cisco UCS Manager allows you to create LDAP group mappings to set granular limits on user privileges.



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

With the LDAP group, you map the authorization components from Cisco UCS Manager to the authorization component in the LDAP server. This mapping is local for Cisco UCS Manager and is needed by the system to know which role, and optionally which locale, to apply to the user after successful authentication. The decision is based on the information for group membership that comes from the LDAP server and the LDAP group map in the Cisco UCS Manager. When the user is authenticated against the LDAP server, the server returns information that the user belongs to the storage group. Based on this information, Cisco UCS Manager knows from the LDAP group map to assign the user to the storage role. The LDAP group map also indicates that the user is assigned to the Americas locale. This information means that the user will be limited to work only with the organizations and suborganizations in this locale.

The admin user is a special case because no locale can be assigned in the LDAP group map. As discussed earlier, the admin user cannot be limited.

https://t.me/learningnets

Summary

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

Summary

- Multidestination simultaneous authentication is supported by creating multiple authentication domains. Authorization is based on roles and locales.
- Local users are provisioned in the local user database. Roles must be assigned for authorization to set the privileges.
- Organizations create a logical grouping of resources. Locales are created from organizations and are used to control access to the logical resources.
- The admin user has rights over the entire system. The effective user rights are the intersection of roles and locales.
- LDAP provider and LDAP provider groups must be created to create an authentication domain.
- Native authentication must be set. The user chooses an authentication domain against which it will be checked.
- An LDAP group map must be created to map roles and locales to LDAP user groups. It is needed for the LDAP group rule.

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

https://t.me/learningnets

Lesson 2

Managing and Upgrading Cisco UCS B-Series Firmware

Overview

Before the introduction of the Cisco Unified Computing System (UCS), firmware management in blade server environments was challenging. Cisco UCS simplifies firmware management. Cisco UCS consists of multiple components. Those components have different approaches for upgrades. To allow for administrative consistency and stateless computing, firmware images in Cisco UCS can be attached as a policy to a service profile. If the service profile is moved to a new blade, then there is no need for manual firmware intervention.

Objectives

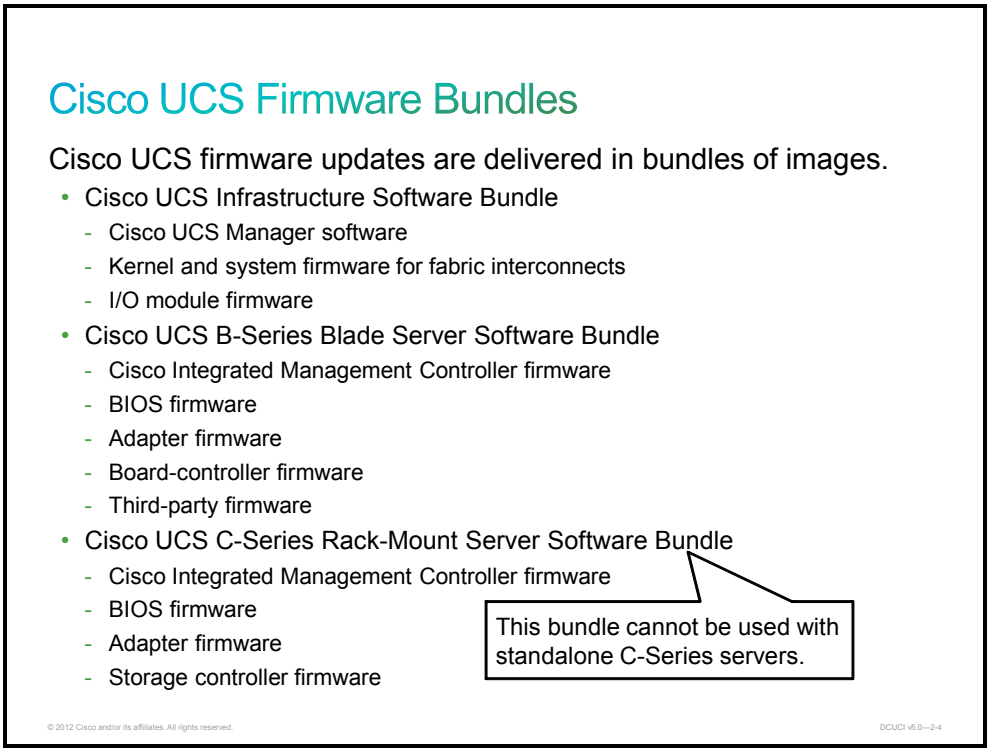
Upon completing this lesson, you will be able to list the processes for managing the firmware repository and upgrade or downgrade Cisco UCS firmware components using Cisco UCS Manager. This ability includes being able to meet these objectives:

- Describe where to find Cisco UCS firmware packages on Cisco.com
- Update Cisco UCS firmware
- Direct upgrade of mezzanine adapter, Cisco Integrated Management Controller, and IOM firmware
- Describe software updates on the fabric interconnect
- Describe the requirement for firmware updates via host firmware packages in the service profile
- Describe the differences between the firmware processes of Cisco UCS fabric interconnect and IOM, Cisco Integrated Management Controller, and adapter
- Describe how to update and activate the hardware capability catalog

https://t.me/learningnets

Finding Cisco UCS Firmware Packages

This topic describes where to find and download Cisco UCS firmware packages.



Firmware images for Cisco UCS components are delivered in bundles. Before Cisco UCS version 1.4, there was one full bundle that contained the firmware images for all components. Since only one bundle was available, you had to wait for the new version of Cisco UCS if you wanted to update adapter card firmware. To fix this problem, starting with Cisco UCS version 1.4, the firmware packages are divided into three bundles:

- Cisco UCS Infrastructure Software Bundle
  - Cisco UCS Manager software
  - Kernel and system firmware for fabric interconnects
  - I/O module firmware
- Cisco UCS B-Series Blade Server Software Bundle
  - Cisco Integrated Management Controller firmware
  - BIOS firmware
  - Adapter firmware
  - Board-controller firmware
  - Third-party firmware

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

- Cisco UCS C-Series Rack-Mount Server Software Bundle
  - Cisco Integrated Management Controller firmware
  - BIOS firmware
  - Adapter firmware
  - Storage controller firmware

Note The Cisco UCS C-Series software bundle cannot be used with C-Series servers in standalone mode.

Note Cisco C-Series integration with Cisco UCS is reviewed in the “Provision Cisco UCS Compute Resources” module.

https://t.me/learningnets

Locate Firmware on Cisco.com

- Browse to http://www.cisco.com/cisco/software/navigator.html
- Log into Cisco.com.

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

To download the software bundles, browse to http://www.cisco.com/cisco/software/navigator.html.

After you log in with your Cisco.com account, from the download options select **Products > Unified Computing and Servers > Cisco UCS Infrastructure and UCS Manager Software**.

Choose Cisco UCS Infrastructure Software Bundle

- Select **Unified Computing System (UCS) Infrastructure Software Bundle**.

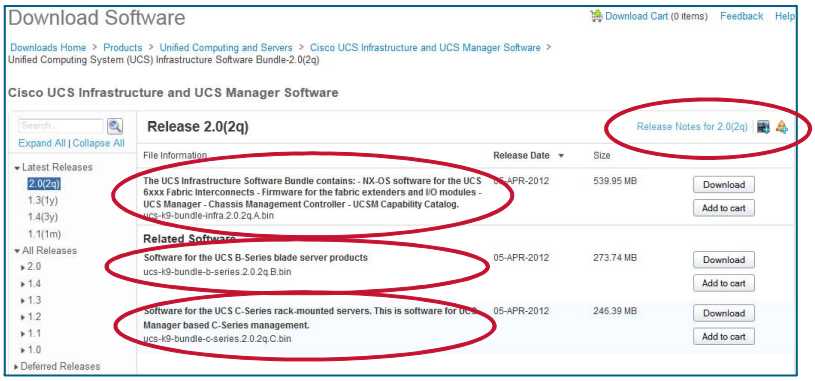
© 2012 Cisco and/or its affiliates. All rights reserved.

Select **Unified Computing System (UCS) Infrastructure Software Bundle**.

https://t.me/learningnets

Bundle Selection

- All Cisco UCS software bundles will be listed.
- Select version and download the bundles.
- Check the release notes.



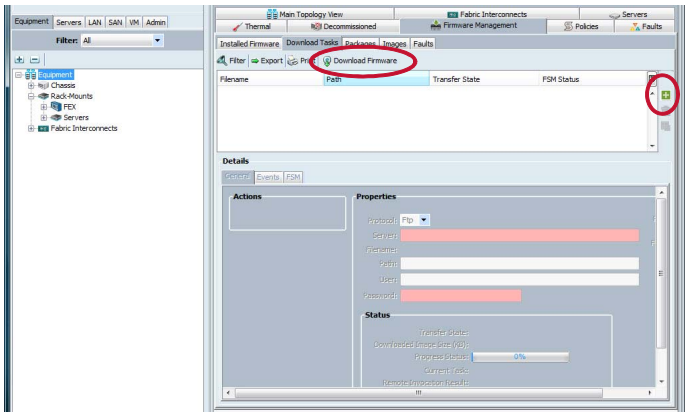
You will be provided with the Cisco UCS infrastructure bundle and also with the related software downloads. This process is an easy way to get the three software bundles from one place.

Select the appropriate version of the Cisco UCS software and download the bundles.

https://t.me/learningnets

Copy Cisco UCS Bundles to Fabric Interconnect

- Navigate to **Equipment > Firmware Management > Download Tasks**.
- Create a new download task.



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

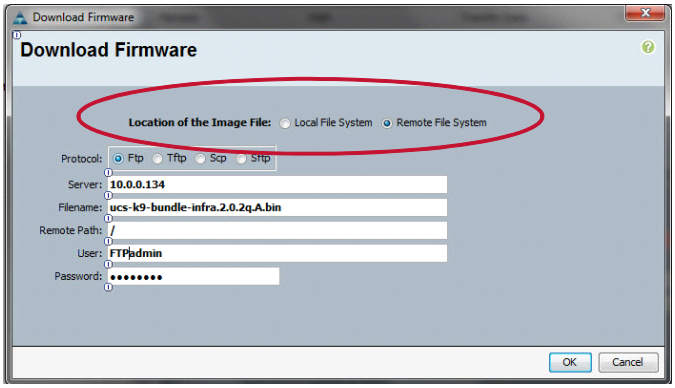
When the bundle image is downloaded, it must be transferred to the flash file system of the active management node. As long as you browse to the virtual IP address of the cluster, the image is updated only to the active management node.

Navigate to **Equipment** > **Firmware Management** > **Installed Firmware**, and then click **Download Firmware**.

https://t.me/learningnets

Provision Copy Method in Download Task

- Select **Local File System** to use HTTP copy.
- Select **Remote File System** to copy using FTP, TFTP, SCP, or SFTP.



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

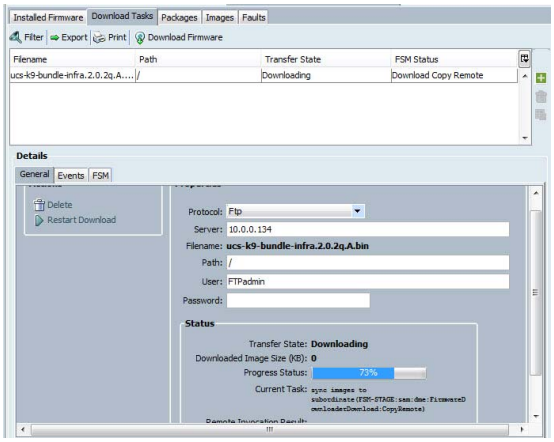
Select how to copy the bundle image:

- **Local File System:** This method will use HTTP-based copy and you will browse for the bundle image file locally on your PC.
- **Remote File System:** With this option, you can choose from FTP, TFTP, Secure Copy Protocol (SCP), and Secure FTP (SFTP). If this option is selected, you have to enter the IP address or fully qualified domain name (FQDN) of the host on which the downloaded bundle image resides, enter the filename and authentication credentials, and click **OK**.

https://t.me/learningnets

Download Status

- Download starts immediately after the download task is created.
- Progress can be observed in the Download Tasks tab.



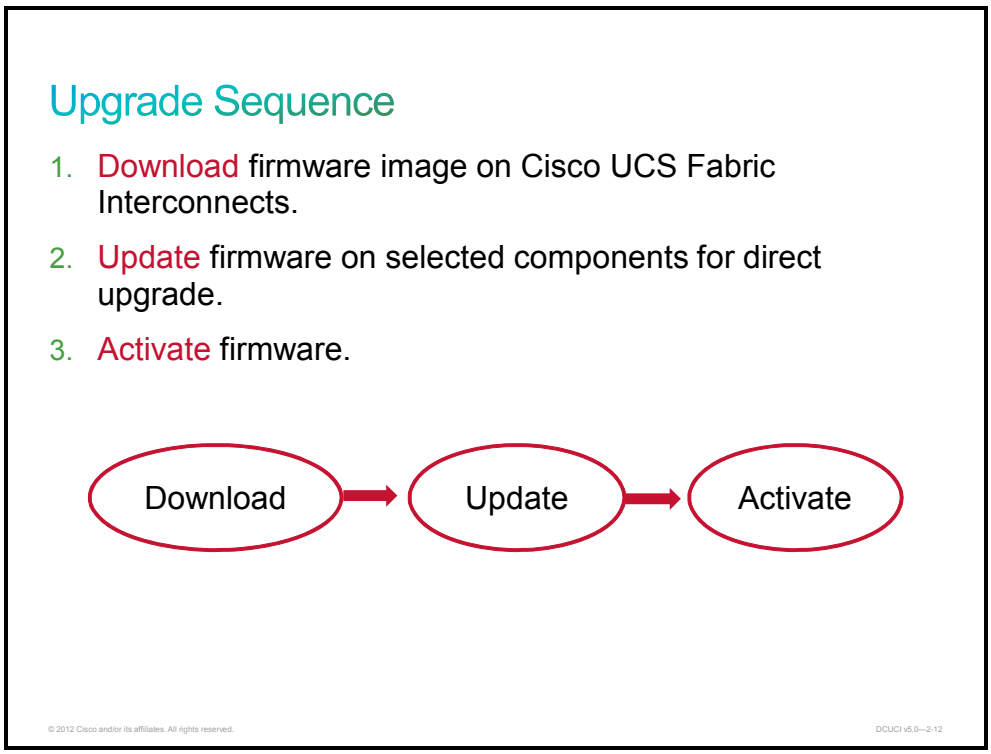
© 2012 Cisco and/or its affiliates. All rights reserved.

The download will start immediately. The progress can be observed in the Download Tasks tab. When the download is successful, the fabric interconnect expands the individual files from the archive and installs them in the correct flash file system partition. The files are then viewable as individual packages or images. The new firmware can be used to update components immediately.

https://t.me/learningnets

Update Cisco UCS Firmware

This topic describes how to update and activate Cisco UCS firmware.



There are three steps in the upgrade sequence:

Step 1 **Download:** With this operation, you copy the files that were downloaded from Cisco.com on the Cisco UCS fabric interconnects.

Step 2 **Update:** The update operation copies and installs the firmware in the backup memory partition on the components that can be directly upgraded.

Step 3 **Activate:** This operation marks which firmware image will be used during the component boot to be loaded.

https://t.me/learningnets

Suggested General Upgrade Practices

- Upgrade all components to the latest level available at initial installation, before deploying operating systems.
- Carefully study the release notes of the new firmware to determine whether version dependencies or open caveats could lead to issues with current production systems.
- Consult with operating system and application vendors for adapter firmware dependencies.
- Test new code, if available, on a Cisco UCS development system for testing.
- Upgrade from outside-in: Upgrade adapter, then Cisco Integrated Management Controller, then IOM, then Cisco UCS Manager, and then the fabric interconnects.
- Do not select all and attempt to activate all components at once.

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

When Cisco UCS is in production use, gaining authorization to update firmware components requires an approval process and a change control window. Therefore, you should update all components of Cisco UCS to the latest version before installing operating system applications and user access.

A step that many administrators neglect is the careful review of the release notes of any new firmware that is to be applied to Cisco UCS. The release notes provide an alert to any version dependencies or open caveats that might relate specifically to the operating system versions or application versions in your production network. Failure to abide by the recommendations in the release notes can result in system instability and loss of availability.

It might seem counterintuitive, but an outside-in approach is recommended when updating the firmware of an entire Cisco UCS. This approach means updating the server adapters first, followed by the Cisco Integrated Management Controller, I/O modules (IOMs), Cisco UCS Manager, and fabric interconnects.

https://t.me/learningnets

Upgrade Overview

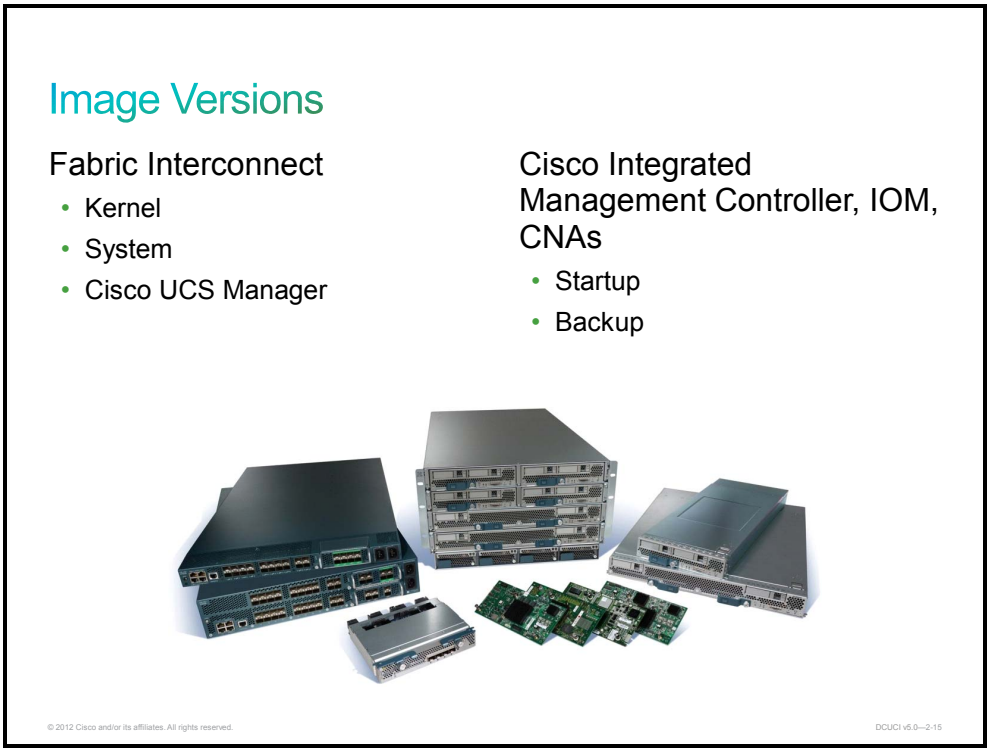
- Components to upgrade
  - Cisco UCS 6xxx Fabric Interconnect
  - IOM
  - Cisco Integrated Management Controller
  - CNAs
  - Option ROMs
  - BIOS
  - LSI (RAID firmware)
- Methods of upgrade
  - CLI
  - GUI
- Downloading images
  - TFTP, FTP, SFTP, and SCP
  - Bundles

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

The following Cisco UCS components are firmware upgradable:

- Cisco UCS 6100 and 6200 Series Fabric Interconnects
- Cisco UCS Manager
- Cisco 2104/2204/2208 IOMs
- Cisco UCS Converged Network Adapters (CNAs)
- Cisco Integrated Management Controller instances
- Cisco Host Bus Adapters (HBAs)
- Cisco HBA option ROMs
- Cisco UCS BIOS

https://t.me/learningnets



The fabric interconnects require three distinct firmware updates:

- **Cisco Nexus Operating System (NX-OS) Kernel:** This update contains the boot loader and low-level operating system and loads Cisco NX-OS.
- **Cisco NX-OS System:** This image is the binary image of Cisco NX-OS. This image loads Cisco UCS Manager.
- **Cisco UCS Manager:** Cisco UCS Manager runs as a process on dedicated management processors in the fabric interconnects.

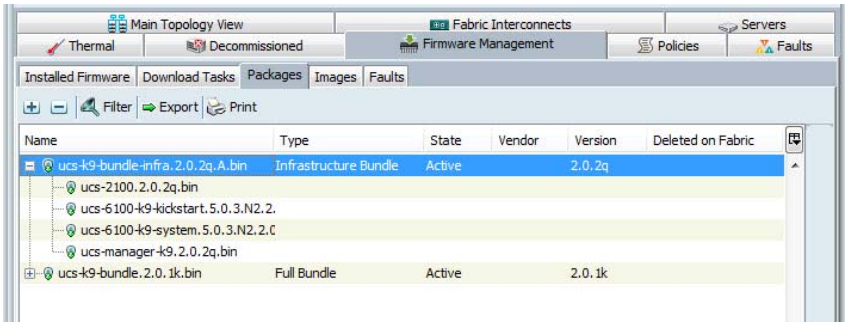
IOMs, Cisco Integrated Management Controller, and CNAs store firmware in two repositories:

- **Startup:** This image is the boot image.
- **Backup:** This image is loaded if the startup image is unavailable or unloadable.

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

Displaying Installable Images

- Installable images and packages can be viewed in the Firmware Management tab of the Equipment content pane.



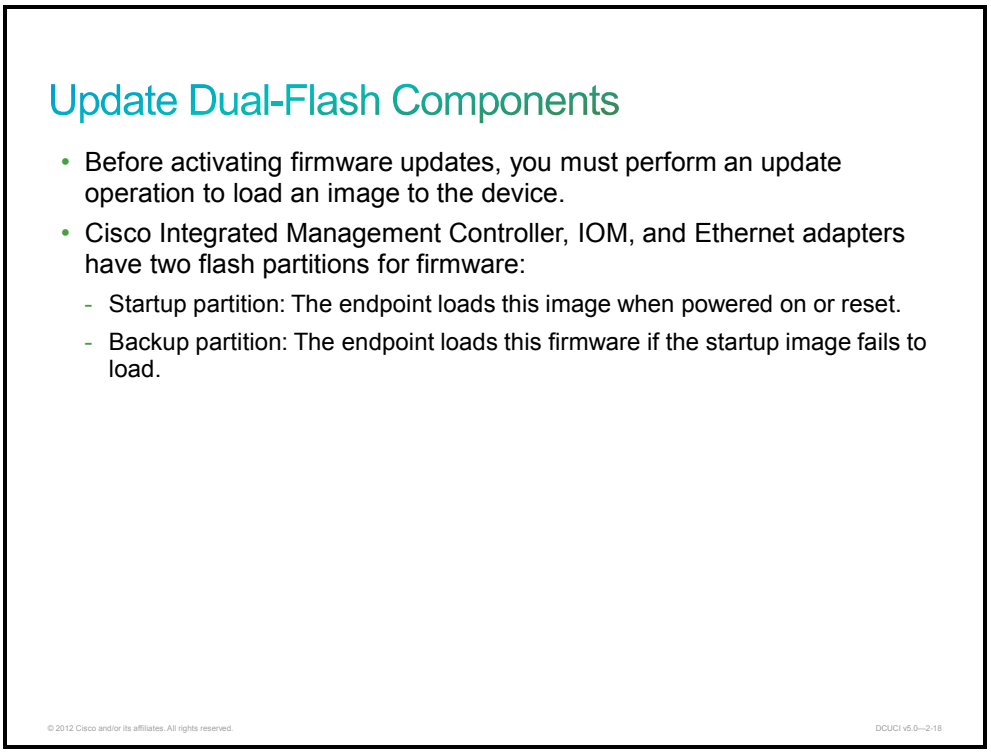
© 2012 Cisco and/or its affiliates. All rights reserved.

The Packages tab lists all of the available bundles. You can expand the bundles to see the firmware images.

https://t.me/learningnets

Upgrading the Mezzanine Adapter, Cisco Integrated Management Controller, and IOM Firmware

This topic describes the direct upgrade for Cisco Integrated Management Controller, mezzanine adapters, and IOMs.



As was discussed earlier in the lesson, IOM, Cisco Integrated Management Controller, and mezzanine components have two flash partitions for firmware images. Before the startup image can be activated on a new version, the backup image must be updated with the desired version.

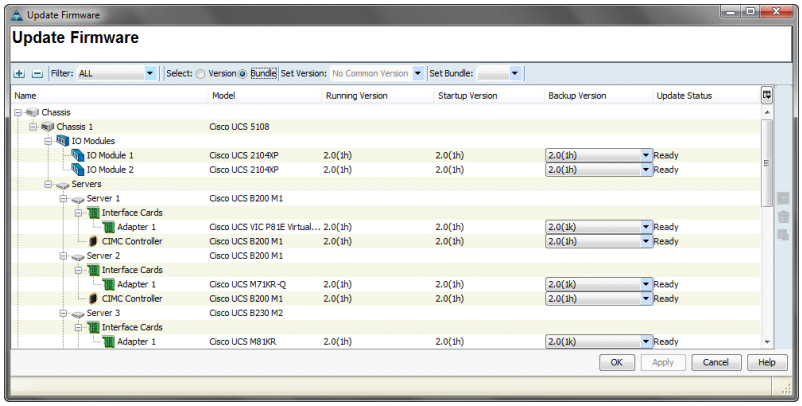
You can update a single component, a single category of components, or all components on a common version of firmware. It is strongly recommended that you do not activate all components in all chassis at one time.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Update Components

- The update process affects only the backup firmware partition and is safe to perform during production (subject to change control policy).
- Cisco Integrated Management Controller, IOM, and adapter must be updated before they can be activated on the new version.

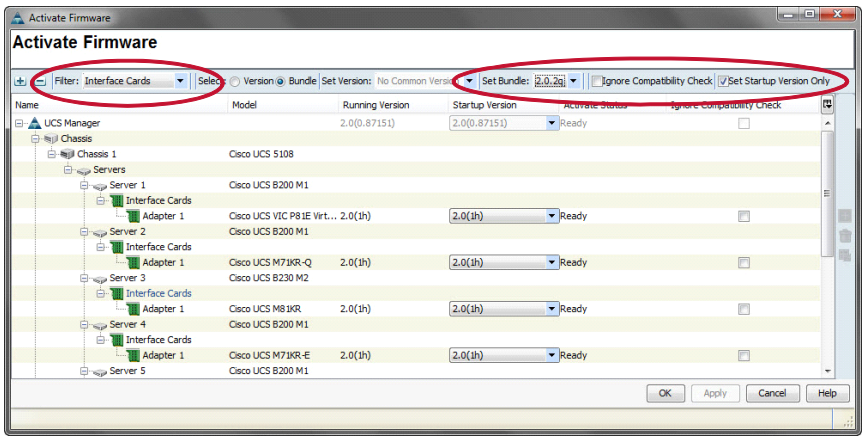


© 2012 Cisco and/or its affiliates. All rights reserved.

The update process operates strictly on the backup partition of flash for a given component. You can safely update the backup partition of any component during regular business hours. Performing this step now will save much time during the maintenance window for activating the new firmware.

Activate All Adapters

- Activating firmware on the interface card causes a server reboot.
- Plan for a maintenance window.



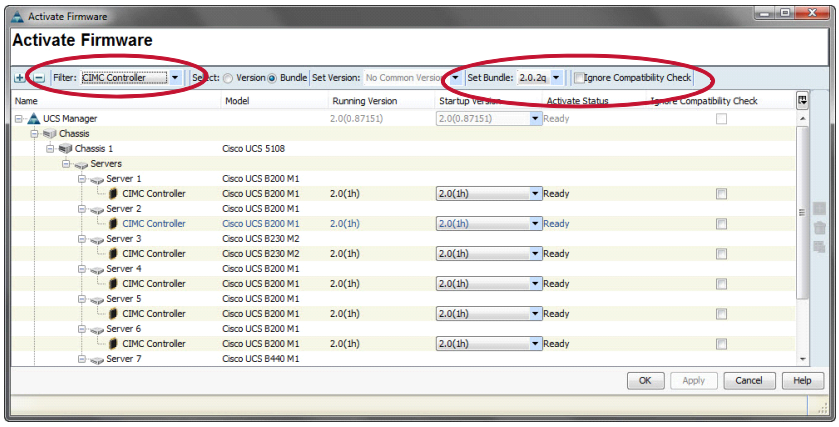
© 2012 Cisco and/or its affiliates. All rights reserved.

Updating the backup flash on the adapter is a safe operation at any time, but activating new firmware on the adapter causes the associated server to reboot. This activation should be performed only during a change control window, or if all virtual machines (VMs) have been moved safely off a hypervisor that runs on the host.

https://t.me/learningnets

Activate All Cisco Integrated Management Controller Instances

- Activating Cisco Integrated Management Controller does not affect the server.
- During Cisco Integrated Management Controller firmware activation, KVM, SoL, and IPMI will be lost.



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

The safest firmware upgrade that an administrator can perform on the Cisco UCS is that of updating and activating Cisco Integrated Management Controller instances. As discussed earlier, updating the backup partition of Cisco Integrated Management Controller has no impact on communications. Activating the new startup version to the eight servers that are shown in the example does not affect any in-band Ethernet or Fibre Channel communications to the blade servers.

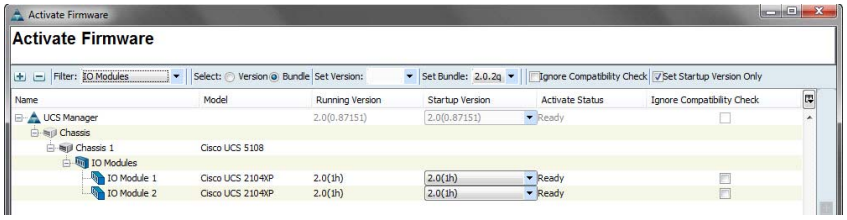
Note	Three out-of-band (OOB) management services are unavailable during activation: keyboard, video, mouse (KVM) over IP, Serial over LAN (SoL), and Intelligent Platform Management Interface (IPMI).

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Activate Both IOMs

- Set the filter to select the IOMs and select a common version or bundle from the drop-down menu.
- Set Startup Version Only updates the startup flash partition but does not take effect until the IOM is reset.
- Check the **Ignore Compatibility Check** check box based on release notes or Cisco TAC recommendation.



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

Navigate to **Equipment > Firmware Management > Installed Firmware** and click **Activate Firmware**. In the Activate Firmware pop-up window, select **IO Modules** from the Filter drop-down menu. Select the common version or bundle that the I/O modules should share from the Set Version drop-down menu. Click **Apply** to start activation. The activation process does not actually copy an image from the backup to the startup partition. Activation simply moves the startup pointer and promotes the backup partition to start up. When the activation is complete, the old startup version becomes the backup version.

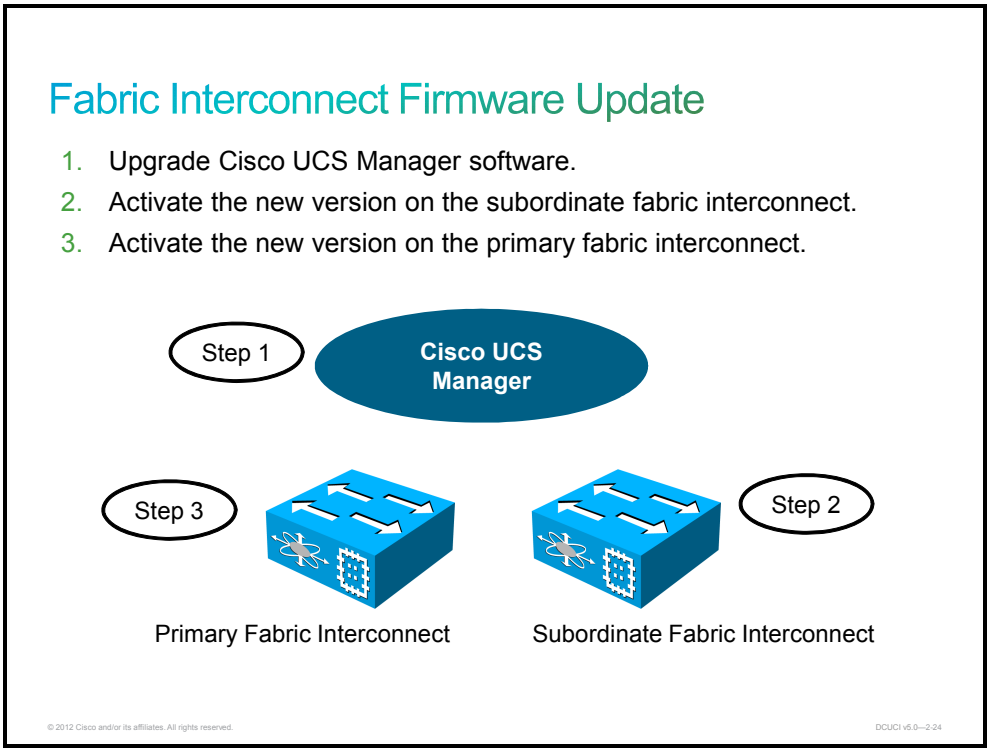
The best practice is to select the Set Startup Version Only check box when activating new firmware on IOMs. This setting causes the IOM to wait until its associated fabric interconnect reboot.

Note	If an IOM is upgraded to a version that is incompatible with its associated fabric interconnect, then the fabric interconnect automatically reactivates the IOM with a compatible version. Therefore, the Set Startup Version Only check box is important.

https://t.me/learningnets

Software Updates on the Fabric Interconnect

This topic describes the upgrade of fabric interconnects.



Because the fabric interconnects operate in a cluster, it is possible to update fabric interconnects during production operations. However, the administrator is strongly encouraged to schedule a change control window to perform this maintenance. This process can be time-consuming to complete and can result in unplanned downtime.

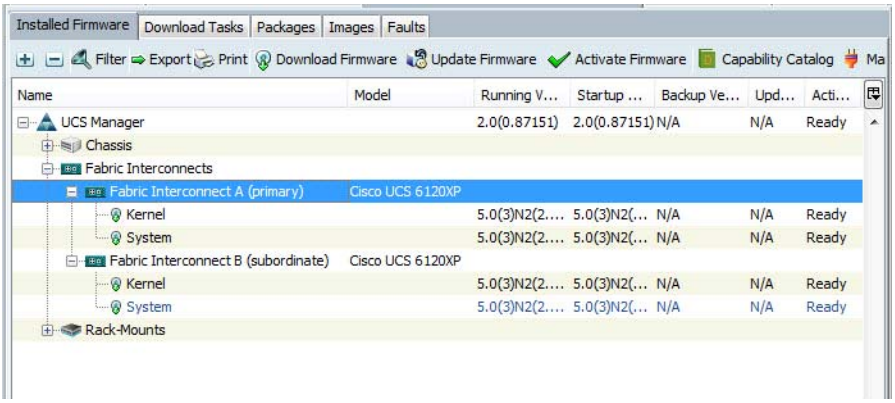
To avoid the worst-case scenario of both fabric interconnects being in a nonuseable state, update them one at a time. Begin by updating the subordinate fabric interconnect. When the new firmware begins activating on the subordinate fabric interconnect, the subordinate fabric interconnect will reboot. A connection to the fabric interconnect serial interfaces or Remote Terminal (RT) server interface that connects to them is useful. This connection will allow you to watch for errors during the update process.

When the subordinate fabric interconnect is back online, updating and activating the primary fabric interconnect should be safe. Depending on the version of firmware, plan on 45 minutes to 1 hour per fabric interconnect. For estimating a change control window, 4 hours should be adequate to allow for either success or rollback.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Display Running Fabric Interconnect Firmware Version



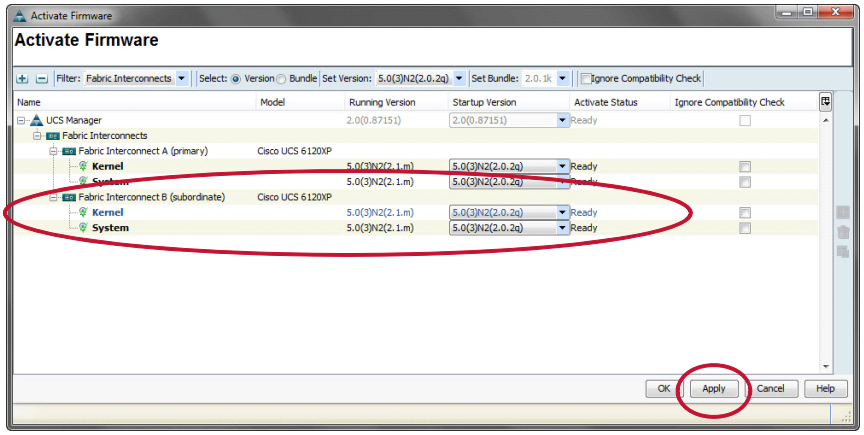
© 2012 Cisco and/or its affiliates. All rights reserved.

Navigate to **Equipment** > **Firmware Management** > **Installed Firmware** to view the running version of firmware on both fabric interconnects.

https://t.me/learningnets

Upgrade the Fabric Interconnect Software

- First, activate the subordinate fabric interconnect.
- The kernel and system image versions must be the same.



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

Navigate to **Equipment** > **Firmware Management** > **Installed Firmware** and click **Activate Firmware**. A new dialog box opens. Select the desired firmware version from the drop-down lists. After you have chosen the correct version of kernel and system images for each fabric interconnect, click **Apply** to begin the upgrade.

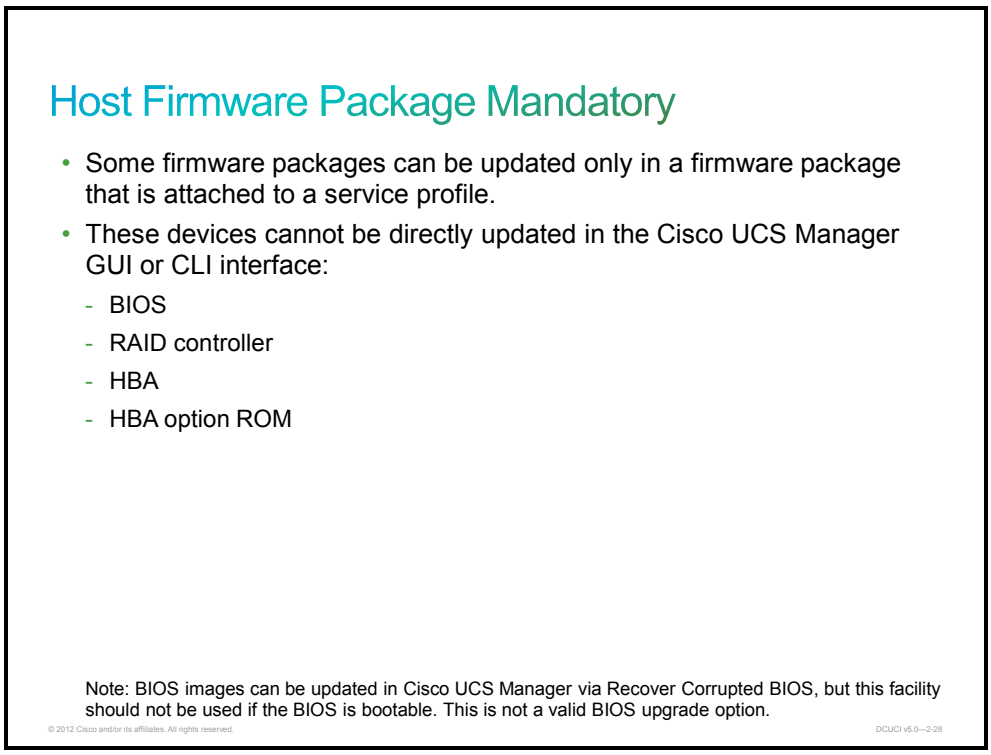
Note	The kernel and system must use the same major version.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Requirements for Firmware Updates via Host Firmware Packages

This topic describes the host firmware package.

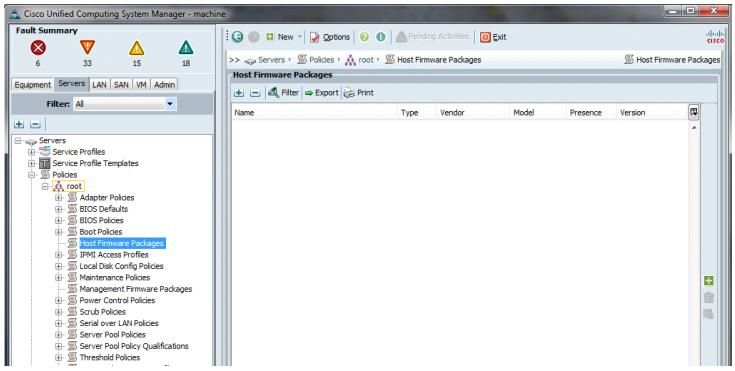


A few upgradable components cannot be updated through direct firmware updates. The server BIOS, HBA, HBA option ROM, and Redundant Array of Independent Disks (RAID) controller firmware must be updated within an operating system that runs on the blade server, or via a host firmware package that is associated with the service profile.

https://t.me/learningnets

Host Firmware Package Creation

- Host and management firmware packages are created, modified, and deleted on the Servers tab under Policies.



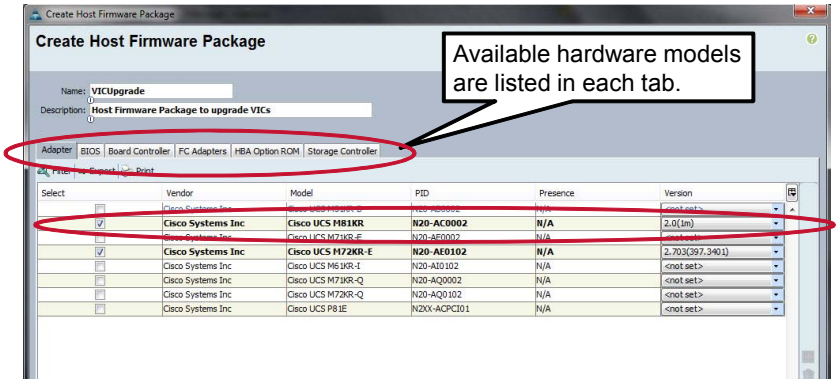
© 2012 Cisco and/or its affiliates. All rights reserved.

Under the Policy category of the navigation pane Server tab, choose **Host Firmware Packages**. The host firmware package creation wizard is started by right-clicking the policy or by clicking the small plus sign (+) in the content pane.

https://t.me/learningnets

Host Firmware Package Tabs

- Tabs for the different components
- Select model and set version



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

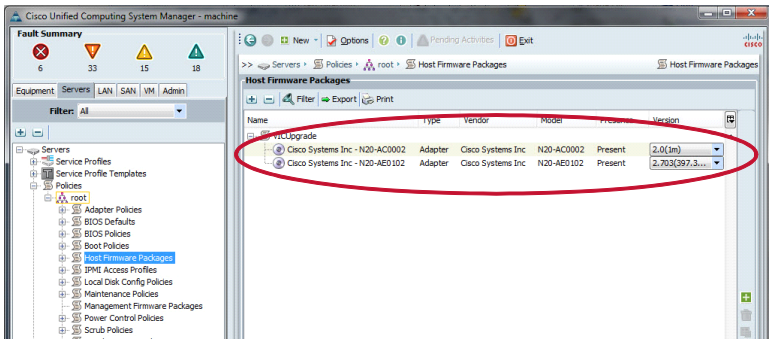
A unique name for the host firmware package must be defined. Optionally, a description can be provided.

In the host firmware package creation window, the hardware components are divided in separate tabs. For the components that must be upgraded, you have to select the corresponding tab, select the model from the list, and set the version.

When done, click **OK**.

Host Firmware Package Ready to Apply

- The VIC Upgrade host firmware package can now be applied to a service policy.



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

The host firmware package is ready to be used in a service profile.

https://t.me/learningnets

Differences in Firmware Processes

This topic describes how different components are upgraded.

Component Firmware Update Differences

Component	Update Requirements
Fabric Interconnect	Activate the subordinate cluster member and allow it to resume normal operation. Then activate the primary fabric interconnect.
Cisco USC Manager	No backup image. Activate on active management node. Automatically synchronized to subordinate node.
Cisco Integrated Management Controller, IOM, Ethernet	These components have two flash partitions for firmware: startup and backup. You can update and activate the backup partition without disrupting the operation of the component.
BIOS, HBA, HBA Option ROM, RAID Controller	Must be updated with the service profile bound to a host firmware update policy.

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

The table summarizes the primary differences between update types. Cisco UCS Manager in the fabric interconnects automatically restarts at activation. IOMs, adapters, and Cisco Integrated Management Controller instances have two flash partitions for firmware updates. Updating and activating the backup partition during production operations is safe. Some components can be updated only from a firmware package that is associated with the service profile or from within the operating system that runs on the blade server.

© 2012 Cisco Systems, Inc.

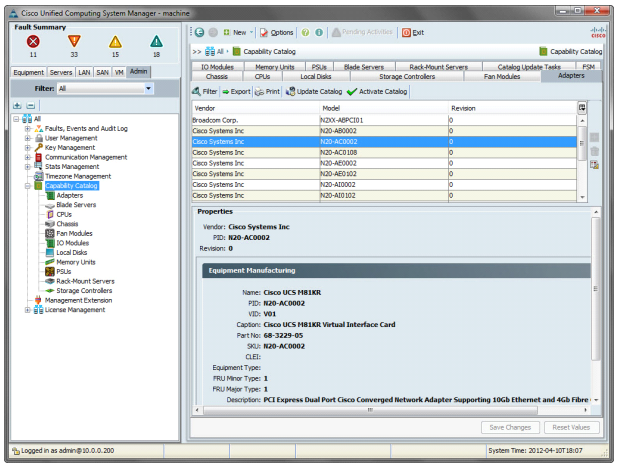
https://t.me/learningnets

Update and Activate the Hardware Capability Catalog

This topic describes the hardware capability catalog.

Cisco UCS Hardware Capability Catalog

- Cisco UCS Manager uses the capability catalog to update the display and support for new hardware.
- The capability catalog is divided by hardware components.



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

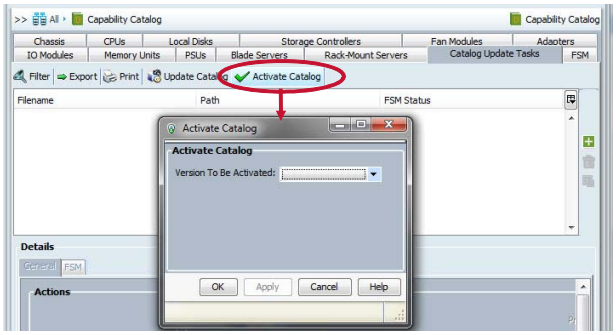
Cisco UCS Manager uses the hardware capability catalog to update the display and support for new hardware, such as new servers and new DIMMs.

The catalog is divided into tabs by different hardware components, such as IOMs, chassis, servers, and so on. You can look at the different components, the models, characteristics, providers, and physical form factor.

https://t.me/learningnets

Updates and Activating the Capability Catalog

- The capability catalog is updated with each Cisco UCS Manager update.
- After the Cisco UCS Manager update, the capability catalog must be activated.



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

The hardware capability catalog is updated when Cisco UCS Manager is upgraded. After an upgrade, you have to activate the new version of the capability catalog.

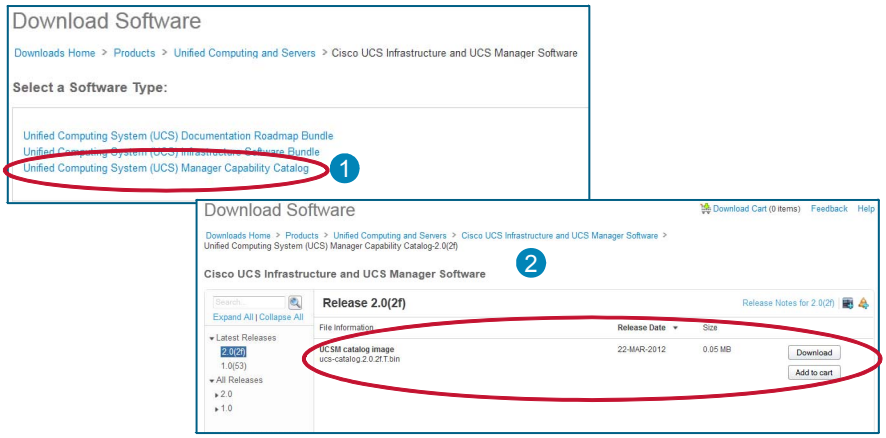
The activation is performed from the Catalog Update Tasks tab. Select **Activate Catalog**, and in the new window, select the version that must be activated.

When an upgrade of Cisco UCS Manager is not performed, or when no individual update is applied, the drop-down menu will contain no options.

https://t.me/learningnets

Download Individual Update

- Individual updates are available.
- Download from Cisco.com.



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

You can download individual updates for the capability catalog.

Navigate to **Cisco.com > Support > Downloads**. Log in with your Cisco.com account.

Select **Product > Unified Computing and Servers > Cisco UCS Infrastructure and UCS Manager Software**.

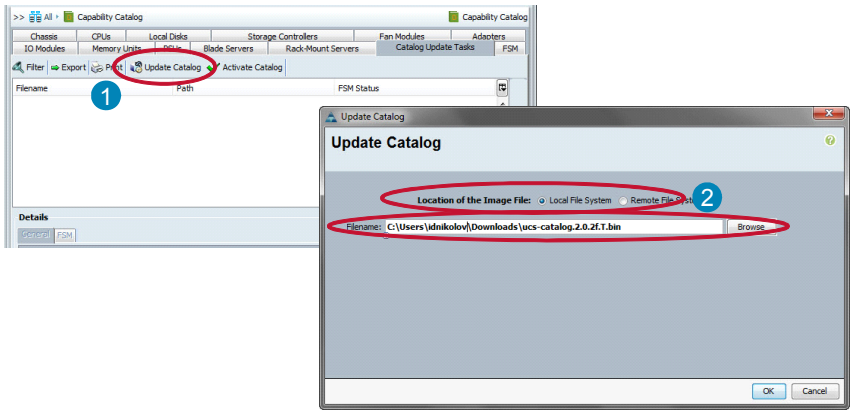
At the next screen, select **Unified Computing System (UCS) Manager Capability Catalog**.

At the new screen, select the version and download the image file.

https://t.me/learningnets

Update Capability Catalog

- From the Catalog Update Tasks tab, select **Update Catalog**.
- Browse for the update image file and select it.
- After a successful update, activate the image.



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

Since the image is available locally either on your PC or on a server, the update must be performed. The result of the update operation is that the capability catalog image is copied to the active fabric interconnect and installed.

To update the capability catalog image, click **Update Catalog** in the Catalog Update Tasks tab.

In the new window, select how the image will be accessed by Cisco UCS Manager. You can choose from your local file system, which is based on HTTP copy, or use transport protocols such as FTP, TFTP, SCP, or SFTP. If the second option is selected, enter the required protocol information and click **OK** to start the update process.

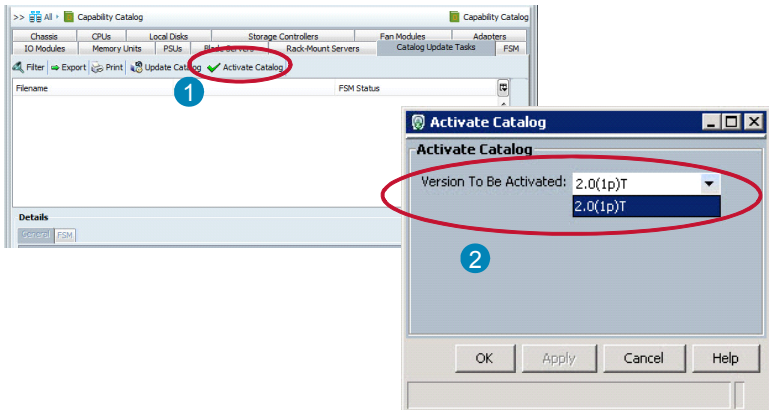
When the update has finished, you have to activate the new version of the capability catalog.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Activate Capability Catalog

- From the Catalog Update Tasks tab, select **Activate Catalog**.
- Select the image file from the drop-down menu.



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

The final task is to activate the new catalog image, which is performed by completing the following steps:

Step 1 Click the **Catalog Update Tasks** tab and select **Activate Catalog**.

Step 2 Select the image from the drop-down menu.

Step 3 Click **OK** to activate the image.

https://t.me/learningnets

Summary

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

Summary

- Cisco UCS infrastructure, B-Series, and C-Series bundles must be downloaded from Cisco.com.
- Software bundles must be copied to the Cisco UCS Manager locally, after which updates and activation can be performed.
- The mezzanine adapter, Cisco Integrated Management Controller, and IOM firmware can be upgraded directly. Those components use a backup and a startup partition.
- Cisco UCS Manager must be upgraded first. After that, the subordinate fabric interconnect and finally the primary fabric interconnect can be upgraded.
- Components that depend on the server operating system are upgraded through a host firmware package.
- Cisco UCS Manager and fabric interconnects follow a sequence for upgrade. The directly upgraded components use a backup and startup partition and the server components are upgraded with the use of a host firmware package.
- The hardware capability catalog is updated with each Cisco UCS Manager update. You only have to activate it. Individual updates are also available.

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

https://t.me/learningnets

Lesson 3

Implementing Backup, Import, and Restore of the Cisco UCS Manager Database

Overview

Good operational procedure includes maintaining up-to-date backups of Cisco Unified Computing System (UCS) configuration data. All configuration data in Cisco UCS is stored in XML format. XML is simply textual data that conforms to the Cisco UCS XML schema. Even large implementations can be backed up and restored relatively quickly.

There are four main backup operations and two options to restore data to the Cisco UCS Manager database.

Objectives

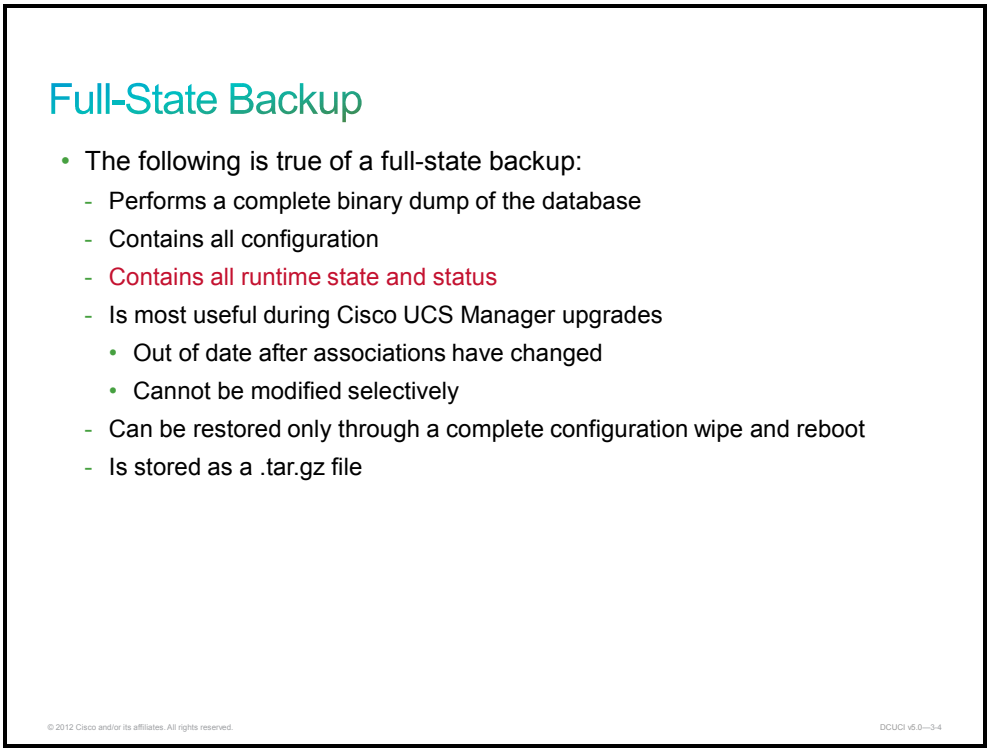
Upon completing this lesson, you will be able to implement backup and restore capabilities in Cisco UCS Manager. This ability includes being able to meet these objectives:

- Differentiate between the supported backup types and the database objects to which they map in the Cisco UCS Manager database
- Differentiate between an import operation and a disaster recovery restore operation
- Implement a backup job
- Implement backup jobs to preserve abstracted identities
- Verify that the backup is created and executed
- Implement an import job to restore the AAA user database
- Verify that the AAA user database is restored
- Configure the Cisco UCS 6100/6200 Series Fabric Interconnect for disaster recovery restore

https://t.me/learningnets

Backup Types in the Cisco UCS Manager Database

This topic describes the supported backup types in Cisco UCS.

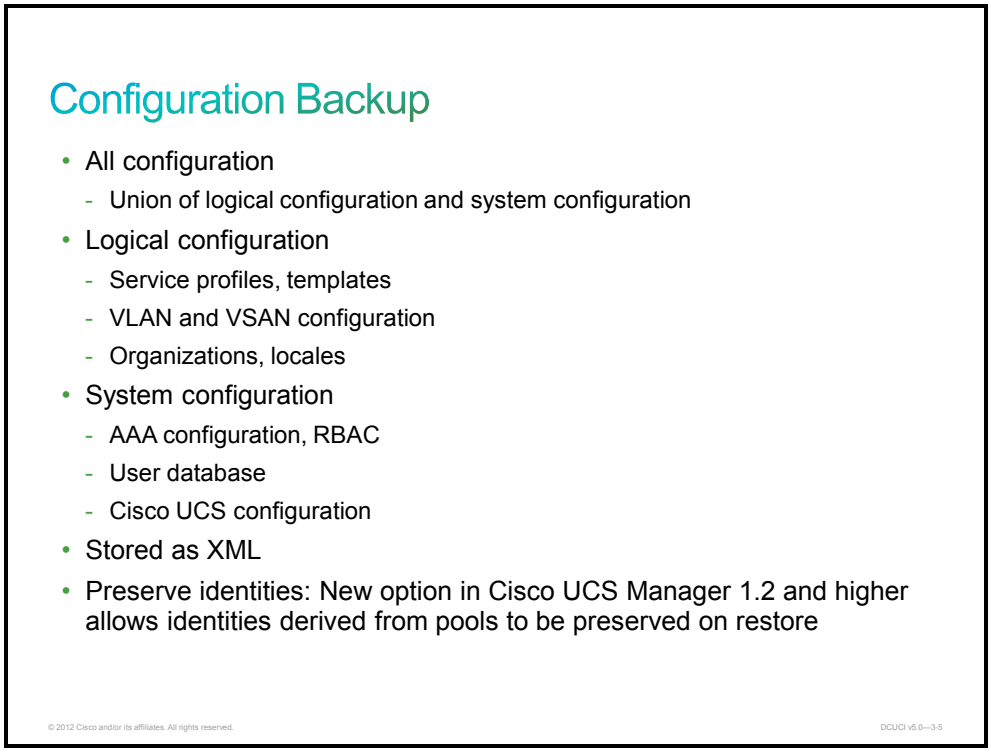


Full-state backups protect against catastrophic failure of both fabric interconnects in the cluster. This backup type includes all the run-time state information, such as the finite state machine (FSM) state of blades, the associated state of service profiles, and so on. This backup type also includes configuration information, such as users, policies, and so on.

Because the full-state backup includes run-time state, this type of backup can quickly become outdated. Any changes to blade service profile associations render this backup obsolete.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



Cisco UCS Manager supports three types of XML backups:

- **Logical configuration:** Logical configuration is all configuration that is not associated with authentication, authorization, and accounting (AAA). This configuration includes configured organizations, configured threshold policies, and configured VLANs and virtual storage area networks (VSANs) in your LAN and SAN clouds, respectively.
- **System configuration:** System configuration is all configuration that specifically pertains to the AAA role. Examples include RADIUS, Lightweight Directory Access Protocol (LDAP), TACACS, and users.
- **All configuration:** All configuration is a combination of the logical and system configurations.

Configuration backups are saved as XML representations of the configuration of the Cisco UCS Manager. These backups can be edited by using an XML editor or text editor. This ability makes configuration backups useful for creating templates that can be applied to other Cisco UCS implementations, or for adjusting the backup files if changes are made to the environment since the backup was last taken. No run-time state data (service profile associations and so on) is stored in these backups.

https://t.me/learningnets

Use of Configuration Backups

- XML configuration backups can be edited easily.
  - Useful for duplicating configuration in other implementations.
  - Can be modified before import in disaster recovery scenarios.
  - Can be prepopulated for use in consulting engagements.

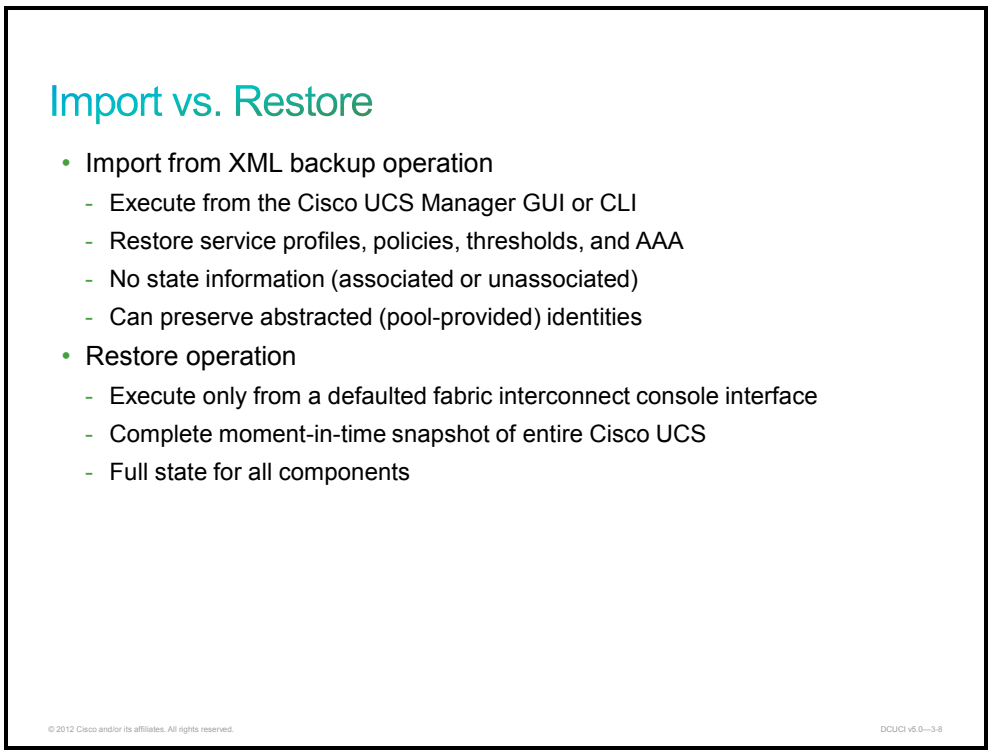
© 2012 Cisco and/or its affiliates. All rights reserved.

XML configuration-level backups can be useful for more than simple recovery of a failed system. XML is easily edited by various editors and can be easily modified or customized before import.

https://t.me/learningnets

Import Operation vs. a Disaster Recovery Restore Operation

This topic describes the import and restore operations.

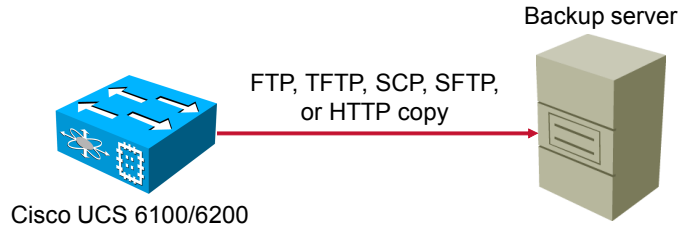


The primary difference between an import operation and a disaster recovery restore operation is the scope of the backup. Configuration backups lack the state information that is required to re-establish server profile-to-blade server relationships.

https://t.me/learningnets

Backup and Import Jobs

- Managed as objects within the Cisco UCS database
- Transfer to remote file system via FTP, TFTP, SCP, SFTP, or HTTP copy
- Contains information about backup parameters
  - Backup type
  - Transfer protocol
  - Destination host
  - Destination path
  - Authentication



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

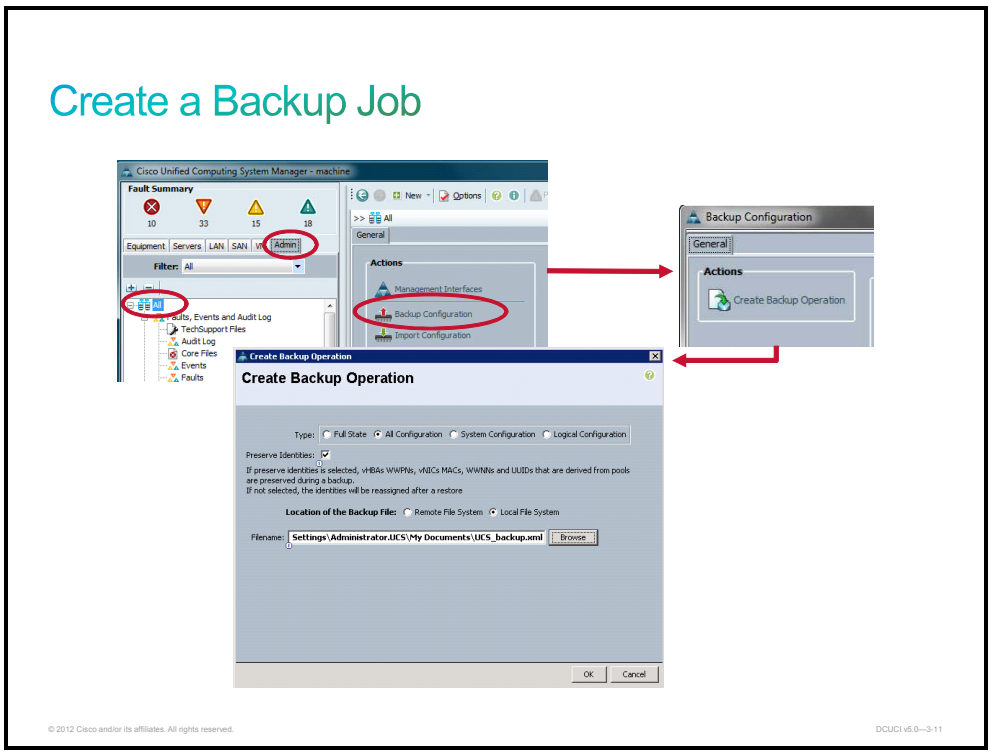
Cisco UCS processes backup and import operations as managed objects within the Cisco UCS Manager database. No backup data is stored within the database. Only the information that relates to the storage and transfer of the backup is stored in the database.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Implement a Backup Job

This topic describes how to implement a backup job.



Currently, only one backup configuration can be created per backup server. Backups are identified in Cisco UCS Manager by using the hostname or IP address of the backup server in the configuration.

Click the **Admin** tab in the navigation pane, and choose the **All** object. Click the **Backup** link in the actions pane, and then click **Create Backup Operation** in the window.

In the example, you can see a backup job that is provisioned to use HTTP-based copy. In this configuration, the backup job will be immediately executed. If you use a remote file system that is based on FTP, Secure Copy Protocol (SCP), TFTP, or Secure FTP (SFTP), you will have to manually start the backup job.

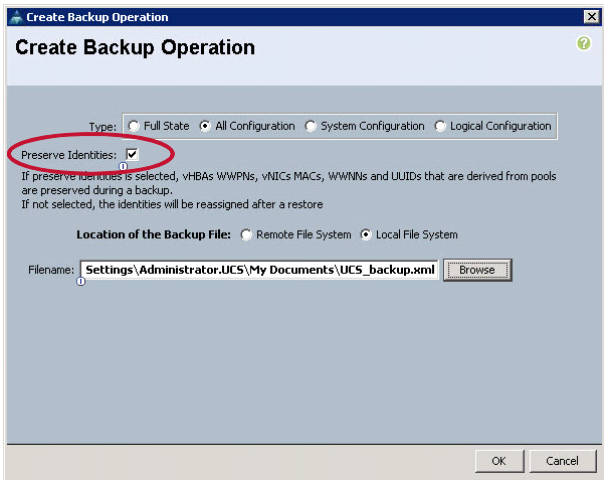
https://t.me/learningnets

Implement Backup Jobs to Preserve Abstracted Identities

This topic describes the preserve identity feature.

Preserve Abstracted Identities

- The Preserve Identities option maintains MAC addresses, UUIDs, and WWNNs.



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

Beginning with Cisco UCS Manager version 1.2, a backup job to preserve universally unique identifiers (UUIDs), MAC addresses, world-wide network nodes (WWNN), and world-wide port names (WWPNs) is derived from pools in service profiles. Previously, any address that was drawn from an identity pool was discarded when the service profile was imported.

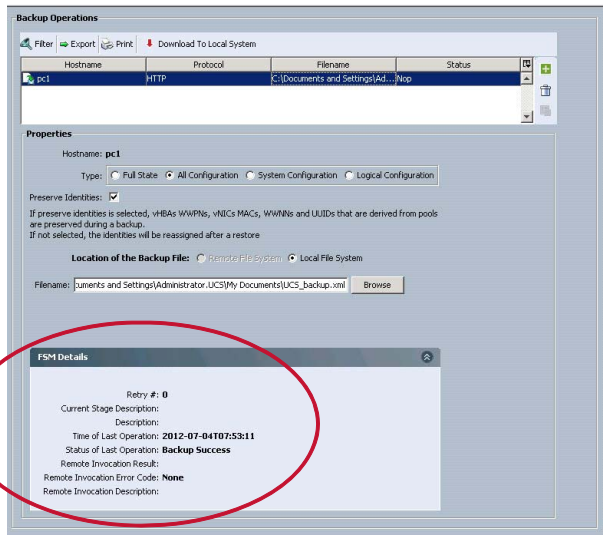
https://t.me/learningnets

Verify the Backup

This topic describes how to verify the backup job.

Verify Backup Job in Cisco UCS Manager

- Return code from the backup job is displayed in the FSM Details window.



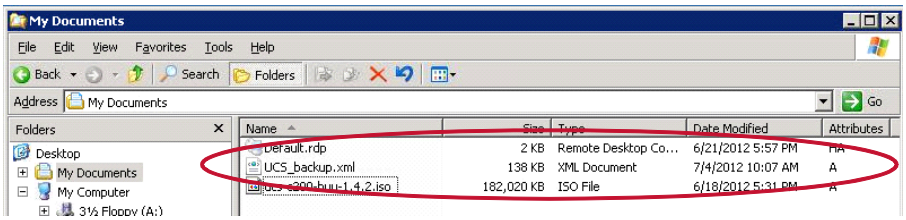
© 2012 Cisco and/or its affiliates. All rights reserved.

After you enable the backup job, click the double down-arrow icon in the upper-right corner of FSM Details to open the FSM Details window. The return code should read “Status of Last Operation.” If any other return code appears, edit the backup job. Be certain that the IP address of the remote file system and authentication credentials are correct.

https://t.me/learningnets

Verify Backup Job on Remote FTP Server

- Verify that the file was received correctly on the remote server.



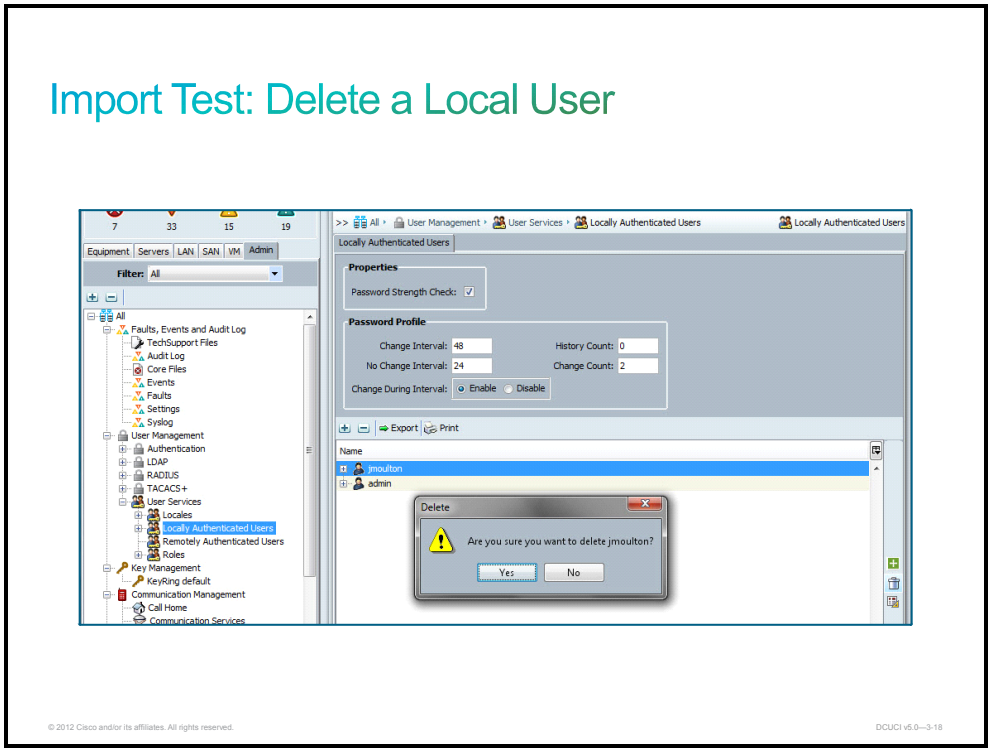
© 2012 Cisco and/or its affiliates. All rights reserved.

You can also verify that the backup operation was successful by monitoring the remote file system. Configuration backups are stored in XML format and can be opened in any text editor.

https://t.me/learningnets

Restore the AAA User Database with an Import Job

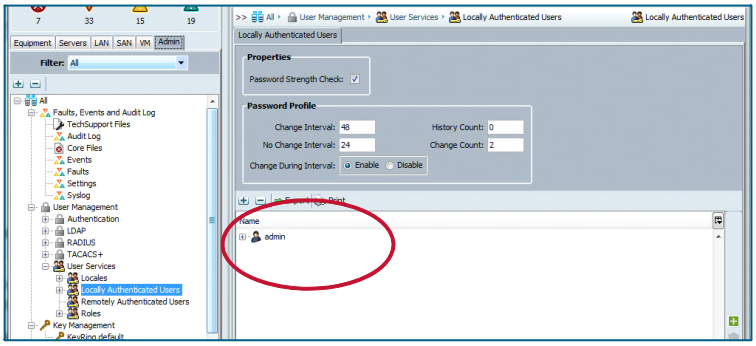
This topic describes the use of the merge action with the import job.



In the backup job that was created previously, the AAA local user database was saved. To prove that it was saved, delete a local user.

https://t.me/learningnets

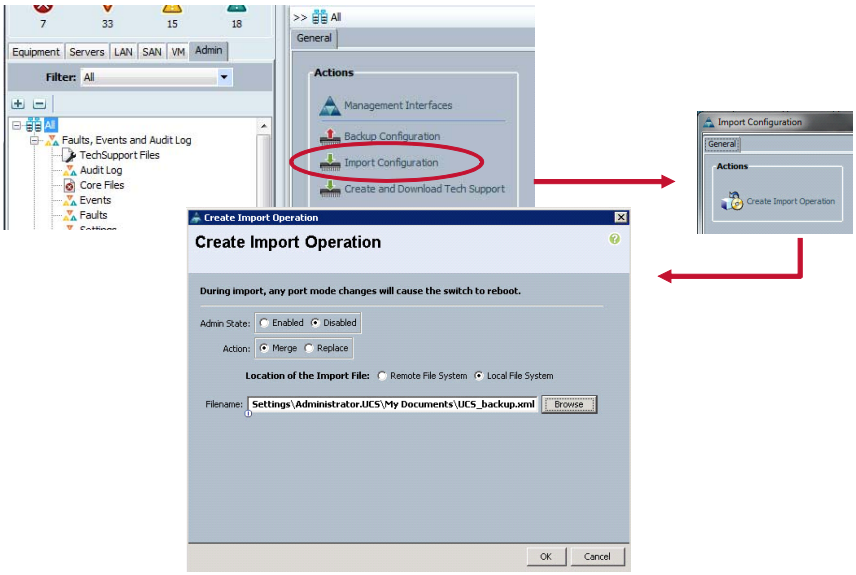
Import Test: Local User Deleted



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

The user jmoulton has been deleted successfully.

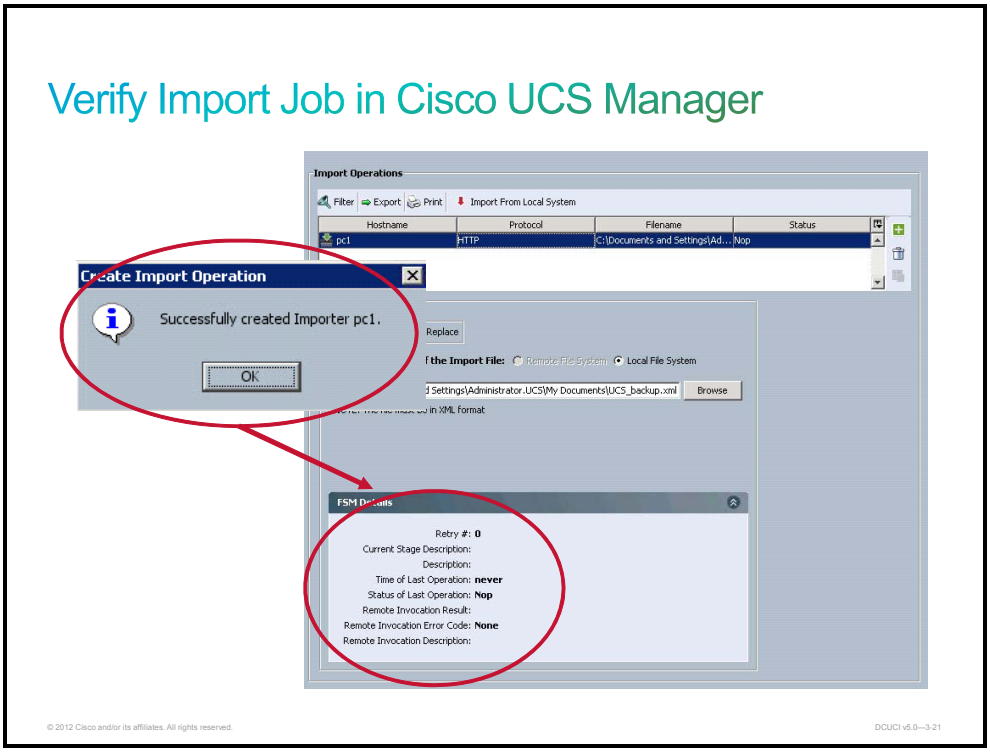
Create Import Job to Restore AAA Database



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

Click the **Admin** tab in the navigation pane and choose the **All** object. Click the **Import Configuration** link in the action pane, and then click **Create Import Operation** in the window. Enter the IP address or name of the remote file system, the name of the backup file, and the authentication credentials to import the file. The figure shows that Local File System is chosen, which means that the import job will be executed immediately.

https://t.me/learningnets



When the Local File System option is chosen, the import job will be executed immediately. A new message window will open that provides information on the status and indicates success or failure. In the FSM Details area, you will see any messages for errors that occurred during the import job.

If you use the Remote File System option, after you enable the import job, click the double down-arrow icon in the upper-right corner of FSM Details to open the FSM Details window. The return code should read “Status of Last Operation.” If any other return code appears, edit the backup job. Be certain that the IP address of the remote file system and authentication credentials are correct.

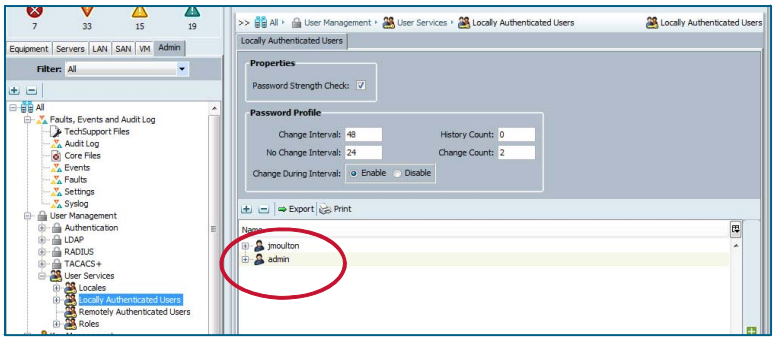
https://t.me/learningnets

Verify AAA User Database Restoration

This topic shows the verification of the result from the import job.

Confirm that AAA Database Was Restored

- After the successful merge, the user is available again.



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

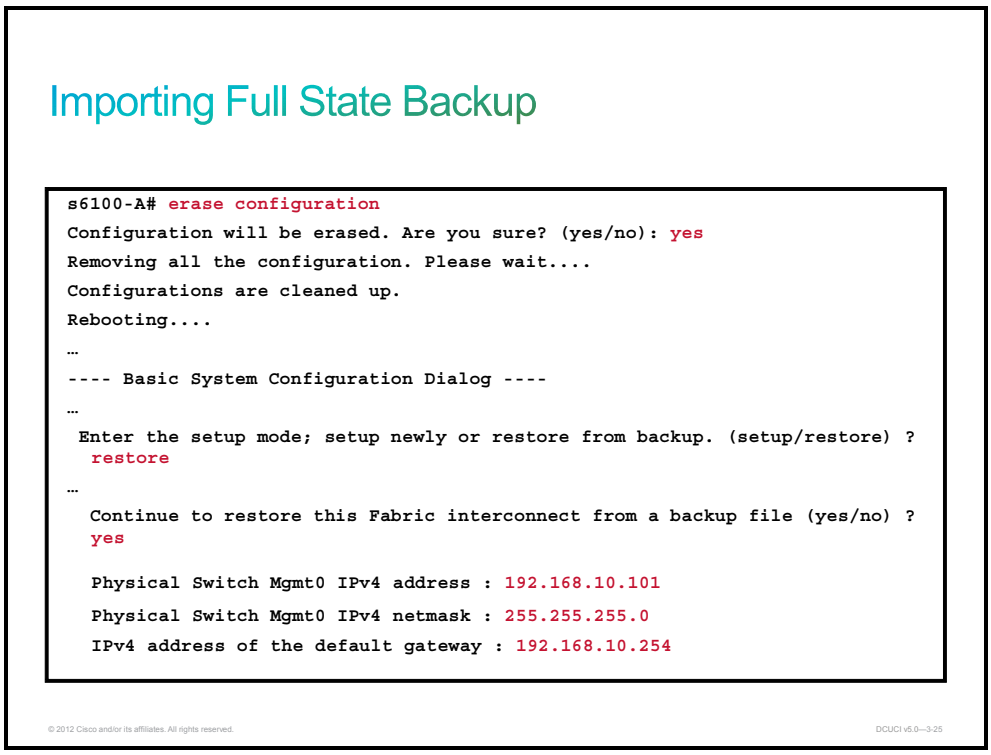
Click the **Admin** tab in the navigation window and select the **User Management** filter from the drop-down list. Expand **User Services** and choose **Locally Authenticated Users**. User jmoulton was restored in the import operation.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Disaster Recovery Restore on the Cisco UCS 6100/6200 Series Fabric Interconnect

This topic describes how to start the restore operation.



A fabric interconnect that contains any configuration data must be initialized to factory defaults before a disaster recovery operation begins. This process can be performed only from a connection to the serial console or to a terminal server that is connected to the serial console.

Connect to the local management shell and issue the **erase configuration** command. The fabric interconnect must be rebooted. This process is similar to issuing the **write erase** and **reload** commands in Cisco IOS Software.

The setup wizard queries the user if this operation is an initial setup or restore. Because a restore operation was indicated, the fabric interconnect needs an IP address to make a connection to the remote file system.

https://t.me/learningnets

Importing Full State Backup (Cont.)

- After retrieving and applying the backup, the system is ready for use.

```
 Enter the protocol to get backup file (scp/ftp/tftp/sftp) ?  ftp
  Enter the IP address of backup server: 10.100.100.30
  Enter fully qualified backup file name: /backups/ucs-fullbackup.tgz
  Enter user ID: adminuser
  Enter password: *******
    Retrieved backup configuration file.
  Configuration file - Ok


Cisco UCS 6100 Series Fabric Interconnect
s6100-A login:
```

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

Enter the transfer protocol, IP address of the remote file system, the full-state backup file, and authentication credentials. When the file transfer and restore operation is complete, a login prompt appears.

https://t.me/learningnets

Summary

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

Summary

- Full state, all configuration, system configuration, and logical configuration backups are available in Cisco UCS.
- A restore operation is used only with full state backup. Configuration backups use the import operation.
- Backup jobs are created and executed in Cisco UCS Manager.
- Selecting the Preserve Identities check box in the Backup Creation dialog box maintains identities that are assigned by a pool in the backup.
- Validate backup jobs by using FSM output and verify that the file exists on a remote file system.
- There is only one type of import job, and it can be used to restore the AAA database, service profiles, policies, and thresholds.
- To verify that the AAA database was restored, select the Admin tab in the navigation pane and select local users.
- Performing a disaster recovery restore requires access to the fabric interconnect serial console or terminal server connection.

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

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 4

Implementing Logging and Monitoring

Overview

When a Cisco Unified Computing System (UCS) implementation is underway and in production operation, detailed knowledge of the logging and monitoring facilities of Cisco UCS Manager can greatly speed configuration and troubleshooting. The Cisco Smart Call Home feature can send predictive failure messages to the Cisco Technical Assistance Center (TAC) so that replacement parts can be shipped before they actually fail.

Objectives

Upon completing this lesson, you will be able to implement syslog, Smart Call Home, and Switched Port Analyzer (SPAN). This ability includes being able to meet these objectives:

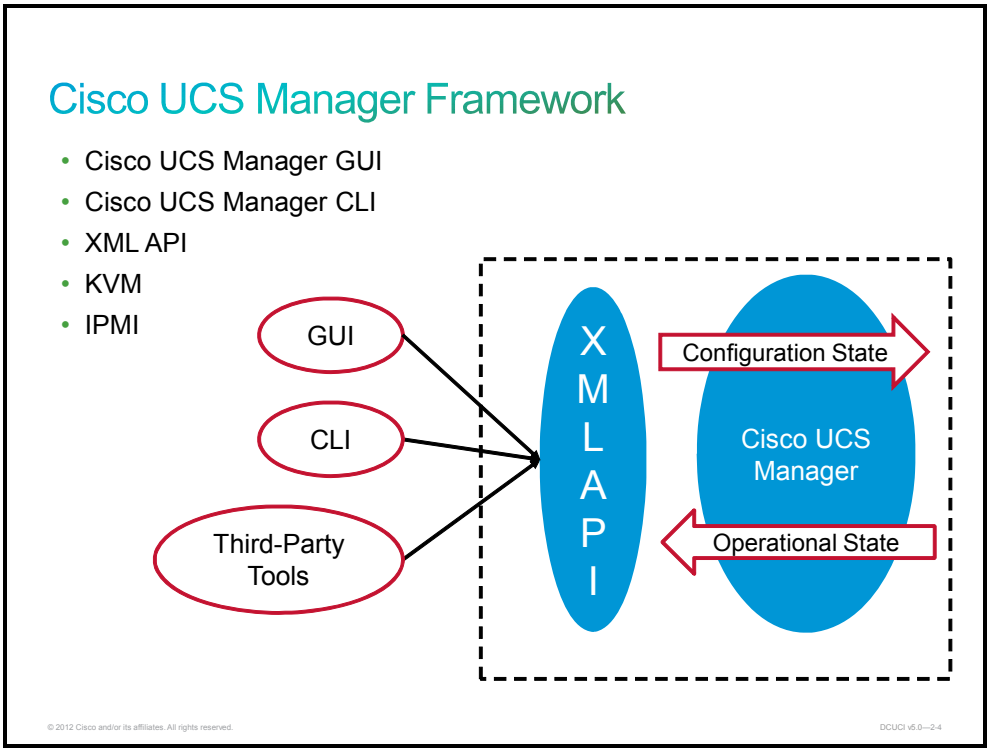
- Describe Cisco UCS Manager management interfaces
- Describe the fault management system and evaluate fault severity levels
- Use the audit log to track administrative changes to the Cisco UCS Manager database
- Describe Cisco UCS Manager operations subject to FSM validation and how to interpret FSM output
- Implement logging options including local buffer, console, and external syslog servers
- Use system event log and system event log policies
- Implement the Smart Call Home feature
- Validate the Smart Call Home feature
- Configure settings for logs, events, and faults

Configure SPAN to allow protocol analysis

https://t.me/learningnets

Cisco UCS Manager Interfaces

This topic describes Cisco UCS Manager interfaces.



Cisco UCS Manager includes the following interfaces for managing a Cisco UCS instance:

- Cisco UCS Manager GUI
- Cisco UCS Manager CLI
- XML application programming interface (API)
- Keyboard, video, mouse (KVM)
- Intelligent Platform Management Interface (IPMI)

The XML API is a powerful full-featured interface, which is in the base of the three-tiered management framework of Cisco UCS Manager. The XML API allows third-party tools to communicate and manage the Cisco UCS.

© 2012 Cisco Systems, Inc.

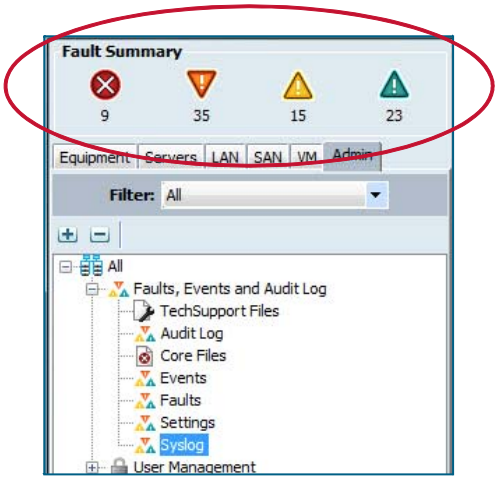
https://t.me/learningnets

Fault Management System and Fault Severity Levels

This topic describes the fault management system in Cisco UCS.

Global Fault Summary

- The Fault Summary bar is a global fault summary that is displayed above the configuration tabs in the navigation pane of Cisco UCS Manager.
- From left to right, the color images represent faults with severity levels:
  - Critical
  - Major
  - Minor
  - Warning



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

The global fault summary lists faults, according to severity, across all elements of Cisco UCS. Each fault severity level is assigned a color. Various elements in the navigation and content panes are highlighted by a rectangle. The color of the rectangle corresponds to the highest level of fault that exists for that component. If the rectangle is red, then at least one critical fault is pending against that element.

https://t.me/learningnets

Fault Severity

Severity Level	Description
Critical	A critical fault is a service-affecting condition that requires immediate corrective action. This severity might indicate that the managed object is out of service and its capability must be restored.
Major	A major fault is a service-affecting condition that requires urgent corrective action. This severity might indicate a severe degradation in the capability of the managed object and that its full capability must be restored.
Minor	A minor fault is a non-service-affecting fault condition that requires corrective action to prevent a more serious fault from occurring. This severity might indicate that the detected alarm condition is not currently degrading the capacity of the managed object.
Warning	A warning is a potential or impending service-affecting fault that currently has no significant effects in the system. Action should be taken to further diagnose, if necessary, and correct the problem to prevent it from becoming a more serious service-affecting fault.
Condition	An informational message about a condition, possibly independently insignificant.
Info	A basic notification or informational message, possibly independently insignificant.

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

In addition to the four severity levels that are listed in the global fault summary window, there are two additional severity levels: info and condition. Although these levels are not displayed in the global fault summary window, they do appear in the global fault log. To find the levels, on the Admin tab, expand **Faults, Events and Audit Log**, and then choose **Faults**.

https://t.me/learningnets

Fault States

State	Description
Active	A fault was raised and is currently active.
Cleared	A fault was raised but did not reoccur during the flapping interval. The condition that caused the fault has been resolved, and the fault has been cleared.
Flapping	A fault was raised, cleared, and then raised again within a short time interval, known as the flap interval.
Soaking	A fault was raised and then cleared within a short time interval, known as the flap interval. Because this might be a flapping condition, the fault severity remains at its original active value, but this state indicates that the condition that raised the fault has cleared. If the fault does not reoccur, the fault moves into the cleared state. Otherwise, the fault moves into the flapping state.

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

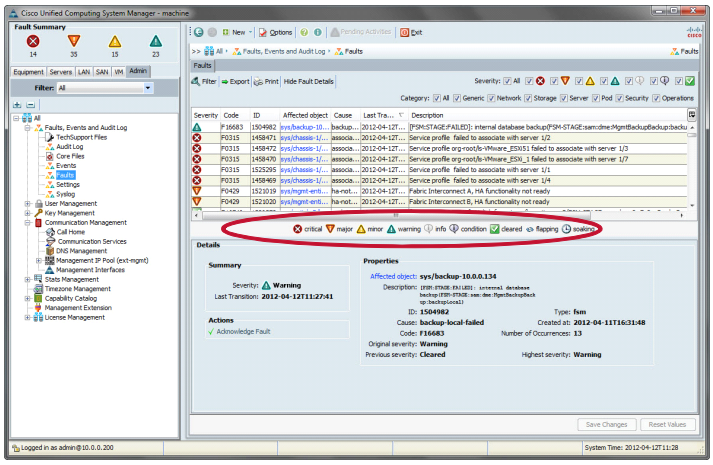
There are four possible fault states in Cisco UCS.

- **Active:** Active faults are displayed along with one of the six severity icons in the Severity column.
- **Cleared:** Cleared faults display a green check mark in the Severity column.
- **Flapping:** Faults in the flapping state display a circular arrow in the Severity column.
- **Soaking:** Faults in the soaking state display a stopwatch in the Severity column.

https://t.me/learningnets

Admin Fault Console

- All Cisco UCS faults are listed on the admin fault console.
- A key for the severity level and state icons is shown.

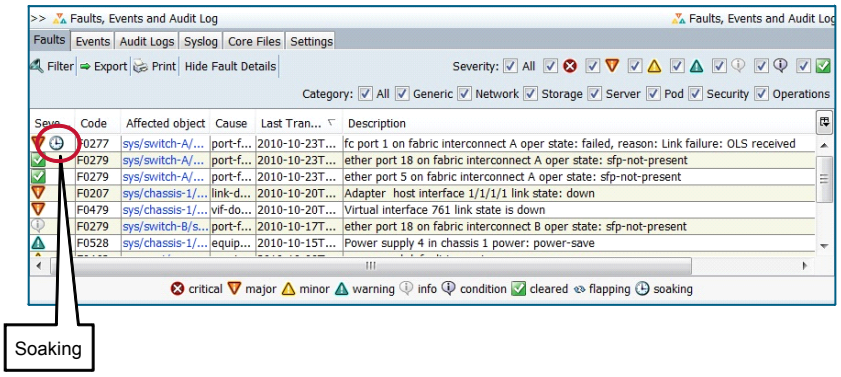


© 2012 Cisco and/or its affiliates. All rights reserved.

Navigate to **Admin > All > Faults, Events and Audit Log > Faults** to access the admin fault console. The fault console lists all of the faults in Cisco UCS.

Fault in Soaking State

- An interface has transitioned between operational and nonoperational within the 10-second flapping interval.



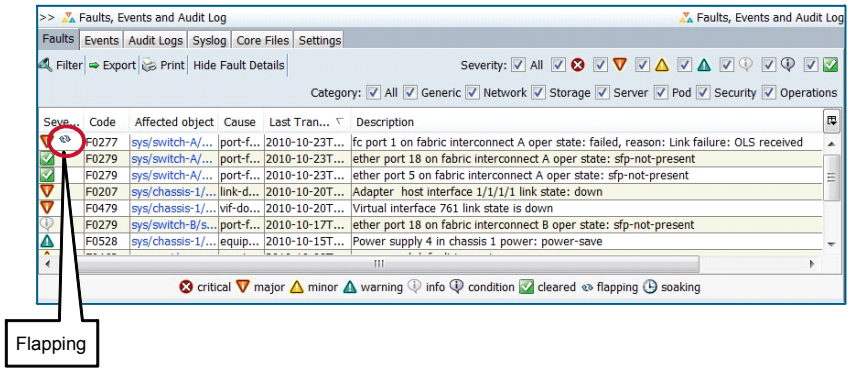
© 2012 Cisco and/or its affiliates. All rights reserved.

The fault is in a soaking state until the system defines whether the flapping condition is active.

https://t.me/learningnets

Fault in Flapping State

- An interface has transitioned between operational and nonoperational for longer than the 10-second flapping interval.

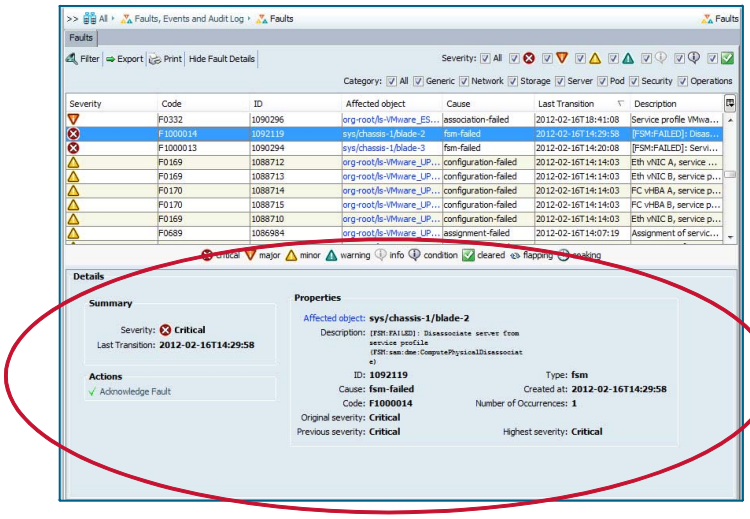


© 2012 Cisco and/or its affiliates. All rights reserved.

A fault in the flapping state indicates that a fault has continually risen and fallen for a duration that is greater than the flapping interval. The default flapping interval is 10 seconds.

Admin Fault Console Detail

- Select a fault to see details.



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

The figure shows an example of the Properties window that displays when you click a fault. The Properties window always displays the complete text of the fault.

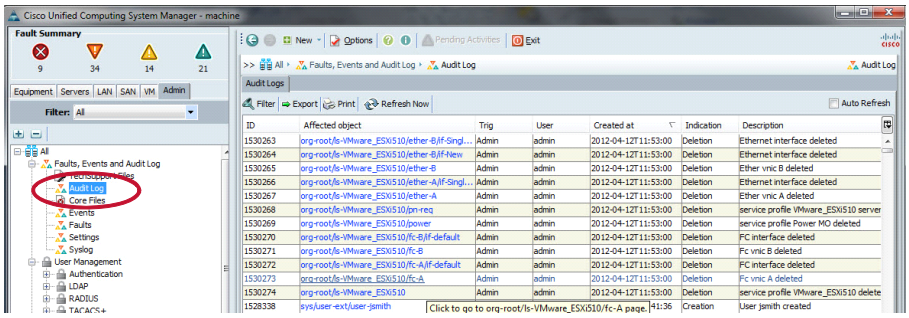
https://t.me/learningnets

Track Administrative Changes in the Cisco UCS Manager Audit Log

This topic describes the audit log in Cisco UCS.

Audit Log

- The actions of every user are tracked in detail.



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

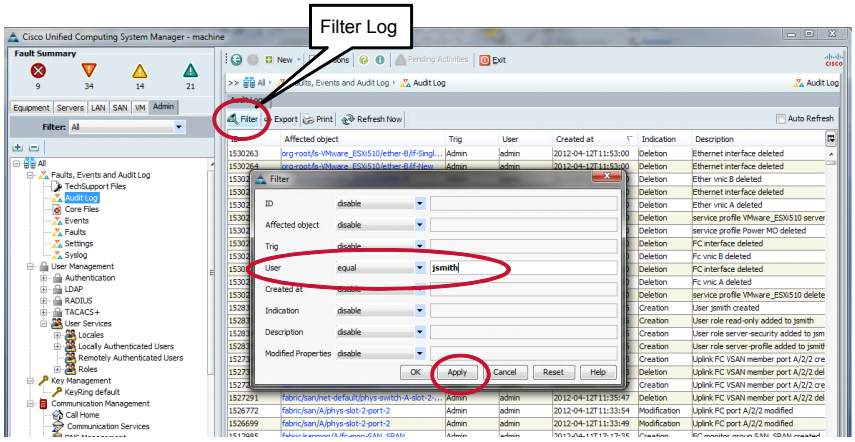
The audit log can be accessed from the Admin tab. Expand **Faults, Events and Audit Log**, and then choose **Audit Log**. The audit log records login events for all users and the actions they performed in the Cisco UCS Manager interface. This information is useful if an unapproved change has been made.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Filter Audit Log Output

- Limit the log display according to user-selected criteria.

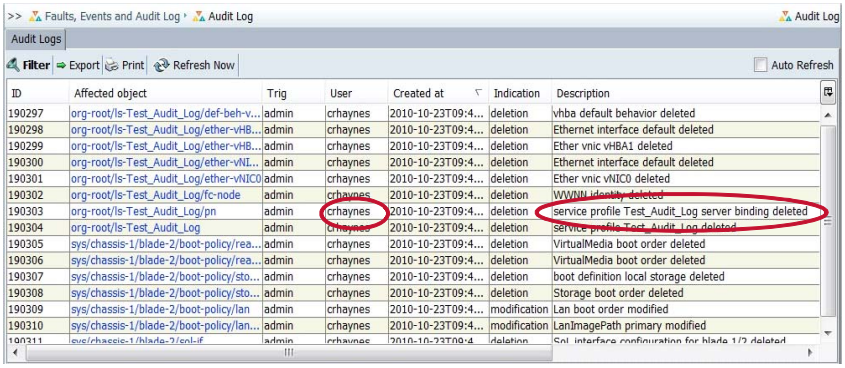


© 2012 Cisco and/or its affiliates. All rights reserved.

The audit log can be intimidating to work with because of the large number of entries. As the example in the figure shows, click **Filter** and then select the criteria on which to filter. In this example, the administrator has decided to determine which configuration changes have been made by user jsmith.

Filtered Audit Log Output

- Server down: A service profile was deleted by user jsmith.



ID	Affected object	Trig	User	Created at	Indication	Description
190297	org-root/ls-Test_Audit_Log/def-beh-v...	admin	crhaynes	2010-10-23T09:4...	deletion	vhba default behavior deleted
190298	org-root/ls-Test_Audit_Log/ether-vHB...	admin	crhaynes	2010-10-23T09:4...	deletion	Ethernet interface default deleted
190299	org-root/ls-Test_Audit_Log/ether-vHB...	admin	crhaynes	2010-10-23T09:4...	deletion	Ether vnic vHBA1 deleted
190300	org-root/ls-Test_Audit_Log/ether-vNI...	admin	crhaynes	2010-10-23T09:4...	deletion	Ethernet interface default deleted
190301	org-root/ls-Test_Audit_Log/ether-vNIC0	admin	crhaynes	2010-10-23T09:4...	deletion	Ether vnic vNIC0 deleted
190302	org-root/ls-Test_Audit_Log/fc-node	admin	crhaynes	2010-10-23T09:4...	deletion	WWNN identity deleted
190303	org-root/ls-Test_Audit_Log/pn	admin	crhaynes	2010-10-23T09:4...	deletion	service profile Test_Audit_Log server binding deleted
190304	org-root/ls-Test_Audit_Log	admin	crhaynes	2010-10-23T09:4...	deletion	service profile Test_Audit_Log deleted
190305	sys/chassis-1/blade-2/boot-policy/rea...	admin	crhaynes	2010-10-23T09:4...	deletion	VirtualMedia boot order deleted
190306	sys/chassis-1/blade-2/boot-policy/rea...	admin	crhaynes	2010-10-23T09:4...	deletion	VirtualMedia boot order deleted
190307	sys/chassis-1/blade-2/boot-policy/sto...	admin	crhaynes	2010-10-23T09:4...	deletion	boot definition local storage deleted
190308	sys/chassis-1/blade-2/boot-policy/sto...	admin	crhaynes	2010-10-23T09:4...	deletion	Storage boot order deleted
190309	sys/chassis-1/blade-2/boot-policy/lan	admin	crhaynes	2010-10-23T09:4...	modification	Lan boot order modified
190310	sys/chassis-1/blade-2/boot-policy/lan...	admin	crhaynes	2010-10-23T09:4...	modification	LanImagePath primary modified
190311	sys/chassis-1/blade-2/sol-if	admin	crhaynes	2010-10-23T09:4...	deletion	SoL interface configuration for blade 1/2 deleted

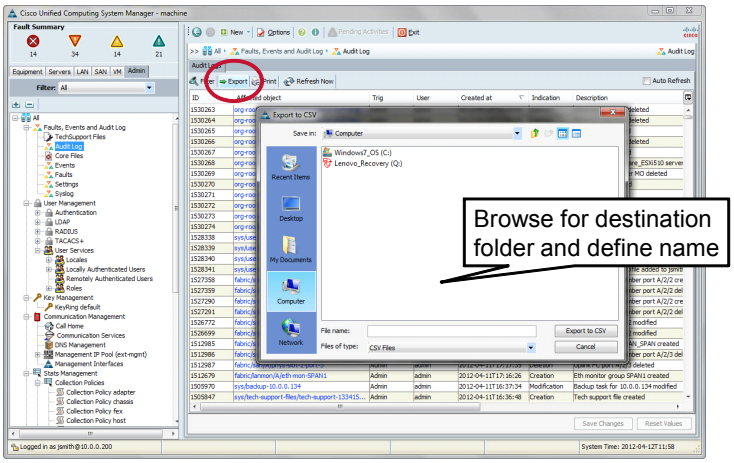
© 2012 Cisco and/or its affiliates. All rights reserved.

A production server went out of service unexpectedly. The example in the figure shows that the administrator deleted the wrong service profile.

https://t.me/learningnets

Export Audit Log

- Save the audit log to a .csv file.



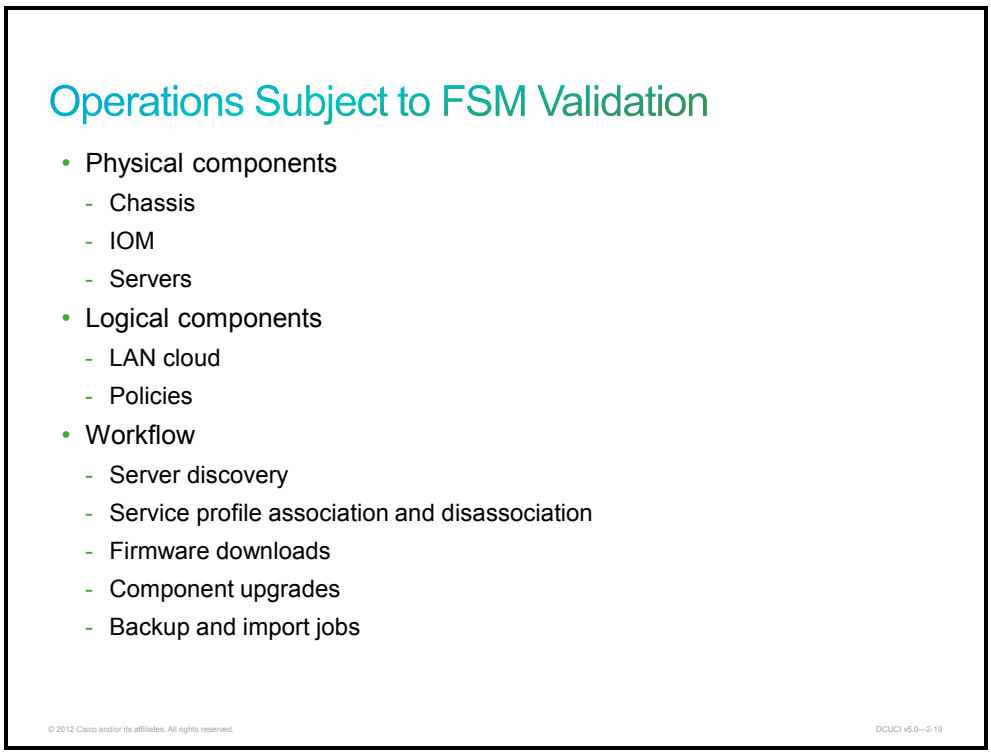
© 2012 Cisco and/or its affiliates. All rights reserved.

Audit log data can be exported manually to a comma-separated values (.csv) file. The file can be read in a text editor or spreadsheet application.

https://t.me/learningnets

Cisco UCS Manager Operations Subject to FSM Validation

This topic describes the finite state machine (FSM) in Cisco UCS Manager.

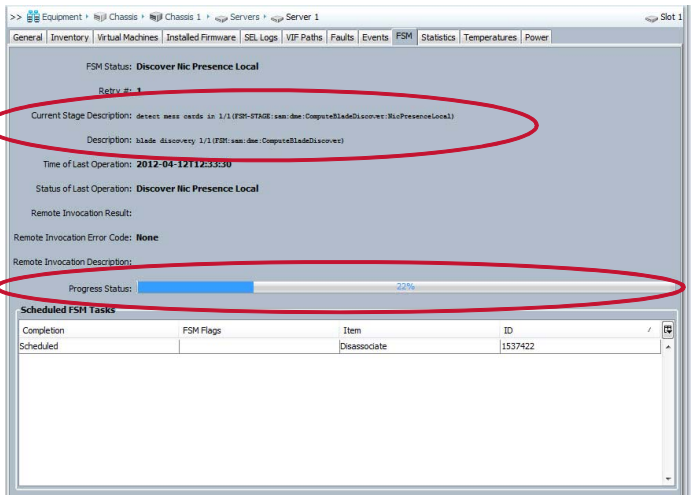


Many components and processes within Cisco UCS are characterized by highly complex state transitions. FSMs are assigned to audit the state transitions and to validate correct operation.

https://t.me/learningnets

Reacknowledge Compute Node: Discovery Process in FSM

- FSM tracking the transition states of compute node discovery



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

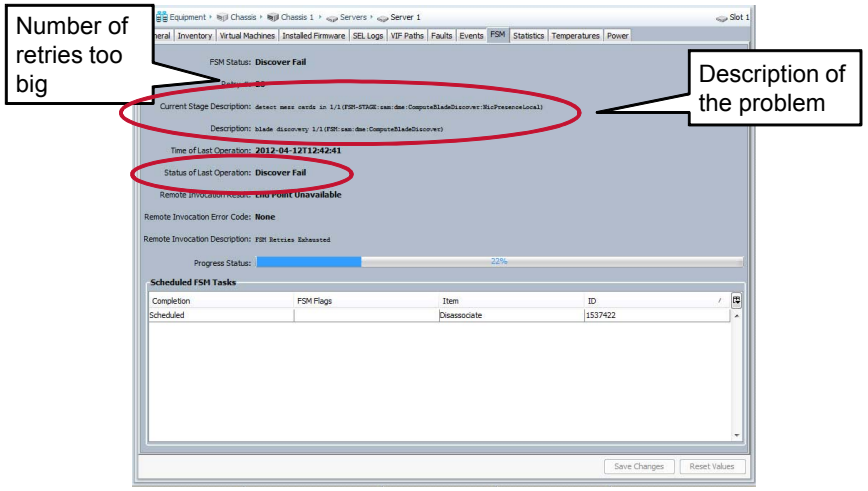
In the example, a compute node was manually reacknowledged. The Current Stage Description field clearly indicates that server discovery is underway.

The Progress Status indicator provides a graphical representation of how far the FSM processed tree has proceeded. In many cases, there might be a long pause at a particular percentage point. This pause is process-specific and is usually nothing to worry about. If an FSM stage times out, the stage retries the operation. If the retry limit is exceeded, the operation fails.

https://t.me/learningnets

Reacknowledge Compute Node: Discovery Failed

- FSM reports Discover Fail
- Description of the stage at which the problem is encountered



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

DCUCI v5.0—2-21

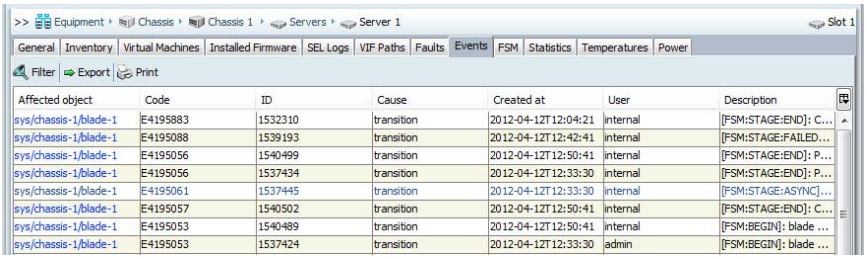
When the entire process finishes, the FSM indicates if the process was successful. In the example, you can see that the process has returned a Discover Fail message. You can see that the Retry counter holds a large value. The number of retries can be one indicator that something is wrong because the number shown indicates how many iterations the system performs during a particular stage of the process.

You will also be provided with descriptions of the stage at which the process failed.

https://t.me/learningnets

FSM Discovery Details

- Click the Event tab to review the log of FSM state transitions.



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

In the Events tab, you will find an event for each state transition for the process. In a failed process, you can get more detailed information.

 © 2012 Cisco Systems, Inc.

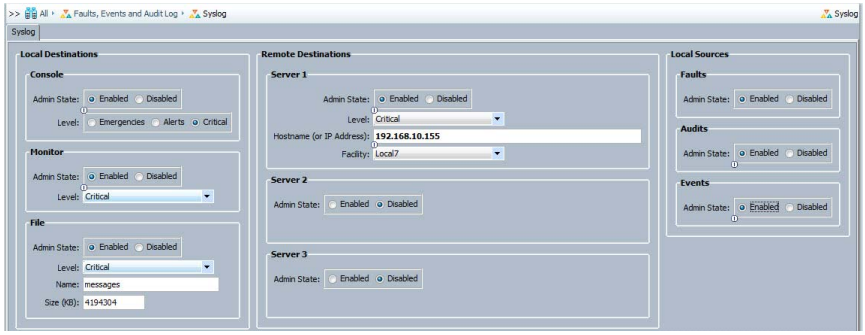
https://t.me/learningnets

Implement Logging Options

This topic describes the logging options in Cisco UCS Manager.

Logging Options

- Logging data is available in several places.
- All logging is disabled by default.



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

By default, all logging in Cisco UCS Manager is disabled.

If the Console option is enabled, then the three lowest levels of logging can be enabled. Log messages of the selected severity are propagated to the serial console of both fabric interconnects.

The Monitor option allows logging messages to be copied via Secure Shell (SSH) to Remote Terminal (RT) sessions. Be conservative when setting the logging level. If enough messages per second are transmitted over the remote session, the connection can easily be overloaded.

The File option allows logging messages to be stored in local flash memory. It is recommended that you change the default file size. Although the created file is a circular buffer, it reduces the available storage base on both fabric interconnects by 4 GB. A circular buffer is one that, once full, begins deleting the oldest messages first.

A best practice is to keep Console, Monitor, and File logging options in the default disabled state.

Cisco UCS Manager allows logging messages to be sent to as many as three syslog servers. Syslog is a standards-based protocol that operates over UDP port 514. Organization policy and regulatory compliance might dictate the use of syslog to archive all logging data.

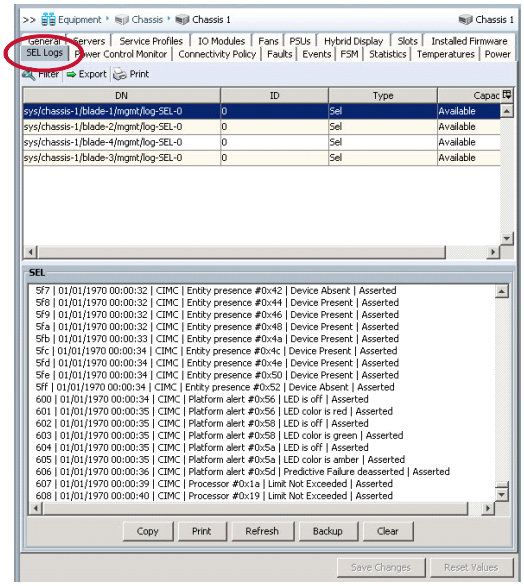
https://t.me/learningnets

System Event Log and Log Policies

This topic describes the system event log (SEL) option in Cisco UCS Manager.

System Event Log

- SEL resides in NVRAM on Cisco Integrated Management Controller.
- SEL gathers environmental logs for the servers.
- The SEL for an individual server or for all the servers in a chassis can be accessed.



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

The SEL resides on the Cisco Integrated Management Controller in NVRAM. The log records most server-related events, such as overvoltage and undervoltage, temperature events, fan events, events from BIOS, and so on. The SEL is mainly used for troubleshooting purposes. The SEL file is approximately 40 KB in size, and no further events can be recorded when it is full. The SEL must be cleared before additional events can be recorded.

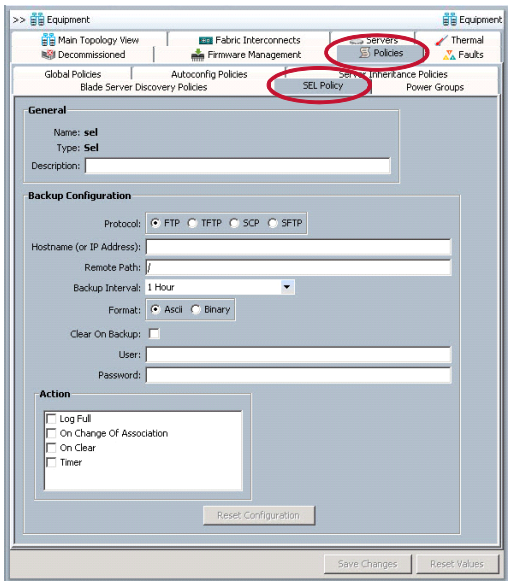
You can access the SEL for a specific server. To do so, navigate to **Equipment > Chassis > *Chassis Number* > Servers > *Server Number* > SEL Logs**.

You can also access the SEL for all the servers in a chassis. You have to navigate to **Equipment > Chassis > *Chassis Number* > SEL Logs**.

https://t.me/learningnets

SEL Policies

- SEL policies are used to back up the system event log.
- Navigate to **Equipment > Policies** to create a SEL policy.



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

DCUCI v5.0—2-27

You can use the SEL policy to back up the SEL to a remote server and, optionally, to clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can occur at regular intervals. You can also manually back up or clear the SEL.

The backup file is automatically generated. The filename format is sel-SystemName-ChassisID-ServerID-ServerSerialNum-Timestamp.

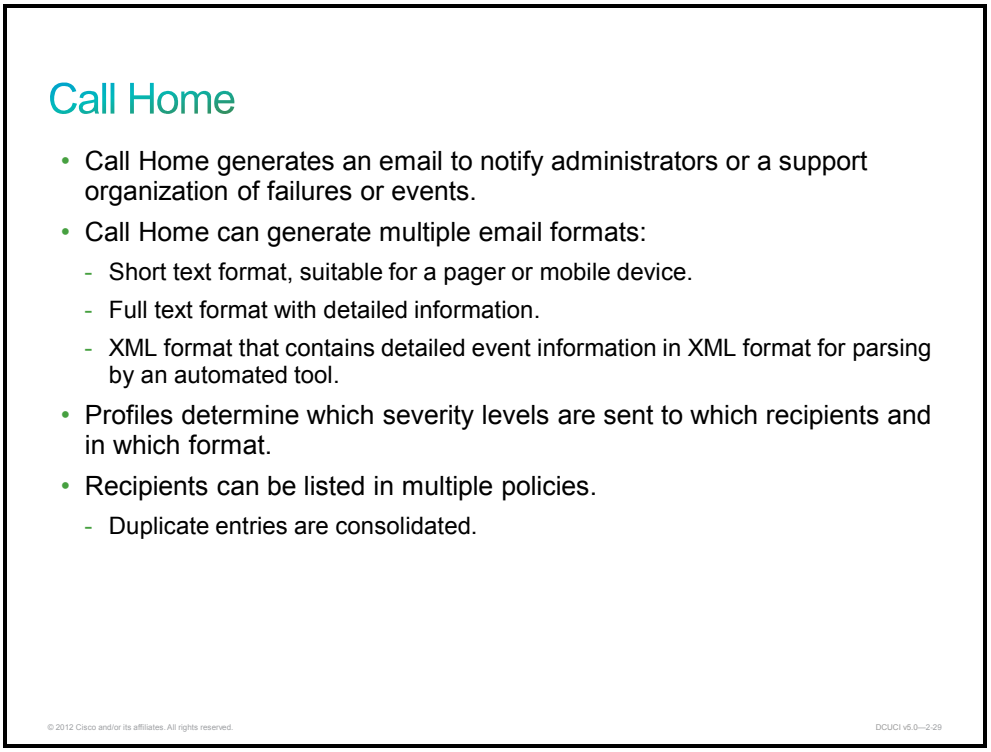
Here is an example of a filename:

```
sel-UCS-A-ch01-serv01-QCI12522939-20091121160736
```


https://t.me/learningnets

Implement the Smart Call Home Feature

This topic describes the Smart Call Home feature in Cisco UCS Manager.



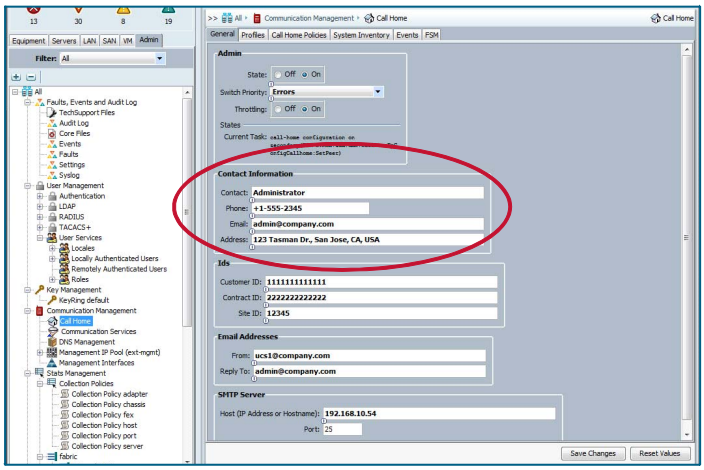
Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a network operations center, or use Cisco Smart Call Home services to generate a case with Cisco TAC.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Contact Configuration

- Begin by configuring the contact information that will be included in the Call Home messages.



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

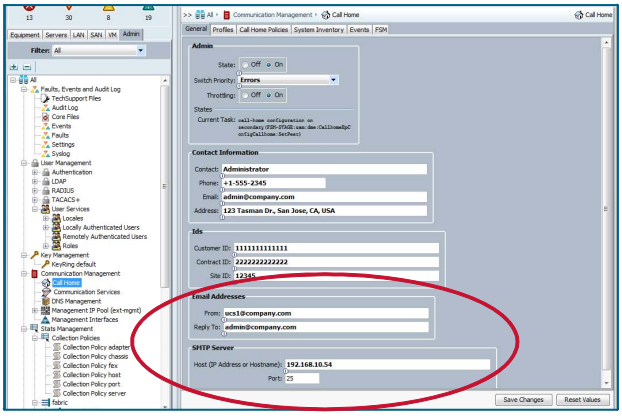
Before Call Home can be enabled, contact information, including the SMARTnet contract ID, site ID, and customer ID, must be entered.

Note	A SMARTnet contract is not required to send failure alerts to members of your organization. SMARTnet is required to send alerts to Cisco TAC for resolution.

https://t.me/learningnets

Email Notification

- Provide any necessary identification information.
- Supply the From and Reply To values for the email envelope.
- Specify the SMTP server to be used for outbound emails.



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

Email notification relies on the configuration of email addresses and a Simple Mail Transfer Protocol (SMTP) server address.

Call Home Profiles

- Three default profiles exist.
  - CiscoTAC-1, which is useful for sending XML data to Cisco TAC.
    - Uses the special CiscoTAC alert group to collect information needed by Cisco TAC.
  - full_txt, for sending full detailed text data.
    - By default, includes all alert groups at warning severity.
  - short_txt, for sending short, plain text data.
    - By default, includes all alert groups at warning severity.
- Alert groups allow profiles to send only data related to specific functional areas.
- Additional profiles can be created as needed.
  - Default profiles can be modified but not removed.

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

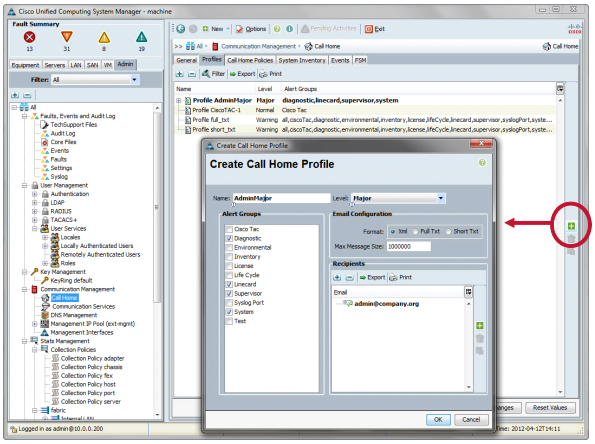
Call Home profiles determine which alert groups and recipients receive email alerts for events that occur at a specific severity. You can also use these profiles to specify the format of the alert for a specific set of recipients and alert groups.

The Cisco TAC-1 profile is configured by default. You can also create profiles to send email alerts to one or more groups when events occur at a level that you specify.

https://t.me/learningnets

Profile Configuration

- Profiles include the severity level and alert groups to monitor.
- Events that match these values are sent by email to the recipients.

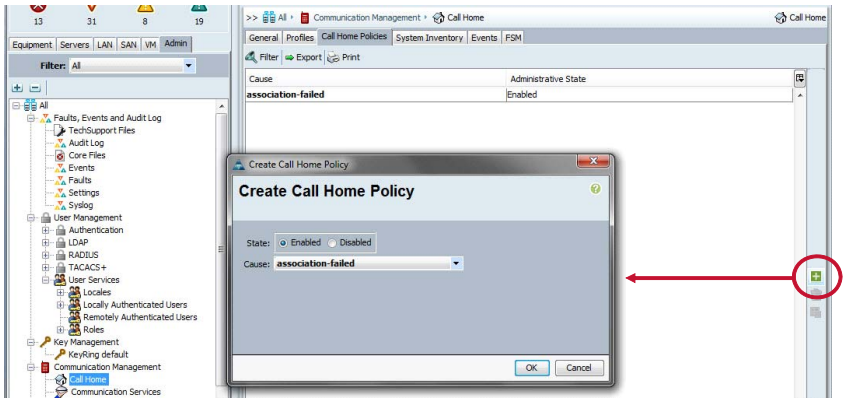


© 2012 Cisco and/or its affiliates. All rights reserved.

Call Home profiles define the alert groups, notification levels, the email format, and users to receive the emails.

Call Home Policies

- Call Home policies add additional conditions to monitor.



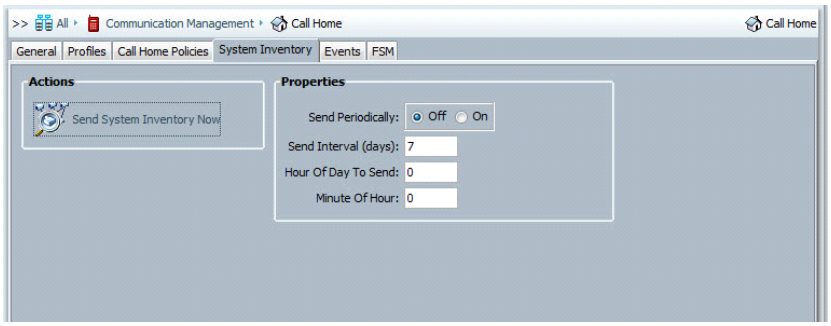
© 2012 Cisco and/or its affiliates. All rights reserved.

Call Home policies can also be created to restrict the conditions that will trigger an alert.

https://t.me/learningnets

System Inventory

- System inventory information can be sent manually or scheduled periodically.
- This information aids support organizations in tracking changes to installed equipment.



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

System inventory can be configured to periodically send information about field-replaceable units (FRUs) to the Cisco TAC, and to email destinations of your choice. For Cisco TAC to provide the best possible service, you must keep their database up-to-date with the components in your system.

© 2012 Cisco Systems, Inc.

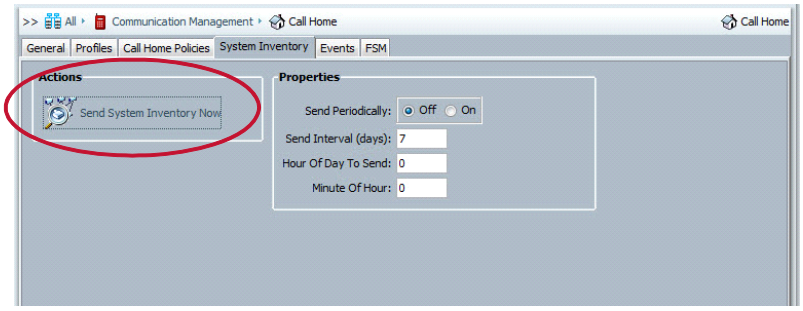
https://t.me/learningnets

Validate the Smart Call Home Feature

This topic shows how to validate the Smart Call Home configuration.

Send System Inventory to Validate Call Home

- Send an inventory dump to an email address in a configured profile.



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

An easy way to validate the configuration of your Smart Call Home setup is to enable a Call Home profile that is set to an email destination. When you click the button to send system inventory, an email should be generated to the destination email address that you configured in the profile.

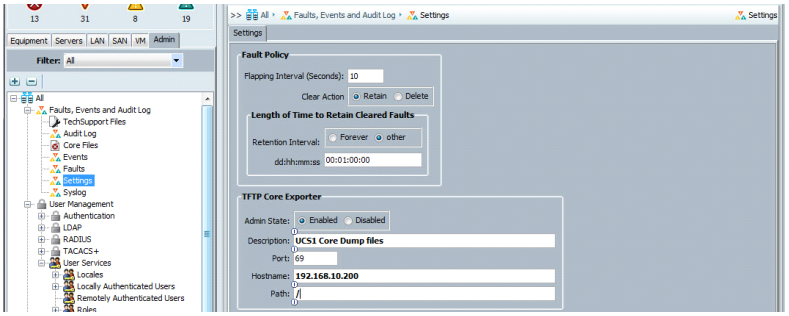
https://t.me/learningnets

Configure Settings for Logs, Events, and Faults

This topic describes the settings for logs, events, and faults.

Fault Settings and Retention Policy

- The configuration of the retention policy is governed by organizational policy and regulatory compliance requirements.
- Use the destination TFTP server to export core dump files.



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

The default settings and retention policy allows the Cisco UCS administrator to tune the flapping interval and faults retention policy. These values should be set according to organizational or regulatory compliance requirements.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Configure SPAN for Protocol Analysis

This topic describes how to create SPAN sessions.

Cisco UCS Traffic Monitoring

- Traffic monitoring is based on SPAN.
- There are a maximum of 16 SPAN sessions per fabric interconnect.
- A maximum of two SPAN sessions can be active per fabric interconnect.
- There is monitoring up to the level of the vNIC or vHBA.
- A Fibre Channel port on a Cisco UCS 6248 cannot be a SPAN source.
- A SPAN source and SPAN destination must be on the same fabric interconnect.
- A SPAN session can be Ethernet or Fibre Channel. The system defines a session based on the SPAN destination port.
- SPAN destination ports can be either a physical Ethernet port or a physical Fibre Channel port.

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

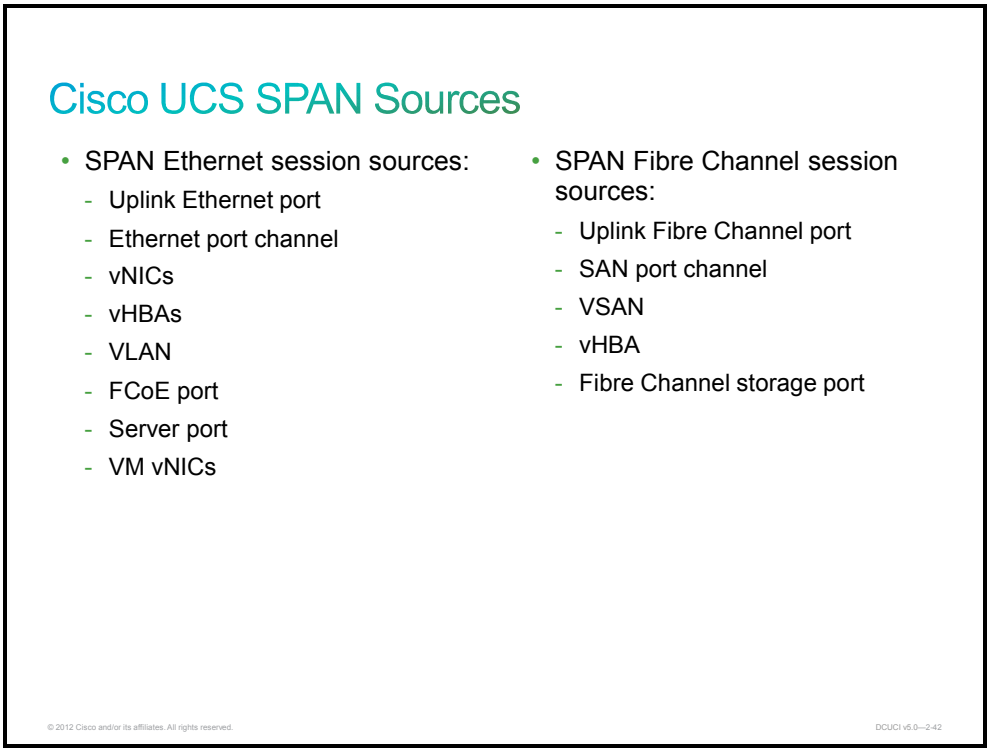
In Cisco UCS Manager, you can use SPAN sessions to monitor traffic that goes through a fabric interconnect. Only local SPAN is supported, which means that both the destination port and the sources of the captured traffic must be on the same fabric interconnect. With the support for SPAN, you have the ability to capture Ethernet or Fibre Channel traffic up to the level of the virtual machines (VMs).

The traffic monitoring sessions can be Ethernet or Fibre Channel. Cisco UCS Manager defines the session as Ethernet when you select an Ethernet port as the destination, and defines it as a Fibre Channel monitoring session when a Fibre Channel port is selected as the destination.

The SPAN destinations can be physical Ethernet or Fibre Channel ports.

You can create a maximum of 16 SPAN sessions per fabric interconnect, but only two can be active simultaneously, which means that you can have a total of four active monitoring sessions per Cisco UCS.

https://t.me/learningnets



The following can be Ethernet SPAN sources:

- Uplink Ethernet port
- Ethernet port channel
- Virtual network interface cards (vNICs)
- Virtual host bus adapters (vHBAs)
- VLAN
- Fibre Channel over Ethernet (FCoE) port
- Server port
- VM vNICs

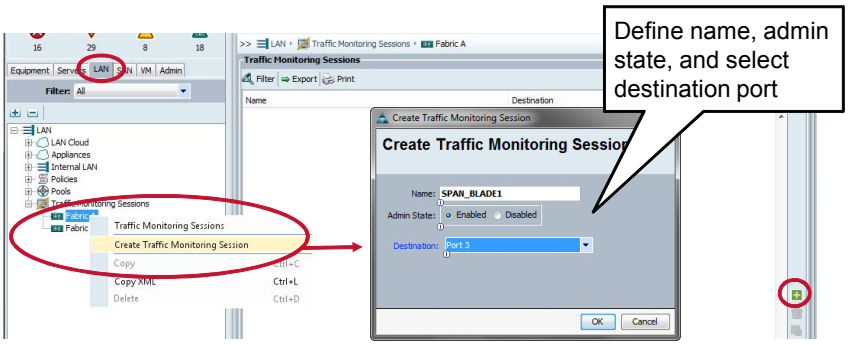
The following can be Fibre Channel SPAN sources:

- Uplink Fibre Channel port
- SAN port channel
- Virtual SAN (VSAN)
- vHBA
- Fibre Channel storage port

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

Ethernet SPAN Session

- Ethernet and Fibre Channel SPAN sessions are created in the same way either from the LAN or SAN tabs.
- The creation is a two-step process:
  1. Create the traffic monitoring session.
  2. Select SPAN sources.



The figure shows how to create an Ethernet SPAN session. A Fibre Channel SPAN session is created in the same way, but under the SAN tab.

There are two steps to create a SPAN session:

Step 1 Create the SPAN session and select a destination port.

Step 2 Define the sources in the newly created SPAN session.

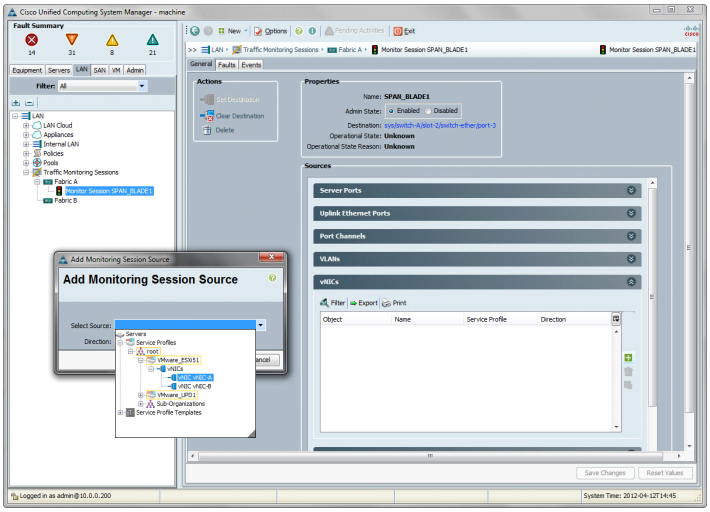
To create the SPAN session, navigate to **LAN** >**Traffic Monitoring Sessions** and select the fabric interconnect on which you want to capture traffic. Right-click **Fabric A** or **B** and choose **Create Traffic Monitoring Session**.

In the new window, specify a name for this object, set the admin state, and select a destination port from the drop-down menu.

https://t.me/learningnets

Select SPAN Sources

- Go to the new SPAN session and select sources.



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

After creating the SPAN session, click the SPAN session in the content pane. Under the General tab, you will be provided with the option to select SPAN sources.

Sources are divided into groups. To expand the group, click the plus sign (+). From the expanded window, choose the source that you need.

From here, you can also change the admin state. When a SPAN session is created, it is recommended to leave the admin state disabled. The disabled state will allow you to add sources without any communication disruption. When the SPAN session is in a disabled state, it is not active. To start capturing traffic, you have to put the session in the enabled admin state.

https://t.me/learningnets

Summary

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

Summary

- Cisco UCS Manager interfaces include Cisco UCS Manager GUI, Cisco UCS Manager CLI, XML API, KVM, and IPMI.
- Cisco UCS Manager maintains faults and errors as managed objects.
- The audit log can be used to track changes made by any user to the Cisco UCS Manager database.
- Several processes in Cisco UCS Manager are subject to FSM validation.
- Logging options include local buffer, console, and external syslog servers.
- The SEL records most server-related events. You can use the SEL policy to back up the SEL to a remote server and to clear the SEL after a backup operation occurs.
- The Smart Call Home feature allows Cisco UCS Manager to send inventory and predictive failure messages to Cisco TAC.
- You can validate the Smart Call Home feature by generating an email.
- Logs, events, and faults have user definable traits.
- Ethernet and Fibre Channel SPAN session can be created to monitor traffic up to the level of VMs.

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

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 5

Implementing High Availability

Overview

When two Cisco Unified Computing System (UCS) 6100/6200 Series Fabric Interconnects are configured in a cluster, both data planes forward actively. The management plane forms an active subordinate-to-peer relationship. Both peers are connected by a private network. Understanding the cluster recovery process that occurs during node isolation is important.

Objectives

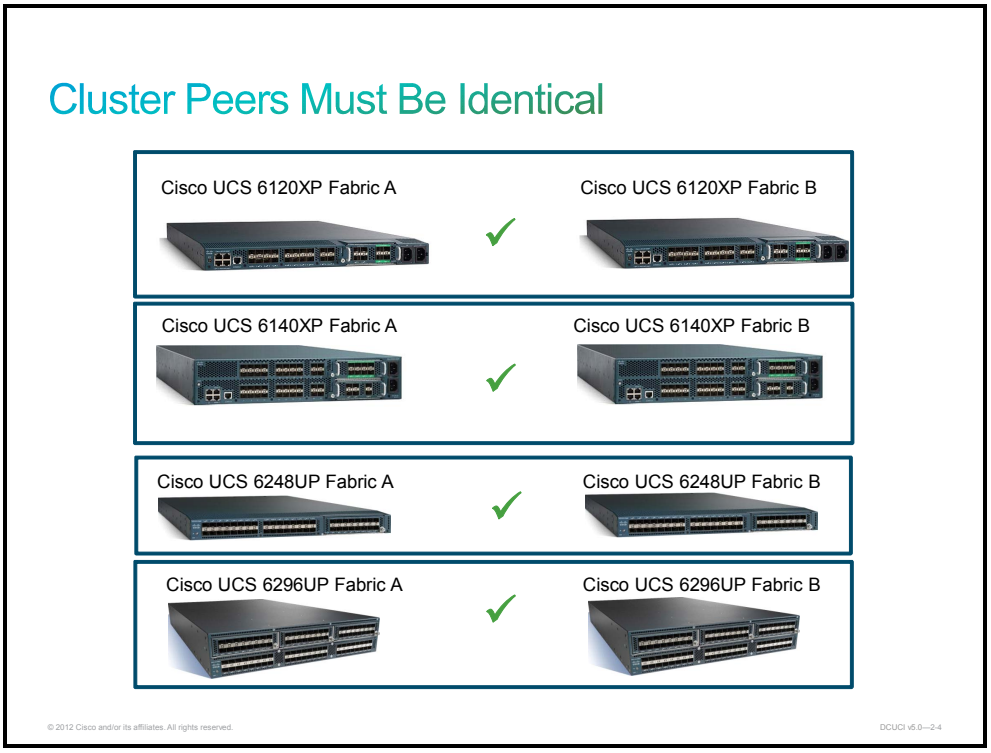
Upon completing this lesson, you will be able to maintain Cisco UCS in a high-availability configuration. This ability includes being able to meet these objectives:

- Describe high-availability cluster connection requirements for Cisco UCS B-Series
- Describe intercluster communications and Cisco UCS Manager database synchronization
- Differentiate between cluster partition-in-time and partition-in-space split-brain conditions
- Describe how the Cisco UCS 5108 Blade Server Chassis SEEPROM resolves a split-brain issue in the high-availability cluster
- Modify cluster IP addressing from the Cisco UCS Manager GUI and CLI

https://t.me/learningnets

High-Availability Cluster Connection Requirements

This topic describes the high-availability connection requirements in Cisco UCS.



Cisco UCS Fabric Interconnect peers in a cluster must run the same version of Cisco UCS Manager and must peer with the same model. A Cisco UCS 6120 Fabric Interconnect cannot peer with a Cisco UCS 6140 Fabric Interconnect. The same requirement is valid for all of the Cisco UCS Fabric Interconnect models, including the Cisco UCS 6248UP and 6296UP.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cluster Peers Can Be Different to Upgrade Cluster

- A Cisco UCS 6120 Fabric Interconnect can be paired with a Cisco UCS 6140 Fabric Interconnect to facilitate upgrading the cluster from 20 ports to 40 ports.
- Cisco UCS 6248UP can be paired with a Cisco UCS 6296UP to facilitate hardware upgrade.
- Dissimilar fabric interconnects are not supported for production operation.

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

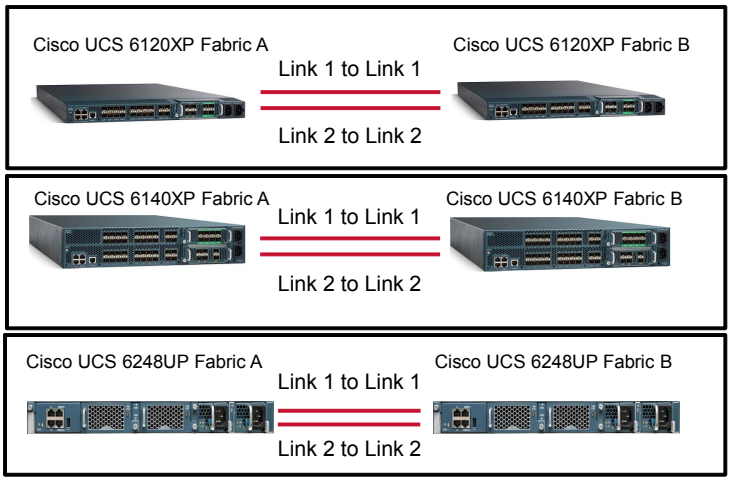
Cisco offers a simple method to update a cluster from a 20-port fabric interconnect to a 40-port fabric interconnect. An unconfigured Cisco UCS 6140 Fabric Interconnect is connected to the active member of the Cisco UCS 6120 cluster. When Cisco UCS Manager has synchronized the database with the Cisco UCS 6140 Fabric Interconnect, the Cisco UCS 6120 Fabric Interconnect is removed from the cluster. When the Cisco UCS 6140 Fabric Interconnect becomes the active cluster peer, the secondary Cisco UCS 6140 Fabric Interconnect is introduced to the cluster and synchronizes with the active peer.

The same process is supported for migrating from Cisco UCS 6248UP to 6296UP.

https://t.me/learningnets

Cluster Cabling

- 1000BaseTX
- Category 6 straight-through Ethernet cable



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

The private cluster interconnect network runs at 1 Gb/s. EIA/TIA Category 6 cabling is required to support reliable communications at complete bandwidth.

The interfaces (Layer 1 and Layer 2) shown in the figure provide a cluster link between two Cisco UCS 6100 Series Fabric Interconnects. The interfaces carry the cluster heartbeat messages between the two fabric interconnects, as well as carrying high-level messages between Cisco UCS Manager elements. The links are part of an IEEE 802.3ad bond that is managed by the underlying operating system. The bond is configured to run Link Aggregation Control Protocol (LACP). The IP addresses on these links are fixed.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Intercluster Communications and Cisco UCS Manager Database Synchronization

This topic describes intercluster communications.

Fabric Interconnect High Availability

- Redundant fabric interconnects synchronize database and state data through dedicated, redundant Ethernet links.
- The architecture prevents split-brain scenarios.
- The “floating” virtual management IP address is used on the primary fabric interconnect.
- Management of redundant fabric interconnects occurs on the active device only. Changes are synchronized to standby.
- Only the management plane is active/standby.
- Data plane is active/active.

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

Redundant fabric interconnects synchronize database and state data through dedicated, redundant Ethernet links. The fabric interconnect architecture can also prevent split-brain scenarios.

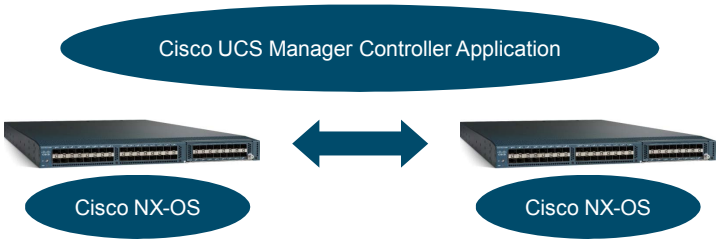
Moreover, management of the redundant fabric interconnects occurs on the active device only. Changes are synchronized to standby.

With the fabric interconnect configured for high availability, only the management interface is active/standby, while data traffic is active/active.

https://t.me/learningnets

Process Management

- Cisco UCS Manager controller
  - Distributed application
  - Separate process running on Cisco NX-OS
  - Defines running mode of Cisco UCS Manager processes
- Cisco NX-OS
  - Starts all Cisco UCS Manager processes
  - Monitors and restarts Cisco UCS Manager processes



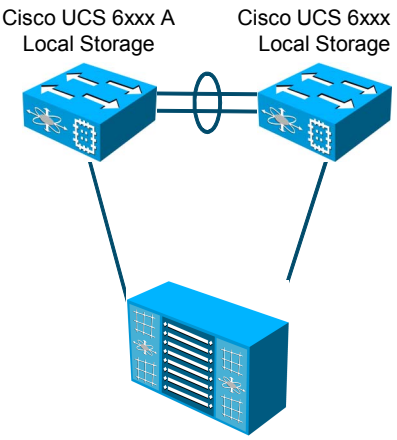
© 2012 Cisco and/or its affiliates. All rights reserved.

The Cisco UCS Manager controller is a distributed application that runs on both the primary and subordinate Cisco UCS Manager instances. Each instance is represented by a unique ID (the same as the node ID). The Cisco UCS Manager controller is implemented as a distinct process. The address-space separation guarantees a higher degree of fault isolation. This separation also allows the controller to distinguish between a failure of other system processes and a failure of the controller itself. The Cisco UCS Manager controller decides which Cisco UCS Manager components should run in primary or subordinate mode.

https://t.me/learningnets

Local and Chassis Data

- Local storage
  - NVRAM and flash stores static data
  - Read and written by local Cisco UCS Manager instance
  - Replicated when both nodes are up
- Chassis EEPROM
  - SEEPROM stores cluster state data
  - Read and written by both chassis management controllers
  - No need to replicate data
  - Used to assist the Cisco UCS Manager in determining state of cluster
  - Needed for high availability



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

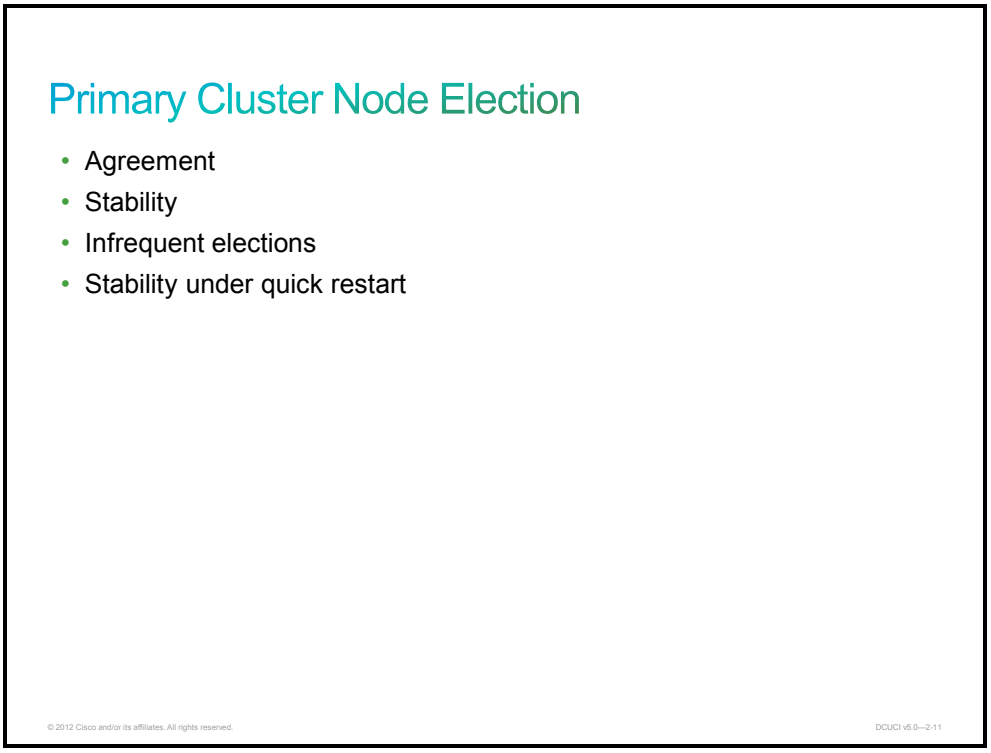
Local Storage

Each Cisco UCS Fabric Interconnect maintains its own local storage in NVRAM and flash memory. Local storage contains static data, that is, storage that does not change with cluster membership changes. For example, installable images are stored in the /bootflash partition of internal flash memory. Data such as installable images are replicated at run time, while both cluster members are present in the cluster. You do not need to (nor can you) download images via the Cisco UCS Manager interface to individual nodes. The download is replicated to both nodes. If a node is not present during an image download, then that image is replicated to that node when the node rejoins the cluster.

Chassis EEPROM

Each chassis management controller maintains its own part of the shared chassis storage in the serial EEPROM (SEEPROM). Chassis storage contains a combination of static and dynamic information. For example, the static portion contains the node ID for each node that is configured in the cluster. The dynamic portion contains the version of the configuration as seen by that node. There is no need to replicate the contents of the SEEPROM. Each node maintains its own portion, whereas both nodes may read from both topics.

https://t.me/learningnets



Agreement

A Cisco UCS Manager instance declares a new leader when these conditions apply:

- The instance has received acknowledgments that its election request has been processed.
- The instance has checked the election counter in the incoming messages to ensure that the messages all relate to the same election request.
- All processes propose the same new leader.

Stability

The leadership should change only in one of these cases:

- An administrative change in the configuration requires the leader to be moved.
- The leader process fails.

Infrequent Elections

Elections are caused only by these events:

- Administrative configuration change
- New process joining the group
- Process exiting the group
- Process failure

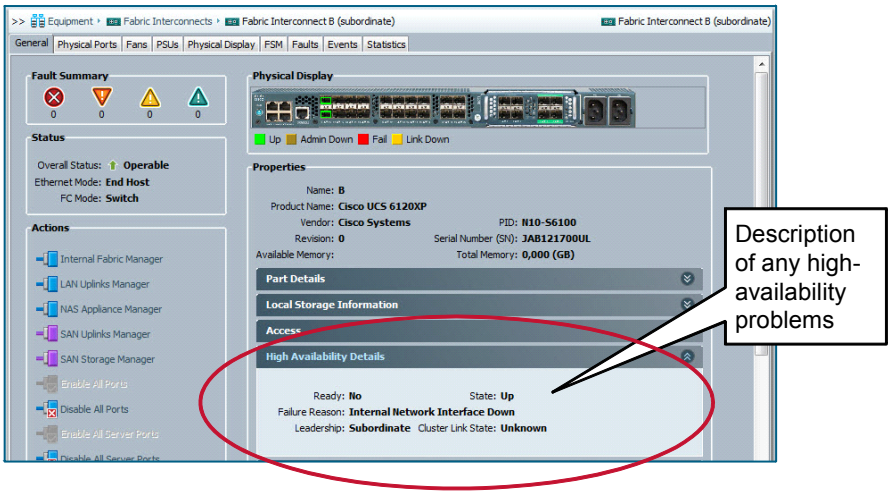
Stability Under Quick Restart

Cisco UCS Manager will allow a leader process to fail, restart, and still join the group as the leader. This allowance prevents a change of leadership when a process (or a node) is the subject of a quick restart. The rationale is that a change of leadership, and therefore a switchover, can be more expensive than waiting for the leader process (or node) to reinitialize.

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

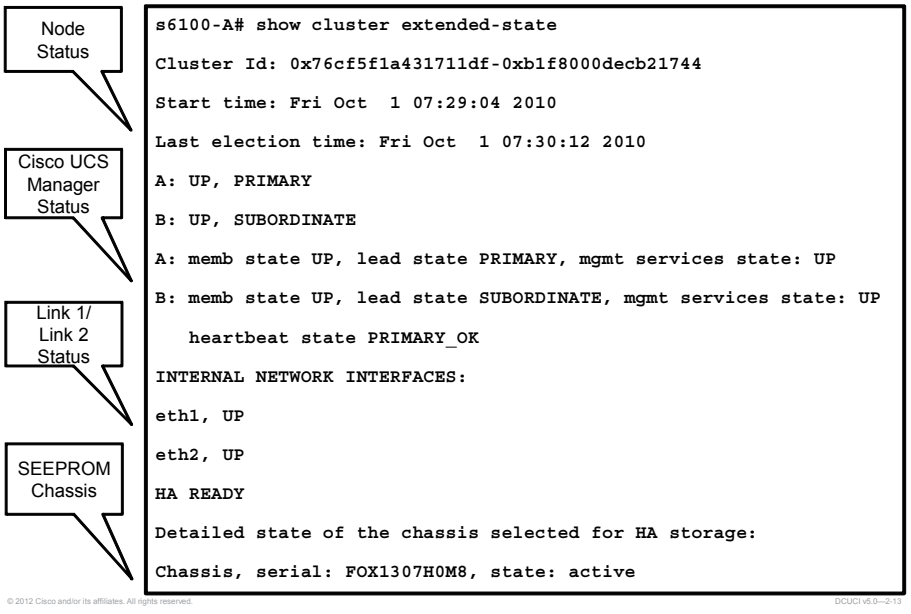
Monitor Cluster Status: GUI

- Equipment > Fabric Interconnects > Fabric Interconnect A or B



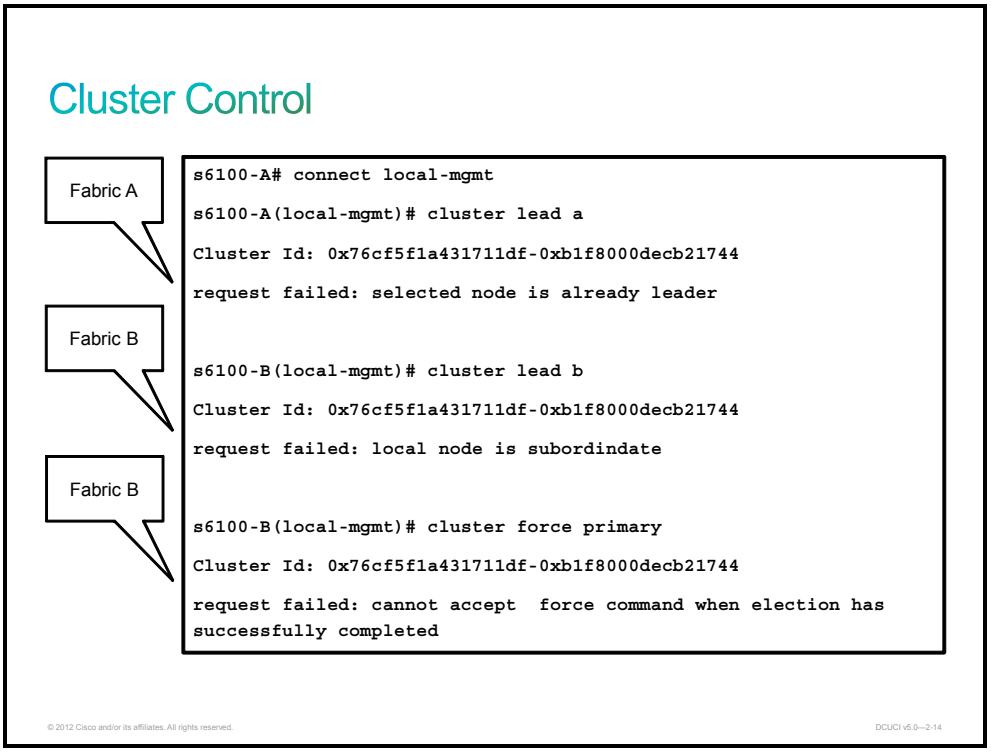
Choose the fabric interconnect from the Equipment tab of the navigation pane. In the content pane, click the double down-arrow icon to the right of High Availability Details.

Monitor Cluster Status: CLI



The **show cluster extended-state** command provides detailed information about cluster operation. The figure indicates the cluster state of both peers, the private network (Layer 1 and Layer 2), and which chassis SEEPROM is used to resolve split-brain conditions. The ID of the chassis that is used to resolve split-brain conditions can be determined only by using the CLI.

https://t.me/learningnets



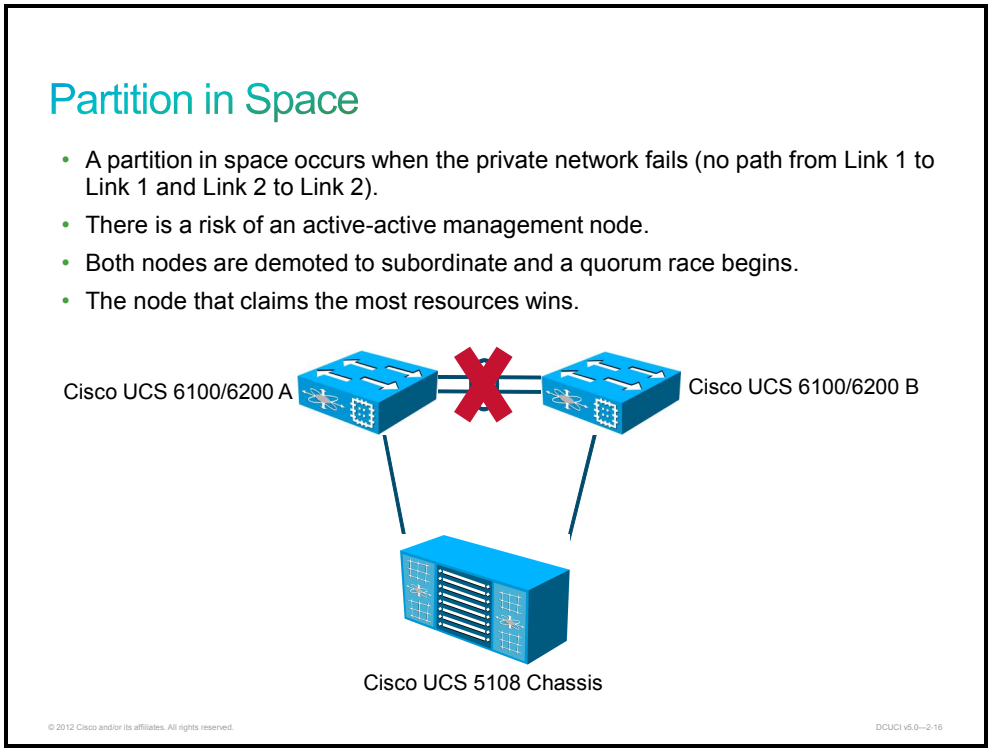
The **cluster lead** and **cluster force primary** commands can be used to change the fabric interconnect that is the active management plane.

Note	As the figure shows, when the election process has finished, neither command causes a switchover.

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

Partition-in-Time and Partition-in-Space Split-Brain Conditions

This topic describes partition-in-time and partition-in-space split-brain conditions.

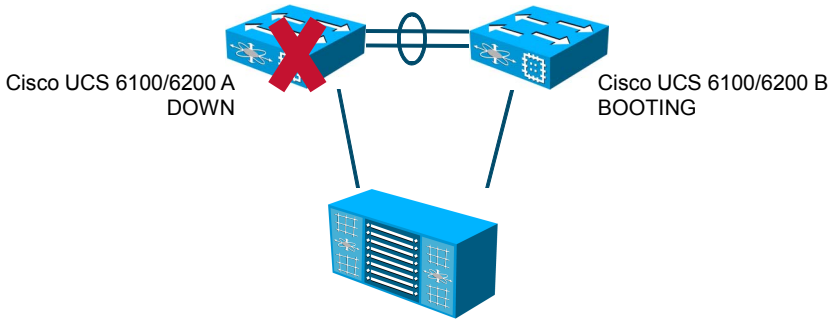


A partition in space occurs when nodes fail to communicate with each other over the private network (Layer 1 and Layer 2 links both fail). To resolve this split-brain condition (assuming that both switches are active at the time of the private network failure), each chassis management controller acts on behalf of the fabric Cisco UCS Manager instance, to reach the SEEPROM first and write its node ID in the primary field. This process is known as a "quorum race." The winner remains in the cluster and the loser aborts. When the links are restored, the losing node can rejoin the cluster and act as the subordinate.

https://t.me/learningnets

Partition in Time

- A partition in time occurs when a node boots alone in the cluster.
- The node compares its database version against the SEEPROM and discovers that its version number is lower than the current database version.
- There is a risk of applying an old configuration to Cisco UCS components.
- This node will not become the active management node.



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

A partition in time occurs when one of the nodes is down for a time, during which changes to the configuration are made on the active primary node. These changes do not replicate to the down node.

If the primary node shuts down after having made configuration changes to the database, but before being able to replicate them to the other (downed) node, and that downed node tries to join the cluster alone, then that condition is referred to as a partition in time.

To resolve this split-brain condition, a version number that represents the configuration is written to the EEPROM. On solo startup, a node compares its version number to that of the other node. (Both nodes can read both parts of the EEPROM.) If the version number of the first node is the same or higher than that of the other node, then the first node can start the cluster. If the version number is lower than that of the other node, then the first node does not become the active management node. This process protects against using an old version of the Cisco UCS Manager database.

Note	To force the fabric interconnect to become the active management node, use the **cluster force primary** command.

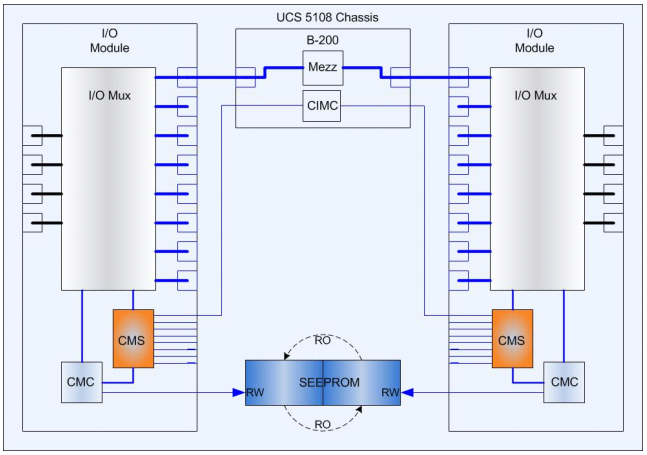
https://t.me/learningnets

Resolving a Split-Brain Issue in the High-Availability Cluster

This topic describes how the Cisco UCS 5108 Blade Server Chassis SEEPROM resolves split-brain issues.

Split Brain

- Caused by failure of cluster network (Link 1 and Link 2)
- Read and written to by chassis management controller



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

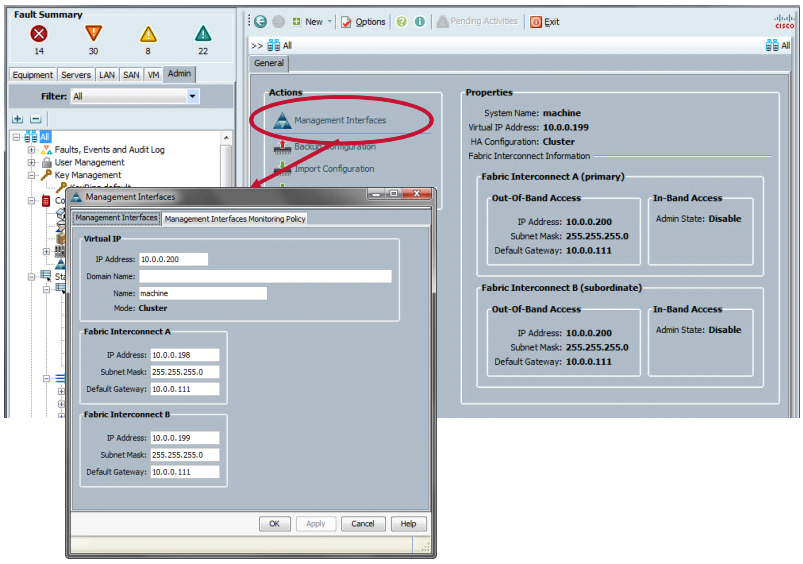
A split-brain condition occurs in a cluster when the private network that is responsible for cluster synchronization is unavailable. In Cisco UCS, a SEEPROM on the Cisco UCS 5108 server chassis midplane is used to resolve split-brain conditions.

The SEEPROM is divided into two sections—one for fabric A and one for fabric B. The chassis management controller on fabric A has read/write access to the fabric A portion of the SEEPROM and read-only access to the section that is under the control of fabric B.

https://t.me/learningnets

Modifying Cluster IP Addressing

Modify Management IP Addressing: GUI



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

To change the IP address of either fabric interconnect, or to change the virtual IP address that is used to access the active management node, select the **Admin** tab in the navigation pane. In the content pane, click the **Management Interfaces** link.

Modify Management IP Addressing: CLI

```
s-6100-A# scope system
s-6100-A /system # set virtual-ip ?
  A.B.C.D  System IP Address

s-6100-A # scope fabric-interconnect a
s-6100-A /fabric-interconnect # set out-of-band ?
  gw       Gw
  ip       Ip
  netmask  Netmask
```

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

The management IP addresses can also be changed from the CLI.

https://t.me/learningnets

Summary

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

Summary

- The high-availability cluster requires an active gigabit link between Link 1 and Link 1 or to Link 2 and Link 2. Mix-and-match connectivity is not supported.
- The active management node synchronizes configuration and firmware images to the subordinate node. The management plane operates in active/standby mode and the data plane operates in active/active mode.
- Partition-in-space and partition-in-time conditions are two types of split-brain issues.
- Data stored in the Cisco UCS 5108 chassis SEEPROM resolves split-brain issues in the fabric interconnect cluster.
- Cluster IP addressing can be modified in the Cisco UCS Manager GUI or CLI.

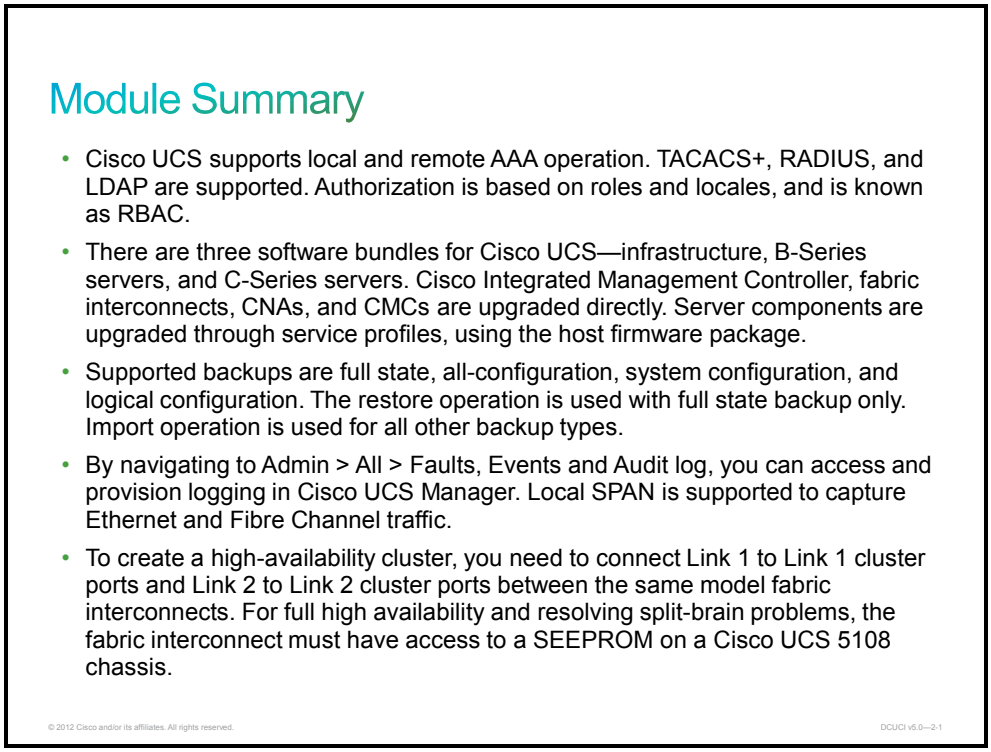
© 2012 Cisco and/or its affiliates. All rights reserved.

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 Unified Computing System (UCS) supports local and remote authentication, authorization, and accounting (AAA). For remote AAA servers, RADIUS, TACACS+, and Lightweight Directory Access Protocol (LDAP) are supported protocols. Authorization is based on using roles and locales. Roles define which features users can access. Locales are groups of organizations. When a locale or multiple locales are applied to a user, the user is allowed access only to the organizations in those locales. Starting with Cisco UCS version 1.4, a new multiple destination authentication and authorization scheme is used. The new scheme allows provisioning of multiple different AAA destinations. AAA servers, including local, are grouped in protocol realms and, within the protocol realms, in provider groups. Authentication domains are created based on this grouping. The user is allowed to select the authentication domain against which to be authenticated.

Cisco UCS software is available in three software bundles. The infrastructure bundle contains firmware for fabric interconnects, Cisco UCS Manager software, and firmware for I/O modules (IOMs) and mezzanine adapters. The Cisco UCS B-Series server bundle contains firmware for components on the blade compute nodes. The Cisco UCS C-Series server software bundle contains firmware for C-Series servers, when integrated with Cisco UCS.

Cisco UCS supports four backup types—full-state, all-configuration, system configuration, and logical configuration. The full-state backup is used with the restore operation to recover the entire Cisco UCS. The other three backup types use the import operation to merge or replace configuration in the running configuration of the Cisco UCS.

Access the main logging features by navigating to Admin > All > Faults, Events and Audit log. Provision the Cisco Smart Call Home feature by navigating to Admin > All > Communication Services. Cisco UCS supports local Switched Port Analyzer (SPAN). Based on SPAN, an Ethernet or Fibre Channel monitoring session can be used to capture and analyze traffic. You can capture and analyze traffic from multiple different sources up to the level of virtual network

https://t.me/learningnets

interface cards (vNICs), virtual host bus adapters (vHBAs), and virtual machine vNICs (VM vNICs).

The high-availability cluster is created when you connect cluster ports on fabric interconnects that are the same model. Also, to achieve full high availability, there must be at least one Cisco UCS 5108 chassis that is connected and reachable. This connection is required because fabric interconnects must have access to the serial EEPROM (SEEPROM) to avoid any active/active situations.

References

For additional information, refer to these resources:

- Cisco, Inc. *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, Inc., *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

© 2011 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 three AAA protocols are supported for communication with external AAA providers? (Choose three.) (Source: Implementing RBAC)

A) TACACS+
B) RADIUS
C) AD
D) LDAP
E) ACS
F) 802.1X

Q2) Which five protocol realms are used in Cisco UCS Manager? (Choose five.) (Source: Implementing RBAC)

A) local
B) none
C) AD
D) LDAP
E) ACS
F) RADIUS
G) TACACS+
H) Apple SecureTalk

Q3) How can AAA servers be grouped within protocol realms? (Source: Implementing RBAC)

A) in security areas
B) in authentication zones
C) in authentication domains
D) in provider groups
E) in authorization zones

Q4) What are roles used for in Cisco UCS Manager? (Source: Implementing RBAC)

A) for user grouping
B) to set user privileges
C) to authenticate users
D) user blacklist

Q5) What is a locale? (Source: Implementing RBAC)

A) group of users
B) external authorization attribute
C) internal set of credentials
D) logical group of organizations

https://t.me/learningnets

Q6) Which three options are Cisco UCS software bundles? (Choose three.) (Source: Managing and Upgrading Cisco UCS B-Series Firmware)

A) Cisco UCS Infrastructure bundle
B) Cisco UCS Manager bundle
C) Cisco UCS B-Series servers bundle
D) Cisco NX-OS bundle
E) Cisco UCS C-Series servers bundle
F) Cisco UCS Application bundle

Q7) Where can you download Cisco UCS software bundles? (Source: Managing and Upgrading Cisco UCS B-Series Firmware)

A) Apple AppStore
B) Cisco.com
C) Google Play Store
D) Microsoft.com

Q8) Which three pieces of software must be upgraded on fabric interconnects? (Choose three.) (Source: Managing and Upgrading Cisco UCS B-Series Firmware)

A) Cisco Integrated Management Controller firmware
B) Cisco UCS Manager software
C) chassis management controller firmware
D) kernel image file
E) system image file
F) mezzanine firmware

Q9) Which two memory partitions are available on the Cisco Integrated Management Controller? (Choose two.) (Source: Managing and Upgrading Cisco UCS B-Series Firmware)

A) initial
B) backup
C) startup
D) loading

Q10) Which option must be created and used in a service profile to upgrade the RAID controller of the compute node? (Source: Managing and Upgrading Cisco UCS B-Series Firmware)

A) RAID upgrade package
B) LSI upgrade policy
C) host firmware package
D) Cisco upgrade push job

Q11) Which four backup types are supported in Cisco UCS Manager? (Choose four.) (Source: Implementing Backup, Import, and Restore of the Cisco UCS Manager Database)

A) full-state
B) all-configuration
C) half-state
D) logical configuration
E) system configuration
F) server configuration
G) server-state backup

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Q12) Which operation is used with a full-state backup file? (Source: Implementing Backup, Import, and Restore of the Cisco UCS Manager Database)

A) import
B) restore
C) recover
D) merge

Q13) Which operation is used with configuration backups? (Source: Implementing Backup, Import, and Restore of the Cisco UCS Manager Database)

A) import
B) restore
C) recover
D) push

Q14) Which type of file is created with a full-state backup? (Source: Implementing Backup, Import, and Restore of the Cisco UCS Manager Database)

A) text file
B) zipped file
C) XML file
D) CSV file

Q15) Which type of file is created with a configuration backup? (Source: Implementing Backup, Import, and Restore of the Cisco UCS Manager Database)

A) zipped file
B) XML file
C) MD5 hash file
D) CSV file

Q16) Which four severity level faults are shown in the fault summary bar? (Choose four.) (Source: Implementing Logging and Monitoring)

A) Critical
B) Major
C) Minor
D) Warning
E) Condition
F) Info

Q17) Where can you track user activity in Cisco UCS Manager? (Source: Implementing Logging and Monitoring)

A) fault console
B) system events log console
C) audit log
D) Smart Call Home

Q18) What is the default flapping interval in Cisco UCS? (Source: Implementing Logging and Monitoring)

A) 1 minute
B) 30 seconds
C) 15 seconds
D) 10 seconds

https://t.me/learningnets

Q19) How many remote syslog servers can be provisioned in Cisco UCS Manager? (Source: Implementing Logging and Monitoring)

A) 1
B) 2
C) 3
D) 4
E) 5

Q20) How many simultaneous active monitoring sessions are supported per fabric interconnect? (Source: Implementing Logging and Monitoring)

A) 1
B) 2
C) 3
D) 4

Q21) Which two options are methods for connecting fabric interconnects for high availability? (Choose two.) (Source: Implementing High Availability)

A) Layer 1-Layer 2
B) Layer 1-Layer 1
C) Server-Layer 1
D) Server-Layer 2
E) Layer 2-Layer 2

Q22) What is the management plane mode of operation in a high-availability cluster? (Source: Implementing High Availability)

A) active/active
B) active/standby
C) standby/standby
D) active/hot standby

Q23) What is the data plane mode of operation in a high-availability cluster? (Source: Implementing High Availability)

A) active/active
B) active/standby
C) standby/standby
D) active/hot standby

Q24) Which hardware component helps solve split-brain situations? (Source: Implementing High Availability)

A) local flash memory
B) Cisco Integrated Management Controller
C) serial EEPROM
D) upstream switch

Q25) Which option best describes a partition-in-space split-brain situation? (Source: Implementing High Availability)

A) lost primary fabric interconnect
B) lost subordinate fabric interconnect
C) lost cluster connectivity
D) lost upstream LAN connectivity

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module Self-Check Answer Key

Q1) A, B, D

Q2) A, B, D, F, G

Q3) D

Q4) B

Q5) D

Q6) A, C, E

Q7) B

Q8) B, D, E

Q9) B, C

Q10) C

Q11) A, B, D, E

Q12) B

Q13) A

Q14) B

Q15) B

Q16) A, B, C, D

Q17) C

Q18) D

Q19) C

Q20) B

Q21) B, E

Q22) B

Q23) A

Q24) C

Q25) C

https://t.me/learningnets

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

Module 3

Implement Cisco UCS B-Series Connectivity

Overview

This module describes the implementation of Cisco Unified Computing System (UCS) generation 1 and generation 2 hardware and connectivity options.

Module Objectives

Upon completing this module, you will be able to install and provision Cisco UCS B-Series blade servers in the Cisco UCS 5108 blade chassis, know the characteristics of the different models of Cisco UCS I/O modules (IOM) and how to install them, understand the different connectivity topologies and options and how the Cisco Nexus Operating System (NX-OS) treats Ethernet and Fibre Channel traffic, and be acquainted with generation 2 hardware and all the newly introduced features.

This ability includes being able to meet these objectives:

- Implement Cisco UCS B-Series physical connectivity
- Install Cisco UCS B-Series hardware
- Implement Cisco UCS B-Series LAN connectivity
- Implement Cisco UCS B-Series SAN connectivity

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 1

Implementing Cisco UCS B-Series Physical Connectivity

Overview

Depending on the applications and operating systems that you plan to deploy in your data center, there will be different bandwidth requirements. The bandwidth requirements will define the needed connectivity for your servers. This lesson describes the physical connectivity of the Cisco Unified Computing System (UCS) B-Series servers, the supported topologies with the different generations of the hardware, the available mezzanine adapters, and the chassis discovery policies.

Objectives

Upon completing this lesson, you will be able to differentiate between physical connections on the I/O module (IOM) and the redundant connections for management and data plane over the I/O multiplexer (MUX) and midplane. This ability includes being able to meet these objectives:

- Describe the relationship between I/O uplinks and bandwidth oversubscription with generation 2 hardware
- Describe the Cisco UCS 2204/2208XP IOM architecture including CMC, I/O MUX, and chassis management switch
- Describe the relationship between I/O uplinks and bandwidth oversubscription with generation 1 hardware
- Describe the Cisco UCS 2104XP IOM architecture including CMC, I/O MUX, and chassis management switch
- Describe the features of the Cisco UCS VIC 1280 and VIC 1240
- Compare the number of virtual interfaces available on the Cisco UCS M81KR VIC and the VIC 1280
- Describe new mezzanine cards including M51, M61, and M72
- Describe the Cisco Integrated Management Controller management component of the B-Series blades
- Describe the creation of port channels from the Cisco UCS 6200 Series Fabric Interconnect to the 2204/2208XP IOM

https://t.me/learningnets

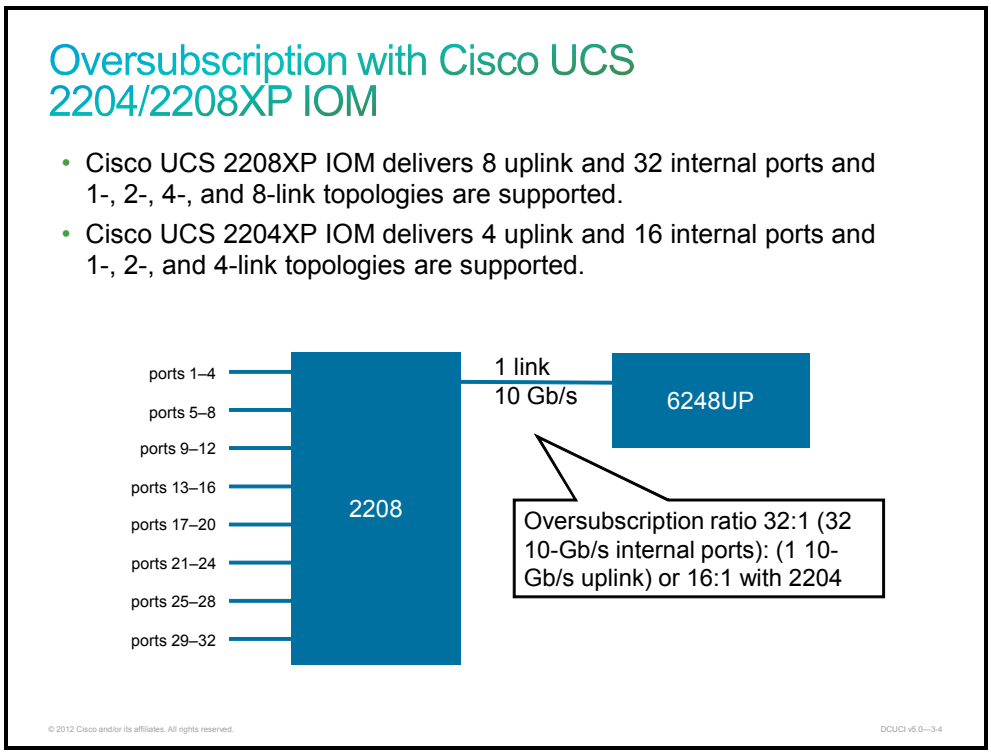
- Describe the difference between server and uplink port personalities in the fabric interconnect
- Describe the chassis discovery process and monitor using the FSM
- Configure the chassis discovery policy

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

I/O Uplinks and Bandwidth Oversubscription in Generation 2 Hardware

This topic describes oversubscription and static pinning with generation 2 hardware.



Cisco UCS 2208 IOM is second-generation hardware. The hardware provides eight 10-Gb/s external ports to connect to the fabric interconnect. The hardware also provides 32 internal ports for the blade servers—4 for each slot.

With the Cisco UCS 2208 IOM, the supported topologies for connectivity with the fabric interconnect are 1-, 2-, 4-, or 8-link topologies. Depending on the number of uplinks that are used, the oversubscription ratio will differ.

When 1-link topology is used, the oversubscription ratio will be 32:1, as all of the internal interfaces, four for each slot, will use only this link.

The Cisco UCS 2204XP IOM is also second-generation hardware. The hardware provides four 10-Gb/s external Ethernet interfaces to connect to the fabric interconnect, and 16 internal 10-Gb/s interfaces—two 10-Gb/s interfaces per server slot.

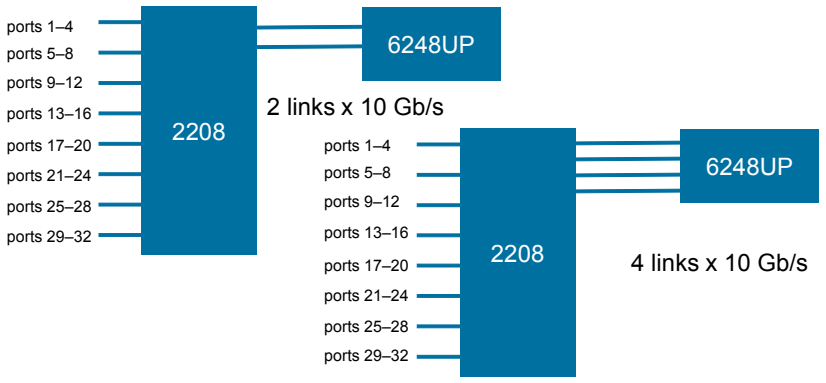
Cisco UCS 2204XP IOM supports 1-, 2-, and 4-link topologies.

With 10-link topology, the oversubscription ratio will be 16:1 (16 internal interfaces: 1 uplink). This ratio can be achieved if you use Cisco UCS Virtual Interface Card (VIC) 1280 or VIC 1240 in your servers. The latter can be used only in the Cisco UCS B200 M3 server.

https://t.me/learningnets

2- and 4-Link Oversubscription

- 2-link topology oversubscription ratio 16:1 (32 10-Gb/s internal):(2 10-Gb/s uplinks) or 8:1 with 2204XP
- 4-link topology oversubscription ratio 8:1 (32 10-Gb/s internal):(4 10-Gb/s uplinks) or 4:1 with 2204



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

In a 2-link topology, there will be 2 uplinks available. The oversubscription ratio will be 32:2 or 16:1. With Cisco UCS 2204XP, the ratio will be 8:1.

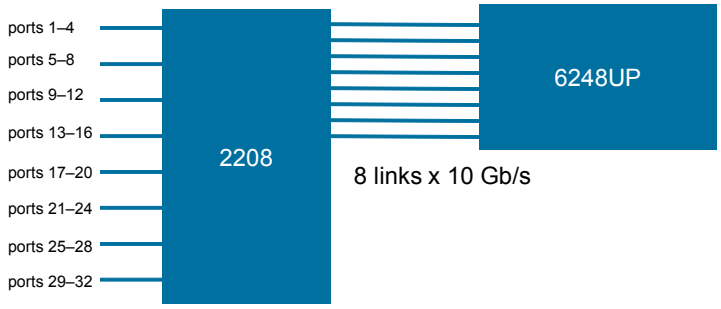
With a 4-link topology, the oversubscription will be 8:1—32 internal interfaces will be using a total of 4 uplinks. With Cisco UCS 2204XP the ratio will be 4:1.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

8-Link Oversubscription

- Oversubscription ratio 4:1 (32 10-Gb/s internal):(8 10-Gb/s uplinks) with Cisco VIC 1280
- Oversubscription ratio 1:1 with Cisco M81KR and 2208 IOM



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

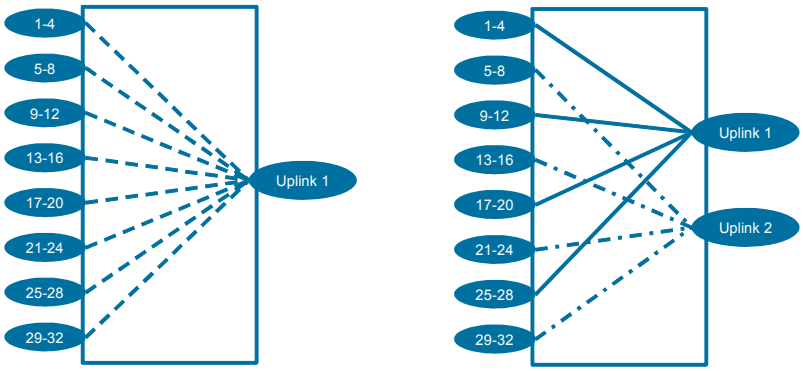
With the Cisco UCS VIC 1280, each compute node is connected with four interfaces to each of the Cisco UCS 2208 IOMs. In this setup, if you use the 8-link topology the oversubscription ratio will be 32:8, or 4:1.

If you use the Cisco UCS M81KR VIC, it will use only one internal interface per server slot. In this setup, you utilize an oversubscription ratio of 1:1.

https://t.me/learningnets

Static Cisco UCS 2204/2208XP IOM Pinning

- Internal static pinning in 1- and 2-link topologies
- The slots are pinned to uplink ports.



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

The static internal pinning for the Cisco UCS 2204/2208XP second-generation hardware follows the same rules as generation 1. Again, the pinning is defined by the uplink topology in use.

With 1-link topology, all the internal slots will be statically pinned to the uplink interface.

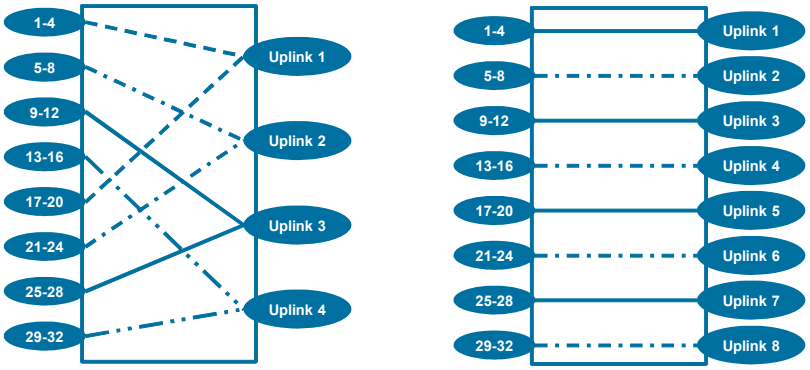
With 2-link topology, the interfaces for slots 1, 3, 5, and 7 will be pinned to the first uplink. The interfaces for slots 2, 4, 6, and 8 will be pinned to the second uplink.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

4- and 8-Link Pinning

- Internal static pinning in 4- and 8-link topologies
- 8-link topology is supported only on Cisco UCS 2208XP



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

With 4-link topology, the pinning will be as follows:

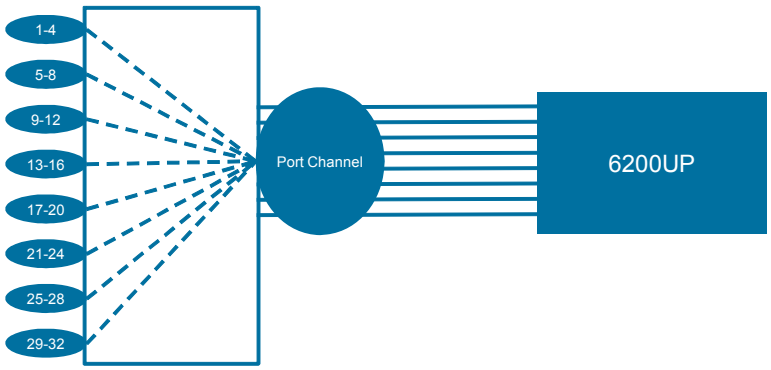
Slot Number	Uplink Interface
1, 5	1
2, 6	2
3, 7	3
4, 8	4

With 8-link topology, each slot will be pinned to an uplink interface. The 8-link topology is supported only on Cisco UCS 2208XP. The pinning follows slot 1 to uplink 1, slot 2 to uplink 2, and so on.

https://t.me/learningnets

Static Cisco UCS 2204/2208XP IOM Pinning with Fabric Port Channel

- Internal ports are pinned to the port channel interface.
- Supported only between Cisco UCS 6200UP and 2204/2208 IOM.
- Cisco UCS 2204XP has only 4 external ports, combined in a port channel.



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

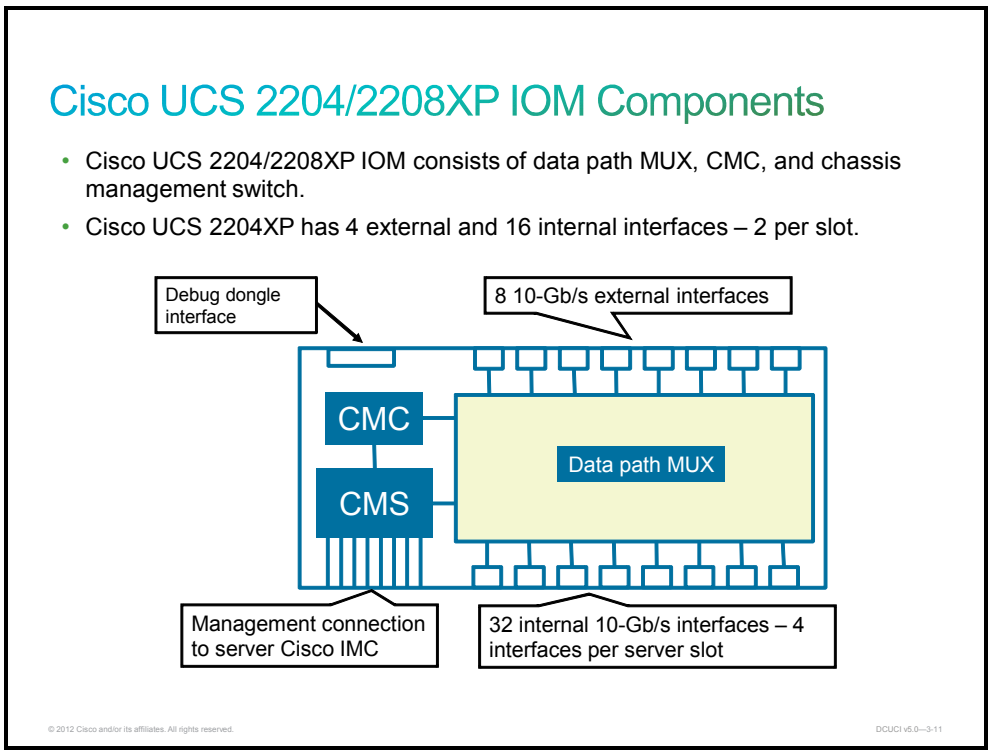
When a Cisco UCS 2200 IOM is connected to a Cisco UCS 6200 Series Fabric Interconnects, the uplinks can be combined into a fabric port channel. In this setup, the internal interfaces for the server slots will be pinned to the port channel interface. The oversubscription will depend on the number of uplinks that form the port channel. The advantage of this setup is that even if there is a failure in the uplinks, the servers will not lose this data path because the port channel interface will be up and operational, as long as there is at least one active link.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS 2204/2208XP IOM Architecture

This topic describes the components of the Cisco UCS 2204/2208XP IOM.



Cisco UCS 2208XP IOM is a second-generation module for the Cisco UCS 5108 chassis. The IOM provides for the data and management connectivity of the blade servers and the blade chassis. The IOM has 8 external 10-Gb/s Fibre Channel over Ethernet (FCoE)-capable external Ethernet interfaces for uplink connectivity to the fabric interconnects. The IOM also has 32 internal interfaces that are 10-Gb/s FCoE-capable, for compute node connectivity. Each slot has four internal interfaces.

The Cisco UCS 2204XP IOM provides 4 external 10-Gb/s interfaces and 16 internal 10-Gb/s interfaces. Each slot is provided with two 10-Gb/s interfaces, which are FCoE-capable.

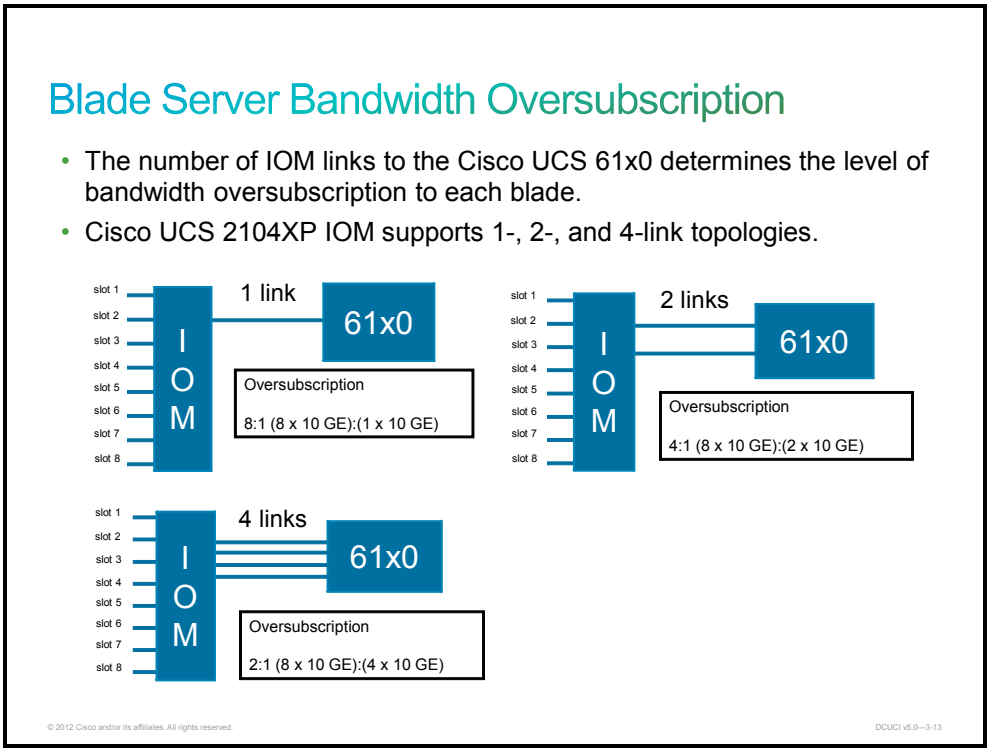
The components of the Cisco UCS 2204/2208XP IOMs are the same as in the Cisco UCS 2104XP IOM. The IOM consists of an I/O MUX, which manages the data communication of the compute nodes between the internal and external interfaces. There is a chassis management controller (CMC), which services the management communication. From one side, the CMC communicates with Cisco UCS Manager by providing environmental and inventory data for the chassis. From the other side, the CMC is used as a proxy in the communication between Cisco UCS Manager and the Cisco Integrated Management Controller of each compute node. This communication is realized through the chassis management switch, which provides eight 100-Mb/s internal interfaces to the Cisco Integrated Management Controllers.

There is also an external debug interface, for use with a dongle cable, that provides a console and Ethernet interfaces.

https://t.me/learningnets

I/O Uplinks and Bandwidth Oversubscription in Generation 1 Hardware

This topic describes the oversubscription ratios and the IOM pinning in generation 1 hardware.

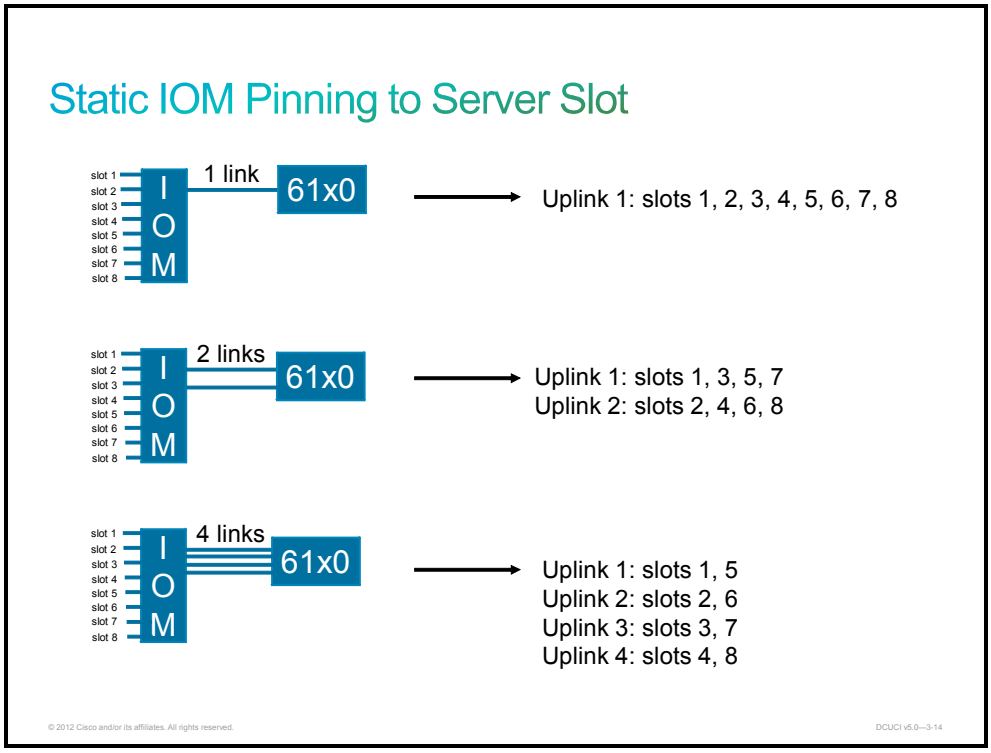


Each Cisco UCS 5108 server chassis supports two IOMs. Each IOM supports one, two, or four 10 Gigabit Ethernet links to each fabric interconnect in the cluster. One IOM connects to fabric A and one to fabric B.

With a 4-link configuration, there are 40 Gb/s of available bandwidth on each IOM. Although the data plane is active on both fabrics, they are designed to operate in active-standby mode. With eight blade servers in a chassis and four links from the IOM, the effective oversubscription rate is 2:1. With two links, the oversubscription rate is 4:1, and with one link per IOM, the rate is 8:1.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



Cisco UCS Manager supports three IOM link topologies: one link, two links, and four links.

With generation 1 hardware, each mezzanine card has one 10-Gb connection to the I/O multiplexer on fabric A and fabric B. A connection on each fabric is statically pinned to one of the four IOM server links to the fabric interconnect.

Number of Links	Server Pinning
1 link	Servers 1–8 are pinned to link 1.
2 links	Odd-numbered servers are pinned to link 1 and even-numbered servers are pinned to link 2.
4 links	Link 1: Servers 1 and 5 Link 2: Servers 2 and 6 Link 3: Servers 3 and 7 Link 4: Servers 4 and 8

Note The number of IOM uplinks is always a power of 2.

https://t.me/learningnets

IOM and High Availability

- What happens when one link is lost in a 4-link topology?
  - Although the IOM does not support a 3-link topology, the three active links will continue to forward traffic until the chassis is reacknowledged.
  - The two servers that were pinned to the failed link are down unless fabric failover is configured.
  - After the chassis is reacknowledged, that IOM will form a 2-link topology and repin odd-numbered blade slots to the odd-numbered server link and even-numbered blade slots to the even-numbered server link.
  - The two servers that failed to the B fabric will be reconnected to the A fabric.

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

When there is more than one IOM link to the fabric interconnect, failure of a link causes a loss of connectivity for servers that are associated with that link. If network interface card (NIC) teaming is configured in the operating system, or hardware-based failover is configured in the service profile, the affected servers will failover to their fabric B connection.

If no failover mechanism is configured for an impacted server, the server loses all connectivity. Upon link loss, the IOM does not automatically repin to a supported topology. You must manually reacknowledge the chassis for the IOM to repin.

https://t.me/learningnets

Effects of Reacknowledging a Chassis

Reacknowledge	No Reacknowledge
IOM repins to 2-link topology	IOM continues with 3 links
20-Gb/s bandwidth (-50%)	30-Gb/s bandwidth (–25%)
Interrupts communication to all eight servers	Interrupts communication to two servers
Manual intervention—Must reacknowledge a second time to move back to the 4-link topology upon link restoration	Automatic fail-back upon link restoration

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

When an IOM link fails, it is important to consider carefully how to proceed. The general rule is to reacknowledge the chassis if an IOM link goes down and the affected servers are not configured for fabric failover at the hardware or operating system level. If the affected servers are configured for fabric failover, the chassis should not be reacknowledged. When the IOM link connectivity is restored, the servers that were impacted by the failure will fail back to their primary fabric.

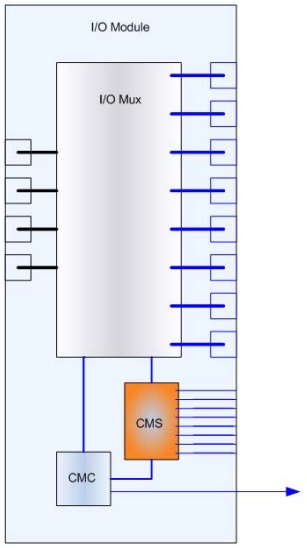
https://t.me/learningnets

Cisco UCS 2104XP IOM Architecture

This topic describes the components of the Cisco UCS 2104XP IOM.

Cisco UCS 2104XP IOM Components

- I/O MUX multiplexes data from the fabric interconnect to host ports.
- Chassis management switch carries management traffic to the Cisco Integrated Management Controller.
- Chassis management controller (CMC) is used in chassis and component discovery.
- CMC also monitors chassis sensors and controls fan speed.



CMS = chassis management switch

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

The Cisco UCS 2104XP IOM provides the data and management planes of the Cisco UCS B-Series servers. The Cisco UCS 2104XP IOM manages the chassis environment—the power supply and fans, as well as the blades—along with the fabric interconnect, which eliminates the need for separate chassis management modules.

This management is performed by a CMC. The CMC collects status data from the IOM using the Intelligent Platform Management Interface (IPMI) protocol over the interintegrated circuit (I2C) serial bus. This information is then communicated to the Cisco UCS Manager using the Ethernet server link. The CMC also serves as a proxy for the Cisco UCS Manager to the blade servers for certain functionality and has a role in the high-availability protocols. Also, if two IOMs are present in a chassis, they will cluster in an active or passive configuration.

The CMC performs the following functions:

- Controls the chassis fan
- Monitors and logs fan speed
- Monitors and logs ingress and egress temperatures
- Powers up and down power supplies
- Monitors and logs voltages, currents, and temperatures inside the chassis
- Detects presence, insertion, and removal of Cisco UCS B-Series blade servers
- Reads the IDs of the chassis, Cisco UCS B-Series blade servers, and IOM

https://t.me/learningnets

Another important component of the Cisco 2104 IOM is the chassis management switch. The chassis management switch provides connectivity to the Cisco Integrated Management Controller on each server blade. The chassis management switch has eight 100-Mb/s dedicated connections to the Cisco Integrated Management Controller. In addition, the chassis management switch has a 1 Gigabit Ethernet connection to the I/O MUX. The chassis management switch provides the vital connection to facilitate the monitoring and configuring of each blade server.

The I/O MUX provides a bridge between the server blades and the fabric interconnects. The I/O MUX is the ASIC that implements the data plane of the IOM.

The IO MUX provides the following:

- Eight 10 Gigabit Ethernet external downlink ports to the server blades
- Four 10 Gigabit Ethernet external uplink ports to the fabric interconnect
- 1 Gigabit Ethernet internal port to connect to the chassis management switch
- 100-Mb/s internal port toward the CMC

By default, mezzanine adapters that are installed on server blades are pinned to uplinks in a predetermined fashion.

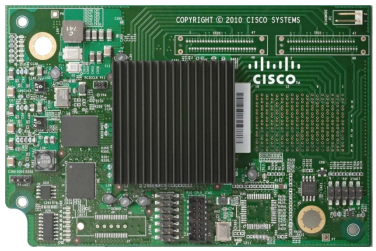
https://t.me/learningnets

Cisco UCS VIC 1280 and VIC 1240 Features

This topic describes the Cisco UCS VIC 1280 and VIC 1240 cards.

Cisco UCS VIC 1280

- 8 10-Gb/s FCoE ports
- PCIe Gen2 x 16 5-Gb/s host interface
- Hardware capable of 256 PCIe devices (8 reserved for internal use and operating system restrictions apply)
- Supports adaptor port channels with Cisco UCS 2208 IOM



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

The Cisco UCS VIC 1280 mezzanine adapter provides acceleration for the various new operational modes that are introduced by server virtualization. This mezzanine adapter is supported by all current Cisco UCS B-Series blade servers. The Cisco UCS VIC 1280 operates with other generation 2 hardware and requires Cisco 6200 Series Fabric Interconnects and the Cisco UCS 2208XP IOM.

In virtualized environments, this highly configurable adapter provides the following:

- Near-bare-metal I/O performance
- Ease of management
- Exceptional network visibility

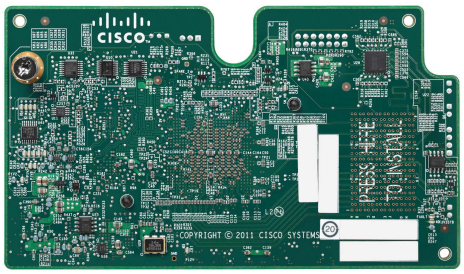
Feature	Description
Total interfaces	256
Interface type	Dynamic
Ethernet interfaces	0–256
Fibre Channel interfaces	0–256
Cisco VM-FEX	Hardware or software
Failover handling	Hardware, no driver needed

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS VIC 1240

- 4 10-Gb/s FCoE ports
- 8 10-Gb/s FCoE ports with optional port expander card
- PCIe Gen2 x 16 5-Gb/s host interface
- Hardware capable of 256 PCIe devices
- Supported only on Cisco UCS B200 M3 server



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

The Cisco UCS VIC 1240 mezzanine adapter provides four 10-Gb/s interfaces for the server. Two are connected through IOM A and the other two through IOM B. With the usage of an optional port expander card, there can be eight interfaces.

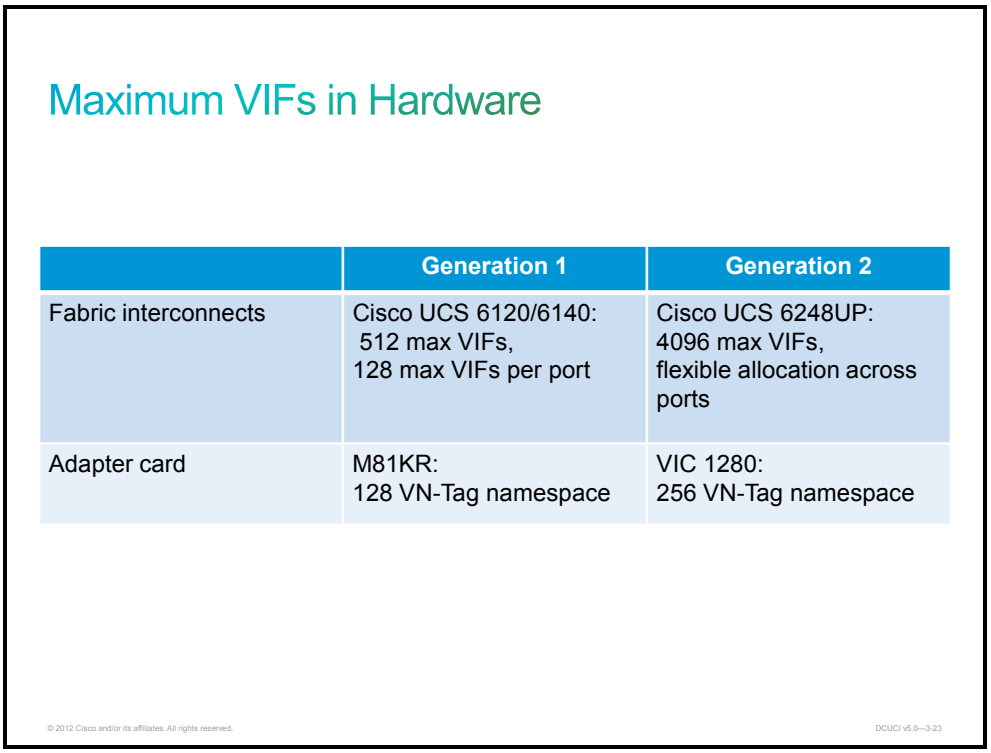
The Cisco UCS VIC 1240 currently can be used only with the Cisco UCS B200 M3 server.

The mezzanine adapter supports up to 256 Peripheral Component Interconnect Express (PCIe) devices (virtual network interface cards [vNICs] and virtual host bus adapters [vHBAs]) in hardware. The communication with the host is based on the PCIe generation 2 interface, providing for 5 Gb/s.

https://t.me/learningnets

Virtual Interfaces on Cisco UCS M81KR VIC and the VIC 1280

This topic describes the maximum virtual interfaces (VIFs) available for the creation of vNICs and vHBAs on the Cisco UCS MK81R and VIC 1280 cards.



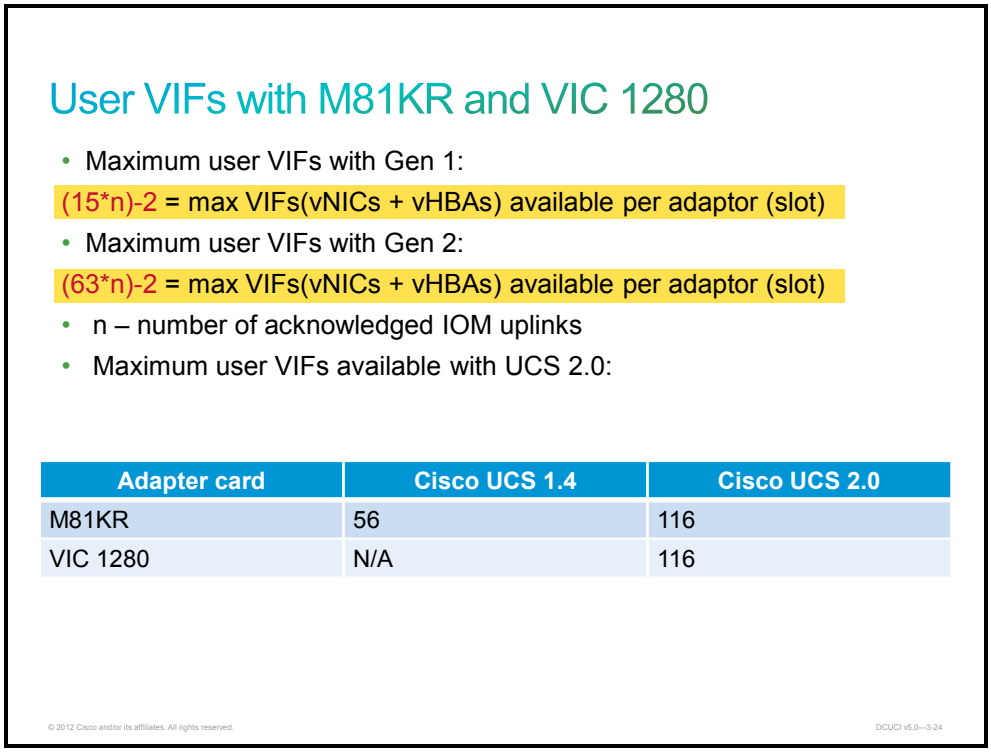
A maximum of 256 virtual PCIe adapters and interfaces (NICs and HBAs) can be created in the ASIC of the VIC 1280, which are presented to the operating system on the compute node. A maximum of 128 adapters can be created in the hardware of the M81KR.

Each of these interfaces is assigned a VIF ID that is controlled and accessed from the fabric interconnect and Cisco UCS Manager. The VIFs are used with the virtual network tag (VN-Tag) technology. The traffic to and from these interfaces is tagged with the corresponding VIF. The number of VIFs that can be used depends on the Cisco UCS version and the capability of the hardware and number of available uplinks between the fabric interconnect and the IOM.

With generation 1 fabric interconnects, such as the Cisco UCS 6120/6140, the maximum VIFs per fabric interconnect are limited to 512. Further, 128 VIFs can be allocated per port. With Cisco UCS 6248UP Fabric Interconnects, 4096 VIFs are supported per port, and there is flexible allocation.

The number of VIFs that are available depends on the number of vNICs and vHBAs that can be created on the VICs.

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



To calculate the available VIFs, use the following formulas. For generation 1 hardware, use this formula:

```
(15*n)-2=max user VIFs (vNICs+vHBAs)
```

In the formula, *n* stands for the number of uplinks between the Cisco UCS 2104 IOM and the 61x0 Fabric Interconnect.

For generation 2 hardware, use this formula:

```
(63*n)-2=max user VIFs
```

Again, *n* stands for the number of uplinks, but this time between the Cisco UCS 2208 IOM and the 6248UP Fabric Interconnect.

As mentioned, the actual number of VIFs depends on the Cisco UCS version. With version 1.4, the maximum user VIFs for the Cisco UCS M81KR was limited to 56. With version 2.0, the maximum number of VIFs supported on both M81KR and VIC 1280 is 116.

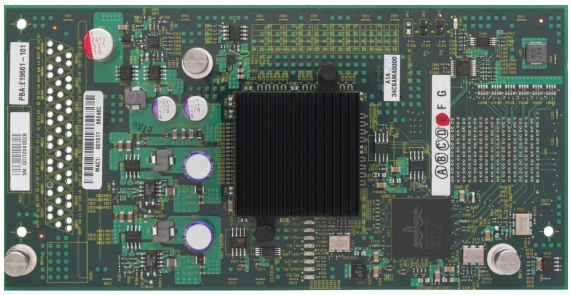
https://t.me/learningnets

New Mezzanine Cards

This topic describes the mezzanine cards available for Cisco UCS B-Series servers.

Cisco UCS M51KR-B 10 Gigabit Adapter

- The Cisco UCS M51KR-B is a dual-port 10-Gb/s Ethernet adapter.
- This adapter includes the TCP Offload Engine in hardware and allows iSCSI boot.



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

The Cisco UCS NIC M51KR-B Broadcom BCM57711 network adapter is a dual-port 10-Gb/s KR Ethernet network adapter and Internet Small Computer Systems Interface (iSCSI) HBA. This adapter features the hardware-based TCP Offload Engine and iSCSI offload. The Cisco UCS NIC M51KR-B supports iSCSI boot.

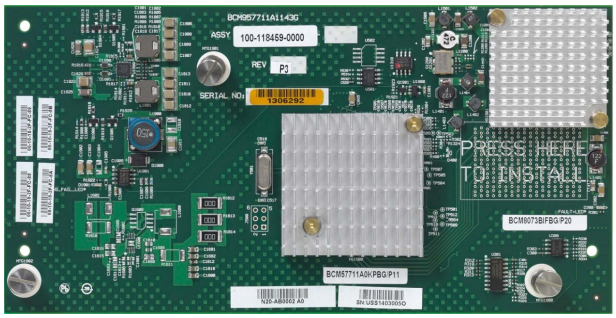
Feature	Description
Total interfaces	2
Interface type	Fixed
Ethernet interfaces	2
Fibre Channel interfaces	0
Cisco VM-FEX	Software
Failover handling	Software NIC bonding driver

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS M61KR-I CNA

- The Cisco UCS M61KR-I is a dual-port 10-Gb/s CNA.
- This adapter provides support for operating systems and hypervisors with software initiators to leverage FCoE.



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

The Cisco UCS Converged Network Adapter (CNA) M61KR-I includes enhancements for virtualized I/O and unified fabric. Intel Virtualization Technology for Connectivity, including Virtual Machine Device Queues (VMDq) and Peripheral Component Interconnect Special Interest Group (PCI-SIG) Single-Root I/O Virtualization (SR-IOV), delivers near-native 10-Gb throughput in virtualized servers while reducing hypervisor CPU utilization. Hardware-based acceleration and support for native operating system FCoE and iSCSI initiators facilitate simple, scalable, and unified networking performance.

Feature	Description
Total interfaces	2
Interface type	Fixed
Ethernet interfaces	2
Fibre Channel interfaces	*0
Cisco VM-FEX	Software
Failover handling	Intel NIC teaming driver

Note Although hardware-based FCoE is not provided, software FCoE initiators are available for select operating systems and hypervisors. Fibre Channel traffic is processed by the host CPU and not on the adapter.

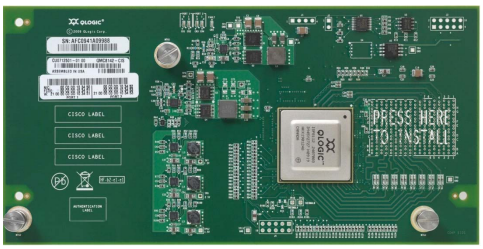
https://t.me/learningnets

Cisco UCS M72KR-E and M72KR-Q CNA

- The Cisco UCS M72KR-E and M72KR-Q are dual-port 10-Gb/s, CNA-based Emulex or QLogic ASICs.
- Both adapters offer much lower power consumption and generate less heat than Generation 1 CNAs.
- Both adapters process FCoE in hardware to provide excellent Fibre Channel performance.

M72KR-E

M72KR-Q



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

The Cisco UCS M21KR-E and M72KR-Q CNAs are Emulex- or QLogic-based FCoE mezzanine cards that provide10 Gigabit Ethernet and 4-Gb Fibre Channel connectivity for Cisco UCS B-Series blades.

These generation 2 CNAs use Emulex or QLogic ASICs that combine 10 Gigabit Ethernet and Fibre Channel hardware in a single ASIC. Generation 2 CNAs feature much lower power consumption and generate less heat than their generation 1 counterparts.

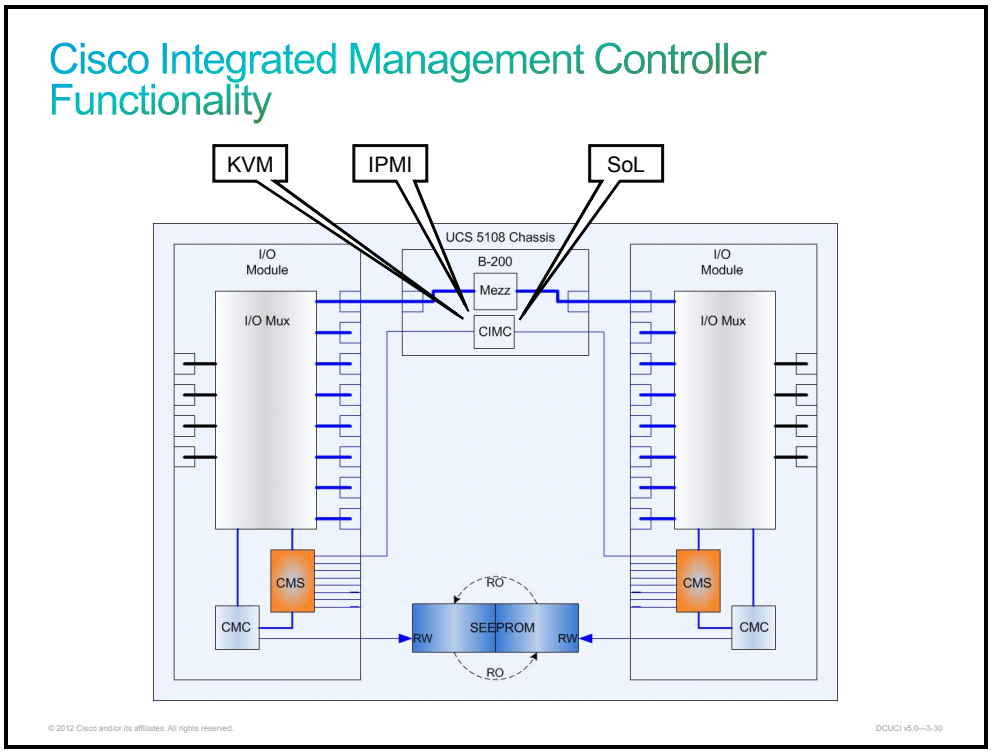
Feature	Description
Total interfaces	2
Interface type	Fixed
Ethernet interfaces	2
Fibre Channel interfaces	2
Cisco VM-FEX	Software
Failover handling	Software NIC bonding driver

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco Integrated Management Controller in Cisco UCS B-Series Blade Servers

This topic describes the Cisco Integrated Management Controller component of B-Series blades.



The Cisco Integrated Management Controller is a chip on the motherboard of each blade server. The Cisco Integrated Management Controller provides for thermal, power, and general health monitoring of the blade. This data is polled by the CMC and relayed to Cisco UCS Manager.

Cisco Integrated Management Controller also enables keyboard, video, mouse (keyboard, video, mouse [KVM]) over IP, Serial over LAN (SoL), and an IPMI 2.0-compliant interface.

KVM over IP allows Cisco UCS administrators to connect remotely to the console of any server in the Cisco UCS system with KVM control.

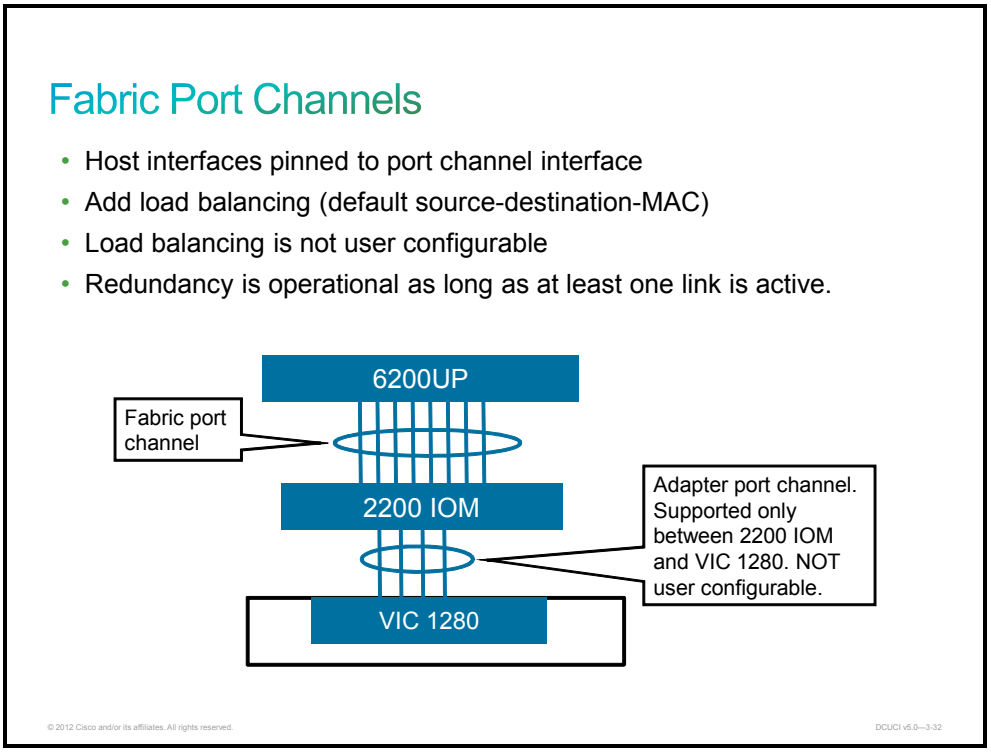
SoL allows an external UDP connection to the serial console port.

IPMI provides external access to the Cisco Integrated Management Controller, even if the server is powered off in standby mode. IPMI connections can poll sensors on the blade and power control. A server can be remotely powered on or off via IPMI.

https://t.me/learningnets

Creating Port Channels with Generation 2 Hardware

This topic describes fabric port channels with second-generation hardware.



With generation 2 hardware only, you can enable Cisco UCS Manager to create port channels between the Cisco UCS 6200UP Fabric Interconnect and the Cisco UCS 2200XP IOM.

The following are benefits of combining the uplinks into a port channel interface:

- The host interfaces are pinned to the port channel interface. The interface will be operational as long as at least one uplink is active.
- The traffic for the host interfaces is load balanced, based on the source-destination-MAC load-balancing scheme. The load-balancing scheme cannot be changed and is not user configurable.

Further, the use of Cisco UCS VIC 1280 also supports adapter port channels. The adapter port channels are internal and combine the interfaces between the VIC 1280 and the Cisco UCS 2208 IOM. This feature is not user configurable. Based on the hardware present, the system will immediately create adapter port channels.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Fabric Port Channel Support Matrix

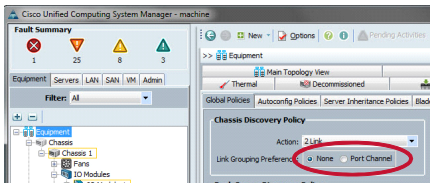
Fabric Interconnect	IOM	Fabric Port Channel	Bandwidth
6120/6140	2204XP	No	Up to 40 Gb/s
	2208XP	No	Up to 40 Gb/s
6248/6296UP	2204XP	Yes	Up to 40 Gb/s
	2208XP	Yes	Up to 80 Gb/s

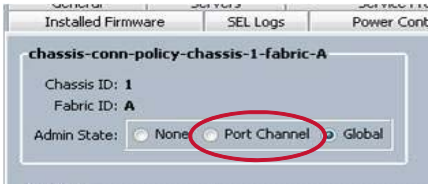
© 2012 Cisco and/or its affiliates. All rights reserved.

The fabric port channels are supported only between Cisco UCS 6200UP and 2200XP IOM.

Fabric Port Channel Configuration

- Global configuration: chassis discovery policy
- Chassis-specific configuration: connectivity policy
- Cisco UCS Manager automatically creates the fabric port channel based on chassis discovery policy, connectivity policy, and hardware compatibility.





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

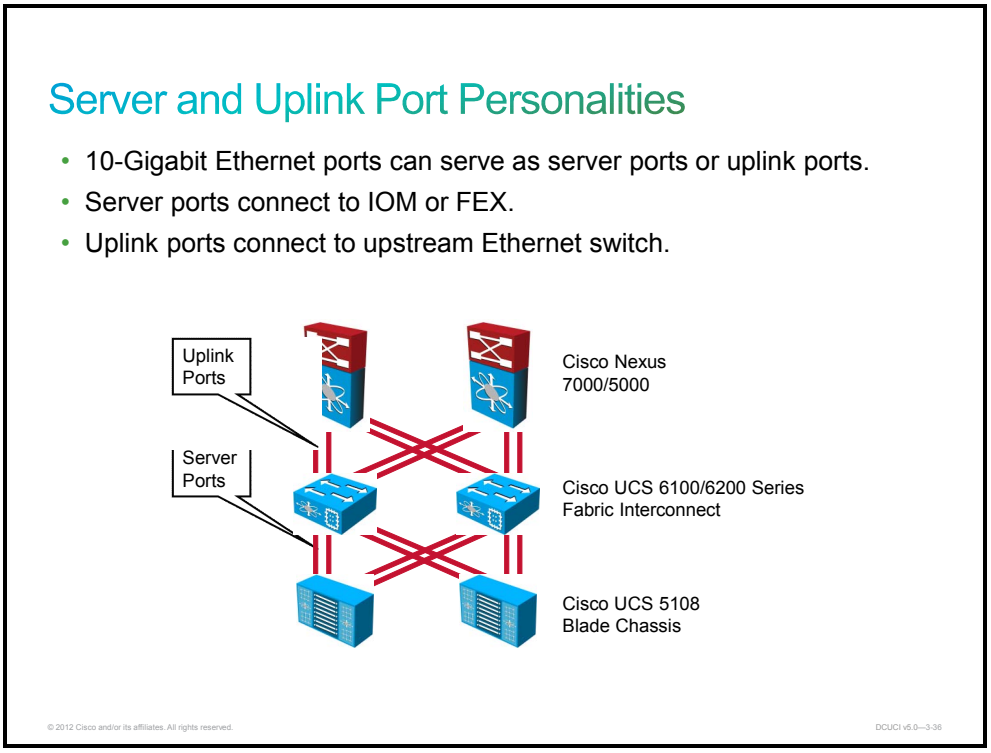
The creation of fabric port channels is done by Cisco UCS Manager. Whether the system will create fabric port channels depends on two settings:

- **Global:** The link grouping preference in the chassis discovery policy must be set to Port Channel.
- **Chassis-specific:** The admin state for the connectivity policy for the chassis must be set to Port Channel.

https://t.me/learningnets

Server and Uplink Port Personalities in the Cisco UCS Fabric Interconnect

This topic describes the server and uplink port personalities in the fabric interconnect.



Ethernet ports on the fabric interconnect can be in one of five states: unconfigured, server, uplink, appliance, or FCoE. By default, all Ethernet ports on the fabric interconnect are unconfigured.

An Ethernet port is configured as a server port when it will be used to provide connectivity for an IOM or for a Cisco Nexus 2000 Series Fabric Extender (FEX). The server port manages the traffic to and from the servers.

On Cisco UCS 61x0 Fabric Interconnects, you can configure only the fixed ports as server ports. On Cisco UCS 6248UP, there is no such restriction.

An Ethernet port will be configured as an uplink port when it will be connected to an upstream Ethernet switch.

© 2012 Cisco Systems, Inc.

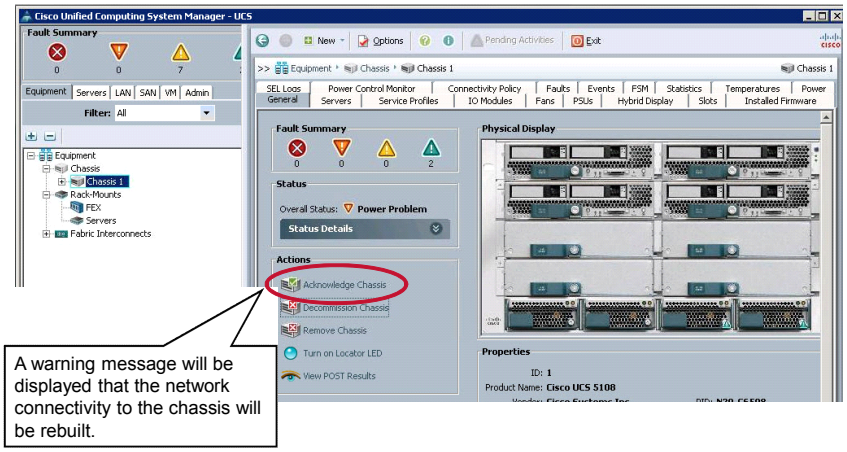
https://t.me/learningnets

Chassis Discovery Process

This topic describes the chassis discovery process and how to monitor it.

Acknowledge Chassis

- Navigate to **Equipment > Chassis 1 > Actions > Acknowledge Chassis**.



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

Chassis discovery occurs when a chassis is initially connected to the fabric interconnect and Cisco UCS Manager detects that a new server link has become active. A connection is made to the CMC. The CMC sends information about the chassis inventory (IOM, fans, power supplies, serial numbers, part IDs, and so on) to Cisco UCS Manager.

If server presence is detected, the inventory of the server (or servers) will be sent to Cisco UCS Manager. The details of the inventory include serial number, vendors, CPU type, installed DIMMs, adapter cards, hard drives, BIOS, and Cisco Integrated Management Controller.

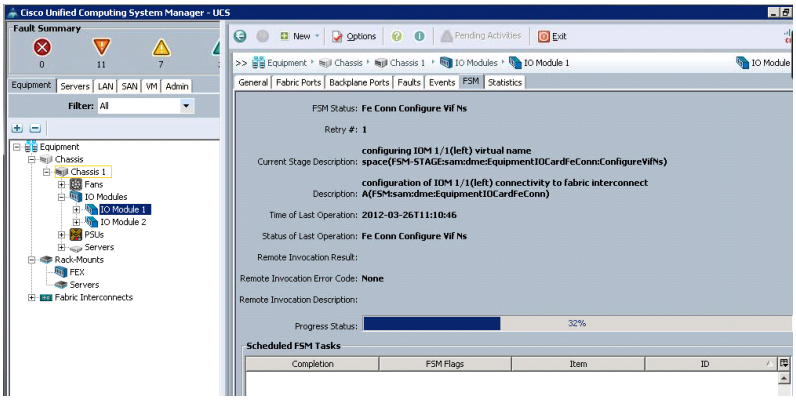
All the inventory details are stored as managed objects by the data management engine (DME).

To observe chassis discovery, you can reacknowledge the chassis and monitor the process.

https://t.me/learningnets

Monitor Discovery in FSM

- Navigate to **Equipment > Chassis 1 > IO Module 1 > FSM**.



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

After the chassis has been reacknowledged, you can watch the process in the FSM tab of either IOM.

A finite state machine (FSM) is a series of logical transitions that occur in a specific order. The chassis and server discovery processes are examples of where an FSM is used to validate a complex series of events.

 © 2012 Cisco Systems, Inc.

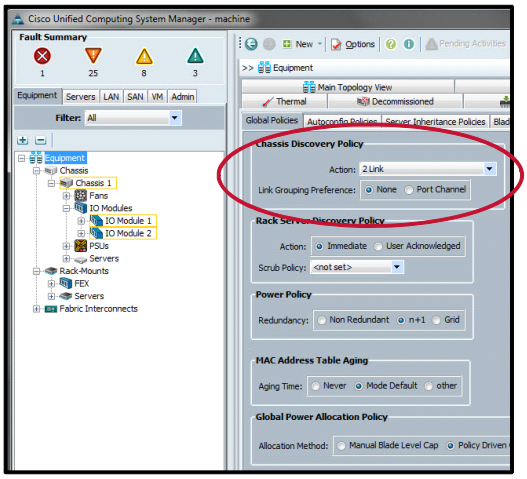
https://t.me/learningnets

Configuring the Chassis Discovery Policy

This topic describes chassis discovery policy provisioning.

Chassis Discovery Policy

- The chassis discovery policy is global for all chassis.
- Navigate to **Equipment > Equipment > Policies > Global Policies**.
- Set the discovery option for new chassis.
- A chassis that is not connected with the minimum required topology will not be discovered.
- Enable or disable creation of fabric port channels.



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

The chassis discovery policy is a global policy for all chassis that are connected to the fabric interconnects. The policy sets the minimum number of IOM links required for chassis discovery.

The policy is flexible to allow either a uniform number of links or a mixed number of links per chassis. The recommended configuration is to set the chassis discovery policy to the lowest number of IOM links allowed on any chassis.

As an example, if you set the policy to one link, a chassis with four links would initially be discovered as a one-link chassis. After you reacknowledge that chassis, the remaining three links would be recognized and become available to service blade servers.

The available policies are 1-Link, 2-Link, 4-Link, 8-Link, and Platform-Max. The Platform-Max policy is used in mixed environments where you have generation 1 and generation 2 hardware. That policy insures that the maximum available uplinks for the hardware will be discovered.

Another available option is Link Grouping. This option is used to instruct the system whether to create port channels if the appropriate hardware is available.

https://t.me/learningnets

Number of Actual Links	1-Link Policy	2-Link Policy	4-Link Policy	8-Link Policy	Platform-Max Policy
1 link to IOM	Chassis are discovered as a 1-link topology.	Chassis will not be discovered.	Chassis will not be discovered.	Chassis will not be discovered.	Chassis discovered and added with 1-link topology.
2 links to IOM	Chassis are discovered initially as a 1-link topology. After chassis reacknowledge, two links active.	Chassis are discovered as a 2-link topology.	Chassis will not be discovered.	Chassis will not be discovered.	Chassis will not be discovered.
4 links to IOM	Chassis are discovered initially as a 1-link topology. After chassis reacknowledge, 4 links active.	Chassis are discovered initially as a 2-link topology. After chassis reacknowledge, 4 links active.	Chassis are discovered as a 4-link topology.	Chassis will not be discovered.	If the IOM has 4 links, then the chassis is discovered. If the IOM has 8 links, then the chassis is not discovered.
8 links to IOM	Chassis are discovered initially as a 1-link topology. After chassis reacknowledge, 8 links active.	Chassis are discovered initially as a 1-link topology. After chassis reacknowledge, 8 links active.	Chassis are discovered initially as a 1-link topology. After chassis reacknowledge, 8 links active.	Chassis will be discovered as an 8-link topology.	Chassis is discovered as 8-link topology.

To set the chassis discovery policy, navigate to **Equipment > Policies > Global Policies**.

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

Summary

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

Summary

- With generation 2 hardware, the oversubscription ratio can reach up to 4:1. With fabric port channel, the internal slots are statically pinned to the port channel interface.
- Cisco UCS 2204/2208XP I/O consists of CMC, I/O MUX, chassis management switch, and the debug dongle interface.
- Cisco UCS 2104XP IOM consists of the CMC, chassis management switch, and I/O MUX.
- The oversubscription ratio with fully populated chassis with generation 1 hardware can reach up to 2:1.
- Cisco UCS VIC 1280 provides for up to 256 VN-Tags in hardware. Cisco VIC 1240 provides four 10-Gb/s interfaces.
- M81KR provides for up to 128 VN-Tags in hardware. The M81KR and VIC 1280 are limited by the Cisco UCS to up to 116 user VIFs.
- There are a variety of mezzanine cards including M51, M61, and M72. M51 and M61 provide limited software support only for FCoE. M72 is the second generation of M71 CNAs.
- The Cisco Integrated Management Controller management component of the B-Series blades provides management communication to the server for the administrator and Cisco UCS Manager.
- Fabric port channels can be created only between Cisco UCS 6200UP and 2200 IOM.
- Server ports on the fabric interconnect are used to connect the IOM or FEX, while the uplink ports are used to connect to an upstream Ethernet switch.
- The chassis discovery process depends on the settings of the chassis discovery policy. The progress can be monitored in the FSM tab.
- The chassis discovery policy defines how the Cisco UCS Manager will discover the chassis.

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

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 2

Installing Cisco UCS B-Series Hardware

Overview

Only properly trained individuals should install Cisco Unified Computing System (UCS) B-Series servers. Installation by trained individuals ensures the safety of installation personnel, reliable operation, and ease of maintenance. Failure to follow installation procedures can result in serious bodily injury or death.

Implementers need to establish that the site is prepared, power is provisioned, and all environmental requirements are met before installation can begin.

Objectives

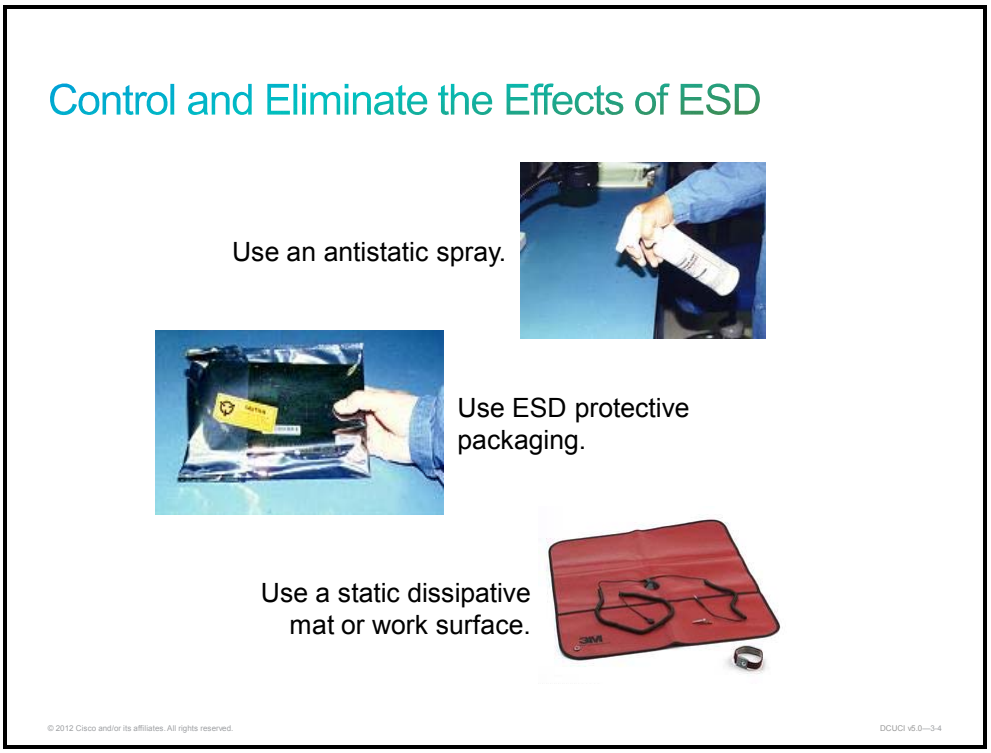
Upon completing this lesson, you will be able to install and power up Cisco UCS B-Series hardware. This ability includes being able to meet these objectives:

- Describe the ESD precautions that are necessary when installing Cisco UCS B-Series components
- List the steps for opening the case of half- and full-slot blade servers
- List the steps for physical installation of rack-mount slides in the enclosure and on the Cisco UCS 5108 chassis
- List the steps for installation and removal of CPU, RAM, and mezzanine cards in Cisco UCS B-Series blade servers
- List the steps for physical installation and removal of local hard drives
- List the steps for physical installation of half- and full-slot blade servers
- List the steps for physical installation of IOMs and power supplies in the Cisco UCS 5108 chassis
- List the steps for physical installation and removal of fan units
- List the steps for physical installation and removal of SFP+ copper twinax and optical modules

https://t.me/learningnets

ESD Precautions for Installing Cisco UCS B-Series Components

This topic describes the ESD precautions that are necessary when working with B-Series components.



ESD from your skin, hair, or clothing can degrade or destroy components of the Cisco UCS B-Series blade servers and I/O modules (IOMs). When a nonconductor and conductor make and break contact, a charge is formed on the conductor. If you rub a plastic comb across wool fabric, enough static charge is formed to make your hair move when the comb gets close. If you touch a doorknob and can feel the shock, the power that was discharged into the doorknob was at least 3000 V. There are components in blade servers that can be damaged or rendered nonfunctional by less than 100 V.

Observe proper ESD precautions whenever you open a blade server. Precautions include wearing a grounded wrist strap and handling components on a static-dissipative work surface. Your data center equipment staging area should have the proper grounded surfaces.

Follow these basic precautions:

- Only remove components from static-shielded bags on a static-safe work surface.
- Follow the site policy for ESD precautions by wearing a wrist strap (and heel strap if required).
- Use antistatic sprays.
- Roll up long-sleeved shirts.
- Tie-back long hair so it cannot make contact with the equipment.
- Remove any jewelry that could dangle onto the equipment.
- If wearing a necktie, tuck it into your shirt.

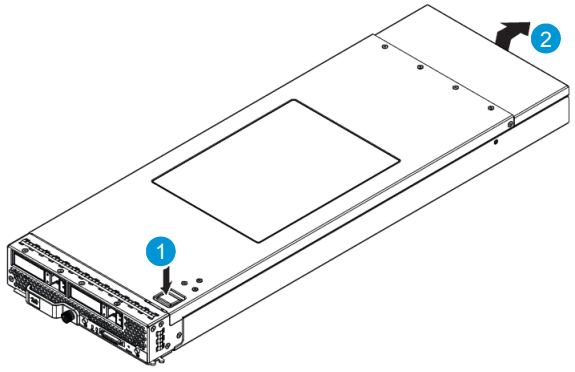
© 2012 Cisco Systems, Inc.
https://t.me/learningnets

Open Half- and Full-Slot Blade Server Cases

This topic describes the steps to remove the covers of the Cisco UCS B-Series servers.

Opening the Cisco UCS B200 M3 Blade Server

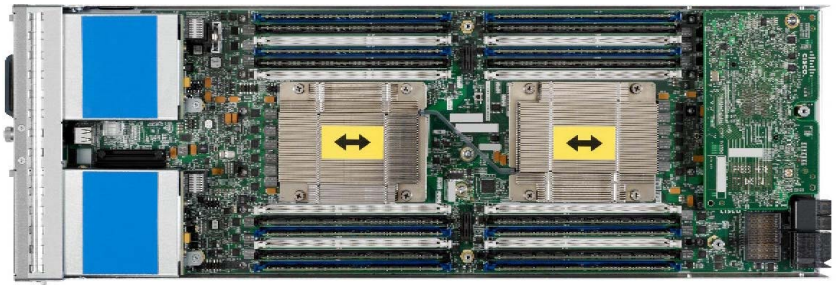
- Before opening the cover, place the server on an ESD-safe work surface and wear a grounded wrist strap.
- Push the button near the front of the case top and slide the cover toward the rear and up.



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

The Cisco UCS B200 M3 model comes with two removable baffles that guide airflow over the DIMMs more efficiently. The baffles are important because the cooling of the server is passive. The baffles help achieve optimum air flows. The baffles drop in with no tooling required.

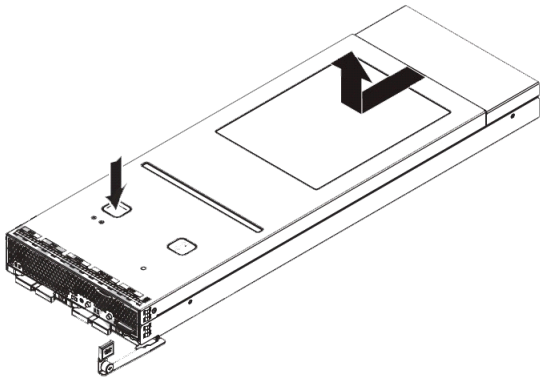
The baffles need to be lifted out to install or remove the CPU and DIMMs. Be certain to replace the baffles before closing the case.



https://t.me/learningnets

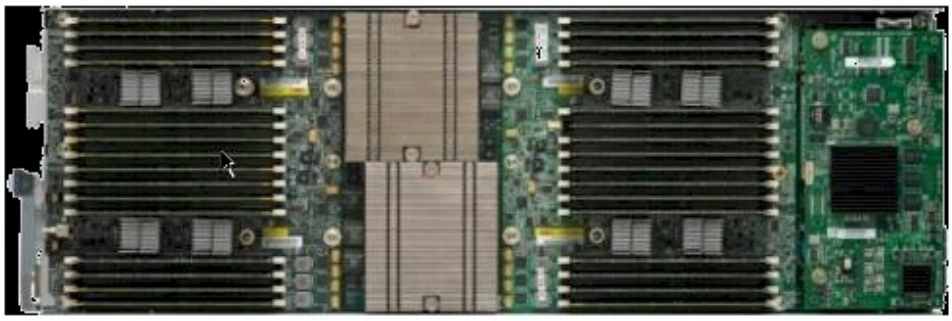
Opening the Cisco UCS B230 M2 Blade Server

- Before opening the cover, place the server on an ESD-safe work surface and wear a grounded wrist strap.
- With the server front facing you, push the button near the front left of the case top and slide the cover toward you and up.



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

The Cisco UCS B230 blade server differs significantly from the B200 M3 blade server. Although the B230 includes two CPU sockets, there are 32 DIMM slots. With the increased density of components on the motherboard, additional care should be taken when installing and removing field-replaceable units (FRUs).

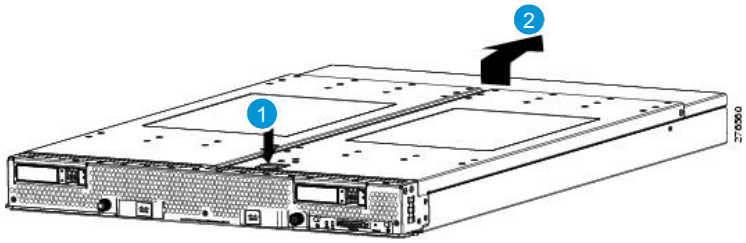


 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

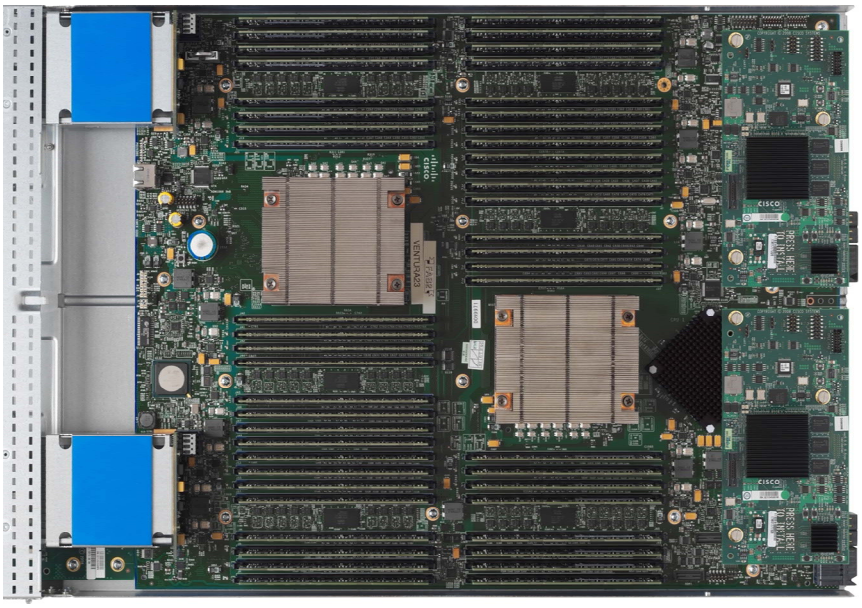
Opening the Cisco UCS B250 M2 Blade Server

- Before opening the cover, place the server on an ESD-safe work surface and wear a grounded wrist strap.
- With the server front facing you, push the button near the front center of the case top. Then slide the cover toward the rear and up.



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

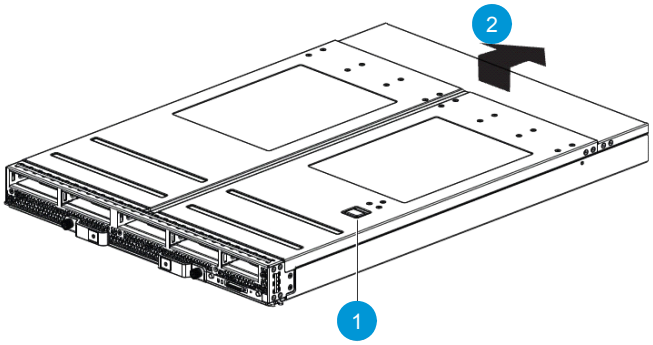
The Cisco UCS B250 M2 is a full-width, two-CPU socket server. The B250 M2 provides 48 DIMMs for up to 384-GB memory and can accommodate up to two mezzanine adapters. The local storage can be formed from up to two internal serial-attached SCSI (SAS) or solid-state drives (SSDs).



https://t.me/learningnets

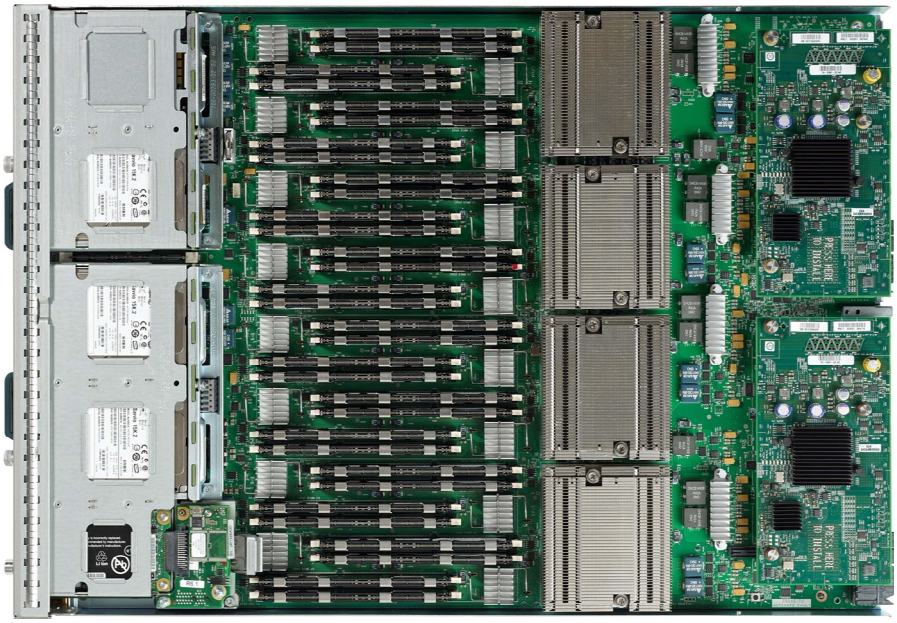
Opening the Cisco UCS B440 M2 Blade Server

- Before opening the cover, place the server on an ESD-safe work surface and wear a grounded wrist strap.
- With the server front facing you, push the button near the front right of the case top. Then slide the cover toward the rear and up.



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

Cisco UCS B440 M2 is a four-CPU, full-width server. The B440 M2 has 32 DIMMs for up to 1 TB of memory. The B440 M2 can have up to two mezzanine adapters and can use up to four internal SAS or SSD drives.



 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Install Rack-Mount Slides

This topic describes the steps to physically mount the Cisco UCS 5108 chassis in a rack.

Unpacking the Cisco UCS 5108 Chassis

- The chassis is pallet-mounted.
- An empty chassis weighs 90 lb (40.83 kg).
- The chassis requires at least two persons to lift.

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

The Cisco UCS 5108 chassis is pallet-mounted. Follow this procedure to unpack the empty chassis:

Step 1 Before accepting receipt of the shipment, carefully inspect the box for damage. If there is evidence of rough handling, reject the shipment and work with your shipper to file a damaged-in-transit claim. Signs of rough handling include a broken pallet, smashed corners, or large holes.

Step 2 Move the pallet as close as possible to your data center staging area.

Step 3 Cut the straps that secure the outer cardboard shell.

Step 4 Lift the outer shell straight up and off.

Step 5 Remove accessory boxes and packing material.

Step 6 Use at least two persons to lift the chassis out of the box.

Note Do not use the handles on the side of the chassis to lift. They were designed for repositioning the chassis only.

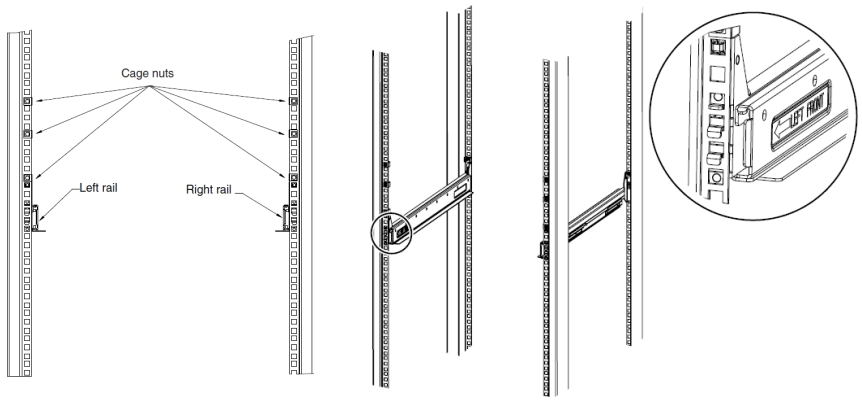
Step 7 Remove power supplies from the bottom of the box.

Step 8 Retain all shipping materials in case you need to ship the unit.

https://t.me/learningnets

Install Rack Rails in Rack or Cabinet

- Use the rack spacing template to mark correct placement of rack rails and cage nuts.
- Extend tool-less rails into the square mounting holes by sliding to fit the depth of the rack.



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

Follow this procedure to install the chassis rack rails:

Step 1 Use the supplied paper template to mark the holes on all rails of the rack where the tool-less rails and cage nuts will be installed.

Step 2 Extend the tool-less rails and attach to the square mounting holes in the rack or cabinet. (Rack rails are clearly marked left and right.)

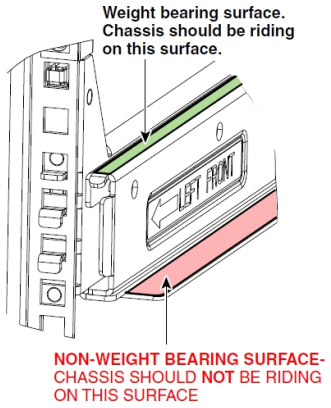
Step 3 Install cage nuts where indicated by the template.

Step 4 Use a level to be sure that the rail is installed correctly.

https://t.me/learningnets

Load-Bearing Member of Chassis Rail

- Be certain that the chassis is installed on the weight-bearing surface of the rail.
- Improper placement can result in severe injury to personnel and damage to the chassis.



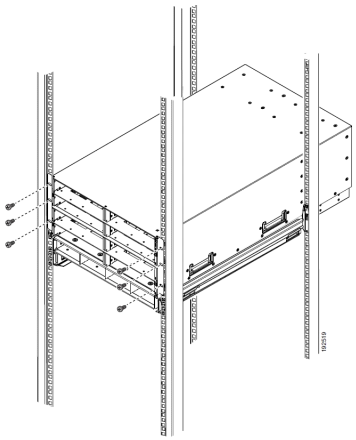
© 2012 Cisco and/or its affiliates. All rights reserved.

Ensure that the chassis is mounted on the load-bearing portion of the rail. Serious injury and equipment damage can result from improper positioning.

https://t.me/learningnets

Install Cisco UCS 5108 Chassis on the Rack Rails

- At least two persons are required to lift the chassis onto the rails. A server jack will greatly reduce the effort to install.
- Secure the chassis using supplied screws.



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

Follow this procedure to install the Cisco UCS 5108 chassis into the rack or cabinet:

Step 1 If the rack or cabinet is on casters, employ the wheel brakes.

Step 2 Using at least two persons, slide the chassis onto the load-bearing portion of the rack rails.

Step 3 Install the six 10-32 x 0.75-inch Phillips round washer-head screws into the cage nuts.

Step 4 Torque the screws to no more than 20 ft-lb (27 Newton meters).

 © 2012 Cisco Systems, Inc.

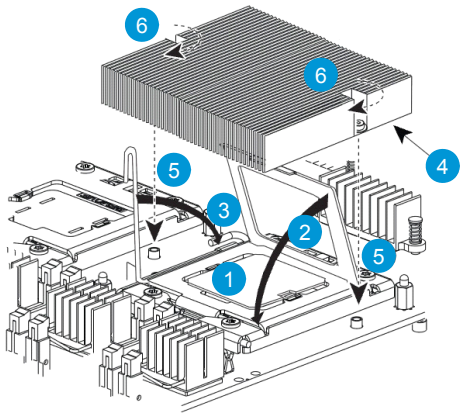
https://t.me/learningnets

Install and Remove CPU, RAM, and Mezzanine Cards

This topic shows how to install and remove components from the B-Series servers.

Install CPU into Cisco UCS B-Series Blade Servers

- Place the server on an ESD-safe work surface and wear a grounded wrist strap whenever working inside the server.
- Handle CPU by the edges only and move to static-shielded bag or box.



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

Follow this procedure to install a CPU into a Cisco UCS B-Series blade server:

Step 1 Wear a wrist strap that is grounded to the blade server.

Step 2 Slide the CPU locking clasp down and to the side to release it (3, in the figure).

Step 3 Move the latch up until it is at a 90-degree angle with the CPU socket (2).

Step 4 Swing the CPU mounting bracket up and remove the CPU cover blank (4).

Step 5 Align the CPU with the socket, which should only fit one way.

Step 6 Lower the mounting bracket and socket latch and secure the CPU.

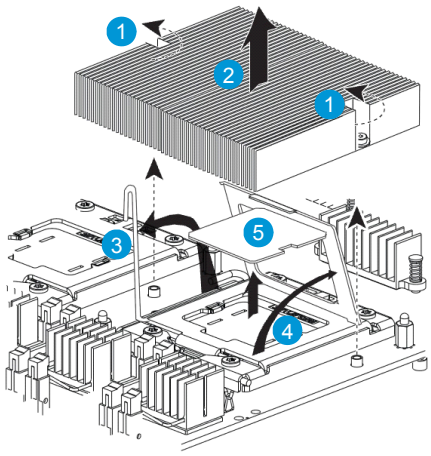
Step 7 Align the heat sink so that the cooling slots face front-to-back. Air must flow through the heat sink.

Step 8 Carefully tighten the heat-sink screws to the motherboard (6). Do not overtighten.

https://t.me/learningnets

Remove CPU from Cisco UCS B-Series Blade Servers

- Place the server on an ESD-safe work surface and wear a grounded wrist strap whenever working inside the server.

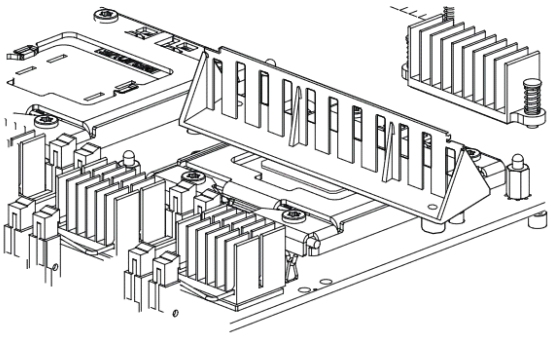


© 2012 Cisco and/or its affiliates. All rights reserved.

The CPU removal process is the reverse of the installation process. Be certain to replace the socket blank over the socket if you do not plan on replacing the CPU. Failure to use the socket cover can result in damage to the socket.

Install CPU Air Blocker into Cisco UCS B440 Blade Server

- If you remove a CPU and leave an empty socket, be sure to install a CPU air blocker to maintain proper internal cooling.



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

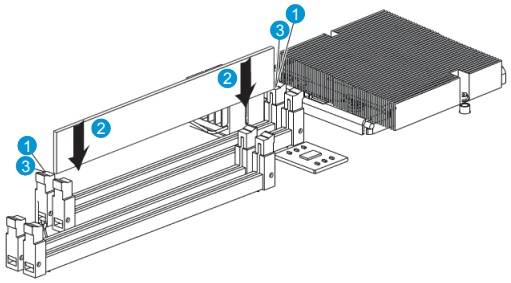
If you have removed a CPU from a Cisco UCS B440 server and do not intend to replace it, you must install an air blocker. The air blocker will allow proper airflow over the components within the blade enclosure.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Install RAM into Cisco UCS B-Series Servers

- Place the server on an ESD-safe work surface and wear a grounded wrist strap whenever working inside the server.
- Handle DIMMs by the edges of the module and do not touch the chips or contacts.



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

Follow this procedure to install DIMMs in any Cisco UCS B-Series server:

Step 1 Wear a wrist strap that is grounded to the blade server enclosure.

Step 2 Open the case.

Step 3 Fold the DIMM retainer clips away from the center of the DIMM slot (1, in the figure).

Step 4 Align the DIMM notch on the bottom of the module with the key in the slot.

Step 5 Push straight down with even pressure on both sides of the DIMM until it is firmly seated (2).

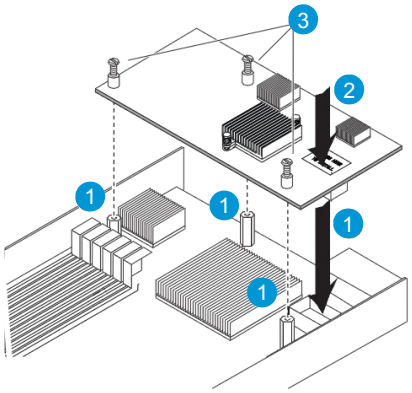
Step 6 Fold the retainer clips toward the center of the DIMM slot (3).

To remove a DIMM, reverse the process.

https://t.me/learningnets

Install Mezzanine Card into Cisco UCS B200 M3 and B230 M2 Blade Servers

- Place the server on an ESD-safe work surface and wear a grounded wrist strap whenever working inside the server.
- Handle mezzanine cards by their edges and avoid touching any component on the card. Press only on the designated point to seat the connector.



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

To install a mezzanine card in a Cisco UCS B200 or B230 blade server, follow this procedure:

Step 1 Wear a wrist strap that is grounded to the blade server enclosure.

Step 2 Open the case (1, in the figure).

Step 3 Handle the card by the edges and align the large Molex connector on the bottom of the module with the receptacle on the motherboard (2).

Step 4 The silkscreen on the card is conspicuously marked “Press Here to Install.” Press down on the marking until the card is fully seated (2).

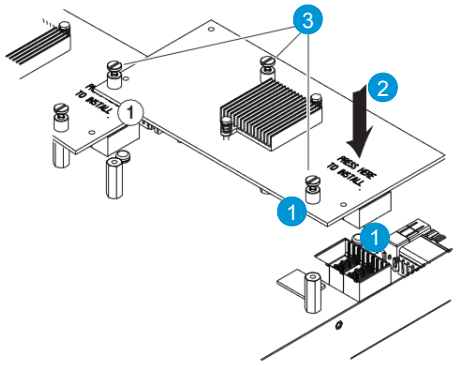
Step 5 Use your fingers only to secure the three captive screws (3). Do not overtighten.

To remove a mezzanine card, reverse the process.

https://t.me/learningnets

Install Mezzanine Card into Cisco UCS B250 M2 and B440 M2 Blade Servers

- Place the server on an ESD-safe work surface and wear a grounded wrist strap whenever working inside the server.
- Handle mezzanine cards by the edges of the card and avoid touching any component on the card. Press only on designated point to seat the connector.



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

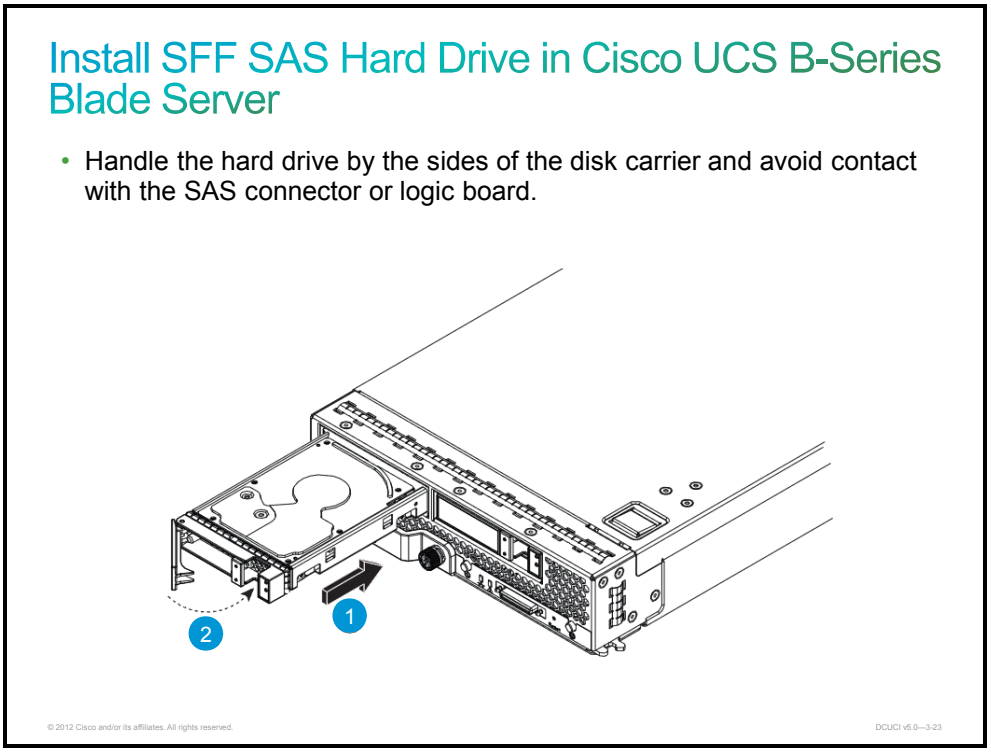
The procedure to install or remove mezzanine cards in the Cisco UCS B250 and B440 blade servers is identical to the procedure used with the Cisco UCS B200 and B230 blade servers. There are, however, version-specific rules for populating the adapters.

In Cisco UCS version 1.2, two adapters can be installed, but they must be the same type. Beginning with Cisco UCS version 1.3, two adapters can be installed and can be different types.

https://t.me/learningnets

Install and Remove Local Hard Drives

This topic describes how to install and remove hard drives.



To install a small form-factor (SFF) SAS drive into Cisco UCS B200, B250, or B440 blade servers, follow this procedure:

Step 1 Wear a wrist strap that is grounded to the blade server enclosure or chassis.

Step 2 Press the release catch on the ejector arm.

Step 3 Slide the hard drive carrier into the slot until fully seated (1, in the figure).

Step 4 Slide the ejector lever into the faceplate until it clicks into the locked position (2).

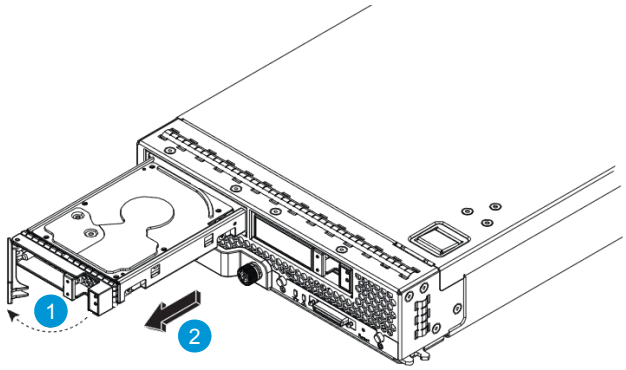
Note Cisco UCS B230 M2 supports only SSD drives. Cisco UCS B200 M3, B250 M2, and B440 M2 support both SAS and SSD drives.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Remove SFF SAS Hard Drive from Cisco UCS B-Series Blade Server

- Handle the hard drive by the sides of the disk carrier and avoid contact with the SAS connector or logic board.
- Place on an ESD-safe work surface or in a static-shielded bag.



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

To remove an SFF SAS drive from a Cisco UCS B200, B250, or B440, follow this procedure:

Step 1 Wear a wrist strap that is grounded to the blade server enclosure or chassis.

Step 2 Press the release catch on the ejector arm and swing it away from the hard drive faceplate (1, in the figure).

Step 3 Slide the hard drive carrier out of the slot (2).

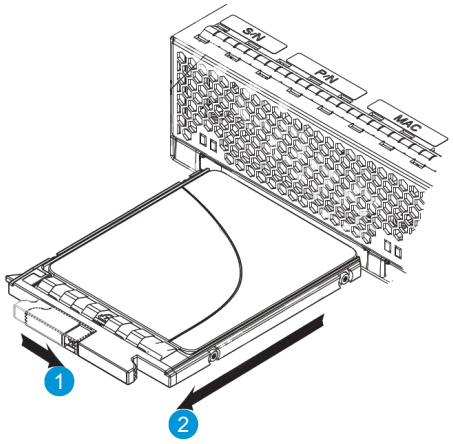
Step 4 Store in a static-shielded bag or enclosure.

Note If you do not plan on replacing the removed hard drive, install a blanking plate to maintain proper airflow through the server.

https://t.me/learningnets

Remove SSD Hard Drive in Cisco UCS B-Series Blade Server

- Handle the hard drive by the sides of the disk carrier and avoid contact with the SSD connector or logic board.
- Squeeze the drive catch to insert or release the carrier from the blade.



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

To remove an SSD drive from a Cisco UCS B230 blade server, follow this procedure:

Step 1 Wear a wrist strap that is grounded to the blade server enclosure or chassis.

Step 2 Press the release catch on the SSD carrier (1, in the figure).

Step 3 Slide the SSD carrier out of the slot (2).

Step 4 Store in a static-shielded bag or enclosure.

Note	If you do not plan on replacing the removed SSD, install a blanking plate to maintain proper airflow through the server.

 © 2012 Cisco Systems, Inc.

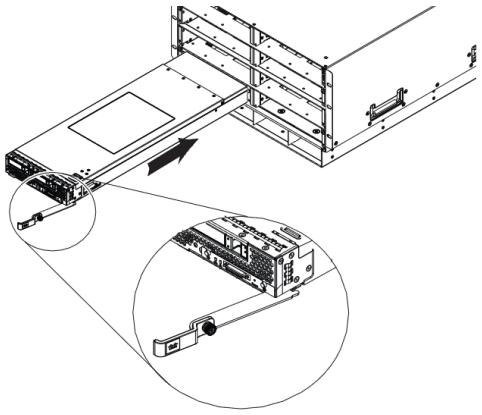
https://t.me/learningnets

Install Half- and Full-Slot Blade Servers

This topic describes how to install in the rack half- and full-width Cisco UCS B-Series servers.

Insert B200 M3 Blade into the Cisco UCS 5108 Chassis

- Hold the blade by its outer shell and slide it into the chassis slot.
- Swing the ejector lever to the left until it makes contact with the faceplate of the blade and use your fingers only to tighten the captive screw.



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

To install a Cisco UCS B200 M3 blade into the Cisco UCS 5108 chassis, perform these steps:

Step 1 Remove the blanking plate, if present.

Step 2 Wear an ESD strap that is grounded to the chassis.

Step 3 Open the ejector lever on the right front of the blade server.

Step 4 Slide the blade into the opening until you cannot push it any farther.

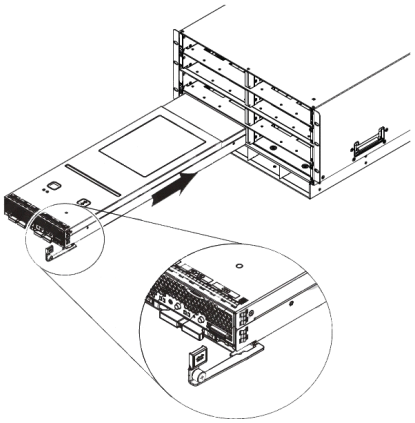
Step 5 Swing the ejector lever toward the faceplate so that it engages the edge of the chassis and press the blade server all the way in.

Step 6 Use your fingers only to tighten the captive screw on the front of the blade to no more than 3 in-lbs.

https://t.me/learningnets

Insert B230 M2 Blade into the Cisco UCS 5108 Chassis

- Hold the blade by its outer shell and slide it into the chassis slot.
- Swing the ejector lever to the left until it makes contact with the faceplate of the blade and use your fingers only to tighten the captive screw.



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

To install a Cisco UCS B230 M2 blade into the Cisco UCS 5108 chassis, perform these steps:

Step 1 Remove the blanking plate, if present.

Step 2 Wear an ESD wrist strap that is grounded to the chassis.

Step 3 Open the ejector lever on the right front of the blade server.

Step 4 Slide the blade into the opening until you cannot push it any farther.

Step 5 Swing the ejector lever toward the faceplate so that it engages the edge of the chassis and press the blade server all the way in.

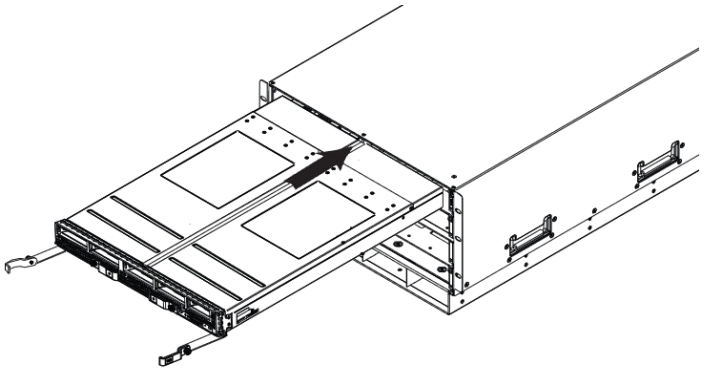
Step 6 Use your fingers only to tighten the captive screw on the front of the blade to no more than 3 in-lbs.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Insert B250 M2 Blade into the Cisco UCS 5108 Chassis

- Remove the slot divider by sliding it straight out of the chassis.
- Hold the blade by its outer shell and slide it into the chassis slot.
- Fold the ejector levers flush to the faceplate of the blade and use your fingers only to tighten captive screws.

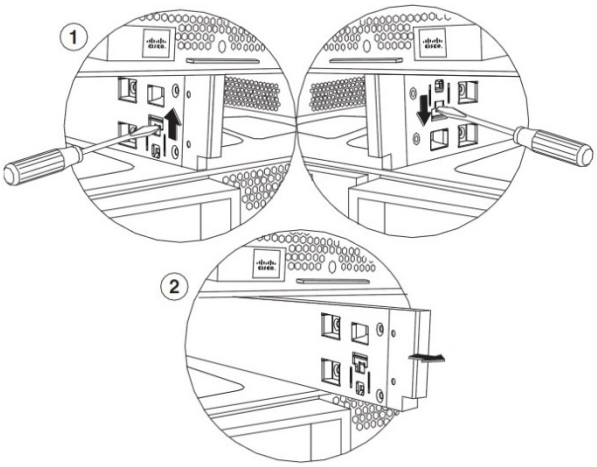


© 2012 Cisco and/or its affiliates. All rights reserved.

The Cisco UCS B250 M2 is a full-width server that occupies two server slots in the chassis. To install a B250 M2 blade into the Cisco UCS 5108 chassis, perform these steps:

Step 1 Remove blanking plates, if present.

Step 2 Remove the slot divider, if present.



Step 3 Wear an ESD wrist strap that is grounded to the chassis.

Step 4 Open the ejector levers in the front of the blade server.

Step 5 Slide the blade into the opening until you cannot push it any farther.

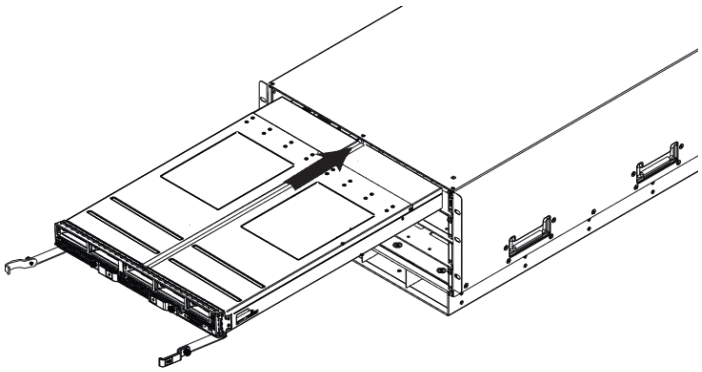
Step 6 Swing the ejector levers toward the faceplate so that they engage the edge of the chassis and press the blade server all the way in.

Step 7 Use your fingers only to tighten the captive screw on the front of the blade to no more than 3 in-lbs.

https://t.me/learningnets

Insert B440 M2 Blade into the Cisco UCS 5108 Chassis

- Remove the slot divider by sliding it straight out of the chassis.
- Hold the blade by its outer shell and slide it into the chassis slot.
- Fold the ejector levers flush to the faceplate of the blade and use your fingers only to tighten captive screws.

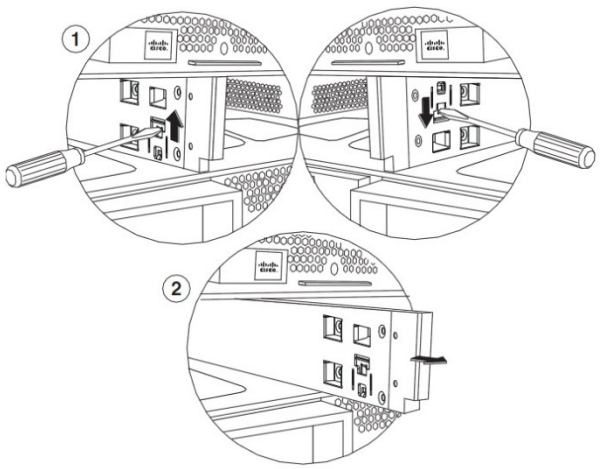


© 2012 Cisco and/or its affiliates. All rights reserved.

The Cisco UCS B440 M2 is also a full-width server. To install a B440 blade into the Cisco UCS 5108 chassis, perform these steps:

Step 1 Remove blanking plates, if present.

Step 2 Remove the slot divider, if present.



Step 3 Wear an ESD wrist strap that is grounded to the chassis.

Step 4 Open the ejector levers in the front of the blade server.

Step 5 Slide the blade into the opening until you cannot push it any farther.

Step 6 Swing the ejector levers toward the faceplate so that they engage the edge of the chassis and press the blade server all the way in.

Step 7 Use your fingers only to tighten the captive screw on the front of the blade to no more than 3 in-lbs.

 © 2012 Cisco Systems, Inc.

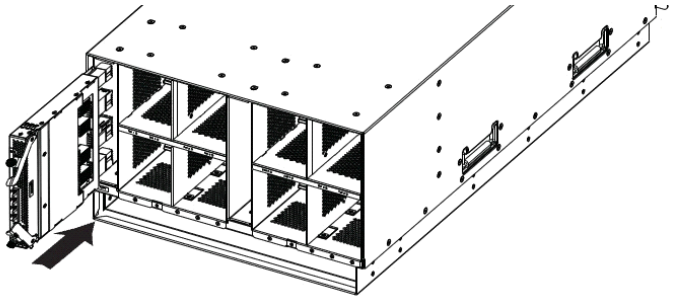
https://t.me/learningnets

Install IOMs and Power Supplies

This topic describes the steps to install and remove IOMs and power supplies in the Cisco UCS 5108 chassis.

Install Cisco UCS 2104/2204/2208 IOM

- Wear an ESD wrist strap grounded to the chassis.
- Handle the IOM by the sides and avoid contact with midplane connectors.
- Slide the IOM into the chassis, swing the ejector levers in toward the faceplate, and use your fingers only to tighten captive screws.



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

To install an IOM, follow these steps:

Step 1 Make sure that the two ejector levers at the front of the IOM are pulled fully open.

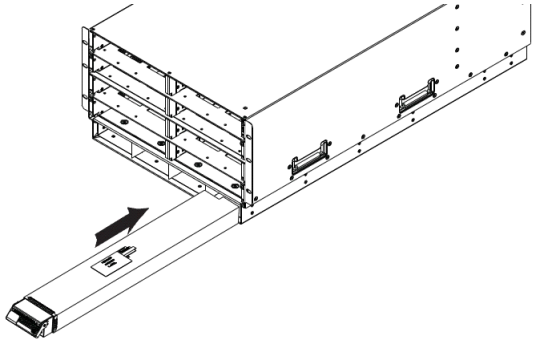
Step 2 Slide the fabric extender into the fabric extender slot, ensuring that the fabric extender is fully seated.

Step 3 Swing the ejection levers into the IOM faceplate and tighten the captive screw on each lever.

https://t.me/learningnets

Install Power Supplies in the Cisco UCS 5108 Chassis

- Handle the power supply modules by the sides and avoid contact with midplane connectors.
- Insert the power supply module into the chassis with the handle in the “up” position, slide the power supply all the way back, and lower the handle to lock.
- Use your fingers only to tighten the captive screw.



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

To install a power supply in the Cisco UCS 5108 chassis, follow these steps:

Step 1 Ensure that the handle orientation of the power supply is in the “up” position.

Step 2 Hold the power supply with both hands and slide it into the power supply bay.

Step 3 Press down the handle and give the power supply a gentle push inward. This push ensures that the power supply is fully seated into the power distribution unit (PDU).

Step 4 Press the power supply handle down to lock the power supply in place.

Step 5 Tighten the captive screw.

Step 6 Plug the power cable into the corresponding 220 VAC-inlet connector on the PDU at the rear of the chassis.

 © 2012 Cisco Systems, Inc.

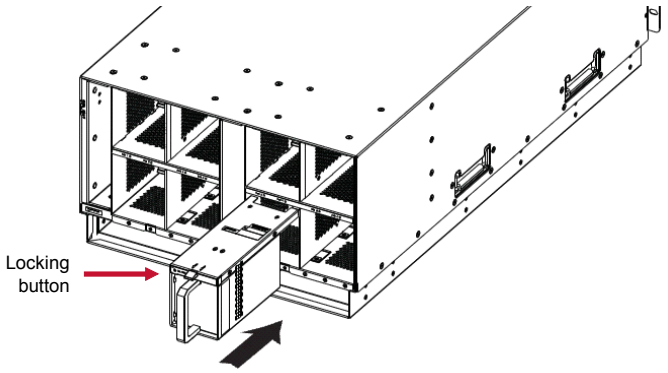
https://t.me/learningnets

Install and Remove Fan Units

This topic describes how to install or remove fan modules.

Install Fan Module into the Cisco UCS 5108 Chassis

- Hold the fan module by its handle and depress the locking button on top.
- Insert the module into the chassis until the locking button clicks.



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

To install a fan assembly into the Cisco UCS 5108 chassis, follow these steps:

Step 1 Ensure that the handle orientation of the fan is in the “up” position with the spring latch at the top of the module.

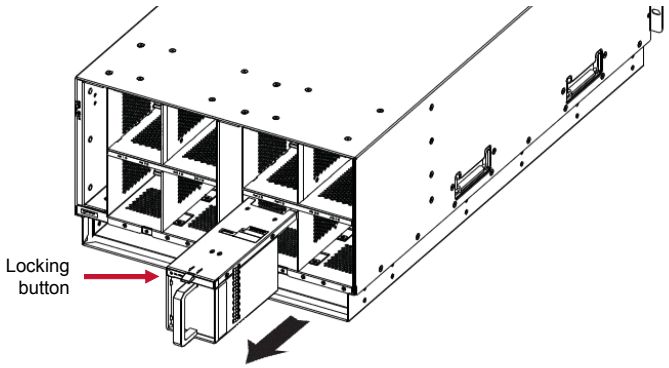
Step 2 Push the fan module into the chassis until it seats properly and the spring latch snaps into place.

Step 3 Listen for the fan if the chassis is powered on. You should immediately hear it operating. If you do not hear it, ensure that the fan module is inserted completely in the chassis and the faceplate is flush with the outside surface of the chassis.

https://t.me/learningnets

Remove Fan Module from the Cisco UCS 5108 Chassis

- Hold the fan module by its handle and depress the locking button on top.
- Pull the module straight out of the chassis.



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

To remove a fan assembly from the Cisco UCS 5108 chassis, follow these steps:

Step 1 Depress the spring latch.

Step 2 Slide the fan module out of the chassis.

Note	Do not operate the Cisco UCS 5108 with more than one fan module removed because it can cause overheating.

 © 2012 Cisco Systems, Inc.

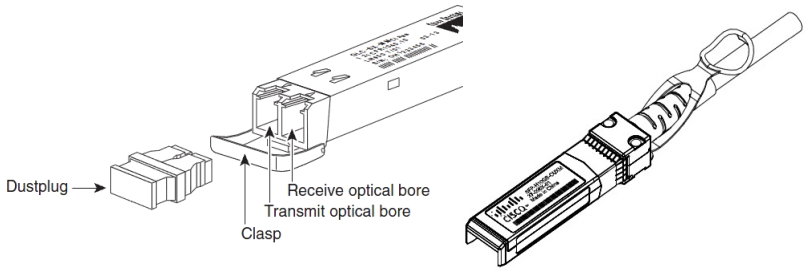
https://t.me/learningnets

Install and Remove SFP+ Copper Twinax and Optical Modules

This topic describes the physical installation and removal of small form-factor pluggable plus (SFP+) copper twinax and optical modules.

Optical and Copper SFP+ Modules Overview

- Wear an ESD wrist strap and ground to the chassis when handling optical SFP+ modules.
- Optical modules are available in SR, LR, and ER to accommodate SMF, MMF, and varying distance requirements.
- SFP+ copper twinax is available in 1 m, 3 m, 5 m, 7 m, and 10 m for FCoE.



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

SFP+ modules are selected based on distance and media. Ten Gigabit Ethernet optical and copper SFP+ modules are available in the following types and lengths.

Supported Cables with Cisco UCS 2104XL IOM

Model	Description
SFP-10G-SR	Short–range optical SFP+ (up to 984 ft [300 m])
SFP-10G-LR	Long–range optical SFP+ (up to 6.2 miles [10 km])
SFP-H10GB-CU1M	10 Gigabit Ethernet—copper SFP+ (3.28 ft [1 m])
SFP-H10GB-CU3M	10 Gigabit Ethernet—copper SFP+ (9.84 ft [3 m])
SFP-H10GB-CU5M	10 Gigabit Ethernet—copper SFP+ (16.4 ft [5 m])
SFP-H10GB-ACU7M	10 Gigabit Ethernet—copper SFP+ (22.9 ft [7 m])
SFP-H10GB-ACU10M	10 Gigabit Ethernet—copper SFP+ (32.8 ft [10 m])

https://t.me/learningnets

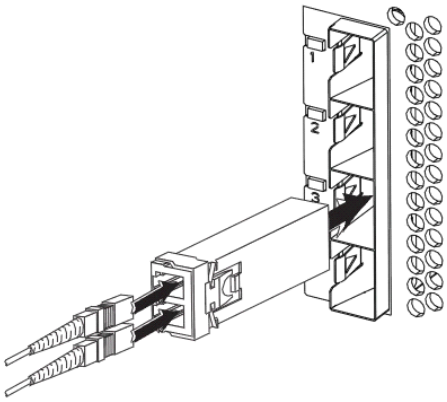
Supported Cables with Cisco UCS 2204/2208XP IOMs

Connector (Media)	Cable	Distance	Standard
SFP+ copper (CU)	Twinax	1, 3, and 5 m	SFF 8431
SFP+ FET	MM OM2 MM OM3 MM OM4	25 and 100 m	IEEE 802.3ae
SFP+ short-reach (SR) and multimode fiber (MMF)	MM OM2 MM OM3 MM OM4	82 and 300 m	IEEE 802.3ae
SFP+ long-reach (LR) MMF and SR	SMF	Up to 300 m over SMF	IEEE 802.3ae

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

Install Optical SFP+ into the Cisco UCS 2100/2200XP IOMs

- Insert into Cisco UCS 2100/2200XP with the Cisco label facing left until it clicks into place.
- Remove the dust cover to insert the appropriate fiber-optic patch cable.



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

Wear an ESD wrist strap that is grounded to the chassis that you are working on whenever handling optical SFP+ modules. Follow these steps to install an optical SFP+ module in Cisco UCS 2104/2204/2208 IOMs:

Step 1 Slide the optical SFP+ module into the slot in the IOM or fabric interconnect until it clicks in place.

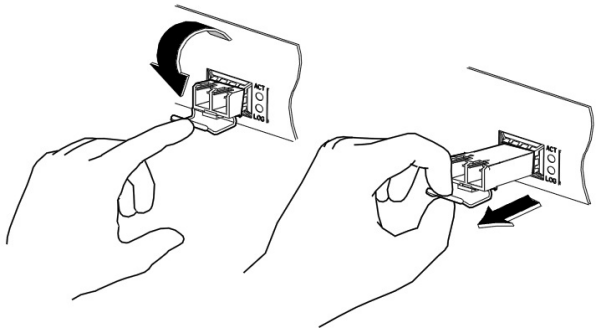
Step 2 Remove the dust cap from the SFP+ module and the dust caps from the fiber-optic cable ferrules.

Step 3 Store dust caps in a clean, sealable plastic bag or plastic parts box. You will need them in the future if you need to remove the fiber-optic cable from Cisco UCS components.

https://t.me/learningnets

Remove Optical SFP+ from the Cisco UCS 2100/2200XP IOMs

- Wear an ESD wrist strap and ground to the chassis when handling optical and copper SFP+ modules.
- Remove the fiber-optic patch cable.
- Lower the bail clasp and pull the SFP+ free.
- Replace the dust cap on the SFP+ module and ferrule ends of the fiber-optic cable.



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

Wear an ESD wrist strap that is grounded to the chassis you are working on whenever handling optical SFP+ modules. Follow these steps to remove an optical SFP+ module:

Step 1 Remove the fiber-optic cable and place clean dust caps over the ferrules. Slide down the bail handle to release the module from the component.

Step 2 Close the bail clasp and insert a clean dust cap.

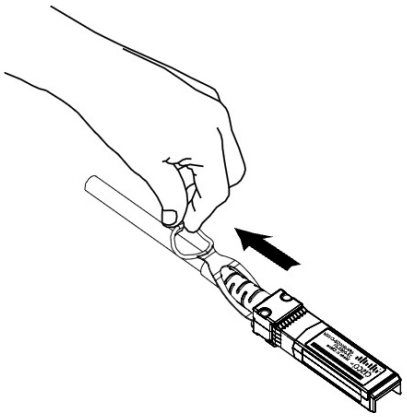
Step 3 Store optical SFP+ modules in a static-shielded container.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Remove Copper SFP+ from the Cisco UCS 2104XP/2204XP/2208XP IOMs

- Pull on the release cord and slide the module from the Cisco UCS 2100/2200 IOM.



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

Wear an ESD wrist strap that is grounded to the chassis you are working on whenever handling optical SFP+ modules. Follow these steps to remove a copper twinax SFP+ module:

Step 1 Grasp the looped cable and gently pull back. The module can then be slid out of the component.

Step 2 Store copper twinax SFP+ cables in a static-shielded container.

https://t.me/learningnets

Summary

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

Summary

- ESD precautionary measures must be taken when installing Cisco UCS B-Series components.
- Cisco UCS B-Series servers have similar procedures to open their cases. Press the release button and remove the cover.
- Cisco UCS 5108 rack rails require four-post mounting in a rack with square holes. Use the provided template to size the rack.
- Follow the specific procedures, including ESD protection, when installing or removing CPU, RAM, and mezzanine cards.
- Cisco UCS B-Series servers share similar hard drive installation procedures, but the B440 uses smaller SSD drives.
- The slot divider must be removed from a row to accommodate full-slot blade servers like the Cisco UCS B250 and B440.
- Cisco UCS 2104XP/2204XP/2208XP IOMs are inserted from the rear of the chassis. The power supplies are installed and removed from the front of the chassis.
- Fan units for the Cisco UCS 5108 have a detent spring that must be pressed for installation and removal.
- There are different procedures for installing and removing copper and optical SFP+ modules.

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

https://t.me/learningnets

Lesson 3

Implementing Cisco UCS B-Series LAN Connectivity

Overview

Unified fabric is an important value that Cisco Unified Computing System (UCS) offers customers. Use of the Fibre Channel over Ethernet (FCoE) protocol greatly reduces cable counts and complexity from the server chassis to the access layer. Correctly configuring LAN Ethernet components is critical for the operation of FCoE. The LAN configuration is the foundation on which all server connectivity and high availability relies.

Objectives

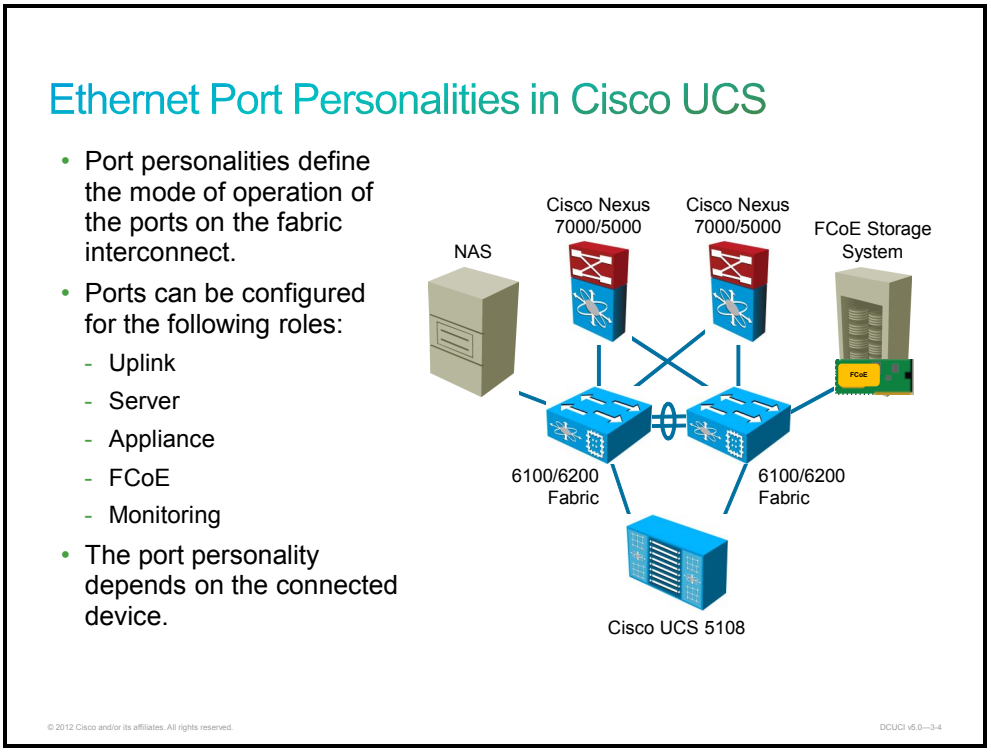
Upon completing this lesson, you will be able to implement LAN connectivity for Cisco UCS B-Series hardware. This ability includes being able to meet these objectives:

- Differentiate between uplink, server, appliance, FCoE storage, and monitoring Ethernet port personalities of 10 Gigabit Ethernet interfaces on the Cisco UCS fabric interconnect
- Describe the requirements and configuration of port channels from the Cisco UCS fabric interconnect to a northbound switch
- Describe end-host mode and its importance in forwarding over multiple Layer 2 links and maintaining a loop-free topology
- Differentiate end-host mode with switched mode
- Describe the requirements to configure VLANs in Cisco UCS Manager
- Describe the role of vNICs to abstract MAC addresses into a service profile
- Describe the automatic pinning process and recovery from failure
- Describe the configuration of manual pinning and recovery from failure
- Describe the configuration of disjoint Layer 2 domains

https://t.me/learningnets

Uplink, Server, Appliance, FCoE Storage, and Monitoring Ethernet Port Personalities

This topic describes the available port personalities.



The fabric interconnects are linked through the Ethernet ports with the blade chassis, upstream Ethernet switches, directly attached FCoE storage systems, storage systems communicating with Internet Small Computer Systems Interface (iSCSI) protocol, and file servers. The end device that is attached to the fabric interconnect requires different port configuration. In Cisco UCS Manager, you do not have to perform specific configuration. You only have to specify what the port personality is, depending on the device that is attached to it.

The following are available port personalities:

- Server
- Uplink
- Appliance
- FCoE storage
- Monitoring

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS 6248UP Ports

- Cisco UCS 6248UP has 32 fixed unified ports.
- The GEM adds 16 unified ports.
- The port type must be configured first—Ethernet or Fibre Channel.

1. Set port type—Ethernet or Fibre Channel.
2. Save configuration and reload.
3. Set port personality.

1. Ethernet ports must be in blocks. Start with the first port on the module and finish on an even port.
2. Fibre Channel ports must be in blocks. The first Fibre Channel port will be after the last Ethernet port.

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

On the Cisco UCS 6100 Series Fabric Interconnects, there are fixed Ethernet ports and additional Ethernet ports on the expansion module, depending on the model of the expansion module.

The Cisco UCS 6248UP fabric interconnect has 32 fixed unified ports and an additional 16 if the general expansion module (GEM) is installed.

To specify the port personality on the Cisco UCS 6248UP, you must first define the unified port type. The type can be Ethernet or Fibre Channel. After the unified port type is set to Ethernet, then you can specify if the port will be an uplink, server, appliance, FCoE, or monitoring port.

There are specific rules when you set the unified port type:

- Ethernet ports are defined in blocks of ports.
- The Ethernet block must start with the first unified port from the fixed ports or the expansion module and end on an even port.
- Fibre Channel ports are also defined in blocks.
- The first Fibre Channel port must start after the last Ethernet port.

Follow these steps to set the port type:

Step 1 Set the port type for the selected block of ports.

Step 2 Save the configuration.

Step 3 Reload the fabric interconnect.

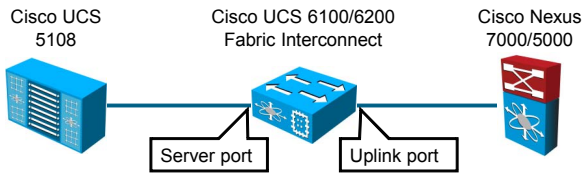
Step 4 Set the port personality.

When you define port types on Cisco UCS 6248UP fabric interconnects, both ports must have the same configuration.

https://t.me/learningnets

Uplink and Server Port Personality

- Uplink ports service data traffic from the upstream Ethernet switch.
- Server ports service traffic from IOMs, rack servers, and FEXs.



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

Uplink ports connect to an upstream Ethernet switch. You can set any of the Ethernet ports on the fabric interconnect as uplink ports.

Server ports are used to connect to blade chassis to service the traffic of the blade servers, to Cisco Nexus 2000 Series Fabric Extenders (FEX), and to Cisco UCS C-Series servers for data communication.

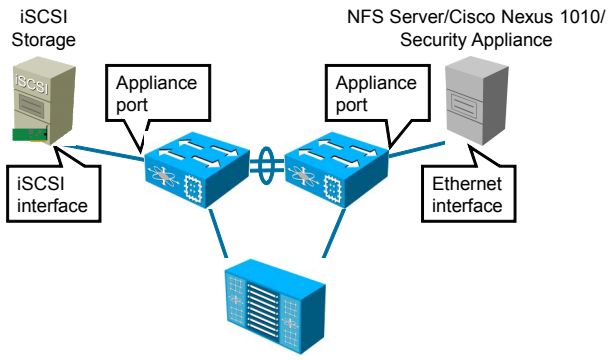
On Cisco UCS 6120/6140 fabric interconnects, you can configure only the fixed Ethernet ports as server ports. On Cisco UCS 6248UP, there is no such limitation, but the port must be set to Ethernet type.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Appliance Port Personality

- Appliance ports are used to directly attach iSCSI storage or NAS storage or specialized appliances, such as Cisco Nexus 1010 or a security appliance to fabric interconnects.
- Appliance ports are used only in end-host mode



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

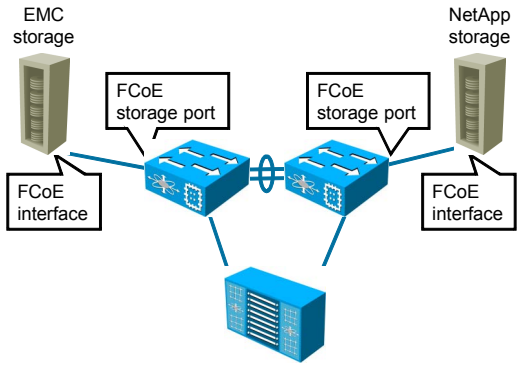
Appliance ports are used to directly attach Ethernet storage systems, a Cisco Nexus 1010 appliance, or a specialized security appliance. Examples of appliances include network-attached storage (NAS) such as Network File System (NFS) or iSCSI. Cisco UCS Manager version 2.0 supports iSCSI interfaces on virtual interface cards (VICs) for iSCSI-based boot.

The fabric interconnects must operate in end-host mode to use appliance ports.

https://t.me/learningnets

FCoE Storage Port Personality

- NetApp and EMC storage systems can be directly 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.

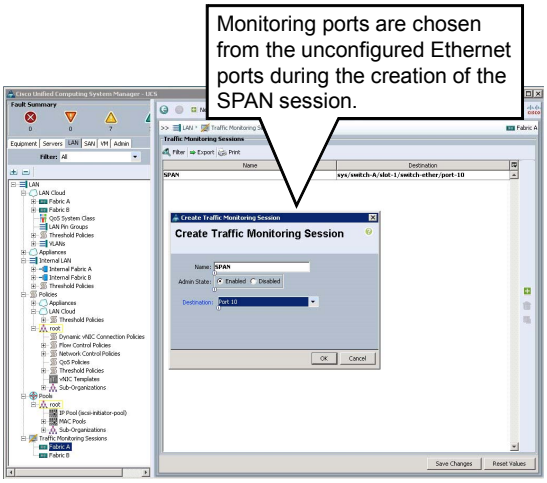
You can connect storage systems that are equipped with FCoE-capable interfaces at 10 Gb/s to FCoE storage ports.

Currently, only EMC and NetApp storage systems are certified by Cisco for use with Cisco UCS.

https://t.me/learningnets

Monitoring Port Personality

- SPAN-based monitoring of server traffic
- SPAN destination ports are Ethernet physical ports
- SPAN source Ethernet ports can be the following:
  - Uplink Ethernet ports or port channels
  - VLAN
  - vNICs or vHBAs
  - FCoE ports
  - Server ports



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

Cisco UCS supports Switched Port Analyzer (SPAN) to capture and monitor the traffic of the server. To use SPAN, create a monitoring session. To create the session, navigate to **LAN > Traffic Monitoring Sessions**.

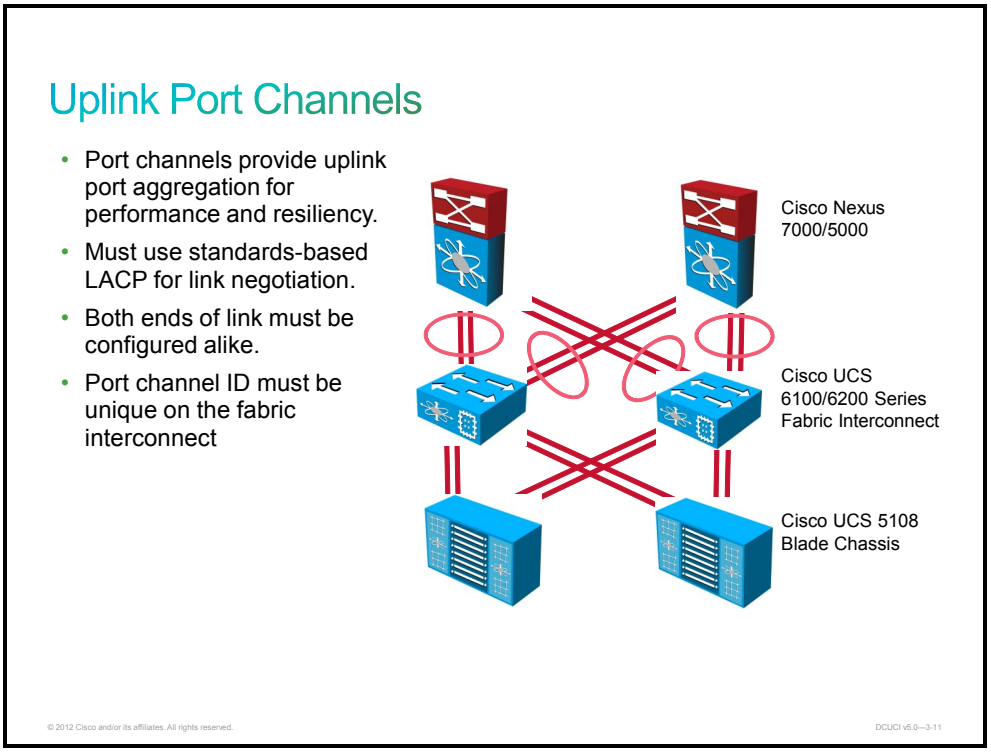
The components of a SPAN monitoring session include the following:

- SPAN sources, where traffic will be captured:
  - Uplink Ethernet ports
  - Uplink port channels
  - Virtual LANs (VLANs)
  - Virtual network interface cards (vNICs) and virtual host bus adapters (vHBAs)
  - FCoE ports
  - Server ports
  - Fibre Channel uplink ports
- SPAN destination: The port where captured data will be sent for analysis, also called a monitoring port. The destination can be any unconfigured Ethernet port. Select the port during the creation of the monitoring session.

https://t.me/learningnets

Requirements and Configuration of Uplink Port Channels

This topic describes uplink port channels.



Uplink ports can be combined in port channels. Port channels add fault tolerance and load balancing, and aggregate the speed of the ports.

On 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 system.

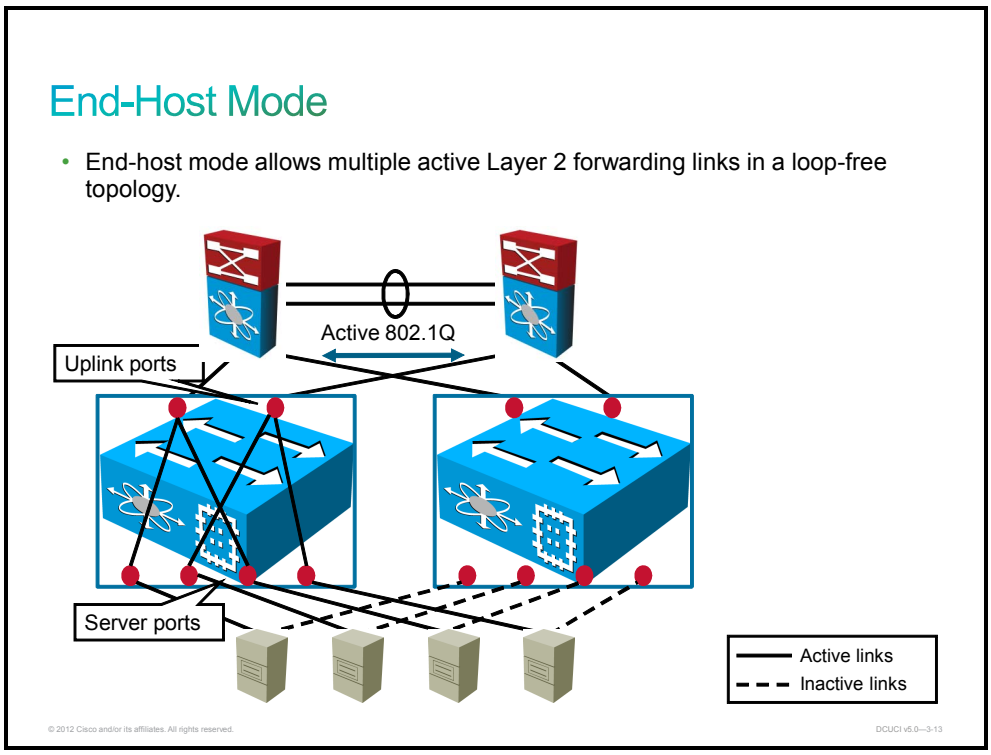
A wizard is available for uplink port channel creation. Specify a unique port channel ID because Cisco UCS Manager refers to this object based on the ID and not on the name. The valid range of port channel IDs is from 1 to 256. In case of a duplicate ID, the system will generate an error message and you will not be allowed to continue.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Importance of End-Host Mode in Maintaining a Loop-Free Topology

This topic describes end-host mode.



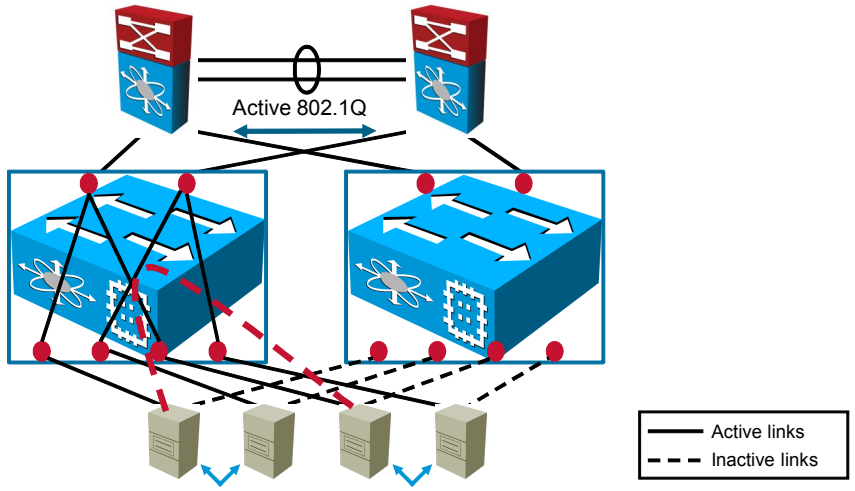
End-host mode or end-host virtualizer (EHV) presents a link to a northbound uplink switch as a host trunk. Because it is a host port, it is not subject to spanning-tree blocking on the port. Server MAC addresses are pinned to an uplink and are persistent, except in the case of uplink failure. After a MAC address has been learned on the uplink ports of the northbound switch, the return path is always maintained. In this way, multiple active Layer 2 links can forward without creating a loop.

A port in EHV mode appears to the uplink switch as a host with many MAC addresses.

https://t.me/learningnets

Server-to-Server Switching

- Server-to-server traffic on the same VLAN is switched locally and does not forward to uplinks.



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

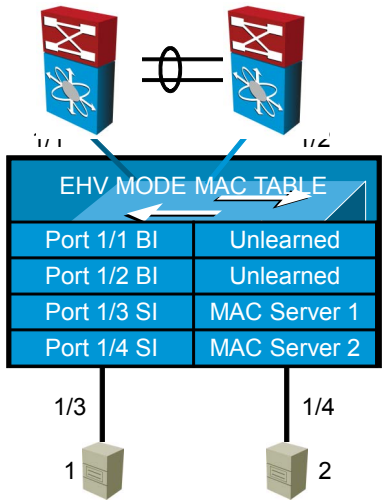
Server-to-server communications on a common VLAN are locally switched by the fabric interconnect. Server-to-server communications across Layer 3 boundaries must be sent up an uplink port to a northbound switch to be routed to the correct VLAN.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

MAC Address Learning

- Learning is disabled on uplinks.
  - MAC addresses are pinned to an uplink.
- Learning is enabled on server links.
  - Traffic to server is forwarded based on destination MAC address.
- Learned MAC addresses never age unless server link goes down or is deleted.
  - Server MAC addresses can move (in the event of repinning).
- Server MAC address can be locally administered.



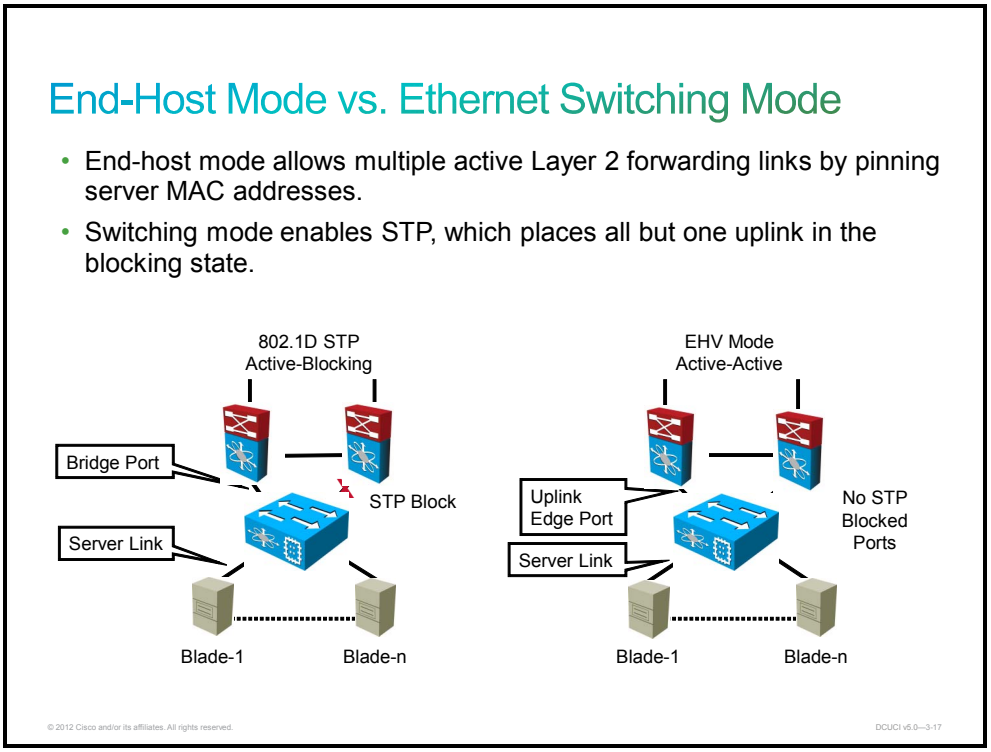
© 2012 Cisco and/or its affiliates. All rights reserved.

An important concept in EHV mode is that a MAC forwarding table (in the traditional Ethernet switching sense) is not used to forward traffic to the uplink switch. Instead, a new server MAC address becomes associated with one uplink. All subsequent communications from that MAC address will be forwarded to the uplink to which it was pinned. A MAC address forwarding table is maintained only for server-to-server communications on the same VLAN.

https://t.me/learningnets

End-Host Mode vs. Switching Mode

This topic describes the difference between end-host mode and switching mode.



Although the fabric interconnects are capable of operating in Ethernet switching mode, default EHV mode is the preferred mode of operation. In Ethernet switching mode, the fabric interconnects must run Spanning Tree Protocol (STP) to maintain a loop-free topology. STP will place all but one redundant uplink into blocking mode, which places constraints on uplink bandwidth and delays recovery from path failures. In EHV mode, a loop-free topology is maintained by pinning server MAC addresses to one particular uplink. In this way, all uplinks are actively forwarding traffic.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Configuring VLANs in Cisco UCS Manager

This topic describes VLAN support in Cisco UCS.

VLAN Basics in Cisco UCS

- The fabric interconnect does not participate in VTPs.
- VLAN configuration is performed in the LAN tab of the Cisco UCS Manager navigation pane.
  - Configure globally to support required VLANs.
  - The default VLAN (VLAN 1) cannot be deleted.
- Each VLAN object configuration can be global or fabric interconnect-specific.
  - Both fabric interconnects typically will share Layer 2 domain and same VLANs.
- VLAN range is 1 to 3967 and 4049 to 4093.

VTP = VLAN Trunking Protocol

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

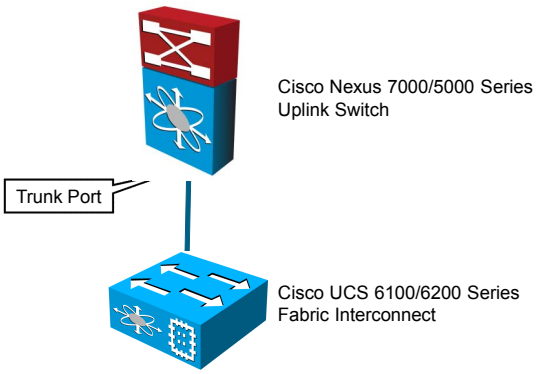
Although all uplinks from the fabric interconnect to the northbound switch are IEEE 802.1Q trunks, no virtual trunking protocol is employed. Therefore, the fabric interconnect requires manual configuration of VLANs.

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

https://t.me/learningnets

Uplink Switch Configuration

- Default behavior: All VLANs on the fabric interconnect are allowed automatically on the uplink ports.
- All ports on the northbound switch that connect to fabric interconnect uplinks must be configured as 802.1Q trunks.



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

Because uplink ports on the fabric interconnects are always trunk ports, the northbound port on the uplink switch must also be configured as a trunk port. It is considered a best practice to limit the allowed VLANs on the northbound switch to the VLANs that are required by Cisco UCS.

Cisco UCS Manager dynamically updates the allowed VLAN list on fabric interconnect uplinks anytime that a VLAN is created, modified, or deleted.

This behavior is the default and is preserved in Cisco UCS version 2.0.

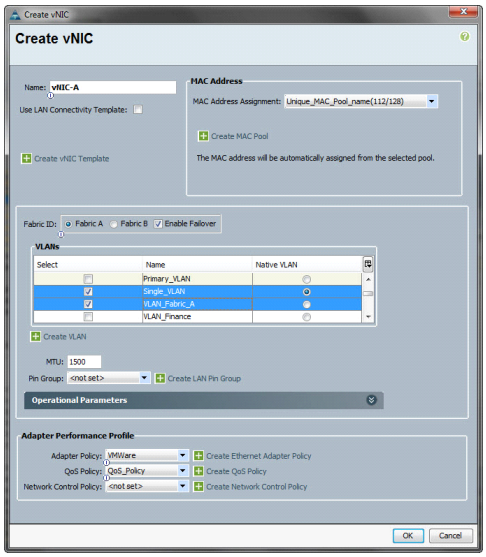
https://t.me/learningnets

Role of vNICs

This topic describes the role of the vNIC object.

vNIC and Locally Administered MAC Address

- vNIC is one of the abstractions of NIC characteristics that is tied to a service profile instead of a physical NIC.
- A MAC address can be assigned manually or with a MAC address pool.



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

The vNIC is the component in the service profile that contains the configuration of the server NIC. In the vNIC object, you specify the MAC address that will be used by the server. The available MAC address assignment methods include the following:

- **Manual:** Specify manually a MAC address.
- **From pool:** The service profile will take the MAC value from a MAC address pool.
- **To use the burned-in MAC address:** This option will make the service profile dependent on the specific physical compute node, which means that the service profile will not be mobile.

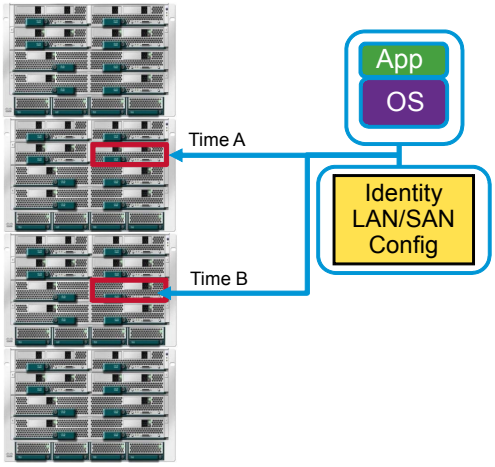
The vNIC also specifies the following:

- Primary data path through Fabric A or B
- Hardware failover
- VLAN or VLANs to be allowed
- Native VLAN
- Maximum transmission unit (MTU) size
- Static LAN pin group
- Adapter policy to configure the hardware of the Ethernet adapter
- QoS policy
- Network control policy

https://t.me/learningnets

vNIC MAC Address Portability

- MAC address moves with service profile from blade to blade.



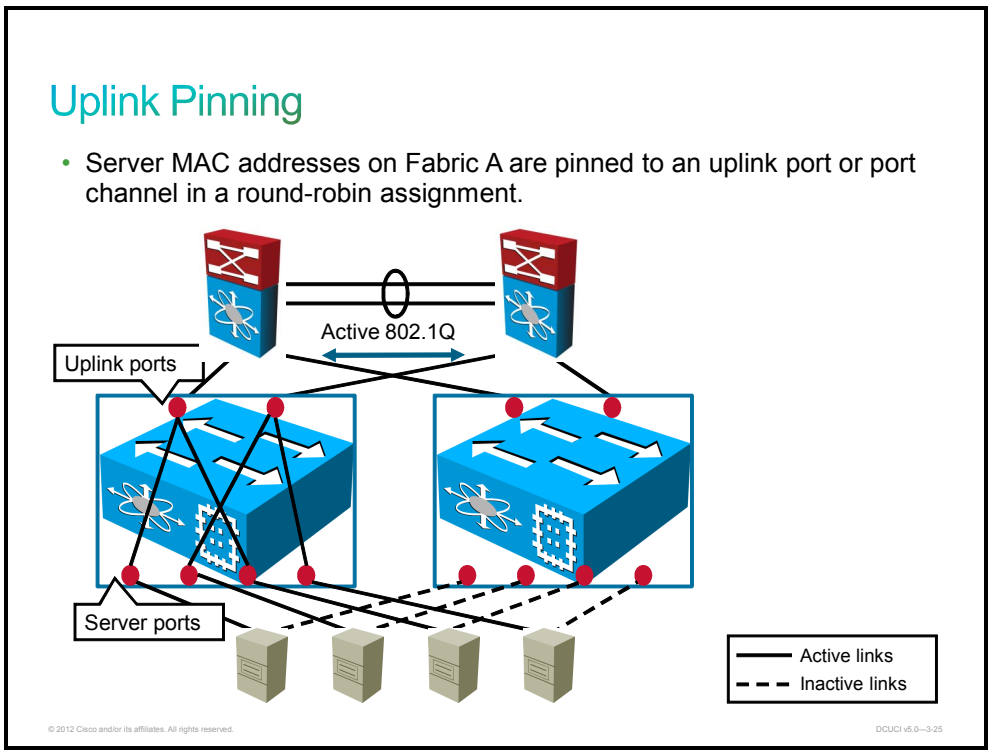
© 2012 Cisco and/or its affiliates. All rights reserved.

The main benefit of virtualizing the MAC address is that if the underlying server hardware fails, a service profile is simply moved to a replacement server. When the operating system boots on the new server, the MAC address is unchanged. From the perspective of the operating system or hypervisor running on the blade server, it is on the same hardware from which it booted the last time.

https://t.me/learningnets

Automatic Pinning and Recovery from Failure

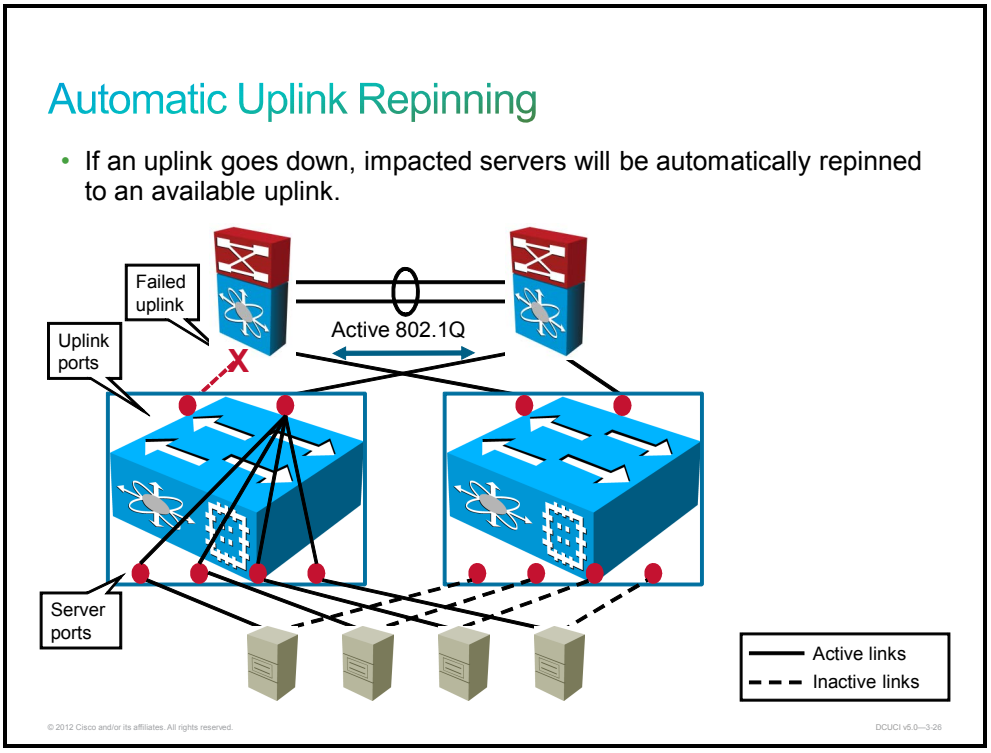
This topic describes the automatic pinning process and recovery from failures.



It is important to understand the difference between I/O module (IOM) pinning and uplink pinning. IOM pinning is static and based on the number of links from the IOM to the fabric interconnect.

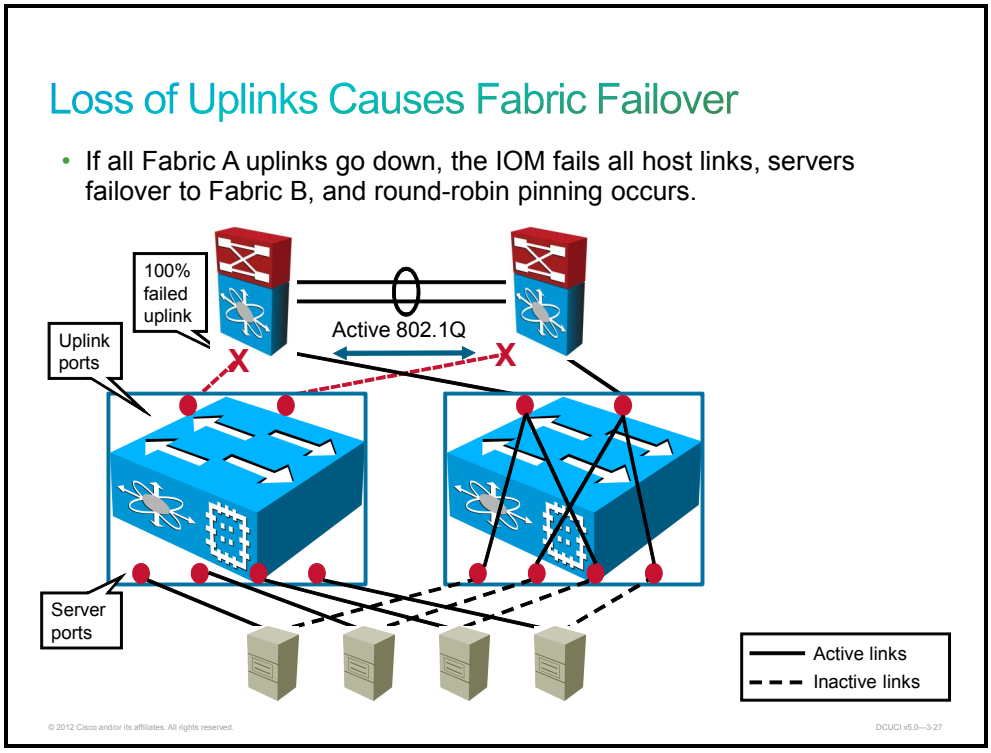
In end-host virtualization mode, a loop-free topology is assured by pinning server MAC addresses to uplink ports. This pinning process can be either automatic or statically configured. By default, server MAC addresses are pinned to uplink interfaces in an automatic round-robin process.

https://t.me/learningnets



With automatic uplink pinning, a link failure will cause all servers to be repinned to remaining uplinks. In the example, there are two uplinks on fabric A. When one of the links goes down, the server is simply repinned to the remaining uplink. The fabric interconnect will send a Gratuitous Address Resolution Protocol (GARP) to the northbound switch on behalf of the servers to announce them on the new port. The switch will update its MAC forwarding table to reflect the new interface.

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



If all uplink ports on the fabric interconnect lose connectivity, the IOM instructs the I/O multiplexer (MUX) to shut down all eight of the host ports. The affected servers will use either NIC teaming or hardware failover to re-establish connectivity on fabric B. If the servers are not configured for high availability in the operating system or service profile, then the servers will be down until at least one uplink is restored on fabric A.

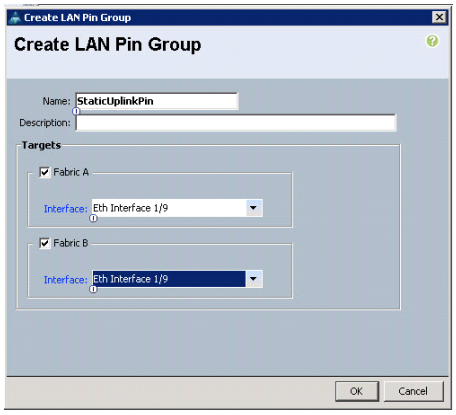
https://t.me/learningnets

Configuring Manual Pinning and Recovery from Failure

This topic describes static LAN pinning.

Static Pin Group

- Pin groups are created and bound to service profiles.
- Automatic pinning is inactive for any service profile that uses a static pin group.
- Other servers continue to be automatically pinned to an uplink.



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

Pin groups are created under the LAN tab of the navigation pane. Pin groups are global policy elements and are replicated to the secondary management node. With static LAN pin groups, you control the traffic that will be pinned from a particular server to a particular uplink port.

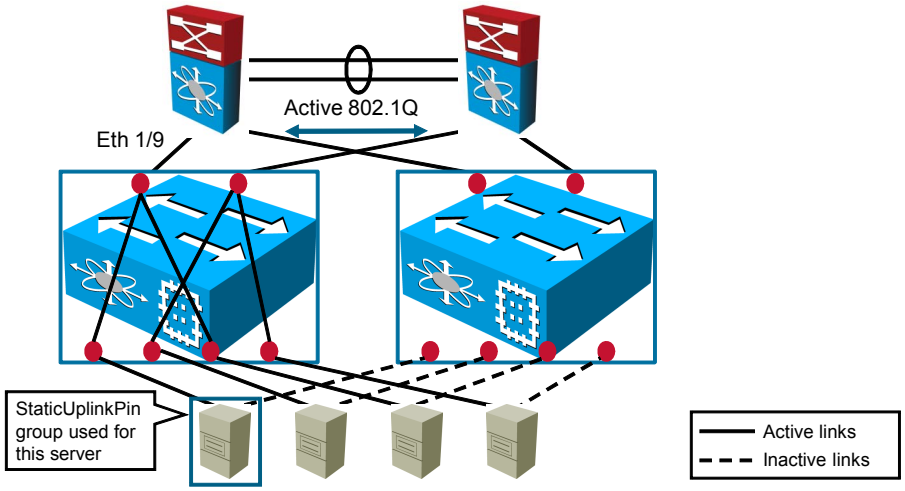
In this example, any service profile that includes this pin group policy will only use uplink Ethernet 1/9 on fabric A. If that uplink goes down, automatic repinning will not occur and the server will have to use fabric failover to re-establish connectivity on fabric B.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Static Pinning

- Servers with the StaticUplinkPin pin group assigned are statically mapped to uplink interface Eth 1/9.

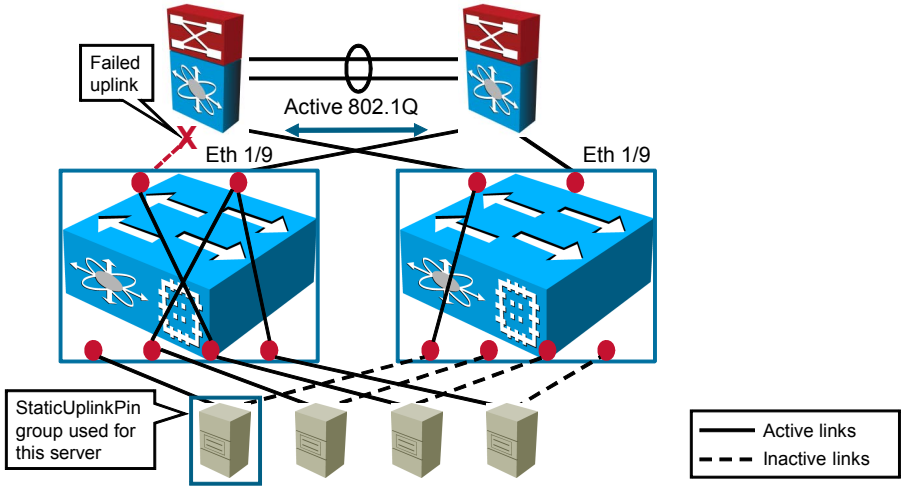


© 2012 Cisco and/or its affiliates. All rights reserved.

In the example that is shown in the figure, the highlighted server is configured to use the static pin group that is called StaticUplinkPin, which was just created. This server will always pin to uplink Ethernet 1/9 on fabric A, or Ethernet 1/9 on fabric B.

Static Pinning on Uplink Failure

- Upon uplink failure, the statically pinned server must fail to Fabric B.
- Hardware failover for the server vNIC must be enabled.



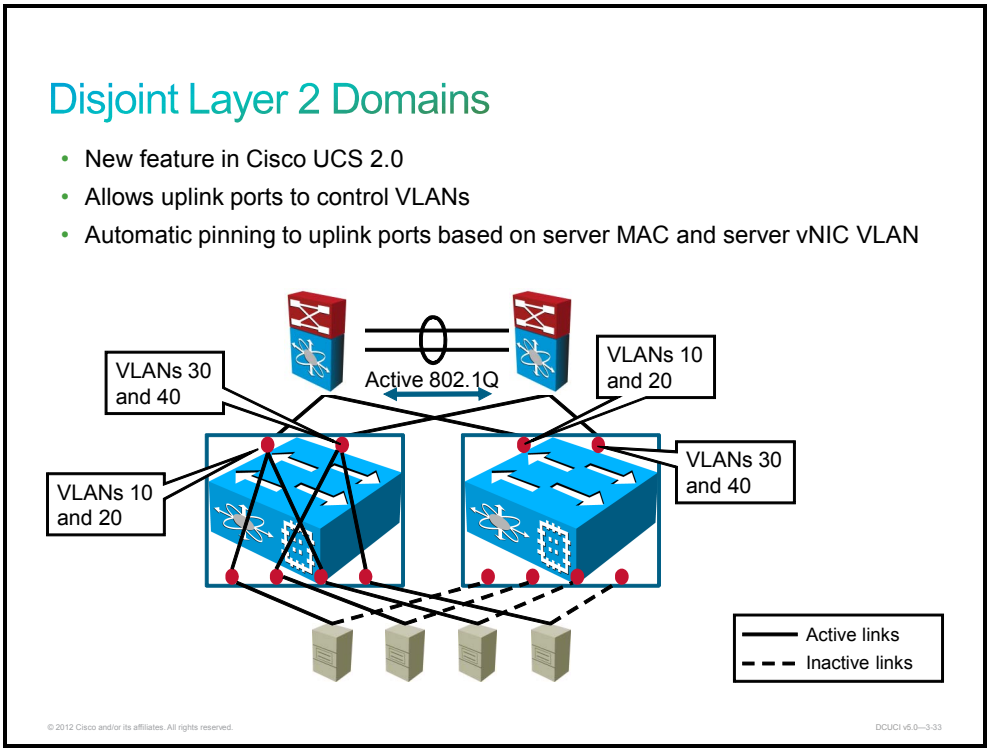
© 2012 Cisco and/or its affiliates. All rights reserved.

When uplink Ethernet 1/9 fails, the server fails over to uplink Ethernet 1/9 on fabric B. Because static pinning is used, the system will not automatically repin the server communication to another uplink on fabric A.

https://t.me/learningnets

Configuring Disjoint Layer 2 Domains

This topic describes the support for disjoint Layer 2 domains.



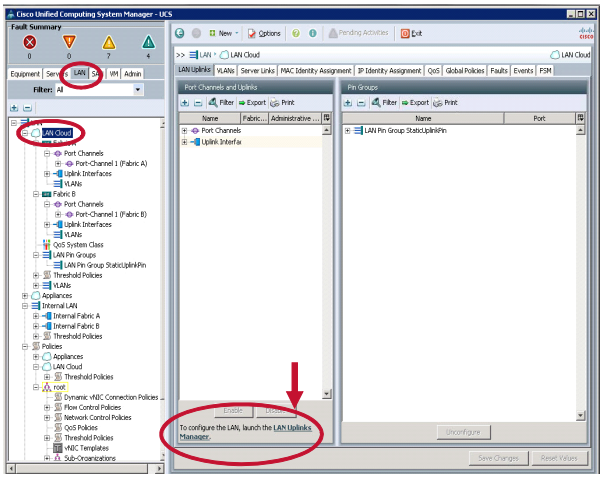
When VLANs are created on the fabric interconnect, they are automatically assigned to the uplink Ethernet interfaces. After that, the server traffic is pinned automatically by the system to the uplink ports, as all uplink ports service all VLANs. Starting with Cisco UCS version 2.0, the support for disjoint Layer 2 domains is a new feature. This new feature means that if you want different uplink ports to connect to different LAN switches that service different VLANs, now you have the capability to manually specify which VLANs will be allowed on which uplink ports. In this situation, the system will still perform automatic pinning of the traffic of the server to uplink interfaces, but it will also use the VLAN membership of the uplink ports.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Disjoint VLAN Configuration

- Must have identical configuration on both fabric interconnects
- Manual configuration in LAN Uplinks Manager
- VLANs must be created identically on both fabric interconnects.



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

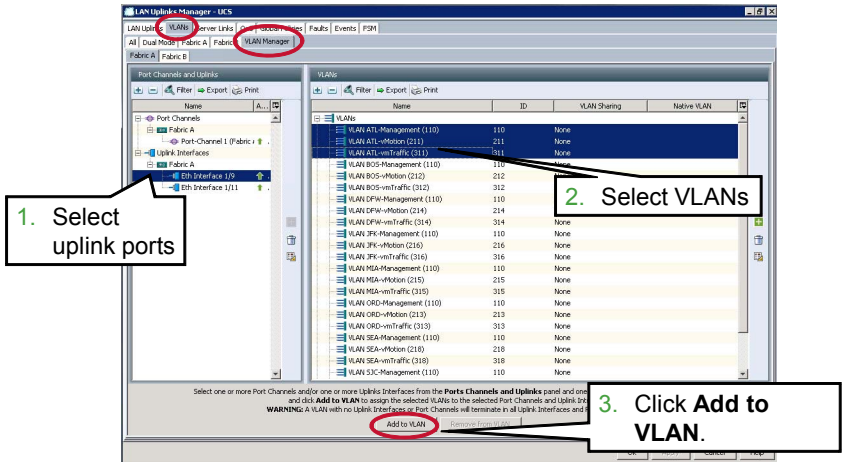
This feature is added functionality. To use the feature, you have to perform manual configuration. The VLANs must be configured globally, that is, to exist and have the same configuration on both fabric interconnects. Also, both fabric interconnects must be configured identically. This means that both fabric interconnects must be connected to the same Ethernet switches. This step is done to secure two separate data paths.

The configuration is performed from the LAN Uplinks Manager. To start the LAN Uplinks Manager, navigate to **LAN > LAN Cloud**. At the bottom of the content pane is a link to start the LAN Uplinks Manager.

https://t.me/learningnets

Assign Uplink Ports to VLANs

- Navigate to **VLANs > VLAN Manager**.
- Perform the configuration for both fabric interconnects.



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

In the LAN Uplinks Manager, navigate to **VLANs > VLAN Manager**.

Follow these steps to configure disjoint VLANs:

Step 1 Select uplink Ethernet interfaces or uplink port channels. You are going to assign them to specific VLANs.

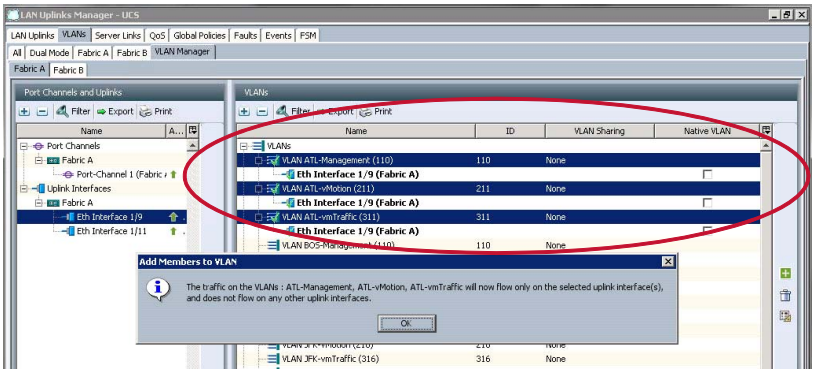
Step 2 Select VLANs. These VLANs will be allowed on the interfaces selected in the previous step.

Step 3 Click **Add to VLAN**.

https://t.me/learningnets

Disjoint VLAN Verification

- The traffic for the selected VLANs will flow only through the assigned uplinks.
- The uplink ports will appear under the VLANs.



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

The traffic for the selected VLANs will flow only through the selected uplink interfaces, which means that only the VLANs that you have selected will be allowed on these uplink ports. The system will provide a message informing you which VLANs will be allowed on the selected interfaces.

The uplink ports will appear under the selected VLANs in the VLAN Manager.

https://t.me/learningnets

Summary

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

Summary

- The Ethernet port type can be uplink, server, appliance, FCoE, or monitoring. The type depends on the device connected.
- Uplink port channels can be created to upstream an Ethernet switch. LACP is supported.
- In end-host mode, the fabric interconnect connects as a server to the Ethernet infrastructure.
- In end-host mode, STP does not include the uplink ports in its topology. The result is that all uplinks are active.
- All VLANs created on a fabric interconnect are automatically allowed on all uplink ports.
- The vNIC represents the configuration of the Ethernet adapter of the server and carries the MAC address to support service profile mobility.
- Server traffic is automatically pinned to uplinks based on the MAC address of the server. On uplink failure, the traffic is repinned to another uplink. On failure of all uplinks, the server traffic goes through the other fabric interconnect based on hardware failover.
- With static LAN pin groups, the uplink to which server traffic will be pinned can be manually controlled. On failure of the uplink port, the traffic will go through the other fabric interconnect.
- The support for disjoint Layer 2 domains allows for manual control of which VLANs will be allowed on which uplink. The configuration must be the same for both fabric interconnects.

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

https://t.me/learningnets

Lesson 4

Implementing Cisco UCS B-Series SAN Connectivity

Overview

Unified fabric is a major benefit of Cisco Unified Computing System (UCS), so you should understand how to integrate Fibre Channel SAN in the context of Fibre Channel over Ethernet (FCoE). After the virtual network interface card (vNIC) is configured and VLANs are established, the virtual host bus adapter (vHBA) is the second half of the FCoE solution.

Objectives

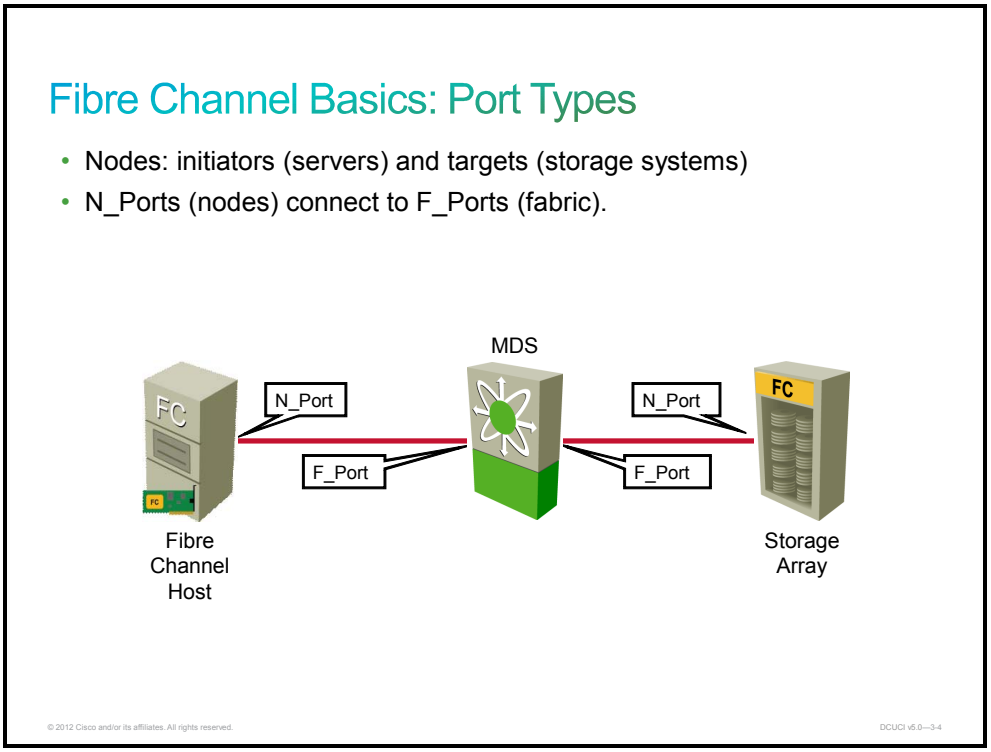
Upon completing this lesson, you will be able to implement SAN connectivity for Cisco UCS B-Series hardware. This ability includes being able to meet these objectives:

- Describe Fibre Channel switching
- Describe NPV
- Differentiate between Fibre Channel uplink, Fibre Channel storage, and Fibre Channel monitoring port personalities of 10 Gigabit Ethernet interfaces on the Cisco UCS fabric interconnect
- Differentiate between benefits and drawbacks of Fibre Channel switching and NPV
- Describe how NPIV allows a single N Port to be associated with multiple FCIDs
- Describe the requirements and configuration of VSANs in Cisco UCS Manager
- Describe the role of the vHBA to abstract WWNNs and WWPNs into a service profile
- Describe the automatic pinning process and recovery from failure
- Describe the configuration of manual pinning and recovery from failure
- Differentiate Ethernet failover from Fibre Channel multipath I/O recovery

https://t.me/learningnets

Fibre Channel Switching

This topic describes the main aspects of Fibre Channel switching.

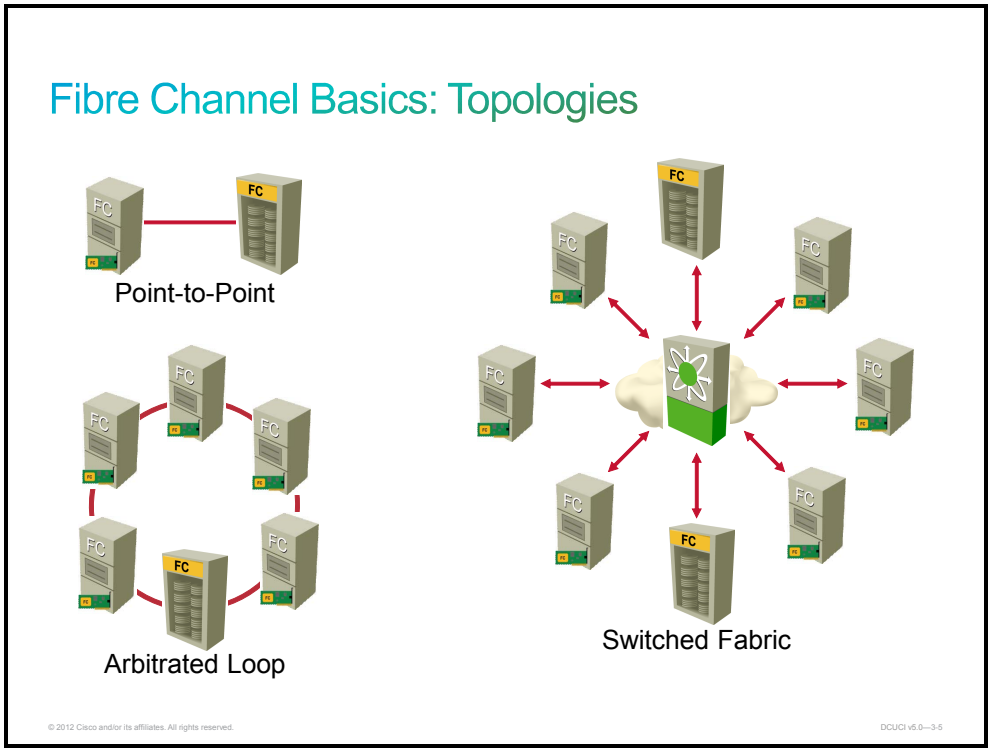


Fibre Channel Protocol (FCP) defines a number of specialized port types. There are rules concerning which port types can connect to other port types.

FCP Port Type	Description	Connects to Which Type
N Port	Node (host) port	F Port
NP Port	Node proxy (NPV Mode)	F Port
F Port	Fabric port on Fibre Channel switch	N Port, NP Port
E Port	Expansion port (interswitch)	E Port
TE Port	Trunking E Port (Cisco only)	TE Port

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



There are three basic topologies in Fibre Channel networks:

- Point-to-point connections are simple but do not scale.
- Arbitrated loop topologies are most commonly used to connect shelves of disks to a Fibre Channel storage controller.
- Switched topologies are the most common method of host attachment to Fibre Channel storage. Switched topologies can theoretically scale to millions of nodes. A Fibre Channel switch is required for FCoE to function.

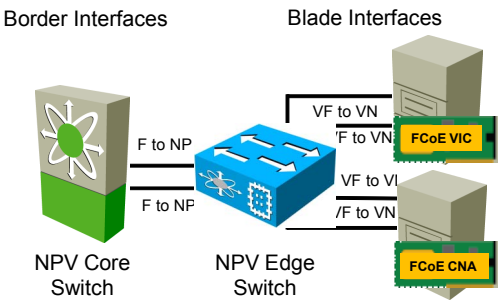
https://t.me/learningnets

NPV Mode

This topic describes N-Port Virtualization (NPV) mode.

Cisco NPV Mode Network Topology

- Fabric treats a fabric interconnect as a Fibre Channel node with multiple ports and FCIDs.
  - Cisco UCS fabric interconnect functions in NPV mode.
  - Uplink ports function as proxy N_Ports (NP_Ports).
  - On fabric interconnects, there are VF_Ports (Virtual Fabric ports) for server connectivity.
  - Blade server interfaces function as VN_Ports (Virtual Node ports).



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

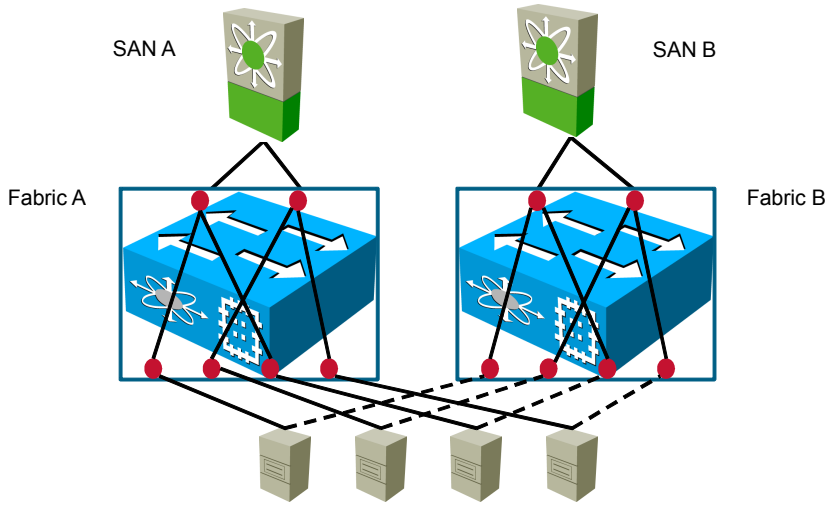
There are two types of interfaces in N-Port ID Virtualization (NPIV) topologies.

- **Server Interfaces:** Server-facing interfaces are either physical Fibre Channels or virtual Fibre Channel interfaces with F-Port modes.
  - There is no local switching.
  - All packets are forwarded.
  - Fabric login (FLOGI)-related processing is relayed in software (FLOGI, fabric discovery [FDISC], and corresponding Link Service Accept [LS_ACC], Link Service Reject [LS_RJT] messages, and so on) to the same uplink interface.
  - NPIV is supported on F Ports.
- **Border Interfaces:** Border interfaces are network-facing and will always be N-Port types.
  - Internal FLOGI is sent to the core Fibre Channel switches.
  - Register with name servers on the successful internal FLOGI.
  - Every uplink can be connected to different Fibre Channel switches and virtual storage area networks (VSANs).

https://t.me/learningnets

Cisco NPV

- Server interfaces are pinned to uplink interfaces on the same VSAN.



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

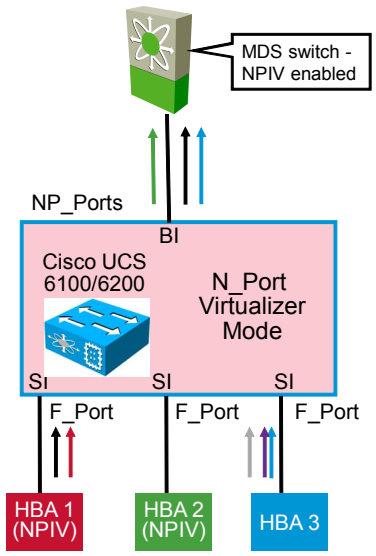
Each server link is pinned to exactly one uplink.

- Pinning logic distributes server links to various uplinks.
- All traffic is passed upstream for switching.

https://t.me/learningnets

Cisco NPV Implementation Detail

- Each server interface is pinned to one border interface.
- All traffic follows the pinned port.
- Pinning is based on a round-robin mechanism.
- Relies on NPIV (NPIV must be enabled on the NPV core switch).
- Retries all failed login requests from a border interface on a new server interface.
- Handles error events by generating proxy LOGOs.



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

NPIV proxy modules in the Cisco Nexus Operating System (NX-OS) provide the proxy function of distributing FLOGI requests from servers over the available border interfaces. The Fibre Channel host bus adapters (HBAs) in servers and Fibre Channel switches assume that they are connected directly to each other by using a physical cable.

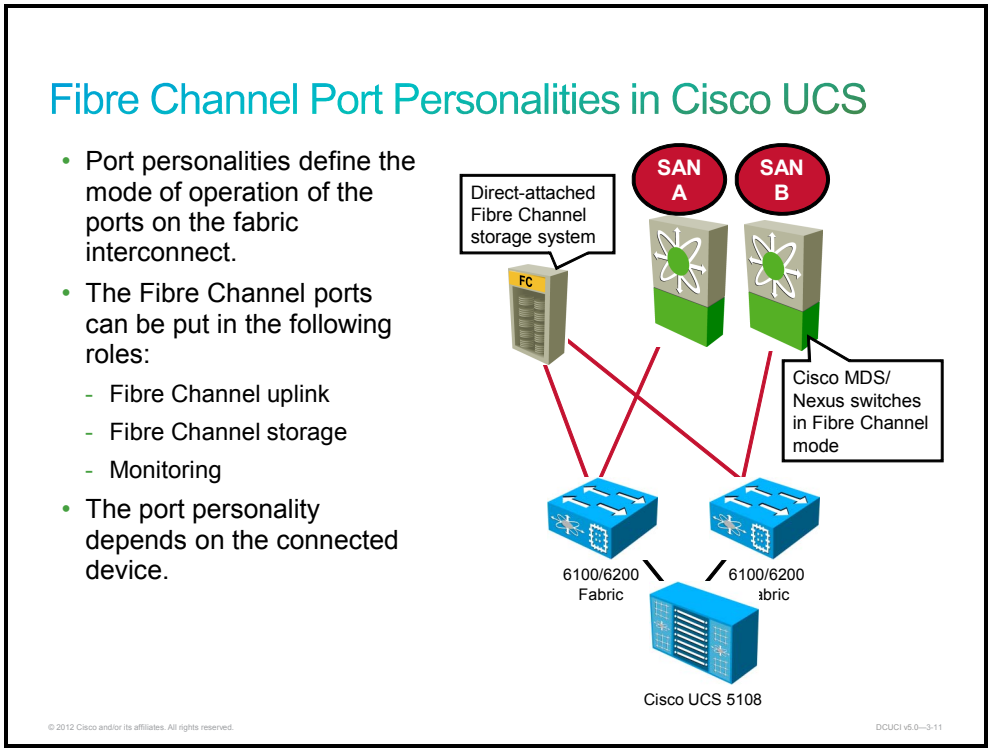
Note	The NPIV proxy function allows the NPIV to be used between the Cisco UCS fabric interconnect and the Fibre Channel switch. This use applies even if some or all HBAs implement only the basics of N-Port functionality.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Fibre Channel Uplink, Storage, and Monitoring Port Personalities

This topic describes Fibre Channel port personalities.



The Cisco UCS fabric interconnects provide SAN connectivity for the compute nodes. The fabric interconnects use native Fibre Channel ports to connect to the SAN infrastructure. Usually, one fabric interconnect is linked to one SAN and the other is linked to another SAN. In this way, redundant paths are secured to the storage systems. The native Fibre Channel ports that connect to the SANs are uplink Fibre Channel ports. By default, all Fibre Channel ports are uplinks.

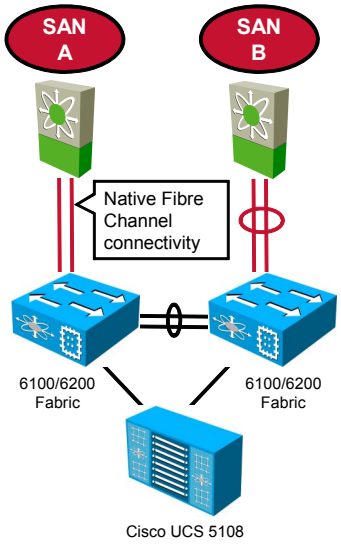
You can directly attach a Fibre Channel storage system to your Cisco UCS. For this attachment, the Fibre Channel port must be configured as Fibre Channel storage port.

If you want to create a Fibre Channel Switched Port Analyzer (SPAN) session, you can specify a Fibre Channel port as SPAN destination.

https://t.me/learningnets

Fibre Channel Uplink Ports

- Native Fibre Channel ports are used to connect to the SAN infrastructure or to directly attach a Fibre Channel storage system.
- By default, Fibre Channel ports on the fabric interconnects are uplink ports.
- Uplink Fibre Channel ports can be combined in Fibre Channel port channels in both NPV mode and Fibre Channel switching mode.
- Uplink Fibre Channel ports support VSAN trunking in both NPV mode and Fibre Channel switching mode.



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

On the Cisco UCS 6100 Series Fabric Interconnects, you can have Fibre Channel ports only on the expansion ports. The maximum number of Fibre Channel ports for the Cisco UCS 6120 Fabric Interconnect 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 Fabric Interconnect, 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) that is used and on the ports at the upstream switch.

On the Cisco UCS 6248UP, you must first set the Type for a block of unified ports to Fibre Channel and then the ports will become uplink ports.

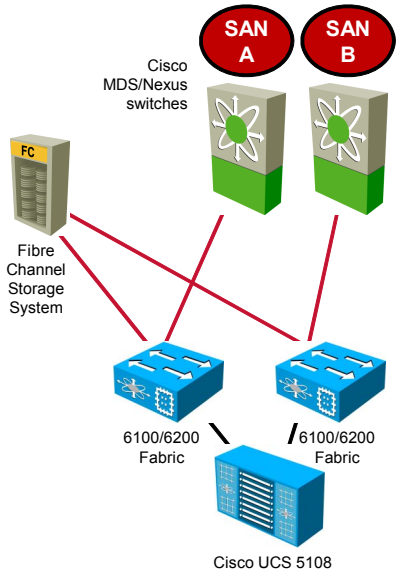
Starting from version 1.4, the Fibre Channel uplink ports can also be combined in Fibre Channel port channels. On the upstream switch, the same configuration must be performed.

Because the fabric interconnects can operate in 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

Fibre Channel Storage Ports

- Fibre Channel storage ports are used for direct-attached Fibre Channel storage.
- Fibre Channel switching mode is required.
- Zoning must be inherited from a Cisco MDS or Cisco Nexus 5000 switch.
- Trunking is not supported on Fibre Channel storage ports
- Fibre Channel port channels are not supported on Fibre Channel storage ports.
- The Fibre Channel storage ports operate in F mode.



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

Beginning with Cisco UCS Manager version 1.4, there is a new role that is called Fibre Channel storage port. This role allows a Fibre Channel storage system to be directly attached. 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.

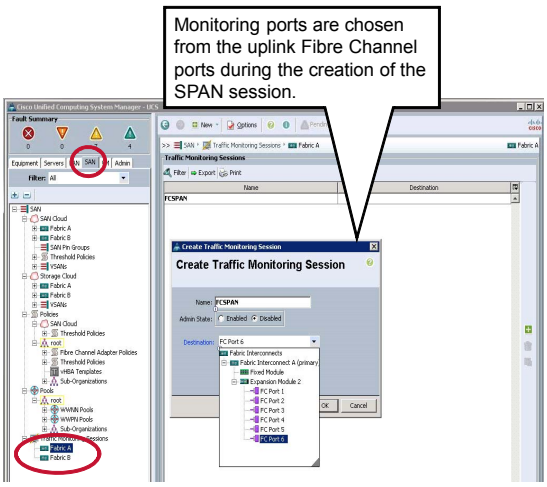
The Fibre Channel storage ports operate as F Ports and do not support VSAN trunking and Fibre Channel port channels.

Currently, 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.

https://t.me/learningnets

Fibre Channel Monitoring Port Personality

- SPAN-based monitoring of Fibre Channel traffic
- Fibre Channel SPAN destination ports are Ethernet or Fibre Channel ports
- Fibre Channel SPAN sources can be the following:
  - Uplink Fibre Channel ports
  - SAN port channels
  - VSAN
  - vHBAs
  - Fibre Channel storage ports
- A Fibre Channel port on Cisco UCS 6248UP cannot be a SPAN source.



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

Cisco UCS supports the SPAN protocol to capture and monitor server traffic. You can capture Ethernet or Fibre Channel traffic. To create a Fibre Channel SPAN session, navigate to **SAN > Traffic Monitoring Sessions**.

The following are components of a Fibre Channel SPAN monitoring session:

- **SPAN sources:** This component is where traffic will be captured.
  - Uplink Fibre Channel ports
  - Uplink SAN port channels
  - VSANs
  - vHBAs
  - Fibre Channel storage ports
  - Fibre Channel port on Cisco UCS 6248UP cannot be a source port.
- **SPAN destination:** This component is the port to which the captured data will be sent for analysis, and is also called the monitoring port. The port can be any Fibre Channel uplink port. The port is selected during the creation of the monitoring session and will no longer be used by the system as an uplink port.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Benefits and Drawbacks of Fibre Channel Switching and NPV

This topic describes the differences between NPV and Fibre Channel switching modes.

NPV vs. Fibre Channel Switching Mode

NPV Mode	Fibre Channel Switching Mode
No Fibre Channel switching	Limited Fibre Channel switching
No zoning required	Default zoning or zone merge (no zoning configuration supported)
No Fibre Channel domain ID	Fibre Channel domain ID
Fibre Channel port channels	Fibre Channel port channels
Trunking	Trunking
NP_Port to F_Port	N_Port to F_Port

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

For large enterprise SANs, scalability is a critical concern. If the fabric interconnect operates in Fibre Channel switching mode, a Fibre Channel domain ID is consumed. Because there are only 239 possible domain IDs available within the Fibre Channel addressing schema, introducing a six- or eight-port Fibre Channel switch can severely limit how large a SAN can grow.

In NPV mode, the fabric interconnect appears to the Fibre Channel switch as a node. As such, no domain ID is required on behalf of the fabric interconnect.

Also, in NPV mode the Fibre Channel services are not operating, which means that the hardware of the fabric interconnects is not loaded.

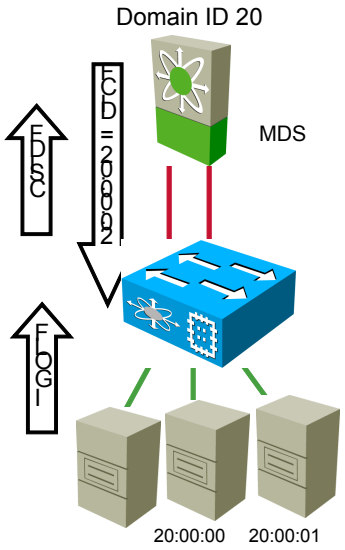
https://t.me/learningnets

N-Port ID Virtualization

This topic describes the NPIV feature.

NPV Login and Addressing

- FLOGI
  - When a blade server sends FLOGI, the fabric interconnect proxies using FDISC.
  - When WWPN is registered with the name server, an FCID is returned to the host.
- Zoning
  - Zoning can be based on host WWPN or WWNN.
  - Zoning configuration is performed on the uplink FC switch.



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

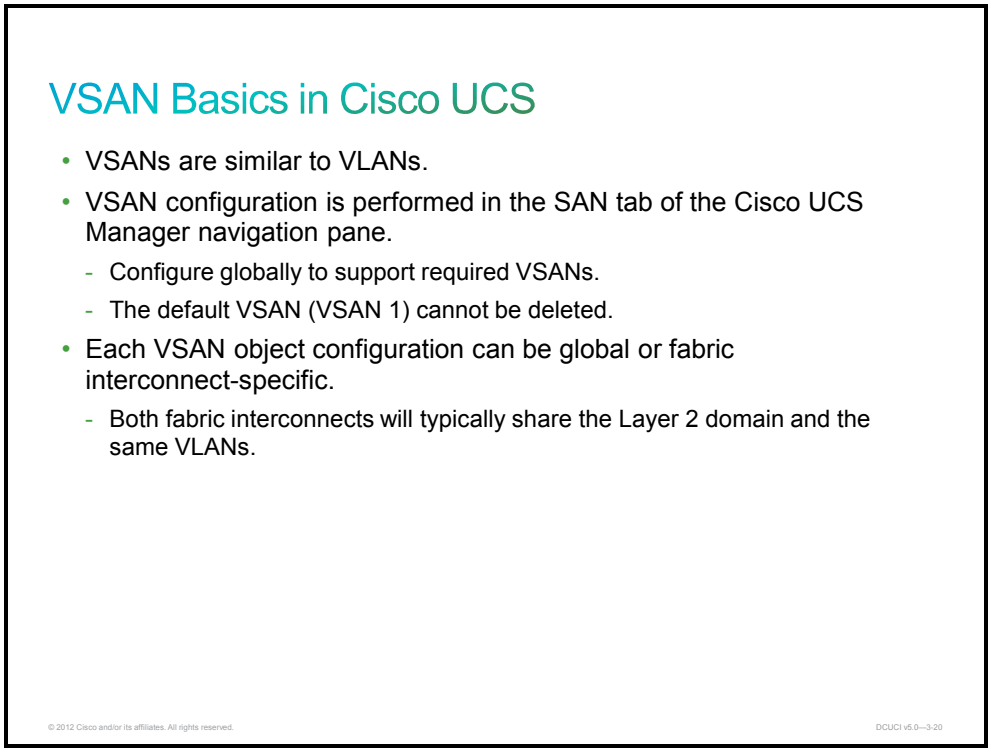
Using NPV, each downstream device (server or blade server) will be pinned to an uplink port based on a round-robin algorithm. The NPV mode switch will no longer service FLOGI requests, operate the name service, perform zoning, or make routing decisions using Fabric Shortest Path First (FSPF). Instead, these operations are passed to the upstream switch, which is known as the NPV core switch. The NPV core switch will use NPIV to interpret multiple logins from the same port.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

VSAN Support in Cisco UCS Manager

This topic describes VSAN support in Cisco UCS.



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

Cisco UCS Manager supports a maximum of 32 active VSANs.

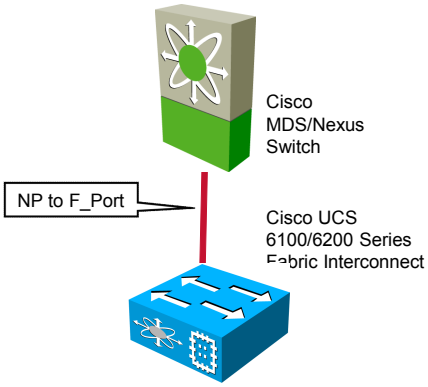
VSAN IDs that are supported are in the range from 1 to 4093. VSAN ID 4079 is reserved because it is used by other protocols in SAN infrastructures. In Cisco NPV mode, VSAN IDs 3840 to 4079 are not available.

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

https://t.me/learningnets

Uplink Switch Configuration

- All ports on the northbound switch that connect to fabric interconnect uplinks must be configured as F Ports.
- If in trunking mode, the same VSANs must be allowed on both ends.
- In NPV mode with trunking enabled, the ports on the fabric interconnect will be TNP and on the Cisco MDS/Nexus will be TF.
- In Fibre Channel switching mode with trunking enabled, the ports on both sides will be TE.



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

The Fibre Channel uplink on the northbound Fibre Channel switch must be configured as an F Port on the same VSAN as the other end of the link on the fabric interconnect. There is a limit of one VSAN per Fibre Channel uplink.

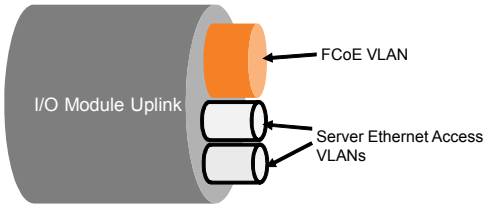
Although the Fibre Channel switching hardware is physically capable of forming Fibre Channel port channels in the same trunking, it currently is not supported in NPV mode.

© 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 FCoE architecture of Cisco UCS, each VSAN that is 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. It is a best practice to dedicate an unused range of VLANs to FCoE traffic.

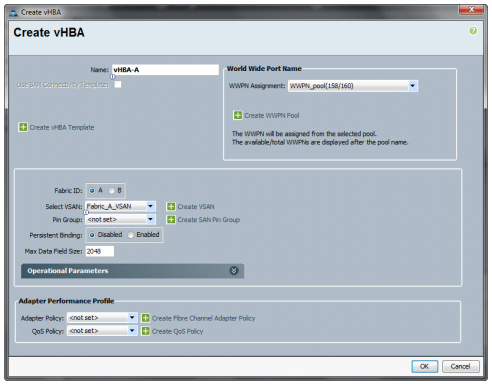
https://t.me/learningnets

Role of vHBAs

This topic describes the role of vHBAs.

Locally Administered WWNNs

- vHBA is one of the abstractions of HBA characteristics that is tied to a service profile instead of a physical adapter.
- WWNN and WWPN can be assigned manually or with WWNN and WWPN address pools.



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

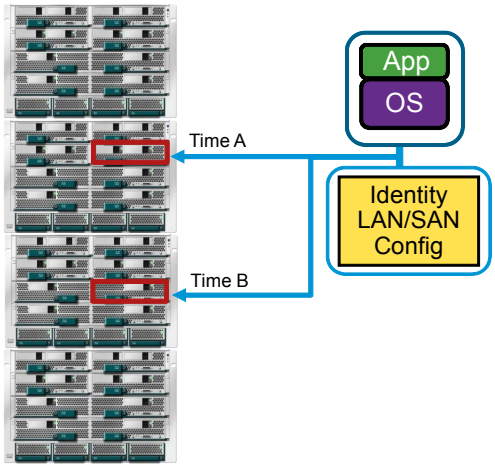
The vHBA is the component in the service profile that contains the configuration of the HBA of the server. In the vHBA configuration, you specify how world wide name (WWN) addresses will be assigned to the HBA of the server. Locally administered Fibre Channel WWNs are another identity resource that can be virtualized and abstracted from hardware in a Cisco UCS service profile. Stateless computing is one of the cornerstone values of Cisco UCS. Cisco UCS administrators have the option of manually configuring WWNs based on the prefix that is supplied by Cisco, using an identity pool, or the burned-in world-wide node name (WWNN) or world-wide port name (WWPN).

Abstracting WWNs in Fibre Channel networks is particularly important. If you use burned-in names and the service profile moves to a new blade server, it will not be able to find its boot logical unit number (LUN) until the SAN administrator rezones the fabric for the new WWNN or WWPN. Using local addressing allows Cisco UCS administrators to move a service profile to a replacement blade server. The old WWNN or WWPN will be preserved when the operating system or hypervisor boots.

https://t.me/learningnets

vHBA WWN Address Portability

- WWNN and WWPN addressing moves with the service profile from blade to blade.



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

The main benefit of virtualizing Fibre Channel WWNs is that if the underlying server hardware fails, a service profile is simply moved to a replacement server. When the operating system boots on the new server, the WWNs are unchanged. From the perspective of the operating system or hypervisor running on the blade server, the service profile is on the same hardware from which it was last booted.

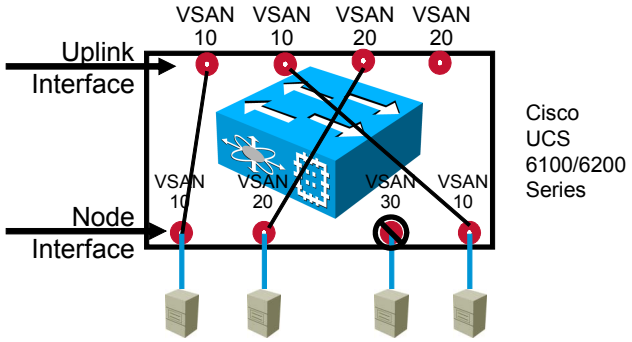
https://t.me/learningnets

Automatic Pinning and Recovery from Failure

This topic describes the automatic pinning process and the recovery from failure.

Uplink Pinning with Multiple VSANs

- When multiple VSANs are introduced on border interfaces and no VSAN trunking is enabled, pinning is based on VSAN.
  - Server interfaces are only pinned to border interfaces with matching VSANs.
  - If no interface is available with a matching VSAN, the link is kept down.



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

By default, uplink interfaces and node interfaces are configured for a single VSAN. You can enable VSAN trunking and then all VSANs will be allowed on the Fibre Channel uplinks. But if you do not work with VSAN trunking, then the node interfaces will only be pinned to a port of the correct VSAN.

The example in the figure shows the following:

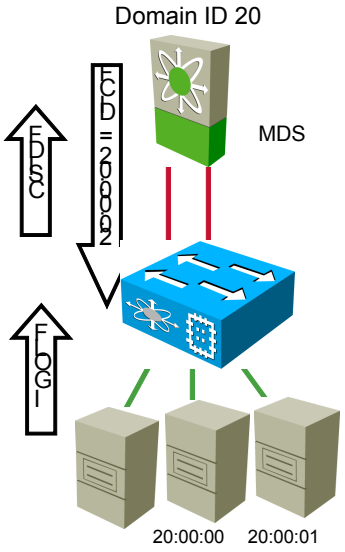
- Two uplink interfaces are configured for VSAN 10 and the other two are configured for VSAN 20.
- Two blade ports are configured for VSAN 10.
- One blade port is configured for VSAN 20.
- One server port is configured for VSAN 30.
- The blades that are configured for VSAN 10 will be pinned on one of the VSAN 10 border interfaces.
- The blade that is configured for VSAN 20 will be pinned to one of the VSAN 20 border interfaces.
- The blade interface that is configured for VSAN 30 will be kept down because there is no matching uplink interface.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Uplink Pinning and Load Balancing

- Pinning
  - Server interfaces pinned to uplink interfaces (not FLOGI).
- Data packets on the server interface
  - Packets are sent to the pinned interface without forwarding lookup. (NPV switches do not participate in FSPF.)
  - Binding checks are performed to ensure that the server IDs are on the right server interface, to prevent address spoofing.
- Load balancing
  - Fibre Channel is inherently multipathing, but the host must run a multipath I/O driver to load-balance.



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

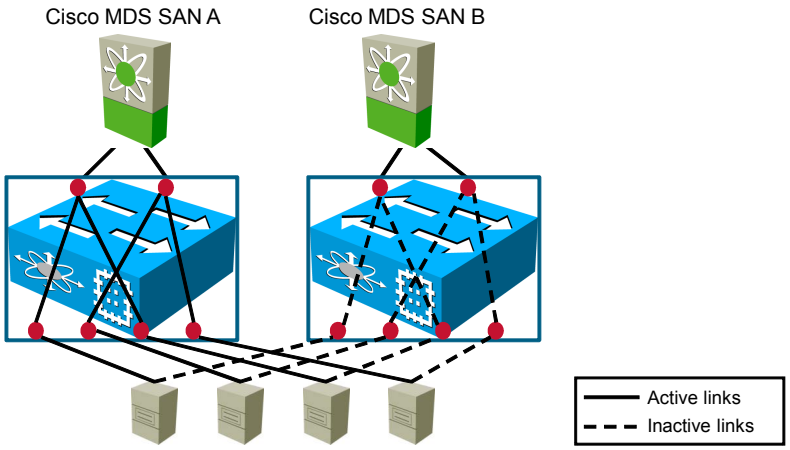
Using NPV, each downstream device (server or blade server) will be pinned to an uplink port based on a round-robin algorithm. These operations are passed to the upstream switch, which is known as the NPV core switch. The NPV core switch will use NPIV to interpret multiple logins from the same port.

Although Fibre Channel is inherently multipathing, load balancing and discovery of path failure are the responsibility of the multipath I/O driver in the operating system or hypervisor. The hardware failover option that is available for Ethernet does not affect Fibre Channel traffic.

https://t.me/learningnets

Uplink Pinning with VSAN Trunking

- Server WWN on Fabric A is pinned to an uplink port in a round-robin assignment.
- With VSAN trunking enabled, all VSANs are allowed on all Fibre Channel uplinks.



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

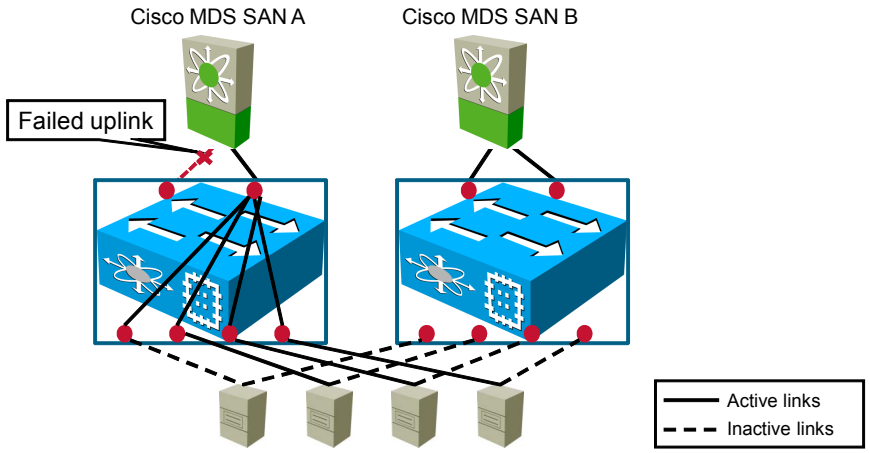
Recall from the discussion of end-host virtualization mode that a loop-free topology is assured by pinning MAC addresses to uplink ports. This pinning process can be either automatic or statically configured. By default, server MAC addresses are pinned to uplink interfaces in a round-robin process. The same process is followed with Fibre Channel traffic. With VSAN trunking, because all of the VSANs are allowed, the automatic pinning of server traffic to Fibre Channel uplink ports will be based only on the server WWN. This also depends on the VSANs that are allowed. If the VSAN of the server is not allowed on the uplink port, then the Fibre Channel communication for the server will be disrupted.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Automatic Uplink Repinning

- If an uplink goes down, affected servers will be automatically repinned to an available uplink on the same VSAN.



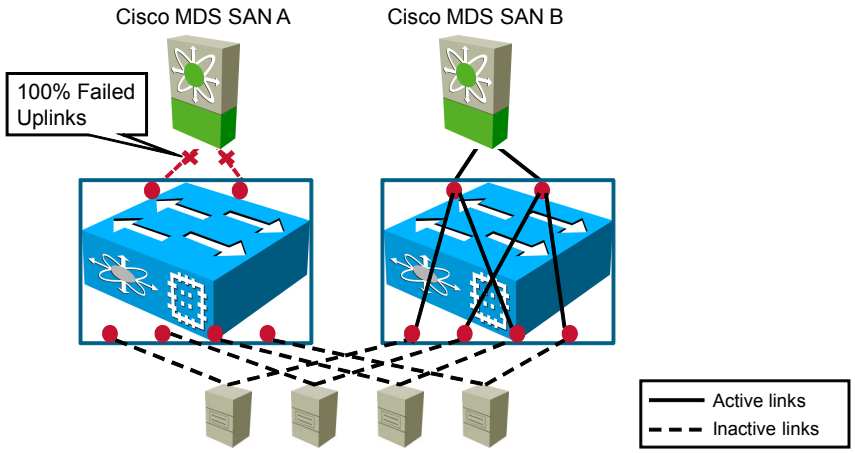
© 2012 Cisco and/or its affiliates. All rights reserved.

With automatic uplink pinning, a link failure will cause all servers to be repinned to the remaining uplinks. In the example, there are two uplinks on fabric A. When one of the links goes down, the server simply repins to the remaining uplink.

https://t.me/learningnets

Loss of Uplinks Causes Fabric Failover

- If all Fabric A uplinks go down, the multipath driver in the host operating system or hypervisor discards the path Fabric A.



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

If all uplink ports on the fabric interconnect lose connectivity, the operating system or hypervisor relies on its multipath I/O driver to discover the path loss and reroute. If the servers are not configured for high availability in the operating system or hypervisor, Fibre Channel communications will be down until at least one Fibre Channel uplink is restored on fabric A.

 © 2012 Cisco Systems, Inc.

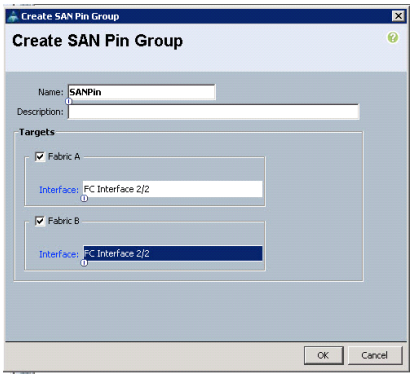
https://t.me/learningnets

Configuring Manual Pinning and Recovery from Failure

This topic describes static pinning and recovery from failure.

Static Pin Group

- Pin groups are created and bound to service profiles.
- Automatic pinning is inactive for any service profile that uses a static pin group.
- Other servers continue to be automatically pinned.



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

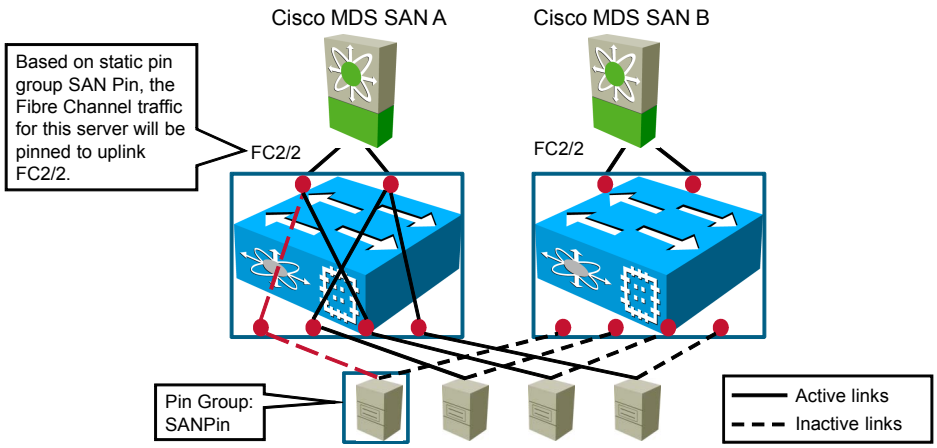
Pin groups are created under the LAN tab of the navigation pane. Pin groups are global policy elements and are replicated to the secondary management node.

In this example, any service profile that includes this pin group policy will only use uplink Fibre Channel 2/2 on fabric A. If that uplink goes down, automatic repinning will not occur and the server will rely on its multipath I/O driver to recognize the path failure and maintain connectivity on fabric B.

https://t.me/learningnets

Static Pinning

- Server WWN on Fabric A is pinned to a Fibre Channel uplink port based on the pin group assigned in the service profile.



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

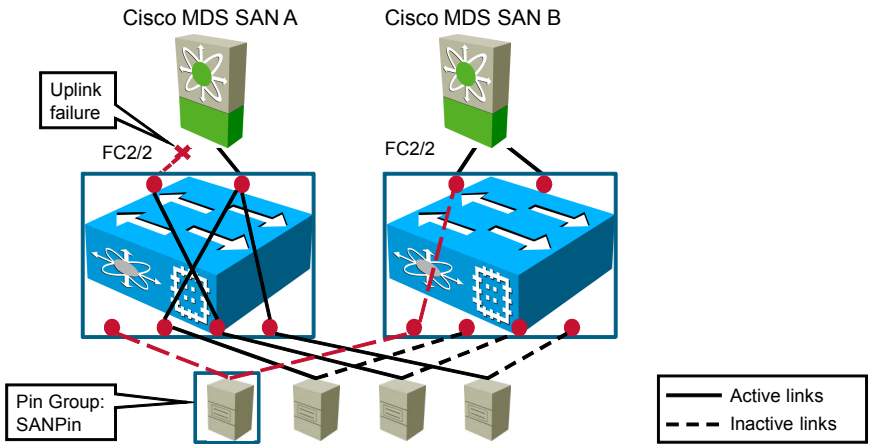
In the example, the highlighted server is configured to use the static pin group called SANPin. This server will always pin to uplink Fibre Channel 2/2 on fabric A, or Fibre Channel 2/2 on fabric B. If a multipath I/O driver is installed in the hypervisor or operating system, the HBA will operate over both fabric paths. If the pinned uplink fails on either fabric, the multipath driver is responsible for recognizing the path failure.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Static Pinning on Uplink Failure

- Upon uplink failure, the multipath driver in the operating system or hypervisor will detect path loss and discontinue using it.



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

In a static pinning environment, the operating system or hypervisor relies on its multipath I/O driver to detect path failure and discontinue using that path. If there is no multipath I/O driver, Fibre Channel communications will halt until the statically pinned uplink is restored.

https://t.me/learningnets

Ethernet Failover and Fibre Channel Multipath I/O Recovery

This topic compares Ethernet failover and Fibre Channel multipath I/O recovery.

Hardware-Based Ethernet Failover vs. Fibre Channel Multipath I/O Recovery

Hardware-Based Ethernet Failover	Fibre Channel Multipath I/O Recovery
Hardware based	Software based
Built-in feature of Cisco UCS	Vendor specific
No load balancing	Load balancing
Only one active path	Multiple active paths
For Ethernet communication (vNICs)	For Fibre Channel communication (vHBAs)
Redundancy	Redundancy
Very fast	Depends on the operating system

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

Hardware-based Ethernet failover is a feature available on the Cisco UCS Virtual Interface Card (VIC) 1280, Cisco VIC 1240, and Cisco M81KR. When this feature is enabled, the virtual interface (VIF) definition for all vHBAs is replicated to both fabric interconnects, with one being active for a given fabric. If there is a link failure, the VIF pointer is simply moved in memory to the other fabric. This yields nanosecond speed failover that is completely transparent to the operating system or hypervisor.

Fibre Channel communication must rely on vendor-specific software, which is called the multipath I/O driver. The software is installed on your server and manages the available Fibre Channel links by providing load balancing, traffic shaping, and redundancy.

https://t.me/learningnets

Summary

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

Summary

- Fibre Channel switching enforces correct port types to be matched with compatible types on each end of a link.
- NPV allows the fabric interconnect to present itself to the Fibre Channel switch as a host with many FCIDs.
- Fibre Channel ports can be Fibre Channel uplink, Fibre Channel storage, and Fibre Channel monitoring ports.
- An important benefit of NPV is not needing a domain ID to be assigned to the fabric interconnect.
- NPIV proxies a fabric login request and allows a single N Port to be associated with multiple FCIDs.
- Like VLANs, VSANs are configured in Cisco UCS Manager with a name and a number.
- vHBAs abstract WWNNs and WWPNs into a service profile and enable stateless computing.
- Automatic uplink pinning allows a vHBA to automatically be assigned to another available uplink on the same fabric, provided that it is on the same VSAN.
- Manual uplink pinning allows deterministic path selection with recovery from failure that is managed by a multipath I/O driver in the operating system or hypervisor.
- Ethernet failover is performed in hardware and used for Ethernet redundancy. Fibre Channel multipath I/O drivers are used in software to provide redundancy for Fibre Channel communication.

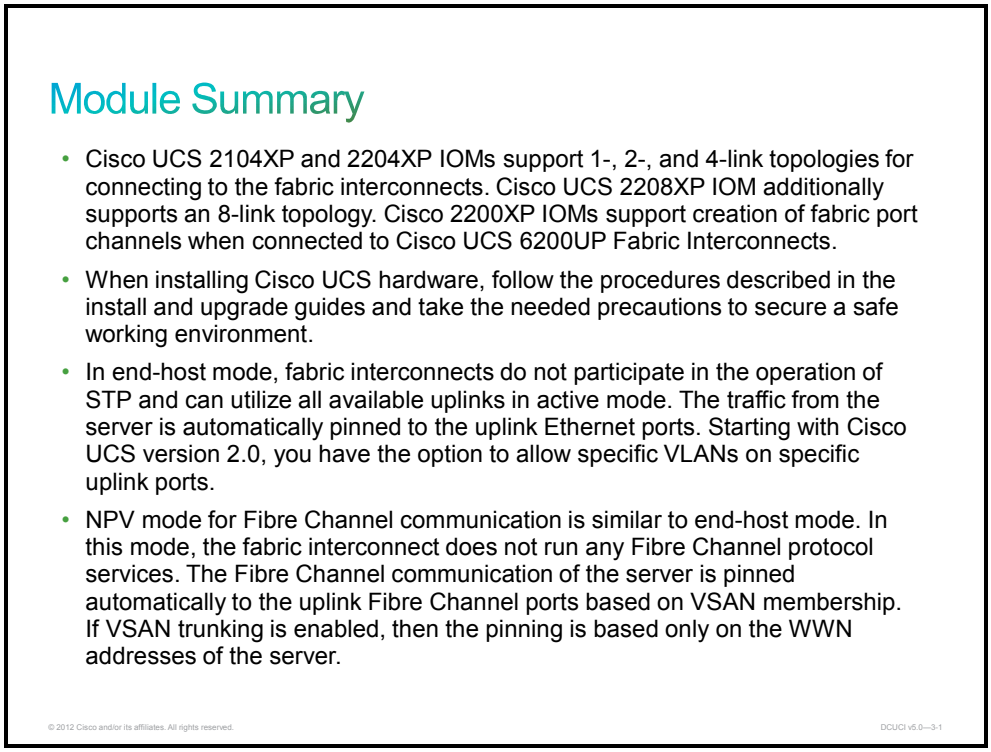
© 2012 Cisco and/or its affiliates. All rights reserved.

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 Unified Computing System (UCS) is a highly integrated system that consists of compute nodes, blade chassis, and fabric interconnects.

You must be acquainted with the procedures for physical installation of the hardware and take measures to avoid damage to the equipment caused by ESD.

Depending on the model of the I/O modules (IOMs), you can use 1-, 2-, 4-, or 8-link topologies for physical connectivity to the fabric interconnects. Based on the selected topology, the server slots will be pinned statically inside the IOMs to the uplink ports with different schemas.

Cisco Nexus Operating System (NX-OS) can operate in end-host mode or in switching mode to process Ethernet traffic. In end-host mode, the fabric interconnects do not participate in Spanning Tree Protocol (STP) and all the uplinks are active. The Cisco UCS Fabric Interconnect presents to the upstream Ethernet switch as if it is a server with multiple Ethernet interfaces. Internally, the server traffic is pinned to the uplink Ethernet ports automatically based on the MAC addresses of the servers. Starting with Cisco UCS version 2.0, there is support for disjoint Layer 2 domains. This support allows you to control which VLANs are allowed on which uplink interfaces. The default behavior of all VLANs being allowed on all uplink ports is preserved. This default means that the support for disjoint VLANs is an additional feature that you must configure if you want to use it.

For Fibre Channel traffic, Cisco NX-OS can operate in N-Port Virtualization (NPV) or in switching mode. NPV mode is similar to the end-host mode on Ethernet. In NPV mode, there are no Fibre Channel Protocol services running on the fabric interconnects. Cisco UCS does not participate in the switched fabric. Again, the Fibre Channel traffic of the server is pinned automatically to the uplink Fibre Channel ports, based on the world-wide name (WWN) addresses of the server and the VSAN membership.

For both Ethernet and Fibre Channel communication, you can perform static or manual pinning by using pin groups.

https://t.me/learningnets

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *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 Systems, Inc. *Cisco UCS 5108 Server Chassis Installation Guide* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/ucs5108_install.html
- Cisco Systems, Inc. *Cisco UCS B200 Blade Server Installation and Service Note* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/blade.html
- Cisco Systems, Inc. *Cisco UCS B440 High Performance Blade Server Installation and Service Note* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/quadblade.html
- Cisco Systems, Inc. *Cisco UCS B230 Blade Server Installation and Service Note* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/B230.html
- Cisco Systems, Inc. *Cisco UCS B250 Extended Memory Blade Server Installation and Service Note* at: http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/fullblade.html
- Cisco Systems, Inc. *Cisco UCS 2100 Series Fabric Extenders* at: http://www.cisco.com/en/US/prod/collateral/ps10265/ps10278/data_sheet_c78-524729.html
- Cisco Systems, Inc. *Cisco UCS 2200 Series Fabric Extenders Data Sheet* at: http://www.cisco.com/en/US/prod/collateral/ps10265/ps10276/data_sheet_c78-675243.html
- Cisco Systems, Inc. *Cisco UCS Virtual Interface Card 1240 Data Sheet* at: http://www.cisco.com/en/US/prod/collateral/modules/ps10277/ps12377/data_sheet_c78-699459.html
- Cisco Systems, Inc. *Cisco UCS Virtual Interface Card 1280 Data Sheet* at: http://www.cisco.com/en/US/prod/collateral/ps10277/ps11551/data_sheet_c78-677682.html
- Cisco Systems, Inc. *Cisco UCS M81KR Virtual Interface Card Data Sheet* at: http://www.cisco.com/en/US/prod/collateral/ps10265/ps10280/data_sheet_c78-525049_ps10277_Products_Data_Sheet.html
- Cisco Systems, Inc. *Cisco UCS CNA M72KR-Q QLogic Converged Network Adapter* at: http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-623738.html
- Cisco Systems, Inc. *Cisco UCS NIC M51KR-B Broadcom BCM57711 Network Adapter Data Sheet* at http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-624706.html
- Cisco Systems, Inc. *Cisco UCS CNA M61KR-I Intel Converged Network Adapter* at: http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-623739.html
- Cisco Systems, Inc. *Cisco UCS CNA M72KR-E Emulex Converged Network Adapter* at: http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-623740.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 three uplink topologies are supported with Cisco UCS 2104/2204XP IOMs? (Choose three.) (Source: Implementing Cisco UCS B-Series Physical Connectivity)

A) 1-link
B) 2-link
C) 3-link
D) 4-link
E) 6-link
F) 8-link

Q2) Which four uplink topologies are supported by Cisco UCS 2208XP IOMs? (Choose four.) (Source: Implementing Cisco UCS B-Series Physical Connectivity)

A) 1-link
B) 2-link
C) 3-link
D) 4-link
E) 6-link
F) 8-link

Q3) Which combination of fabric interconnects and IOMs supports fabric port channels? (Source: Implementing Cisco UCS B-Series Physical Connectivity)

A) Cisco UCS 6120 and 2104
B) Cisco UCS 6140 and 2104
C) Cisco UCS 6248UP and 2204
D) Cisco UCS 6248UP and 2208
E) Cisco UCS 6248UP and 2104

Q4) Which three options are components of an IOM? (Choose three.) (Source: Implementing Cisco UCS B-Series Physical Connectivity)

A) CMC
B) Cisco IMC
C) CMS
D) I/O MUX
E) HBA
F) NIC

Q5) What is the maximum number of VIFs (vNICs and vHBAs) supported on Cisco UCS VIC 1280 and Cisco UCS VIC 1240 with Cisco UCS version 2.0? (Source: Implementing Cisco UCS B-Series Physical Connectivity)

A) 36
B) 58
C) 92
D) 116
E) 124
F) 256

https://t.me/learningnets

Q6) Identify four recommended ESD best practices when working with Cisco UCS components? (Choose four.) (Source: Installing Cisco UCS B-Series Hardware)

A) antistatic sprays
B) hold a colleague
C) ESD wrist-strap
D) ESD tie
E) ESD work surface
F) ESD-shielded packaging
G) ESD pants

Q7) Which two steps are required to open the cover of a Cisco UCS B-Series server? (Choose two.) (Source: Installing Cisco UCS B-Series Hardware)

A) Remove screws.
B) Press release button.
C) Use vacuum hand cups.
D) Slide the cover to remove it.

Q8) How much does an empty Cisco UCS 5108 blade chassis weigh? (Source: Installing Cisco UCS B-Series Hardware)

A) 80 lbs (36 kilos)
B) 90 lbs (41 kilos)
C) 110 lbs (50 kilos)
D) 290 lbs (132 kilos)

Q9) Which type of rack hole is required to install the Cisco UCS 5108 blade server chassis? (Source: Installing Cisco UCS B-Series Hardware)

A) round
B) square
C) EIA/TIA elliptical
D) flat

Q10) What must be installed in place of an empty CPU socket of the Cisco UCS B440 server? (Source: Installing Cisco UCS B-Series Hardware)

A) protective cap
B) CPU emulator
C) CPU air blocker
D) Cisco ASIC

Q11) Which four options are Ethernet port personalities? (Choose four.) (Source: Implementing Cisco UCS B-Series LAN Connectivity)

A) uplink
B) server
C) FEX
D) appliance
E) Fibre Channel storage
F) Ethernet storage
G) Fibre Channel monitoring

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Q12) Which port channel protocol is supported in Cisco UCS? (Source: Implementing Cisco UCS B-Series LAN Connectivity)

A) PAgP
B) LACP
C) PPTP
D) VRRP

Q13) MAC addresses are stored in a forwarding table for which port type in end-host mode? (Source: Implementing Cisco UCS B-Series LAN Connectivity)

A) uplink ports
B) server ports
C) monitoring ports
D) cluster ports

Q14) Which item is used to make the automatic uplink decision from the Cisco UCS Fabric Interconnect to an upstream switch in Cisco NX-OS? (Source: Implementing Cisco UCS B-Series LAN Connectivity)

A) destination MAC address
B) server MAC address
C) TCP port number
D) upstream Ethernet switch MAC address

Q15) How must VLANs be created if you are going to use disjoint Layer 2 domains? (Source: Implementing Cisco UCS B-Series LAN Connectivity)

A) globally with different configuration
B) globally with the same configuration
C) only on Fabric A
D) only on Fabric B

Q16) Which port type do Fibre Channel HBAs use to connect to a Cisco MDS Fibre Channel switch? (Source: Implementing Cisco UCS B-Series SAN Connectivity)

A) F port
B) E port
C) TE port
D) NP port
E) N port

Q17) What is the port type of an uplink Fibre Channel port on an NPV edge switch? (Source: Implementing Cisco UCS B-Series SAN Connectivity)

A) FP port
B) NE port
C) NP port
D) TN port

Q18) Which two Fibre Channel port personalities are correct? (Choose two.) (Source: Implementing Cisco UCS B-Series SAN Connectivity)

A) Fibre Channel uplink
B) Fibre Channel storage
C) FCoE monitoring
D) FCoE storage
E) Fibre Channel switch server

https://t.me/learningnets

Q19) Which two parameters are used by Cisco UCS for automatic Fibre Channel uplink pinning? (Choose two.) (Source: Implementing Cisco UCS B-Series SAN Connectivity)

A) server WWN
B) MDS WWNN
C) VSAN membership
D) hash algorithm
E) vHBA MAC address

Q20) Which statement about fabric failover for Fibre Channel communication is true? (Source: Implementing Cisco UCS B-Series SAN Connectivity)

A) You can enable hardware Fibre Channel failover.
B) Cisco UCS load balances Fibre Channel traffic between the two fabrics.
C) You must use a Fibre Channel multipath I/O driver.
D) You do not have to use anything.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module Self-Check Answer Key

Q1) A, B, D

Q2) A, B, D, F

Q3) D

Q4) A, C, D

Q5) D

Q6) A, C, E, F

Q7) B, D

Q8) B

Q9) B

Q10) C

Q11) A, B, D, G

Q12) B

Q13) B

Q14) B

Q15) B

Q16) E

Q17) C

Q18) D, E

Q19) A, C

Q20) C

https://t.me/learningnets

© 2012 Cisco Systems, Inc.

https://t.me/learningnets