DCUCT

Troubleshooting Cisco Data Center Unified Computing

Volume 1

Version 5.0

Student Guide

Text Part Number: 97-3217-01

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 5
Your Training Curriculum 6
Additional Resources 8
Introductions 10

Cisco UCS B-Series Troubleshooting ***1-1***

Overview 1-1
Module Objectives 1-1

Troubleshooting Cisco UCS B-Series Architecture and Initialization **1-3**

Overview 1-3
Objectives 1-3
Cisco UCS System Architecture 1-4
Extended Statelessness: Service Profiles 1-5
Converged Networking: Unified Fabric 1-5
Enhanced Virtualization 1-5
Expanded Scalability 1-5
Simplified Management 1-5
Cisco UCS B22 M3 Server Blade 1-6
Cisco UCS B200 M3 Server Blade 1-6
Cisco UCS B250 M2 Server Blade 1-7
Cisco UCS B230 M2 Server Blade 1-7
Cisco UCS B420 M3 Server Blade 1-8
Cisco UCS B440 M2 Server Blade 1-8
Cisco Troubleshooting Methodology 1-20
Troubleshoot Cisco UCS System Initialization 1-22
Gather Information with Embedded Tools 1-38
Troubleshoot Cisco UCS Hardware Discovery 1-54
Summary 1-66

Troubleshooting Cisco UCS B-Series Configuration **1-67**

Overview 1-67
Objectives 1-67
Cisco UCS B-Series Configuration 1-68
Cisco UCS Server Deployment Configuration 1-73
Troubleshoot Cisco UCS Server Deployment 1-79
Troubleshoot Cisco UCS Management Configuration 1-91
Organization 1-94
Locale 1-94
Role-Based Access Control 1-94
Cisco UCS Password Recovery 1-107
Summary 1-114

Troubleshooting Cisco UCS B-Series Operation **1-115**

Overview 1-115
Objectives 1-115
Cisco UCS Power Management 1-116
Troubleshoot UCS Manager Remote Access 1-128
Troubleshoot Cisco UCS B-Series Server Boot 1-134
Troubleshoot Operating System Software Drivers 1-138
Summary 1-145

https://t.me/learningnets

Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity 1-147
Overview 1-147
Objectives 1-147
Cisco UCS B-Series LAN Connectivity 1-148
Cisco UCS B-Series LAN Connectivity Troubleshooting 1-154
Troubleshoot Redundant Connectivity 1-165
Cisco UCS B-Series SAN Connectivity 1-168
Troubleshoot Cisco UCS B-Series SAN Connectivity 1-174
Troubleshoot Cisco UCS B-Series SAN Boot 1-181
SPAN for Troubleshooting 1-183
Verify Packet Flow 1-187
Troubleshoot Cisco UCS Integration with Virtualization Platform 1-195
Summary 1-202
References 1-202
Troubleshooting and Upgrading Cisco UCS Manager 1-203
Overview 1-203
Objectives 1-203
Firmware Packaging Identification 1-204
Cisco UCS Firmware Installation Plan 1-211
Firmware Levels on Cisco UCS Components 1-215
Firmware Upgrade Process 1-217
Summary 1-231
Troubleshooting Cisco UCS B-Series Hardware 1-233
Overview 1-233
Objectives 1-233
Defective Hardware 1-234
Memory Troubleshooting 1-253
Summary 1-263
References 1-263
Module Summary 1-265
References 1-265
Module Self-Check 1-267
Module Self-Check Answer Key 1-271

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

DCUCT

Course Introduction

Overview

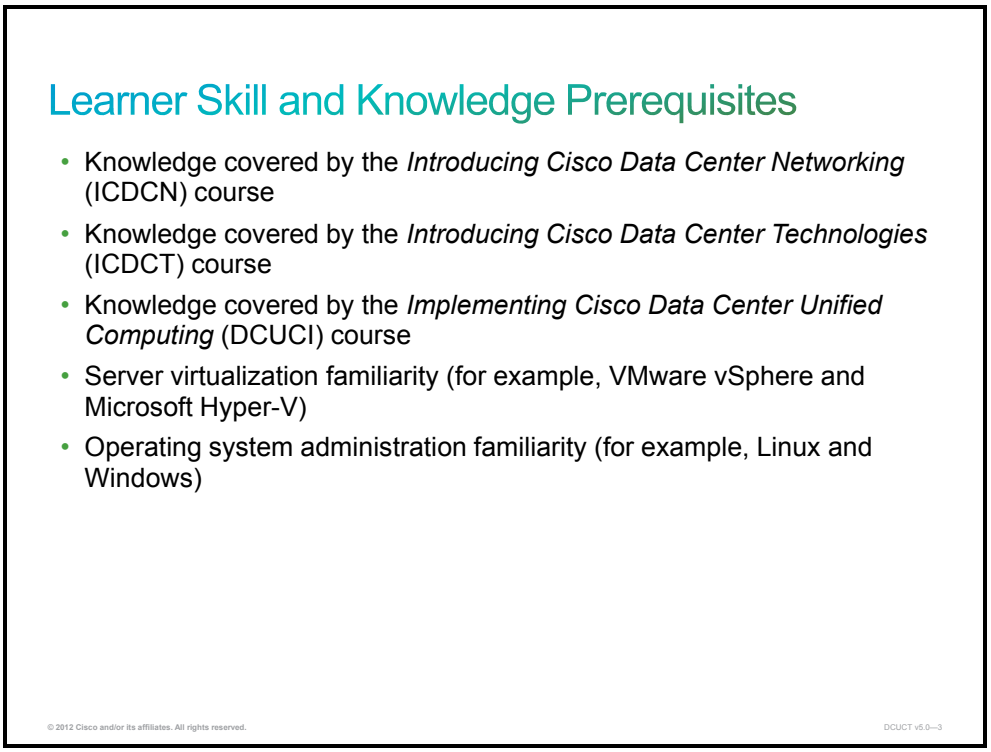
Troubleshooting Cisco Data Center Unified Computing (DCUCT) v5.0 is a three-day instructor-led training (ILT) course that provides system engineers and implementers with the knowledge and hands-on experience to properly troubleshoot Cisco Unified Computing System (Cisco UCS) B-Series and C-Series servers that are operating in standalone and integrated modes.

The student will gain hands-on experience with proper configuration procedures and will become familiar with common troubleshooting scenarios and recommended solutions.

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 students should first complete to benefit fully from this course.



The knowledge and skills that a learner must have before attending this course are as follows:

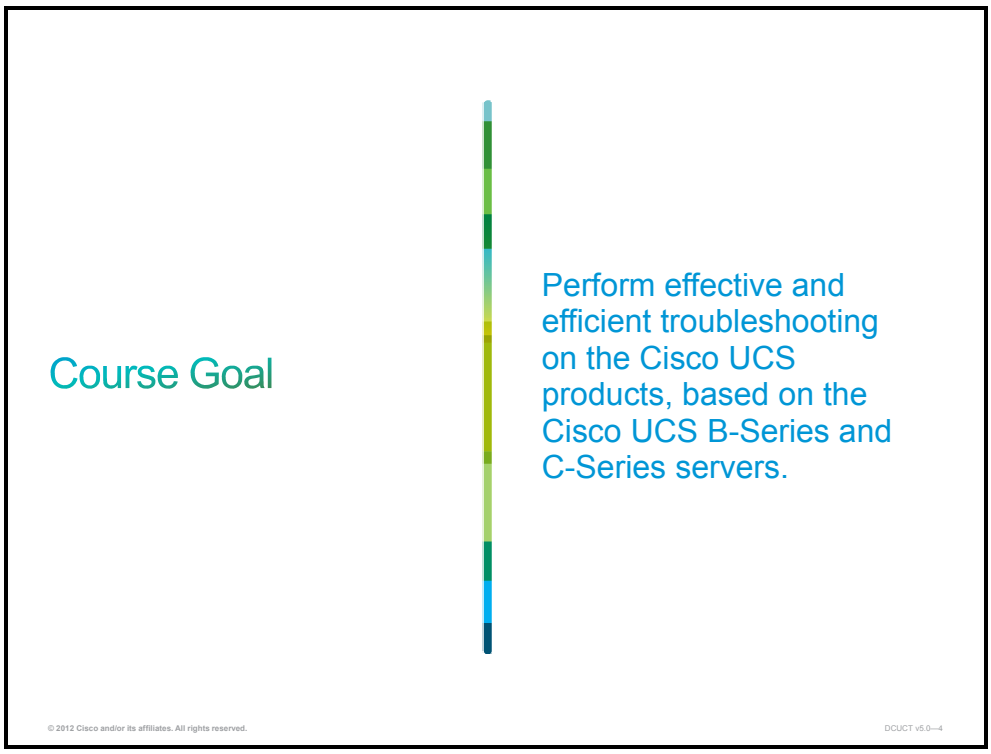
- Knowledge covered by the *Introducing Cisco Data Center Networking* (ICDCN) course
- Knowledge covered by the *Introducing Cisco Data Center Technologies* (ICDCT) course
- Knowledge covered by the *Implementing Cisco Data Center Unified Computing* (DCUCI) course
- Server virtualization familiarity (for example, VMware vSphere and Microsoft Hyper-V)
- Operating system administration familiarity (for example, Linux and Windows)

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Course Goal and Objectives

This topic describes the course goal and objectives.



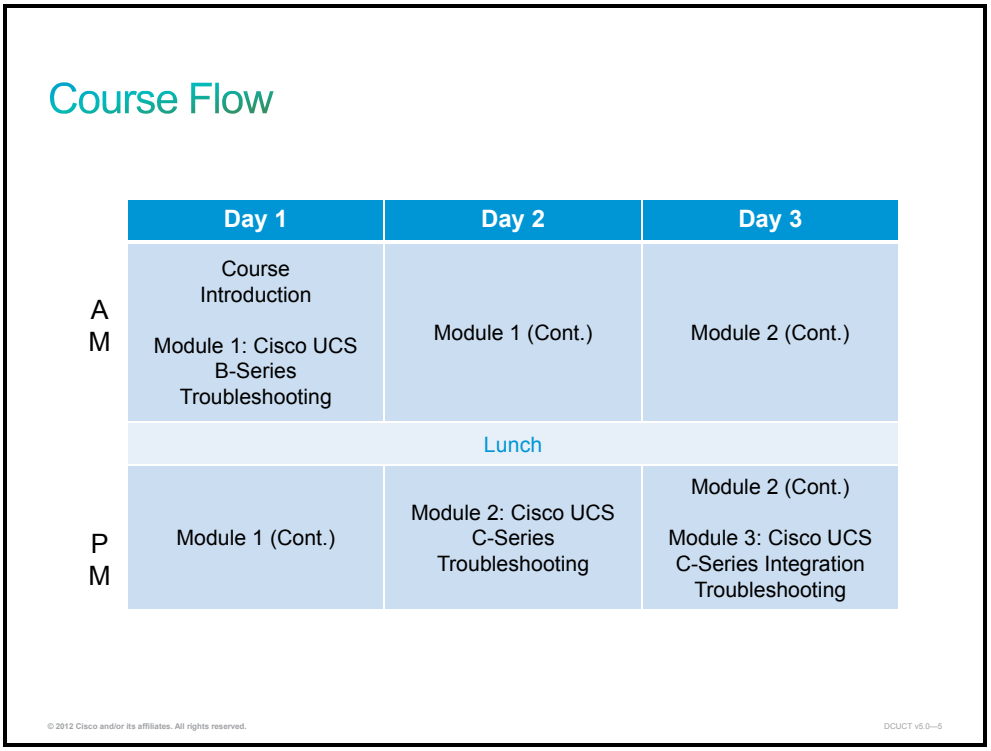
Upon completing this course, you will be able to meet these objectives:

- Describe the Cisco UCS B-Series architecture, installation, and configuration, as well as the process and tools for troubleshooting related issues
- Describe troubleshooting processes on the standalone Cisco UCS C-Series deployments
- Describe the valid Cisco UCS C-Series integrated architecture and the process of determining issues that are related to integration of the Cisco UCS C-Series server with Cisco UCS Manager

https://t.me/learningnets

Course Flow

This topic presents the suggested flow of the course materials.



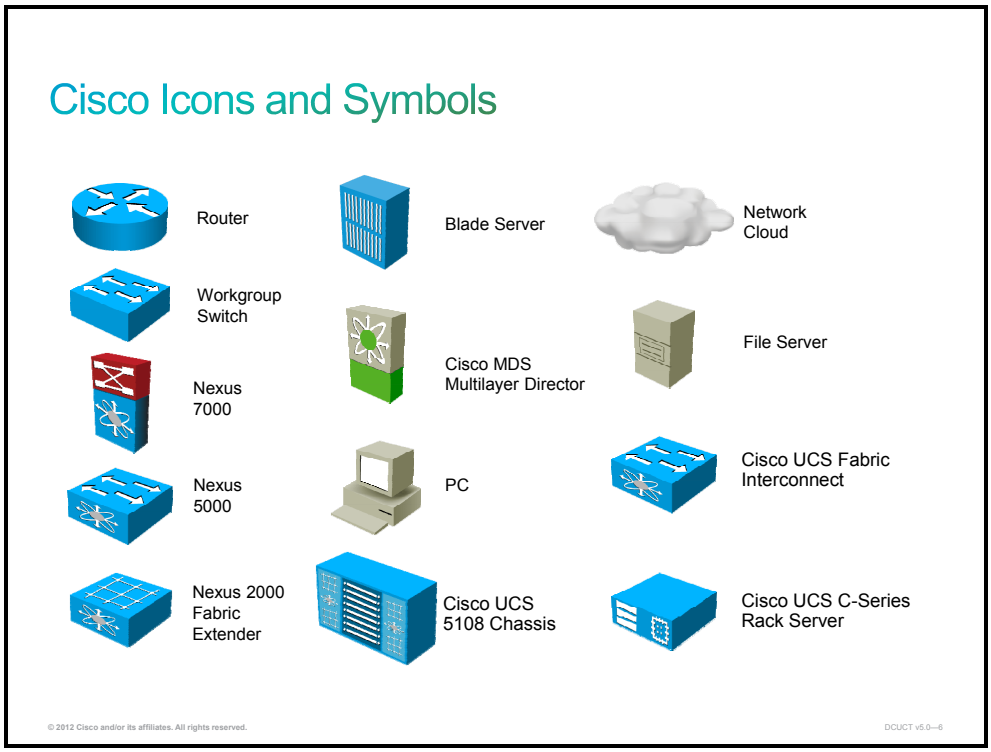
The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

© 2012 Cisco Systems, Inc.

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 Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* at http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA).

https://t.me/learningnets

Your Training Curriculum

This topic presents the training curriculum for this course.

The Cisco Learning Network

Developing a world of talent through collaboration, social learning, online assessment, and mentoring

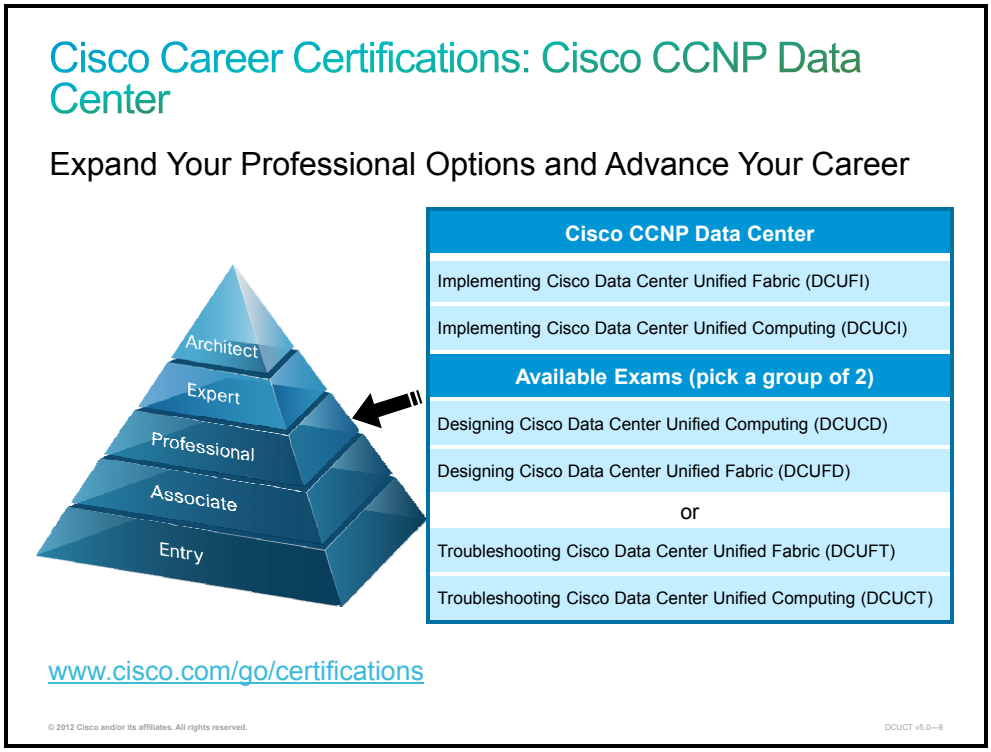
https://learningnetwork.cisco.com

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

DCUCT v5.0—7

To prepare and learn more about IT certifications and technology tracks, visit The Cisco Learning Network at https://learningnetwork.cisco.com.

https://t.me/learningnets



You are encouraged to join the Cisco Certification Community, a discussion forum that is open to anyone holding a valid Cisco Career Certification:

- Cisco CCDE®
- Cisco CCIE®
- Cisco CCDP®
- Cisco CCNP®
- Cisco CCNP® Data Center
- Cisco CCNP® Security
- Cisco CCNP® Service Provider
- Cisco CCNP® Service Provider Operations
- Cisco CCNP® Voice
- Cisco CCNP® Wireless
- Cisco CCDA®
- Cisco CCNA®
- Cisco CCNA® Data Center
- Cisco CCNA® Security
- Cisco CCNA® Service Provider
- Cisco CCNA® Service Provider Operations
- Cisco CCNA® Voice
- Cisco CCNA® Wireless

The forum is a gathering place for Cisco certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit http://www.cisco.com/go/certifications.

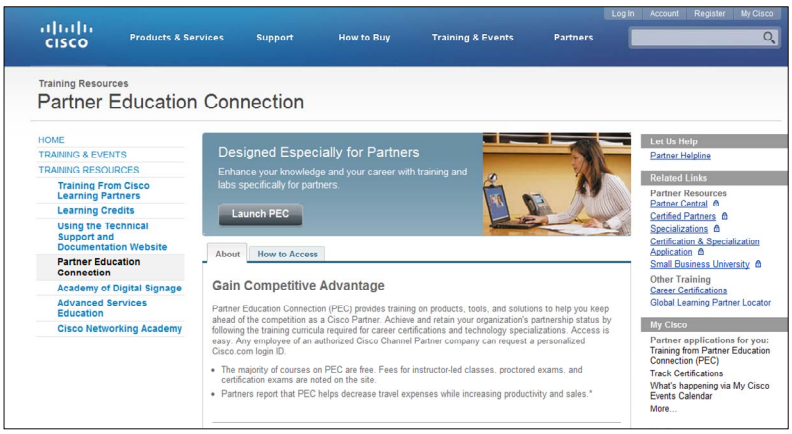
https://t.me/learningnets

Additional Resources

For additional information about Cisco technologies, solutions, and products, refer to the information that is available on these website pages: Cisco Partner Education Center, Cisco Support Community, and Cisco NetPro.

Cisco Partner Education Center

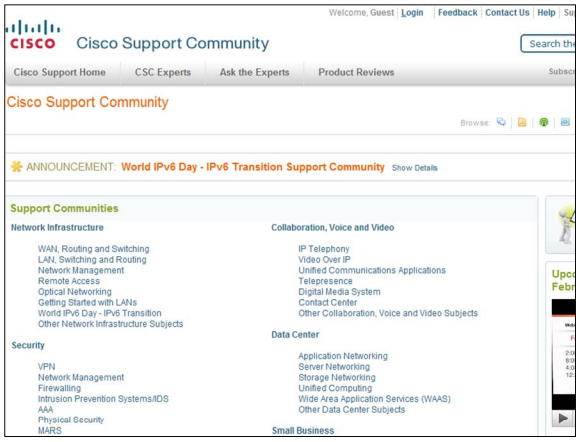
http://www.cisco.com/go/pec



© 2012 Cisco and/or its affiliates. All rights reserved.
DCUCT v5.0—9

Cisco Support Community

https://supportforums.cisco.com/index.jspa

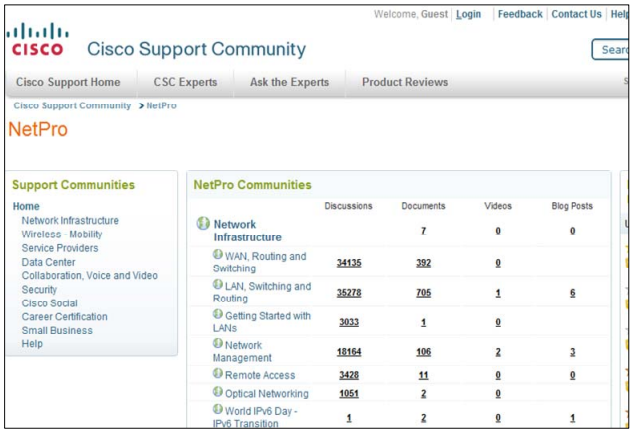


© 2012 Cisco and/or its affiliates. All rights reserved.
DCUCT v5.0—10

https://t.me/learningnets

Cisco NetPro Forums

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



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

https://t.me/learningnets

Introductions

Please introduce yourself to your classmates so that you can better understand the colleagues with whom you will share your experience.

General Administration

Class-related:

- Sign-in sheet
- Length and times
- Break and lunchroom locations
- Attire
- Cell phones and pagers

Facilities-related:

- Participant materials
- Site emergency procedures
- Restrooms
- Telephones and faxes

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

Student Introductions

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

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

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module 1

Cisco UCS B-Series Troubleshooting

Overview

Cisco Unified Computing System (Cisco UCS) B-Series offers a range of tools and service aids for troubleshooting and interpretation of output. This module provides a structured approach to troubleshooting that minimizes time to resolution. It provides learners with the knowledge that is necessary to identify the source and resolution of operational, installation, and maintenance issues.

Module Objectives

Upon completing this module, you will be able to describe the Cisco UCS B-Series architecture, installation, and configuration, as well as the process and tools for troubleshooting related issues. This ability includes being able to meet these objectives:

- Describe Cisco UCS B-Series architecture, initial setup, tools, and service aids that are available for Cisco UCS troubleshooting and interpretation
- Describe Cisco UCS B-Series configuration and troubleshooting of related issues
- Describe Cisco UCS B-Series operation and troubleshooting of related issues
- Describe LAN, SAN and Fibre Channel operations, including in-depth troubleshooting procedures
- Identify best practices that are associated with upgrading Cisco UCS components and how to identify and resolve upgrade failures
- Identify best practices for troubleshooting Cisco UCS B-Series hardware

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 1

Troubleshooting Cisco UCS B-Series Architecture and Initialization

Overview

This lesson describes Cisco Unified Computing System (Cisco UCS) B-Series architecture, initial setup, tools, and service aids that are available for Cisco UCS troubleshooting and interpretation of output.

Objectives

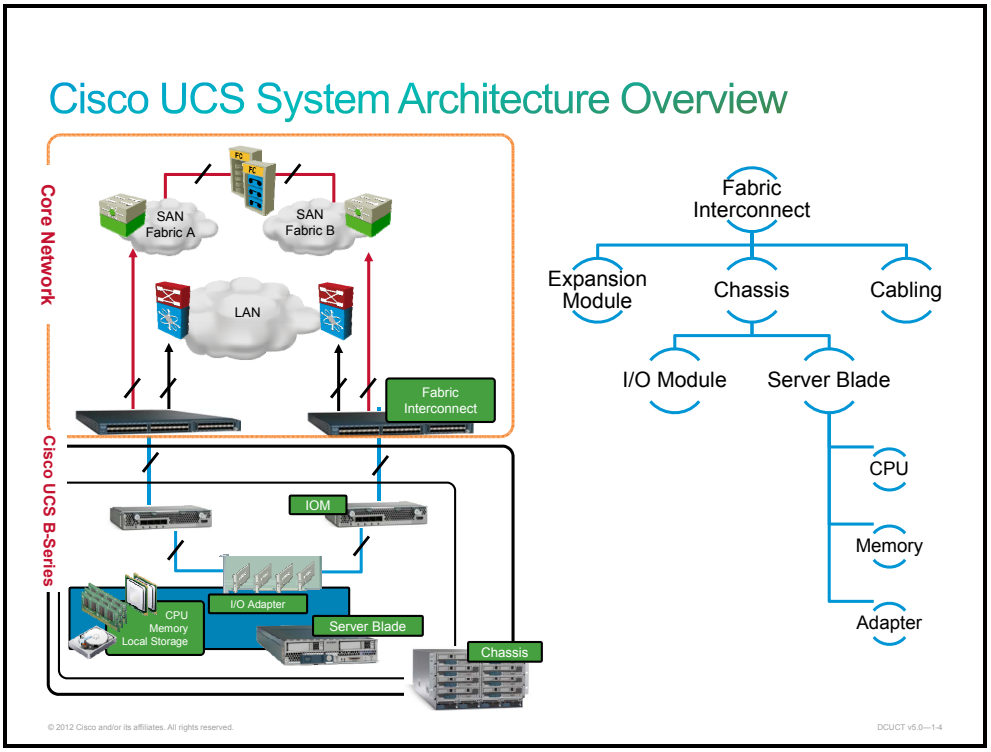
Upon completing this lesson, you will be able to describe Cisco UCS B-Series architecture, initial setup, tools, and service aids that are available for Cisco UCS troubleshooting and interpretation of output. This ability includes being able to meet these objectives:

- Identify Cisco UCS B-Series system architecture
- Understand the Cisco troubleshooting methodology
- Troubleshoot Cisco UCS B-Series system initialization
- Troubleshoot the Cisco UCS B-Series system with embedded tools
- Troubleshoot Cisco UCS B-Series hardware discovery

https://t.me/learningnets

Cisco UCS System Architecture

This topic identifies Cisco UCS B-Series system architecture.



Cisco UCS is a data center platform that represents a pool of compute resources that is connected to existing LAN and SAN core infrastructures. The system is designed to perform the following activities:

- Improve responsiveness to new and changing business demands
- Ease and accelerate design and deployment of new applications and services
- Provide a simple, reliable, and secure infrastructure

From the perspective of server deployment, Cisco UCS represents a cable-once, dynamic environment that enables the rapid provisioning of new services. Because the unified fabric is an integral part of Cisco UCS, fewer cables are required to connect the system components and fewer adapters need to be installed in the servers.

The networking aspect of the Cisco UCS ecosystem is realized with the fabric extender (FEX) concept, which results in fewer switch devices, easier configuration, and better control.

Fewer system components also result in lower power consumption, which makes the Cisco UCS solution greener. You will achieve a better power consumption ratio per computing resource.

Cisco UCS offers increased scalability because a single instance of the unified fabric can consist of up to 40 chassis, and each chassis hosts up to 8 server blades. This scalability means that the administrator has a single management and configuration point for up to 320 server blades.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Extended Statelessness: Service Profiles

Using service profiles, Cisco UCS is able to abstract the items that make a server physically unique. This ability allows the system to see the blades as being hardware-agnostic so that moving, repurposing, upgrading, and making servers highly available is simplified in Cisco UCS.

Converged Networking: Unified Fabric

A unified fabric consolidates the different network types that are used for network communications to a single 10 Gigabit Ethernet network. Cisco UCS uses a single link for all communications (data and storage), with the fabric provided through the system-controlling device. Therefore, no matter to which blade you move a server, the fabric and communications remain the same.

Enhanced Virtualization

As part of its statelessness, Cisco UCS is designed to provide visibility and control to the networking adapters within the system. This visibility and control are achieved with the software running on Cisco UCS and the implementation of the virtual interface card adapters, which, in addition to allowing the creation of virtualized adapters, also increase performance by alleviating the management overhead that is normally managed by the hypervisor.

Expanded Scalability

The larger memory footprint of the Cisco UCS B250 M2 two-socket extended memory blade server offers several advantages to applications that require more memory space. One of those advantages is the ability to provide a large memory footprint, using standard-sized and lower-cost DIMMs.

Simplified Management

Cisco UCS Manager is embedded device-management software that manages the system from end to end as a single logical entity through an intuitive GUI, a CLI, or an XML application programming interface (API). It manages all Cisco UCS devices within the domain of the Fabric Interconnect.

https://t.me/learningnets

Cisco UCS B-Series Server Comparison

Cisco UCS B-Series generations

- Gen 1
- Gen 2
- Gen 3

	Cisco UCS B22 M3	Cisco UCS B200 M3
Generation	Gen 3	Gen 3
Sockets	1 or 2 (up to 6 cores per socket)	2 (up to 8 cores per socket)
Processor	Intel Xeon E5-2400 series	Intel Xeon E5-2600 series
Memory	12 DIMMs (maximum 192 GB)	24 DIMMs (maximum 384 GB)
DIMMs	4, 8, or 16 GB DDR3 at 1333 or 1600 MHz	4 GB DDR3 at 1333 MHz; 8 or 16 GB DDR3 at 1333 or 1600 MHz
Disks	2 x 2.5" SAS, SATA , or SSD, hot-swap	2 x 2.5" SAS, SATA , or SSD, hot-swap
Storage	Up to 1.2 TB	Up to 2.0 TB
RAID	0, 1	0, 1
I/O	1 slot Up to 2 x 4 x 10 Gb/s	1 slot Up to 2 x 4 x100 Gb/s
Size	Half-width	Half-width

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

This table compares Cisco UCS B200 M3 and Cisco UCS B22 M3 with maximum hardware configurations.

Note that some models are at their end-of-support dates. Details are available on the Cisco website in the end of sale (EOS) and end of life (EOL) matrix.

Cisco UCS B22 M3 Server Blade

The Cisco UCS B22 M3 half-width server blade has the following features:

- Up to two Intel Xeon E5-2400 Series processors, which adjust server performance according to application needs
- Up to 12 x 1333 or 1600 MHz DDR3 DIMM memory, which balances memory capacity and overall density
- Two optional small form-factor (SFF) Serial Attached SCSI (SAS) hard drives or 15 mm SATA solid-state drives (SSDs), with an LSI Logic 1064e controller and integrated RAID
- One mezzanine slot for Cisco UCS Virtual Interface Card (VIC) 1280 or third party mezzanine card
- Dual 10-Gb optional modular LAN on motherboard (LOM) with Cisco UCS VIC 1240

Cisco UCS B200 M3 Server Blade

The Cisco UCS B200 M3 half-width server blade has the following features:

- Up to two Intel Xeon E5-2600 processor product family for enterprise performance and advanced capabilities
- Up to 384 GB of DDR3 RAM with 24 DIMM slots
- Up to two SAS, SATA, or SSD drives

https://t.me/learningnets

- Cisco UCS VIC 1240 is a 4 x 10 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE)-capable modular LOM and, when combined with an optional I/O expander, allows up to 8 x 10 Gigabit Ethernet blade bandwidth.
- One mezzanine, third-generation Peripheral Component Interconnect Express (PCIe) slot

Cisco UCS B-Series Server Comparison (Cont.)

	Cisco UCS B250 M2	Cisco UCS B230 M2	Cisco UCS B420 M3	Cisco UCS B440 M2
Generation	Gen 2	Gen 2	Gen 2	Gen 2
Sockets	1 or 2 (up to 6 cores per socket)	2 (up to 10 cores per socket)	2 or 4 (up to 10 cores per socket)	2 or 4 (up to 10 cores per socket)
Processor	Intel Xeon 5600 Series	Intel Xeon E7-2800	Intel Xeon E5-4600	Intel Xeon E7-4800
Memory	48 DIMMs (maximum 384 GB)	32 DIMMs (maximum 512 GB)	48 DIMMs (maximum 1.5 TB)	32 DIMMs (maximum 1 TB)
DIMMs	4 or 8 GB DDR3 at 1066 or 1333 MHz	4, 8, 16, 32 GB DDR3 at 1066 or 1333 MHz	4, 8, 16, 32 GB DDR3 at 1600 MHz	4, 8, 16, 32 GB DDR3 at 1066 or 1333 MHz
Disks	2 x 2.5" SAS, SATA, or SSD, hot-swap	2 x 2.5" SSD, hot-swap	4 x 2.5" SAS, SATA, or SSD, hot-swap	4 x 2.5" SAS, SATA, or SSD, hot-swap
Storage	Up to 1.2 TB	Up to 200 GB (SSDs)	Up to 2.4 TB	Up to 2.4 TB
RAID	0, 1	0, 1	0, 1, 5, 10	0, 1, 5, 6
I/O	2 slots Up to 40 Gb/s	1 slot Up to 20 Gb/s	2 slots Up to 160 Gb/s (LOM)	2 slots Up to 40 Gb/s
Size	Full-width	Half-width	Full-width	Full-width

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

This table compares other Cisco UCS B-Series M2 server blades with maximum hardware configurations.

Cisco UCS B250 M2 Server Blade

The Cisco UCS B250 M2 server blade has the following features:

- Up to two Intel Xeon 5600 Series processors, which adjust server performance according to application needs
- Up to 384 GB based on the Samsung 40 nanometer class (DDR3) memory technology, for demanding virtualization and large dataset applications or a more cost-effective memory footprint for less demanding workloads
- Two optional SFF SAS hard drives that are available in 73-GB 15,000-RPM and 146-GB 10,000-RPM versions with an LSI Logic 1064e controller and integrated RAID
- Two dual-port mezzanine cards for up to 40 Gb/s of I/O per blade. Mezzanine card options include either a Cisco UCS VIC M81KR, a converged network adapter (Emulex- or QLogic-compatible), or a single 10 Gigabit Ethernet adapter.
- Two optional front-accessible, hot-swappable SSDs and an LSI SAS2108 RAID Controller

Cisco UCS B230 M2 Server Blade

The Cisco UCS B230 M2 server blade has the following features:

- Supports the Intel Xeon processor E7-2800 product family
- 32 DIMM slots

https://t.me/learningnets

- Up to 512-GB DDR at 1066 MHz, based on the Samsung 40 nm class technology
- Four optional front-accessible, hot-swappable small form-factor pluggable (SFP) drives and an LSI SAS2108 RAID Controller
- It has one dual-port mezzanine card for up to 20 Gb/s I/O per blade. Options include a Cisco UCS VIC M81KR or converged network adapter (Emulex- or QLogic-compatible).

Cisco UCS B420 M3 Server Blade

The Cisco UCS B420 M3 server blade has the following features:

- Up to four Intel Xeon processor E5-4600 processor family CPUs with a maximum of 32 cores per server
- 48 DIMM slots for error checking and correction (ECC) DIMMs, and up to 1.5 TB of memory (using 32-GB LRDIMMs)
- Three mezzanine connectors enable up to 160-Gb/s bandwidth:
  - One dedicated connector for Cisco VIC 1240 modular LOM (mLOM)
  - Two connectors for Cisco VIC 1280, VIC port expander, or third-party network adapter cards
- Four hot-pluggable drive bays supporting SAS, SATA, and SSD drives
- RAID 0, 1, 5, and 10, with optional 1-GB flash memory-backed write cache

Cisco UCS B440 M2 Server Blade

The Cisco UCS B440 M2 server blade has the following features:

- Two or four Intel Xeon processor E7-4800 processor family CPUs with a maximum of 40 cores per server
- 32 DIMM slots for DDR3 DIMMs for maximum memory capacity of 1 TB
- Four front-accessible, hot-pluggable SFF hard drives with an LSI Logic SAS2108 controller and integrated RAID
- Two dual-port mezzanine-card connections for up to 40 Gb/s of redundant I/O throughput

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

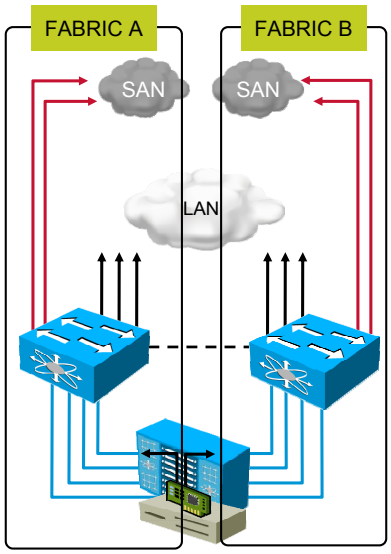
Cisco UCS B-Series Connectivity

Connectivity aspects

- Server blade to IOM
- IOM to Fabric Interconnect
- Fabric Interconnect Ethernet and Fibre Channel uplinks

Dual-fabric design

- Redundant connectivity
- Two Fabric Interconnects and IOMs



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

The Cisco UCS B-Series connectivity should be observed from different perspectives when compared to previous network connectivity for servers:

- The individual server blade
- The Cisco UCS chassis and cumulative requirements of the server blades that are installed in the chassis
- Individual Fabric Interconnect and cumulative requirements of the chassis connected to the switch, and the upstream LAN and SAN connectivity requirements

The Cisco UCS B-Series connectivity architecture follows the dual-fabric design. This design can be used to either achieve high availability (with failover on the Cisco UCS level or on the operating system level) or to achieve more throughput by networking servers to Fabric A and to Fabric B with pinning. It is also possible to direct traffic to both fabrics, combining redundancy and higher throughput.

Unified Fabric Design

The “physical” fabric consists of two fabrics—Fabric A (left) and Fabric B (right).

The LAN fabrics are two physical devices on the Cisco UCS Fabric Interconnect level, but can be (and typically will be) on the same devices in the LAN core.

The SAN fabrics are physically separated on the Cisco UCS Fabric Interconnect level and typically remain separated on the devices in the SAN core.

https://t.me/learningnets

Fabric Interconnect Comparison

Generations

- Gen 1
- Gen 2

	Cisco UCS 6248UP	Cisco UCS 6296UP
Generation	Gen 2	Gen 2
Form Factor	1 RU	2 RU
Expansion Slot	1	3
Total, Fixed Ports	48, 32	96, 48
Additional ports	16 with expansion module	48 with 3 expansion modules
Throughput	960 Gb/s	1920 Gb/s
SFP+	10 Gigabit SR, LR, CU (1,3,5 Twinax) 10 Gigabit FET MMF	10 Gigabit SR, LR, CU (1,3,5 Twinax) 10 Gigabit FET MMF
SFP—all ports	1 Gigabit SW, LW, UTP 4, 8 Gigabit Fibre Channel SW, LW SFP	1 G SW, LW, UTP 4, 8 Gigabit Fibre Channel SW, LW SFP
Port licensing	12 + additional licenses	18 + additional licenses
VLANs	1024	1024

Expansion module with 16 unified ports

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

Cisco UCS 6248UP

The Cisco UCS 6248UP is a Fabric Interconnect that doubles the switching capacity of the data center fabric to 1 Tb/s, reduces end-to-end latency by 40 percent to improve application performance (from 5.2 usec to 3.2 usec), and provides flexible unified ports to improve infrastructure agility and transition to a fully converged fabric.

- 48 ports in a single rack unit (RU)
  - 32 fixed ports on the base switch
  - 16 optional ports on the expansion module
- Redundant front-to-back airflow
- Dual power supplies for both AC and DC -48V. The power consumption of the Fabric Interconnect itself is approximately half of first-generation Fabric Interconnects.
- All ports on the base and expansion module are “unified ports.”
- Each of these ports can be configured as Ethernet, FCoE, or native Fibre Channel.
- Depending on optics, these can be used as SFP 1 Gigabit Ethernet, small form-factor pluggable plus (SFP+) 10 Gigabit Ethernet, Cisco 8/4/2 Gb/s Fibre Channel, 10 Gigabit Fabric Extender Transceiver (FET) multimode fiber (MMF) and 4/2/1 Gb/s Fibre Channel.

https://t.me/learningnets

Cisco UCS 6296UP

The Cisco UCS 6296UP 96-Port Fabric Interconnect is a 2-RU 10 Gigabit Ethernet, FCoE and native Fibre Channel switch that offers up to 1920 Gb/s throughput, up to 96 ports, and reduced port-to-port latency (from 3.2 usec to 2.0 usec). The switch has 48 1/10-Gb/s “Universal style” fixed Ethernet, FCoE, and Fiber Channel ports as well as three expansion slots.

- 96 ports in 2 RU
  - 48 fixed ports
  - Additional 48 ports available through three expansion modules
- Redundant front-to-back airflow
- Dual power supplies for both AC and DC -48V. The power consumption of the Fabric Interconnect itself is approximately half of first-generation Fabric Interconnects.
- All ports on the base and expansion module are “unified ports.”
- Each of these ports can be configured as Ethernet, FCoE, or native Fibre Channel.
- Depending optics, these can be used as SFP 1 Gigabit Ethernet, SFP+ 10 Gigabit Ethernet, Cisco 8/4/2 Gb/s Fibre Channel, 10 Gigabit FET MMF and 4/2/1 Gb/s Fibre Channel.

https://t.me/learningnets

IOM Comparison

IOM generations

- Gen 1
- Gen 2

	IOM 2104XP*	IOM 2204XP	IOM 2208XP
Generation	Gen 1	Gen 2	Gen 2
IOM Uplinks	4 x 10 Gigabit Ethernet FCoE-capable	4 x 10 Gigabit Ethernet FCoE-capable	8 x 10 Gigabit Ethernet FCoE-capable
IOM EtherChannel	No	Yes	Yes
Server Ports—Half-width Slot	2 x 10 Gigabit Data Center Bridging (DCB)	2 x 10 Gigabit DCB	4 x 10 Gigabit DCB
Server Ports—Full-width Slot	2 x 10 Gigabit DCB	4 x 10 Gigabit DCB	8 x 10 Gigabit DCB
SFP+	10 Gigabit SR, LR, CU (1,3,5 Twinax)	10 Gigabit SR, LR, CU (1,3,5 Twinax) 10 Gigabit FET MMF	10 Gigabit SR, LR, CU (1,3,5 Twinax) 10 Gigabit FET MMF

* IOM 2104XP is only compatible with Cisco UCS 61*xx* Fabric Interconnects

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

Cisco UCS 2104XP IOM

The Cisco UCS 2104XP is a chassis I/O module (IOM) that is used in the first generation of Fabric Interconnect. It has four 10 Gigabit Ethernet, FCoE-capable, SFP+ ports that connect the blade chassis to the Fabric Interconnect. Each Cisco UCS 2104XP has eight 10 Gigabit Ethernet ports that are connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 80 Gb/s of I/O to the chassis.

Cisco UCS 2208 IOM

The Cisco UCS 2208XP is a chassis IOM that doubles the bandwidth to the chassis to improve application performance and manage workload bursts (from 80 Gb to 320 Gb to the blade). The Cisco UCS 2208XP Fabric Extender has eight 10 Gigabit Ethernet, FCoE-capable, SFP+ ports that connect the blade chassis to the Fabric Interconnect. Each Cisco UCS 2208XP has thirty-two 10 Gigabit Ethernet ports that are connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 160 Gb/s of I/O to the chassis.

Cisco UCS 2204 IOM

The Cisco UCS 2204XP Fabric Extender has four 10 Gigabit Ethernet, FCoE-capable, SFP+ ports that connect the blade chassis to the Fabric Interconnect. Each Cisco UCS 2204XP has sixteen 10 Gigabit Ethernet ports that are connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 80 Gb/s of I/O to the chassis.

https://t.me/learningnets

Cisco UCS B-Series VIC Adapter Comparison

VIC adapter generations

- Gen 1
- Gen 2

	VIC 1240	VIC 1280	M81KR VIC
Generation	Gen 2	Gen 2	Gen 2
Total Interfaces	256	256	128
Interface Type	Dynamic	Dynamic	Dynamic
Ethernet NICs	0-256	0-256	0-128
Fibre Channel HBAs	0-256	0-256	0-128
VM-FEX	Yes	Yes	Yes
Adapter-FEX	Yes	Yes	Yes
Failover Handling	Hardware, no driver needed	Hardware, no driver needed	Hardware, no driver needed
Form Factor	Modular LOM	Mezzanine	Mezzanine
Network Throughput	40-80* GB	80 GB	20 GB
Server Compatibility	M3 blades	M1 or M2 blades	M1 or M2 blades

* With use of Port Expander Card for VIC 1240 in the optional mezzanine slot

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

DCUCT v5.0—1-10

The Cisco UCS virtual interface card (VIC) supports network interface card (NIC) virtualization either for a single operating system or for VMware vSphere. Support for other hypervisors, such as Microsoft Hyper-V, Citrix Xen, and keyboard, video, mouse (KVM), is planned for the future. The number of virtual interfaces that are supported on an adapter depends on the number of uplinks between the IOM and the Fabric Interconnect, as well as the number of interfaces that are in use on other adapters that share the same uplinks.

https://t.me/learningnets

Cisco UCS B-Series Quad-Interface Adapter Comparison

QLogic and Emulex Converged Network Adapter (CNA) Generations

- Gen 2
- Gen 3

	M72KR Q/E	M73KR Q/E
Generation	Gen 2	Gen 3
Total Interfaces	4	4
Interface Type	Fixed	Fixed
Ethernet NICs	2	2
Fibre Channel HBAs	2	2
VM-FEX	No	No
Adapter FEX	No	No
Failover Handling	Software, bonding driver	Software, bonding driver
Form Factor	Mezzanine	Mezzanine
Network Throughput	20 GB	20 GB
Server Compatibility	M1 or M2 blades	M3 blades

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

You can create up to two virtual network interface cards (vNICs) using the Cisco UCS 82598KR-CI adapters. You must match the physical setting (the first adapter goes to Fabric A, the second adapter goes to Fabric B), and failover is not permitted.

“Q” is the QLogic version of these adapters. “E” is the Emulex version of these adapters.

The primary advantages are low power, software drivers (Emulex or QLogic), and moderate pricing.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS B-Series Dual-Interface Adapter Comparison

CNA Generations

- Gen 1
- Gen 2
- Gen 3

	Intel M61KR-I CNA	Broadcom M51KR-B 57711	Broadcom M61KR-B 57712
Generation	Gen 2	Gen 2	Gen 2
Total Interfaces	2	2	2
Interface Type	Fixed	Fixed	Fixed
Ethernet NICs	2	2, iSCSI TOE	2, iSCSI TOE
Fibre Channel HBAs	Future	0	0
VM-FEX	No	No	No
Adapter-FEX	No	No	No
Failover Handling	Software, bonding drive	Software, bonding driver	Software, bonding driver
Form Factor	Mezzanine	Mezzanine	Mezzanine
Network Throughput	20 GB	20 GB	20 GB
Srv. Compatibility	M1 or M2 blades	M1 or M2 blades	M3 blades

Adapter data sheets can be found at http://www.cisco.com/en/US/products/ps10280/products_data_sheets_list.html.

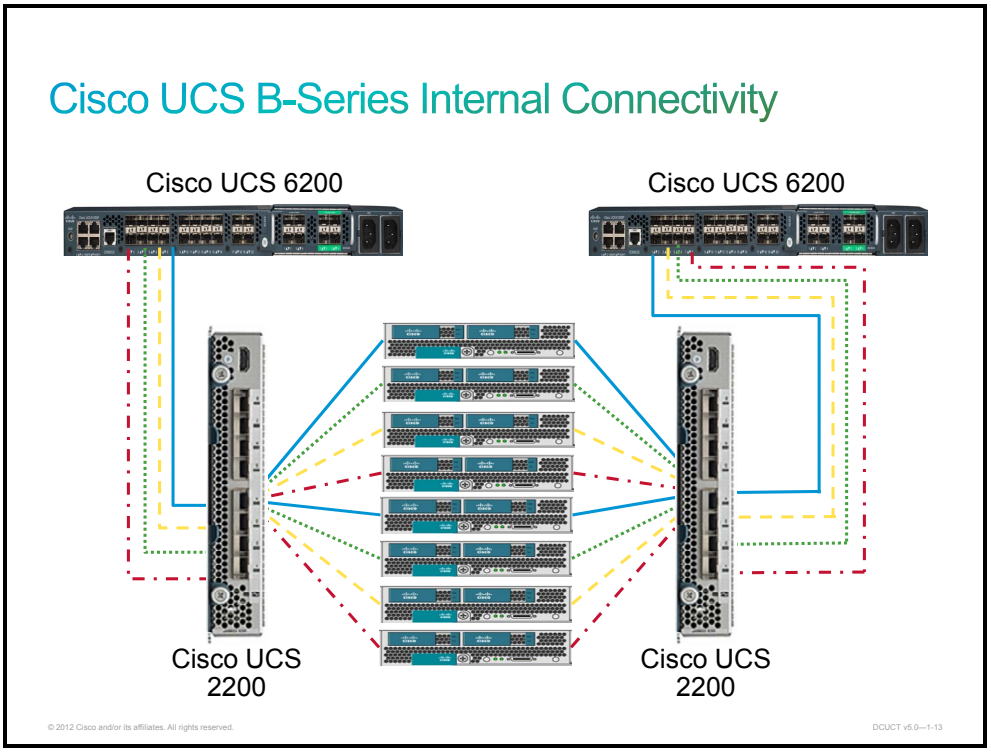
© 2012 Cisco and/or its affiliates. All rights reserved.

This table compares the two-interface adapters that are available for Cisco UCS B-Series. These adapters offer low power, low price, and limited features and capabilities when compared to other adapters.

The Intel and Broadcom adapters have some similarities. One of them is a NIC that is installed in a server internal bus with no virtualization or FCoE features available.

Note The adapter data sheets contain more details about the specific adapters and can be found at http://www.cisco.com/en/US/products/ps10280/products_data_sheets_list.html.

https://t.me/learningnets



When fully populated, links between the Cisco UCS Fabric Interconnect and chassis IOMs can be oversubscribed, depending of the IOM type.

Cisco UCS components are interconnected using physical and logical interfaces or ports.

The Fabric Interconnects are connected in the following manner:

- Via physical uplink ports to an external LAN
- Via physical uplink ports to an external SAN network
- Via physical server ports to IOMs

Each IOM provides the following:

- Internal backplane ports (to each blade in the chassis)
- External fabric ports (to the Fabric Interconnects)
- Internal management network (within the Cisco UCS 5100 chassis)

An individual IOM is connected in this manner:

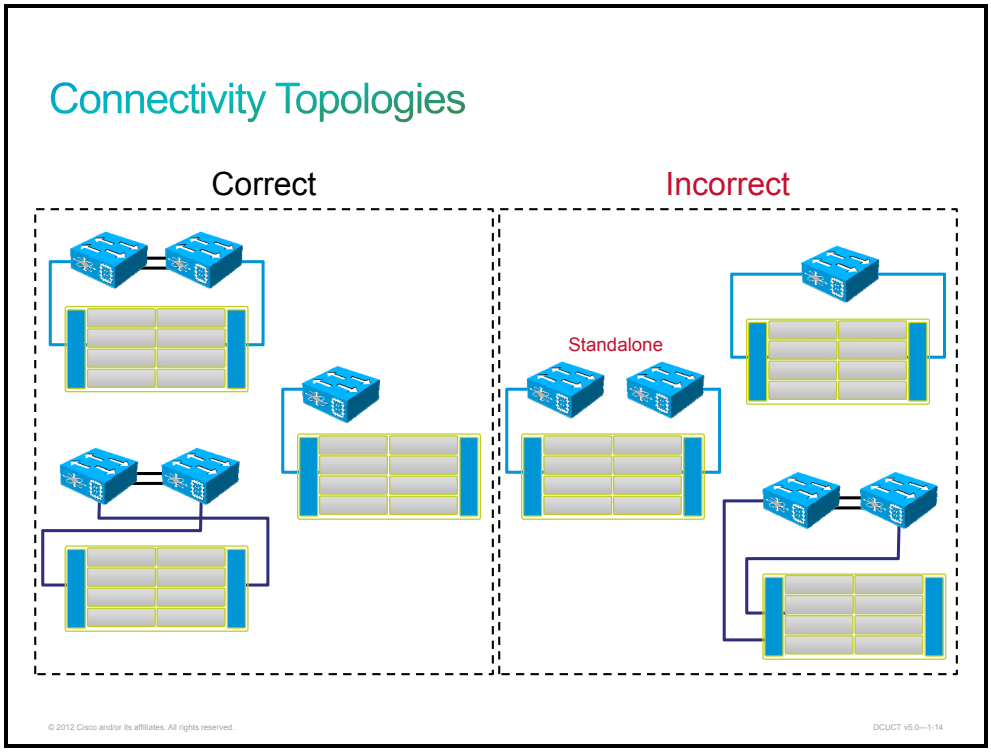
- Via physical fabric port to Fabric Interconnect server port
- Via logical backplane port through chassis midplane to each individual server blade

An individual server blade is connected to both IOMs. Depending on the number of IOM fabric ports, the server blade ports are pinned in this manner, for example:

- All server blades are pinned to IOM port 1 when a single fabric port is used.
- When two fabric ports are used, server blades 1, 3, 5, and 7 are pinned to IOM port 1, and server blades 2, 4, 6, and 8 are pinned to IOM port 2.
- When four fabric ports are used, server blades 1 and 5 are pinned to IOM port 1, server blades 2 and 6 are pinned to port 2, server blades 3 and 7 are pinned to port 3, and server blades 4 and 8 are pinned to port 4.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

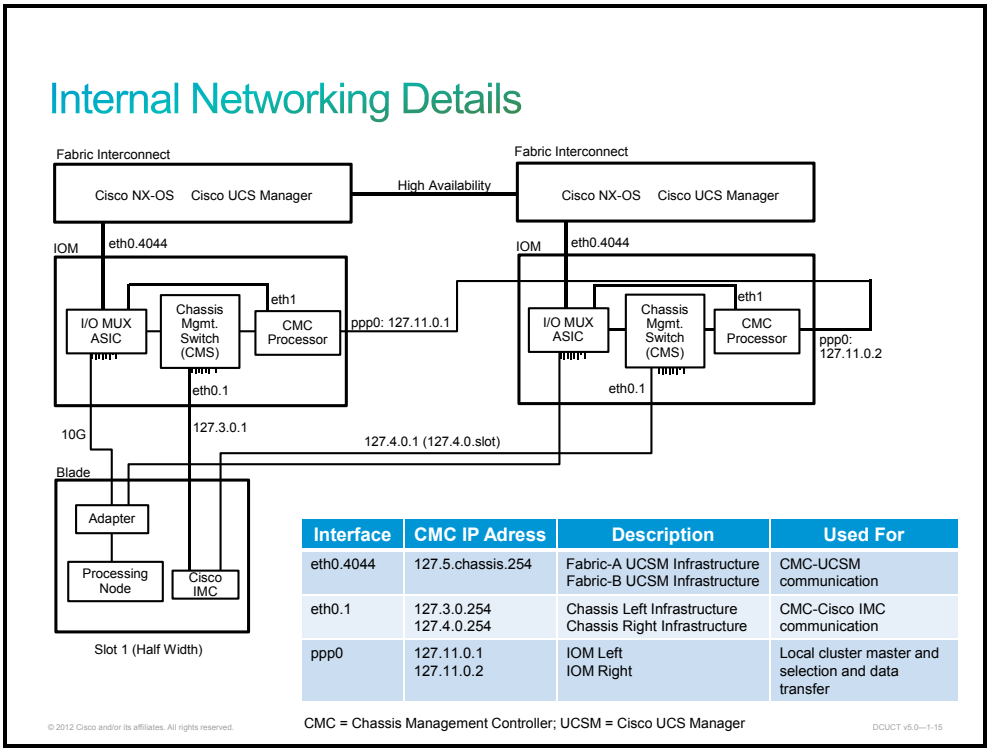


The Fabric Interconnect to IOM connectivity has the following characteristics:

- Fabric Interconnect server ports are configurable. They depend on the actual Fabric Interconnect to IOM connectivity.
- IOM fabric ports are fixed. Depending on the actual Fabric Interconnect to IOM connectivity, they may or may not be used.

Individual IOMs can be connected to only one fabric at a time. Connecting the IOM and chassis in a way that is not supported will result in broken connectivity.

https://t.me/learningnets



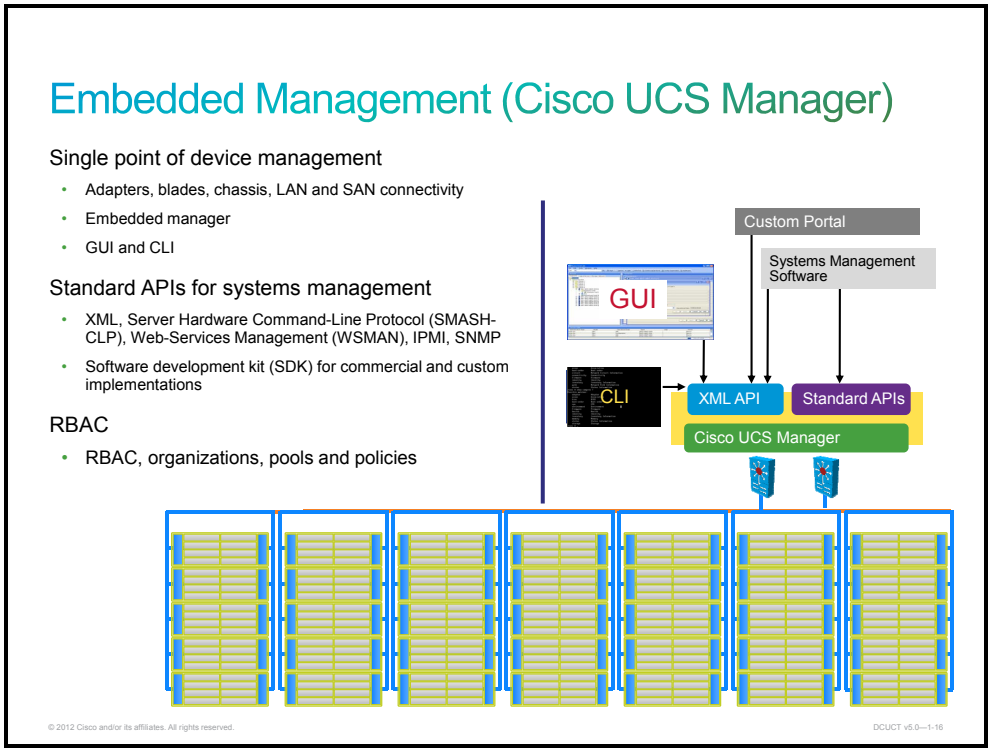
The major service components of Cisco UCS include the Fabric Interconnects, IOMs, and the blades. Control and management traffic is delivered via an internal network.

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—four for each slot. With Cisco UCS 2208 IOM, the supported topologies for connectivity with the Fabric Interconnect are 1-, 2-, 4-, or 8-link. Depending on the number of uplinks that are used, the oversubscription ratio will differ.

Cisco UCS IOMs consist of an I/O multiplexer (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, 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 (Cisco IMC) of each compute node. This communication is realized through the chassis management switch, which provides eight 100-Mb/s internal interfaces to the Cisco IMCs. There is also an external debug interface, for use with a dongle cable, providing console and Ethernet interfaces.

The blade servers essentially consist of the processing node, one or more adapters and, in the case of Cisco UCS C-Series, a Cisco IMC. The Cisco IMC is used for management and monitoring of the Cisco UCS C-Series rack servers. Cisco IMC provides options like Web-GUI, CLI, and Intelligent Platform Management Interface (IPMI) for management and monitoring tasks. Cisco IMC runs on a separate chip on the Cisco UCS C-Series servers and is therefore able to provide services in case of any major hardware failure or system crash. Cisco IMC also performs user management tasks and supports user access levels of Admin (full access), User/Operator (can change host features but not Cisco IMC), and Read Only (can only see information). Cisco IMC uses IPMI to monitor thermal and voltage sensors in the servers. Cisco IMC is useful for initial configuration of the server and troubleshooting any problems in server operation; however, Cisco IMC cannot be used for tasks like deploying an operating system, deploying software patches, installing software applications and managing external storage on the SAN or network-attached storage (NAS).

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



The embedded Cisco UCS management system provides for a single point of management for the entire Cisco UCS environment, including Fabric Interconnects, LAN, SAN, chassis, blades, and adapters.

The Cisco UCS management system uses standard APIs and can be extended and accessed by third-party utilities.

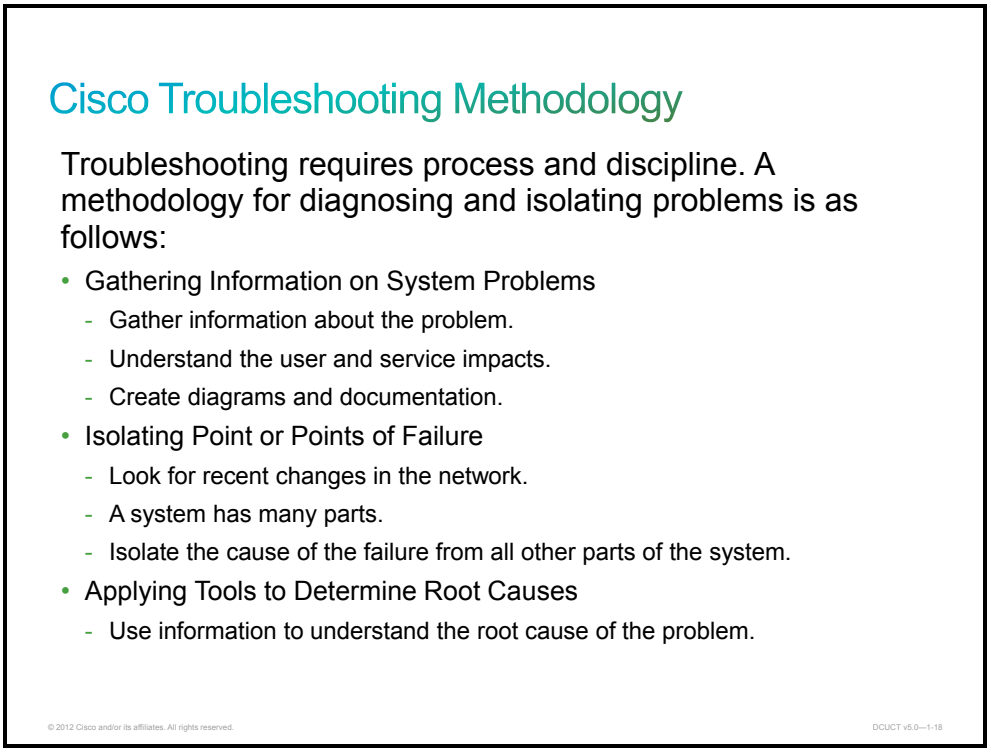
Ports to be opened for accessing Cisco UCS Manager through a firewall include the following:

- TCP 22
- TCP 23 if Telnet is enabled (It is off by default.)
- TCP 80
- UDP 161 or 162 if SNMP is enabled (It is off by default.) (UDP 162 Simple Network Management Protocol [SNMP] trap is outbound, and UDP 161 SNMP is inbound.)
- TCP 443 if HTTPS is enabled (It is off by default.)
- UDP 514 if syslog is enabled (outbound from Cisco UCS Manager)
- TCP 2068 (KVM)

https://t.me/learningnets

Cisco Troubleshooting Methodology

This topic provides the best practices for Cisco UCS troubleshooting.



Troubleshooting a system problem requires attention to detail and clearly defined processes. It is more effective to have a methodology to approach problem resolution. There is no “right” or “correct” method because it will change for each technology or network, and the engineer must develop skills to troubleshoot effectively.

As a starting point, consider a simple three-step process:

- Gather information
- Isolate the fault and fix the failure
- Verify and solve the root cause the problem

Information gathering can mean reviewing documentation and diagrams, and connecting to devices to check the status and connectivity. Validate the problem report and narrow the exact service impacts that the user is experiencing.

Isolating the fault can include checking logs, physical connections, and power status, and using commands to determine the exact location of errors to correlate them with the problem report from the user. In more complex systems where applications, operating systems, server, and network combine to form the solution, the engineer will work toward isolating the fault rapidly to ensure minimum downtime.

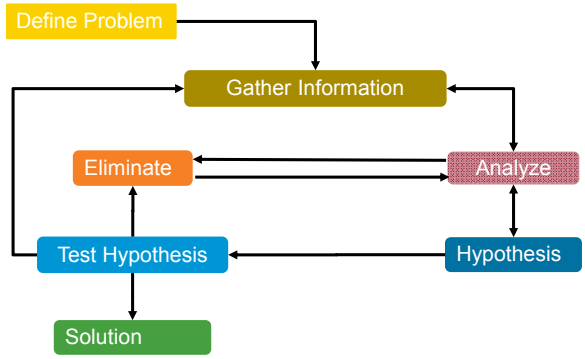
After the fault has been fixed or a workaround has been implemented, determine the root cause of the problem and look for ways to prevent recurrence or mitigate the impact.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Troubleshooting Methodology

- Use a structured approach to troubleshooting.
- Define, gather, analyze, test, eliminate, and solve.



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

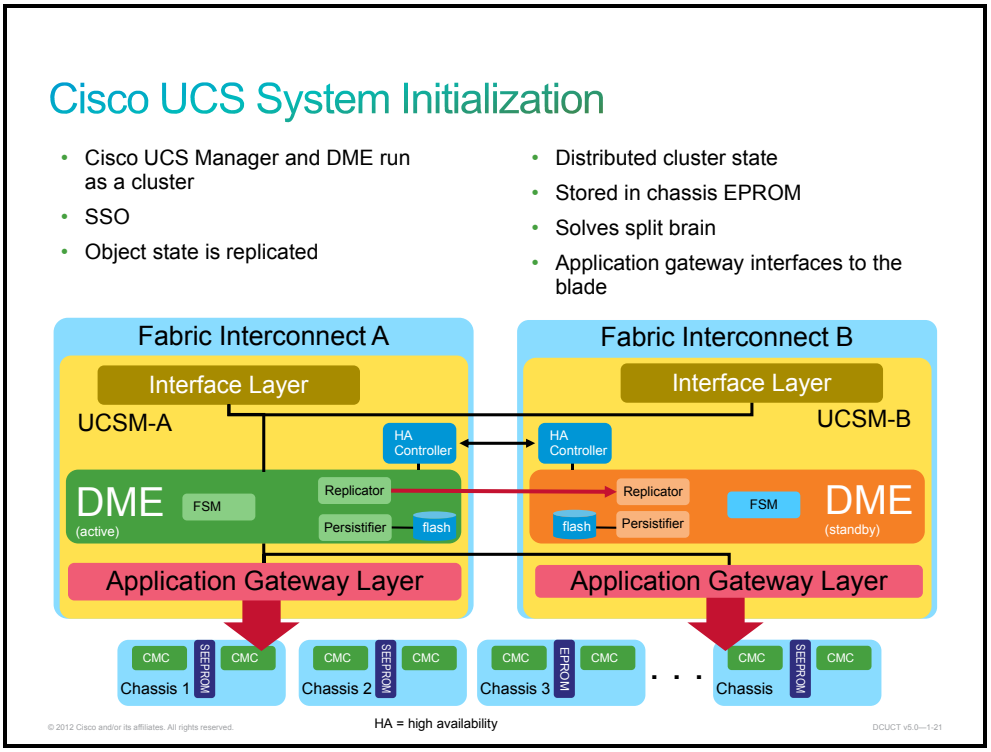
When troubleshooting a problem, it is important to take a structured and methodical approach to the process. In practice, troubleshooting is an organic process involving skill, experience, and some inspiration to achieve a solution. The most successful engineers use a structured troubleshooting process that uses a continuous improvement cycle, as shown in the slide, to solve problems more reliably and quickly.

Your own process will vary according to your needs and experience. You might have experienced a similar fault previously, or know enough about a system to go directly to the fix that is required.

https://t.me/learningnets

Troubleshoot Cisco UCS System Initialization

This topic describes how to troubleshoot Cisco UCS B-Series system initialization.



Almost everything within the Cisco UCS environment is intelligent. The data management engine (DME) enables interrogation and control through an agentless out-of-band (OOB) network.

The architecture allows for a Stateful Switchover (SSO) if the primary Fabric Interconnect fails. Each cluster node maintains an up-to-date copy of the Cisco UCS management database and is able to resolve cluster failures that would otherwise result in a split-brain scenario.

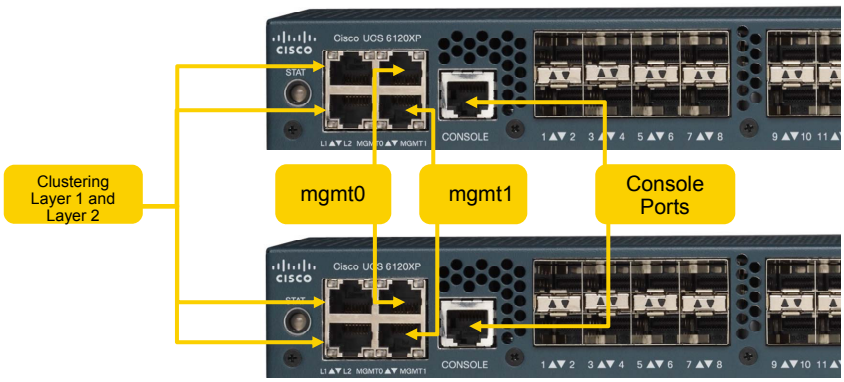
To resolve a potential split-brain cluster failure, the Fabric Interconnects interrogate up to three serial EPROMs to establish a single active switch. Administrator intervention can restore the Fabric Interconnect to full high-availability mode.

Learners should understand the internal process that the Fabric Interconnect goes through to achieve a high-availability state.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Port Functions on Cisco UCS Fabric Interconnect



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

The Cisco UCS Fabric Interconnect provides multiple physical management interfaces into a Cisco UCS cluster. Each switch has a serial console port that is primarily used for initial switch configuration. Each switch has its own mgmt0 port, which is assigned an IP address at initial system configuration for LAN-based network management.

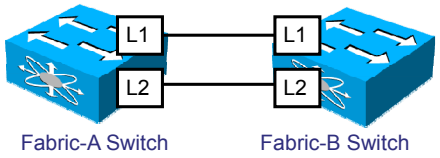
Cluster communications take place over the gigabit Layer 1 and Layer 2 interfaces. As shown in this slide, port Layer 1 on one Fabric Interconnect connects to port Layer 1 on the second Fabric Interconnect. The same applies to Layer 2 ports.

A second management port (mgmt1) is not currently used.

https://t.me/learningnets

Cisco UCS Cluster Wiring Issues

Issue	There are physical connectivity problems.
Possible Cause	The ports in the cluster are wired incorrectly.
Solution	Check the wiring. The wiring must follow the Layer 1 to Layer 1, Layer 2 to Layer 2 cabling requirement.



L1 = Layer 1
L2 = Layer 2

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

Cisco UCS is usually deployed in a clustered fashion, that is, with two Cisco UCS Fabric Interconnect switches that are connected over dual cluster links. This setup provides redundancy for management as well as switching functionality. The Cisco UCS Fabric Interconnects that are in a cluster are either of these two nodes:

- Primary node: The Fabric Interconnect that is active.
- Subordinate node: The Fabric Interconnect that is on standby.

The standby node runs a Cisco UCS Manager instance with reduced functionality.

The following connectivity requirements must be met for successful deployment of a highly available Cisco UCS cluster:

- Connect Layer 1 of Fabric Interconnect A to Layer 1 of Fabric Interconnect B.
- Connect Layer 2 of Fabric Interconnect A to Layer 2 of Fabric Interconnect B.
- Connect Fabric Interconnect A to IOM A of each chassis, using one to eight uplinks.
- Connect Fabric Interconnect B to IOM B of each chassis, using one to eight uplinks.

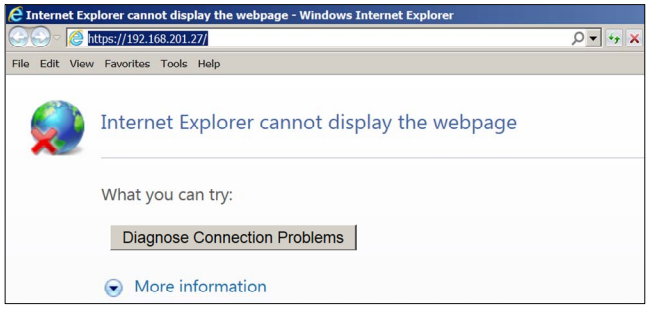
Cluster interfaces provide a cluster link between two Cisco UCS 6100 Series Fabric Interconnects. They carry the cluster heartbeat messages between the two Cisco UCS Fabric Interconnects as well as high-level messages between Cisco UCS Manager elements. These links are part of an IEEE 802.3ad bond that is managed by the underlying operating system. The bond is configured to run Link Aggregation Control Protocol (LACP), which brings up the bond link only when there is either a single link between two LACP-enabled nodes or when both links are between LACP-enabled peers. The IP addresses on these links are fixed.

The management port (mgmt0) of each Fabric Interconnect should be connected to the same Layer 2 network to facilitate failover and failback of the management IP address. Each Fabric Interconnect should connect to only one “side” of each chassis.

https://t.me/learningnets

IP Connectivity Failure—Symptom

- Failure to launch Cisco UCS Manager
- Cannot connect to the virtual IP address via either HTTPS or SSH
- Potential issues: IP address overlap, missing setting, device or devices not connected to the network



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

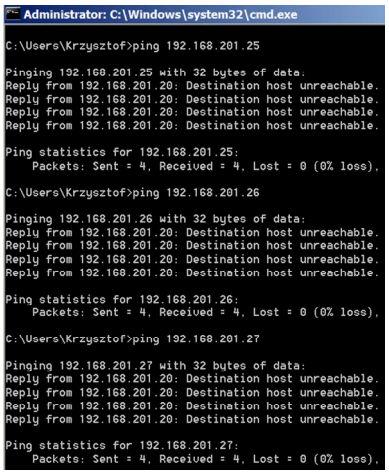
This troubleshooting scenario illustrates an approach that consists of multiple phases: symptom identification, information gathering, remediation, and verification.

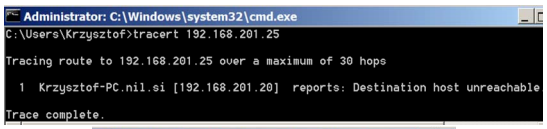
The symptom of the problem is that you cannot launch Cisco UCS Manager when directing your browser at Fabric Interconnect virtual IP address 192.168.201.27 and using HTTPS as the access method. If you cannot launch Cisco UCS Manager or cannot establish another management session, you have an IP connectivity problem. The problem can result from an incorrect configuration in which the IP addresses have not been set properly, from overlapping IP addresses, from wrong wiring, or from other similar faults.

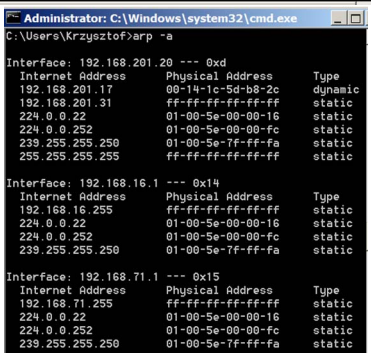
https://t.me/learningnets

IP Connectivity Failure Info Gathering

- Connectivity failure to both Fabric Interconnect management IP addresses and virtual address
- Common tools: **ping**, **traceroute**, ARP cache verification



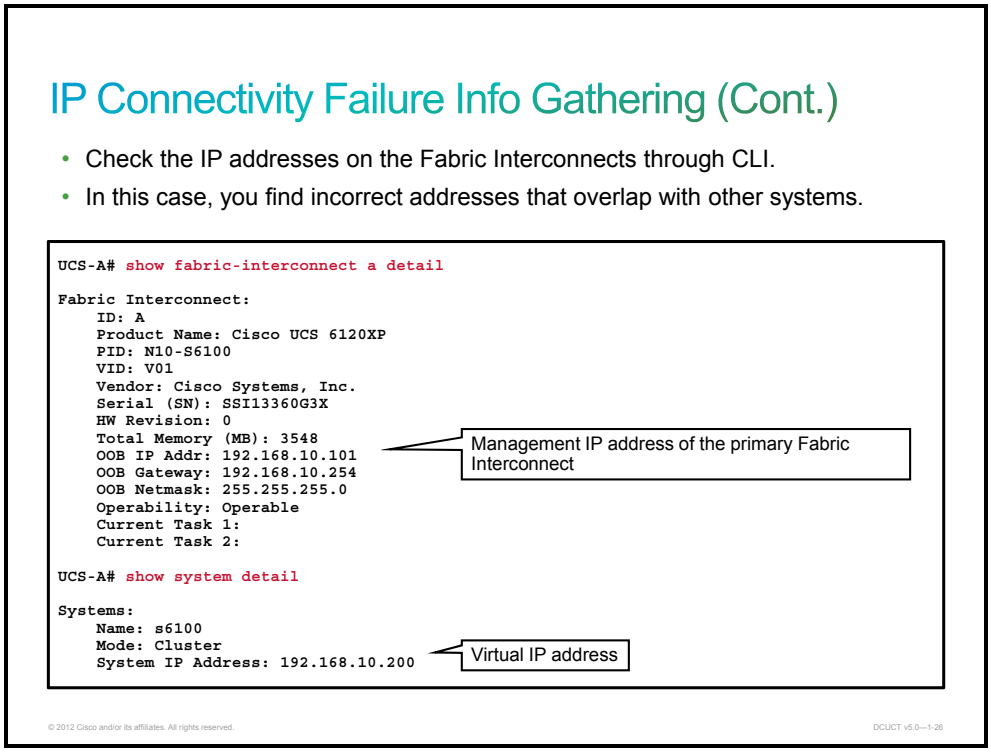




© 2012 Cisco and/or its affiliates. All rights reserved.

In the information gathering phase, you can use various tools, such as the **ping** and **traceroute** utilities. You can also verify the information that is available in the Address Resolution Protocol (ARP) caches on adjacent devices. Depending on your network topology, you can perform similar tests on hosts, routers, switches, or security appliances.

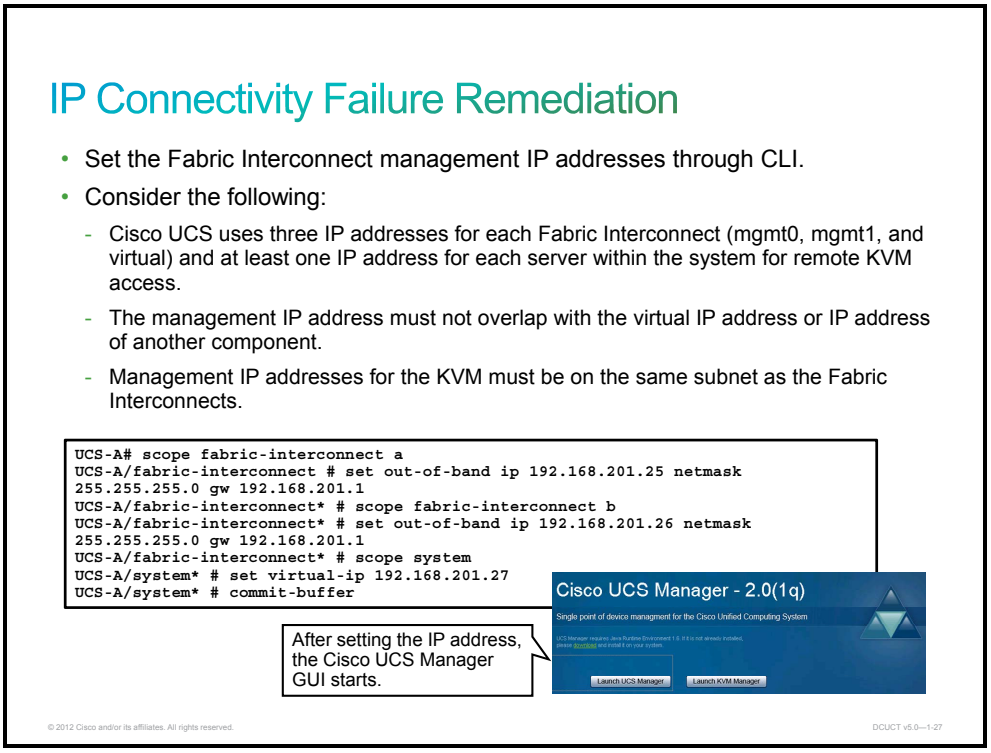
https://t.me/learningnets



Because you could not connect to the Fabric Interconnects using any in-band method, verify the IP address that is configured on them. You can connect to both Fabric Interconnects via the console port. The **show fabric-interconnect a/b detail** and **show system detail** commands display the IP addresses for the management interfaces and the virtual IP address of the cluster.

In this case, incorrect IP addresses have been assigned to the Fabric Interconnects. These addresses overlap with an IP address range that was allocated to other devices. You must resolve the IP address conflict.

https://t.me/learningnets



In this scenario, you identified a missing configuration of the appropriate IP addresses as a likely cause. You can set the IP addresses in the console CLI, as shown in this figure.

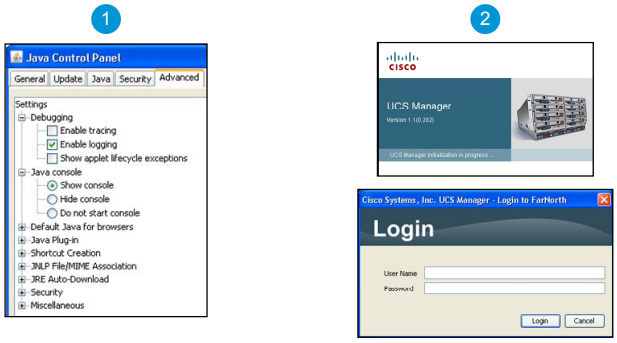
When configuring Fabric Interconnect IP addresses, consider this information:

- Cisco UCS requires three IP addresses for each Fabric Interconnect (mgmt0, mgmt1, and virtual) and at least one IP address for each server within the system for remote KVM access.
- Make sure that the management IP addresses do not overlap with the virtual IP address or IP address of another component, such as KVM.
- Management IP addresses for the KVM must be on the same subnet as the Fabric Interconnects.

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

Troubleshooting Cisco UCS Manager Initialization

1. Enable logs for Cisco UCS Manager access and KVM access:
   - In the Java control panel, found in the system control panel
   - Check the Enable logging check box and the Show console radio button
2. Attempt to access Cisco UCS Manager.



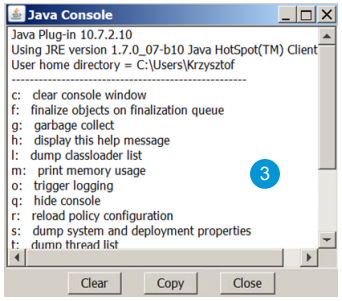
© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco UCS Manager is a Java application that provides “run anywhere” software management for Cisco UCS. By default, Java does not log application errors. If you are experiencing client problems, enable logs to diagnose the cause. This figure shows Java logging and the Java console being enabled so that the Java logs can be examined to debug Cisco UCS Manager access issues.

https://t.me/learningnets

Troubleshooting Cisco UCS Manager Initialization (Cont.)

3. Java console enables you to run verification commands.
4. Logs in Microsoft Windows 7 are written in C:\users\userid\AppData\LocalLow\SunJava\Deployment\log\.ucsm.



4

```
$.NuLoginService] - Establishing communication with 10.91.42.230:80 [secure port=80]
$.NuCommunicationManager] - validated server name 10.91.42.230
$.NuCommunicationManager] - validated port number (unsecure) 80
$.NuCommunicationManager] - validated port number (secure) 80
$.NuCommunicationManager] - started worker pool Comms Worker Pool
$.NuCommunicationManager] - created serverCommunicationManager
$.NuCommunicationManager] - calling login method
$.NuServerCommunicationManager] - create login method
$.NuServerCommunicationManager] - added user name and password
$.NuServerCommunicationManager] - Sending login request
$.NuServerCommunicationManager] - getting connection for requestcom.nuova.centrale.imp
$.NuServerCommunicationManager] - [------------ Sending Request to Server -----------
$.NuServerCommunicationManager] - Sending requestcom.nuova.centrale.imp.aaa.LoginMe@cC
$.NuHttpConnection] - lSessionCookie=[null], lRequestCookie=[null]
```

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

The Java Runtime Environment (JRE) has a different directory structure on each operating system so the location of the logs is not always the same. Common log locations are as follows:

- **Windows XP Pro:** C:\Documents and Settings\Username\Application Data\Sun\Java\Deployment\log\.ucsm
- **Windows Vista:** C:\Documents and Settings\Username\AppData\LocalLow\SunJava\Deployment\log
- **Windows 7:** C:\users\userid\AppData\LocalLow\SunJava\Deployment\log\.ucsm
- **Mac OSX:** \home_directory\Library\Caches\Java\log\.ucsm

This figure shows the Java Console window with some of the commands that are available for troubleshooting, and also how to open and view the Java log.

https://t.me/learningnets

Cisco UCS CLI

- Use the CLI for direct troubleshooting or for verification of proper configuration from Cisco UCS Manager.
- The CLI provides good understanding of XML structure for third-party API configurations and uses of navigation.
- As the system administrator for troubleshooting, you will need to be somewhat familiar with the CLI.

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

Cisco UCS is not intended to be configured from the CLI. However, the CLI offers a powerful debugging tool that is used by support engineers to verify the Cisco UCS configuration.

Programmers who write scripts to configure Cisco UCS can often find helpful code by viewing the configuration file from the Fabric Interconnect shell.

You can find more information about scripting and available APIs on Cisco Developer Network here: http://developer.cisco.com/web/unifiedcomputing/home.

Cisco UCS includes an innovative XML API, which offers a programmatic way to integrate or interact with any of the more than 9000 managed objects in Cisco UCS. Managed objects are abstractions of Cisco UCS physical and logical components such as adapters, chassis, blade servers, and Fabric Interconnects.

Developers can use any programming language to generate XML documents containing Cisco UCS API methods. The complete and standard structure of the Cisco UCS XML API makes it a powerful tool that is simple to learn and implement.

https://t.me/learningnets

KVM Issue 1: KVM Launch Failure

- This is the symptom that you encounter:
  - The KVM console fails to launch.
- The administrator installed a new management computer.
- Reportedly, all settings and applications are identical to the parameters on the old computer, where KVM worked properly.

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

In this first KVM-related troubleshooting scenario, an administrator contacts you about a problem with launching the KVM.

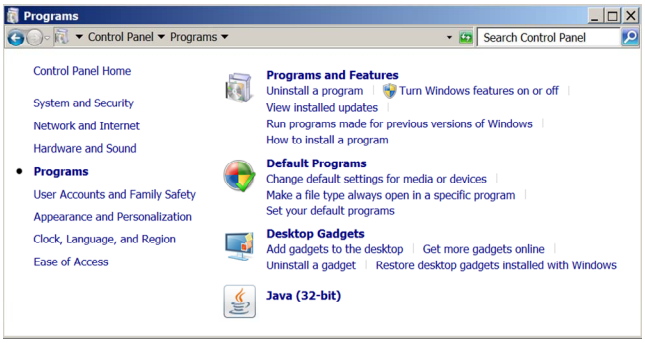
The administrator has recently installed a new management computer. Reportedly, all settings and applications on the new computer are configured identically to the ones on the old computer, where KVM worked without any problems.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

KVM Issue 1: Gathering Data

- Verify IP connectivity:
  - Ping to the KVM IP address works.
- Verify your environment:
  - JRE is installed.
  - JRE version is JRE 1.6_05.

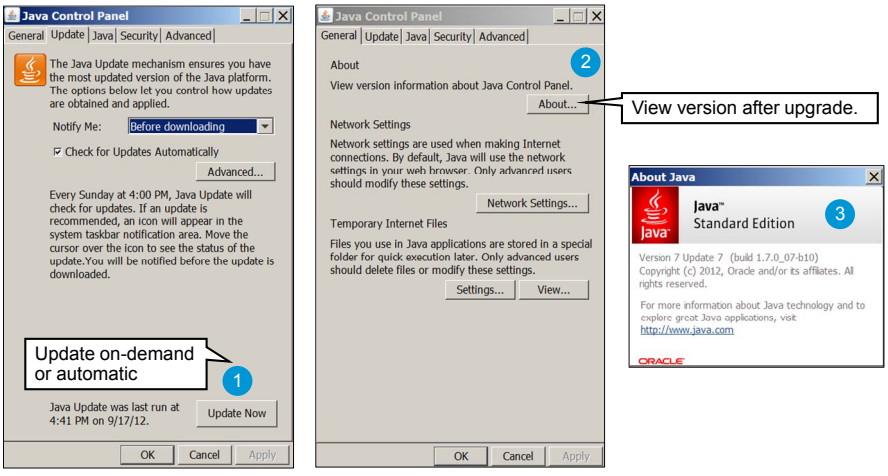


© 2012 Cisco and/or its affiliates. All rights reserved.

In the data gathering phase, you verify that the IP connectivity of the new computer is successful. Further, you verify the Java environment. You find that the JRE version 1.6_05 is installed.

KVM Issue 1: Remediation

- Previous JRE version is incompatible with Cisco UCS KVM.
- Update Java environment to release JRE 1.6_11 or newer.



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

You cross-check the installed JRE version with the Java requirements that are described on Cisco.com. You find that the installed version is not compatible with the KVM console. To remediate the problem, you upgrade the Java environment to release 1.6_11 or newer.

https://t.me/learningnets

KVM Issue 2: Error at KVM Launch

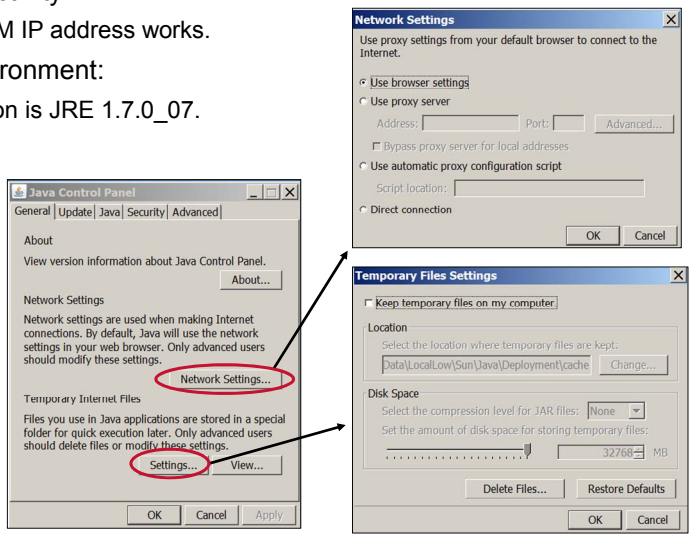
- This is the system that you encounter:
  - The KVM fails to launch.
- An error is reported:
  - “BadFieldException”
  - This error appears when the KVM is launched.

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

Although you updated the Java environment, you still cannot launch the KVM console. In the second KVM-related troubleshooting scenario, you receive the error “BadFieldException” when trying to launch the KVM.

KVM Issue 2: Gathering Data

- Verify IP connectivity:
  - Ping to the KVM IP address works.
- Verify your environment:
  - The JRE version is JRE 1.7.0_07.



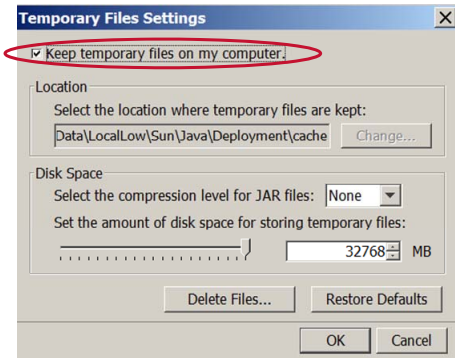
© 2012 Cisco and/or its affiliates. All rights reserved.

Because you already verified the IP connectivity and have a sufficient JRE version, you check the network settings and the temporary file settings in the Java Control Panel. You find that the environment is configured to use browser settings and to *not* keep temporary files on the local computer.

https://t.me/learningnets

KVM Issue 2: Remediation

- In Java settings, perform the following:
  - Check the Keep temporary files on my computer check box.
- If it is not configured correctly, this will occur:
  - Java Web Start disables the cache by default when it is used with an application that uses native libraries.



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

When you compare the actual settings with the recommended Java configuration that can be found on Cisco.com, you find that the current option regarding temporary files is incorrect. To remediate the problem, you must enable the option to “Keep temporary files on my computer.” If you fail to do so, Java Web Start disables the cache by default when it is used with an application that uses native libraries.

https://t.me/learningnets

KVM Issue 3: KVM Stopped Working

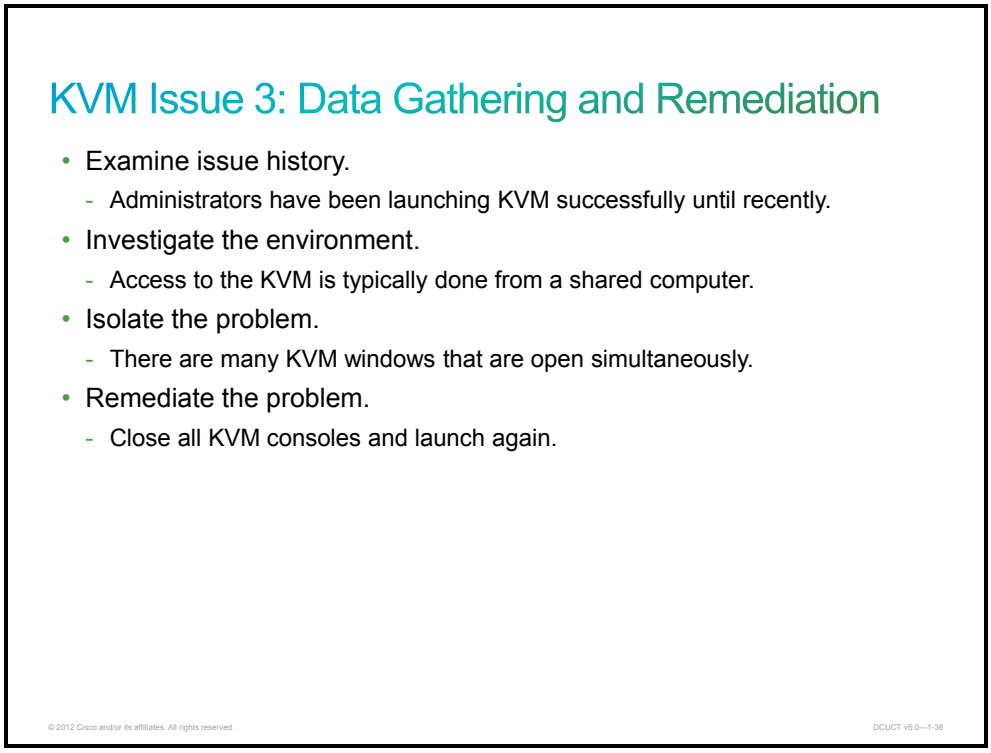
- This is the system that you encounter:
  - KVM fails to launch.
  - JRE displays the message “Unable to launch the application.”

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

The setting for the temporary files storage resolved the problem for several days. Now you receive another problem report about the KVM functionality on this computer. The KVM console fails to start again. This time the JRE displays the message “Unable to launch the application.”

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets



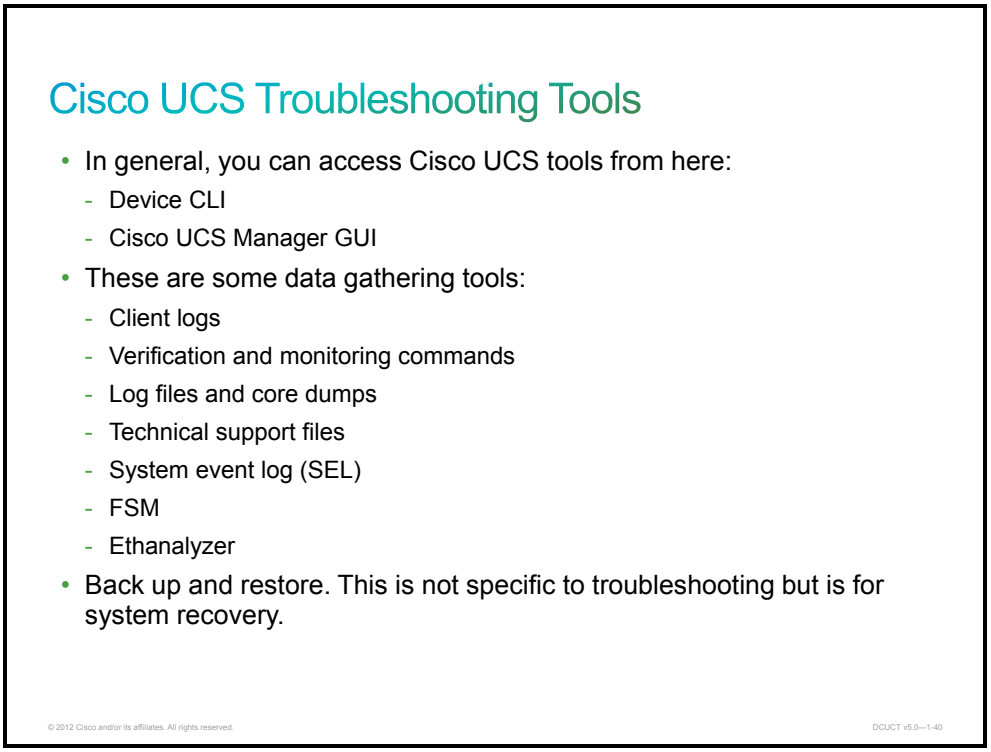
During the data gathering phase, you examine the history of the issue and find that the administrators have been launching KVM successfully until the problem appeared again. When you investigate the environment, you realize that the KVM consoles are accessed from a shared computer.

This knowledge enables you to isolate the problem by noticing that many KVM windows are open simultaneously. To remediate the problem, you close all KVM consoles and launch it again. You instruct the administrators to close the KVM consoles when they complete their tasks.

https://t.me/learningnets

Gather Information with Embedded Tools

This topic describes how to gather information with Cisco UCS B-Series embedded tools.



In general, the Cisco UCS troubleshooting tools are accessible through the device CLI and the Cisco UCS Manager GUI. Most tools are related to data gathering and include the client logs, verification and monitoring commands, log files and core dumps, finite state machine (FSM), and Ethanalyzer.

Backup and restore tools are not specifically related to troubleshooting but ensure that the system can be recovered from major faults.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS CLI Scope

- Scoping: Moving to different Cisco UCS configuration components
  - Details regarding hardware components are found with the **scope** command.
- You should be on the primary Fabric Interconnect for most tasks.

```
FarNorth-B# scope

adapter                     Mezzanine Adapter
chassis                     Chassis
eth-server                  Ethernet Server Domain
eth-uplink                  Ethernet Uplink
fabric-interconnect         Fabric Interconnect
fc-uplink                   FC Uplink
firmware                    Firmware
host-eth-if                 Host Ethernet Interface
host-fc-if                  Host FC Interface
monitoring                  System Monitor
org                         Organizations
security                    Security Mode
server                      Server
service-profile             Service Profile
system                      Systems
vhba                        VHBA
vnic                        VNIC
```

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

The **scope** command moves the CLI to different configuration components. From a troubleshooting perspective, one of the primary uses of the **scope** command is to access component resident log files.

Effective use of the **scope** command improves your CLI experience and your ability to gather information and resolve faults more quickly.

The Cisco UCS Manager Equipment tab enables administrators to access different physical components of Cisco UCS. Similarly, the **scope** command from the Cisco UCS CLI enables various components to be accessed. Navigation commands include the following:

- **where:** Displays the mode of the **scope** command
- **up:** Moves the CLI up one level in the hierarchy
- **top:** Moves the CLI to the top of the hierarchy

When you access a component with the **scope** command, a Unix-like path is displayed in the command prompt.

https://t.me/learningnets

Viewing the Switch Configuration

```
T6100-A# show configuration | begin "scope fabric-interconnect a"
 scope fabric-interconnect a
     activate firmware kernel-version 4.2(1)N1(1.4m)
     activate firmware system-version 4.2(1)N1(1.4m)
     set out-of-band ip 192.168.10.101 netmask 255.255.255.0 gw 192.168.10.254
 exit
 scope fabric-interconnect b
     activate firmware kernel-version 4.2(1)N1(1.4m)
     activate firmware system-version 4.2(1)N1(1.4m)
     set out-of-band ip 192.168.10.102 netmask 255.255.255.0 gw 192.168.10.254
 exit
```

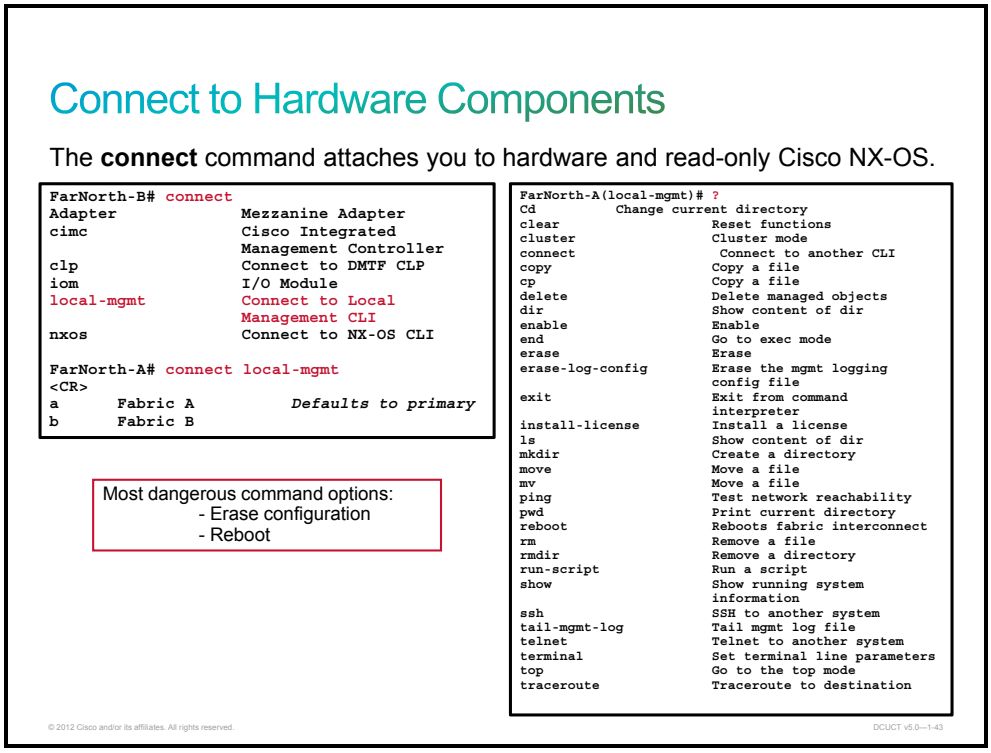
© 2012 Cisco and/or its affiliates. All rights reserved.

The switch configuration file is searched to reveal the installed firmware and OOB management interface for both Fabric Interconnects. As part of the information gathering phase, it is useful to check the version of Cisco UCS Manager that is currently running and note whether to check for more recent software versions or consider check bug reports for that version on Cisco.com.

Note the use of the filtering pipe with **“scope-interconnect a”** to start the configuration display at a specific point.

 © 2012 Cisco Systems, Inc.

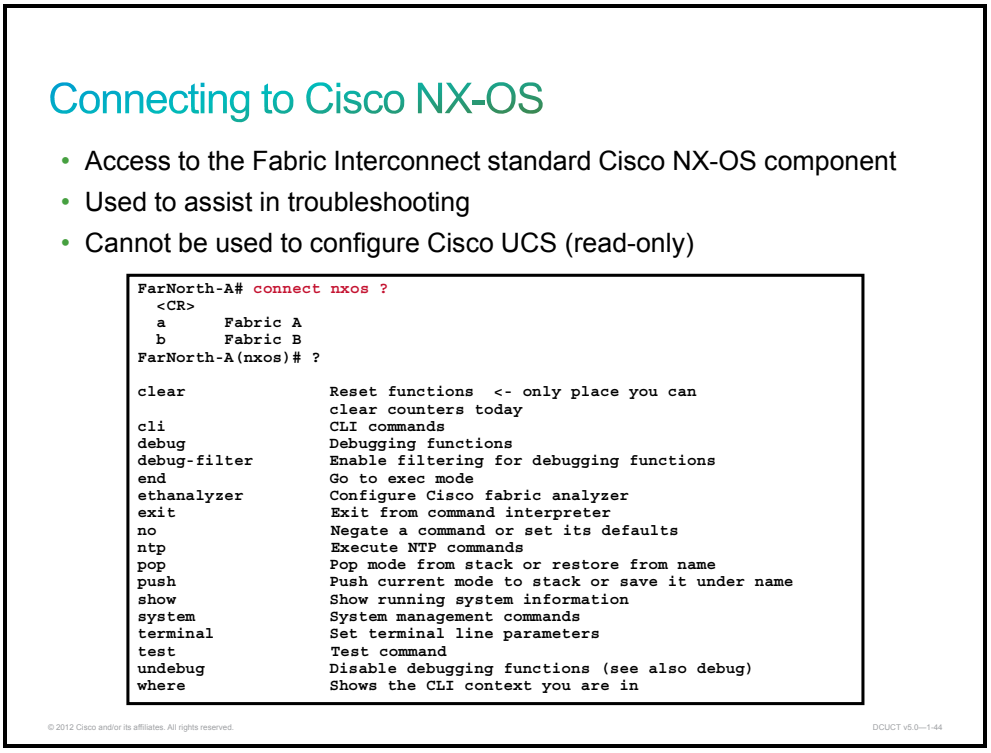
https://t.me/learningnets



From the Fabric Interconnect main shell, you can connect to various hardware components as well as the read-only Cisco Nexus Operating System (Cisco NX-OS) shell.

Connecting to all devices in the chassis is part of the gathering information phase and, later, in the diagnosis phase.

https://t.me/learningnets

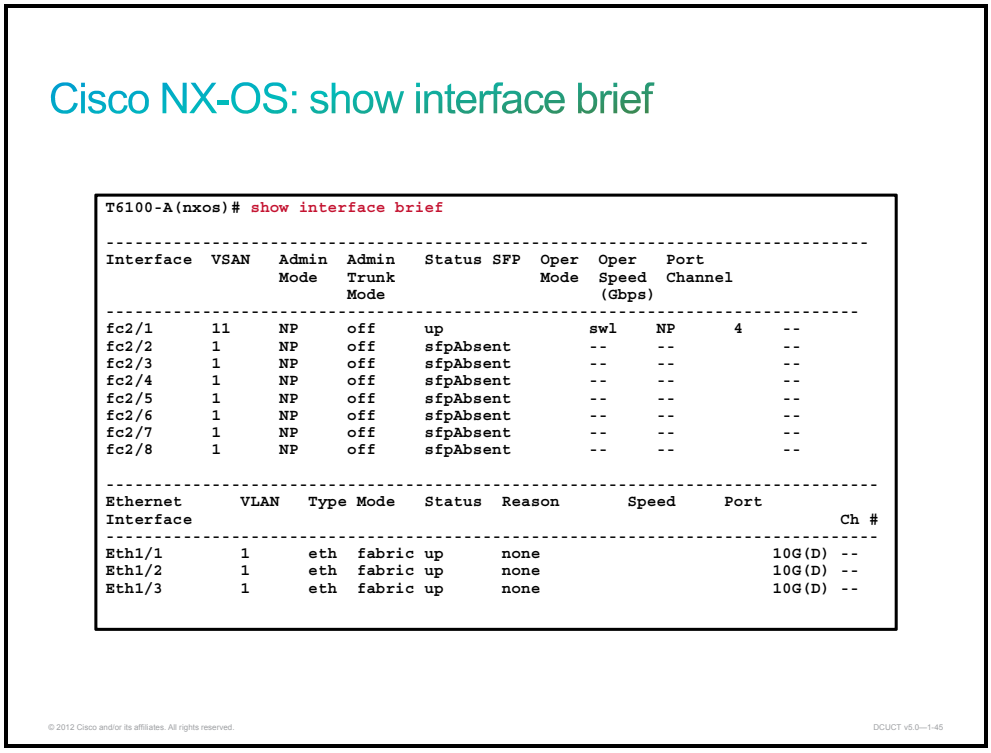


Cisco UCS runs on Cisco NX-OS, which is the same operating system that is used by the entire Cisco Nexus and Cisco MDS product lines. As a troubleshooting tool, this shell enables a support engineer to determine the state of Fabric Interconnect ports, run debug commands, view the running configuration file, enable and run Ethanalyzer, and clear and view port counters.

By default, the **connect nxos** command connects to the active node of the Cisco UCS cluster. However, the standby node can be specified. Popular **show** commands that are run from the Cisco NX-OS shell include the following:

- **show running-config**
- **show fex detail**
- **show interface**
- **show lacp neighbor**
- **show npv flogi-table**
- **show mac address-table**
- **debug**

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



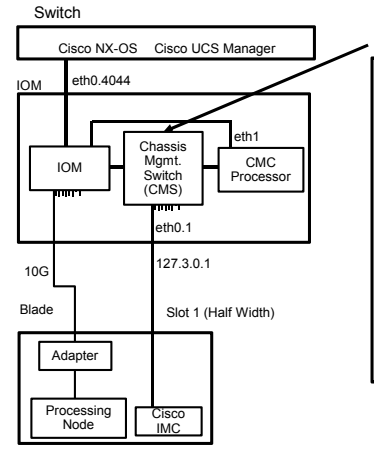
Two important troubleshooting commands from the Cisco NX-OS prompt are **show interface** and **show interface brief**. In this figure, you see the state of the Fibre Channel ports in the Fabric Interconnect expansion module.

The output that describes the other Ethernet ports on Fabric Interconnect A is not shown here.

https://t.me/learningnets

IOM Monitoring

- IOM-related problems can affect the server connectivity.
- Connect to the appropriate IOM.
- Verify connections to the baseboard management connector on blades.



Chassis Management Switch Statistics

```
T6100-A# connect iom 1
Attaching to FEX 1 ...
To exit type 'exit', to abort type '$.'
fex-1# show platform software cmcctrl cms all
0       up
1       Up
2       up
3       up
4       up
5       up
6       down
7       down
8       down
9       no_phy
10      no_phy
```

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

If you experience connectivity problems inside a chassis, you should verify the operation of the IOM. From the Cisco UCS Manager CLI, you can connect to the appropriate IOM by using the **connect iom** command.

From the Cisco NX-OS shell, you can use the **show platform software cmcctrl cms all** command to display connections to the baseboard management connector on each blade.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Data Gathering

There are multiple sources for data gathering:

- Verification and monitoring commands
- Log files and core dumps
- dmidecode
- FSM
- Ethanalyzer

```
FEX-1# term len 0
FEX-1# show platform software redwood rate
+-------++------------+----------+------------++------------+----------+------------+-------+-------+---+
| Port  || Tx Packets | Tx Rate  |  Tx Bit    || Rx Packets | Rx Rate  |  Rx Bit    |Avg Pkt|Avg Pkt|   |
|       ||            | (pkts/s) |  Rate      ||            | (pkts/s) |  Rate      | (Tx)  | (Rx)  |Err|
+-------++------------+----------+------------++------------+----------+------------+-------+-------+---+
| 0-NI3 ||         24 |        4 |   7.68Kbps ||         58 |       11 | 11.65Kbps |   200 |   125 |   |
| 0-NI2 ||          2 |        0 |   3.41Kbps ||          2 |        0 |  2.07Kbps |  1068 |   648 |   |
| 0-NI1 ||          2 |        0 |   3.41Kbps ||          5 |        1 |  2.54Kbps |  1068 |   318 |   |
| 0-NI0 ||         22 |        4 |  16.36Kbps ||          2 |        0 |  2.07Kbps |   465 |   648 |   |
| 0-HI7 ||          3 |        0 | 472.00 bps ||          0 |        0 |  0.00 bps |    99 |     0 | . |
| 0-HI5 ||          3 |        0 | 472.00 bps ||          0 |        0 |  0.00 bps |    99 |     0 |   |
| 0-HI1 ||          3 |        0 | 472.00 bps ||          0 |        0 |  0.00 bps |    99 |     0 |   |
| 0-BI  ||         34 |        6 |   4.84Kbps ||         27 |        5 |  5.49Kbps |    89 |   127 |   |
| 0-CI  ||         28 |        5 |  12.09Kbps ||         28 |        5 | 26.80Kbps |   270 |   598 |   |
```

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

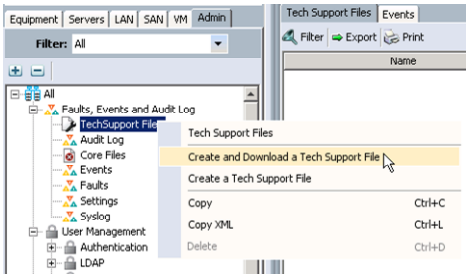
There are various tools that can be employed to gather critical support data for diagnosing and resolving support issues.

In this example, you see how to use the **show platform software redwood rate** command, which can be used to determine how much traffic is flowing through the IOM ports.

- **Host Interface:** Host facing
- **Network Interface:** Fabric Interconnect facing

https://t.me/learningnets

Tech Support File in Cisco UCS Manager



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

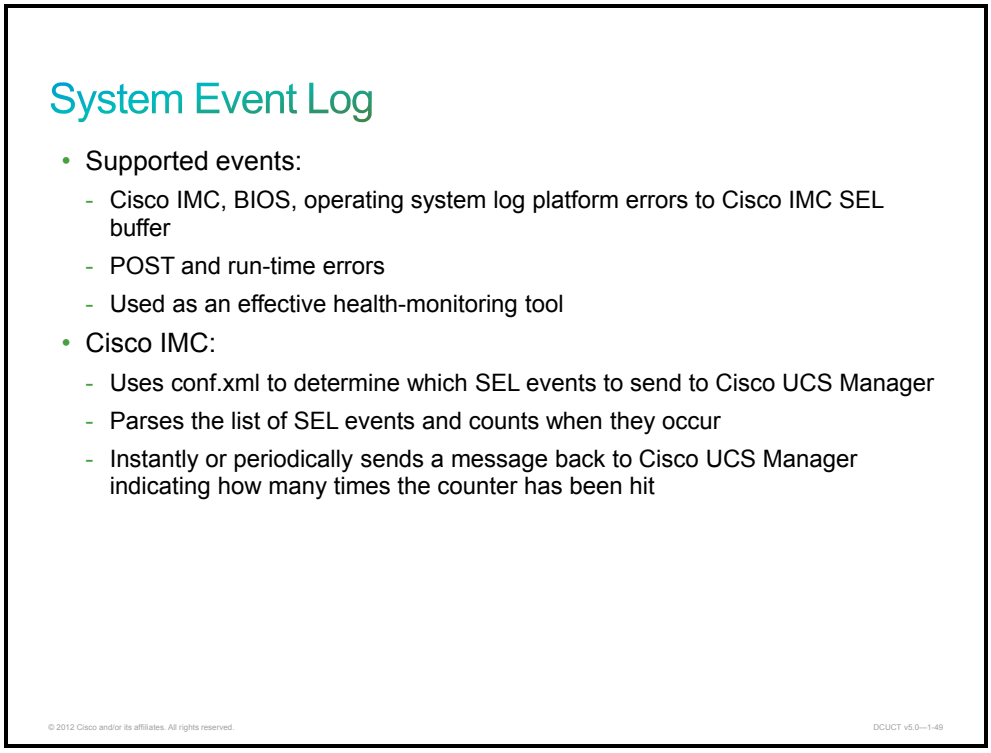
The **show tech-support** command can be run across Cisco UCS Manager in its entirety or on individual components. The file that is generated contains a wide array of information about the operational state of the Cisco UCS environment.

The command can be run from the CLI or from Cisco UCS Manager. One advantage of running the command from Cisco UCS Manager is that it can be automatically downloaded to the network management station of the user.

If your issue needs to be escalated to Cisco support, output from this command will be one of the first requests from the Cisco Technical Assistance Center (TAC) engineer. The **show tech-support** output can be uploaded directly to the Cisco Technical Support TFTP server (171.69.17.19). The following output shows an example of how information has been gathered and then moved to the TFTP site:

```
A(local-mgmt)# show tech-support chassis <chassis id> all
detail
A(local-mgmt)# copy
workspace:///techsupport/<name_of_the_file>.tar
tftp://171.69.17.19
```


https://t.me/learningnets



The system event log (SEL) records most server-related events, such as overvoltage, undervoltage, temperature events, fan events, and events from the BIOS to the Cisco Integrated Management Controller buffer. The SEL is an effective health monitoring tool and is usually used for troubleshooting purposes.

The SEL resides on the Cisco Integrated Management Controller in NVRAM.

The SEL file is approximately 40 KB in size and no further events can be recorded when it is full. It must be cleared before additional events can be recorded.

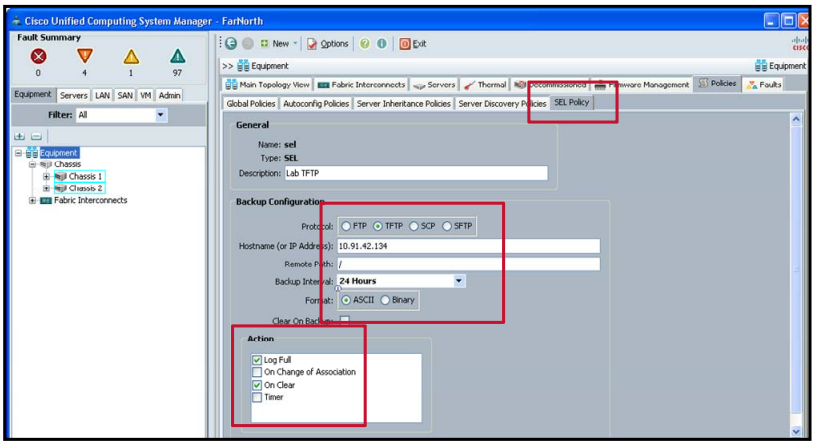
You can use the SEL policy to back up the SEL to a remote server, and you can optionally clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions or they can occur at regular intervals. You can also manually back up or clear the SEL.

The backup file is automatically generated. The filename format is as follows: sel-SystemName-ChassisID-ServerID-ServerSerialNumber-TimeStamp. An example is sel-UCS-A-ch01-serv01-QCI12522939-20091121160736.

https://t.me/learningnets

SEL Configuration

- Users can define rules (policies) for backing up and clearing the SEL across all servers in Cisco UCS, or users can manually trigger an SEL backup on individual servers.

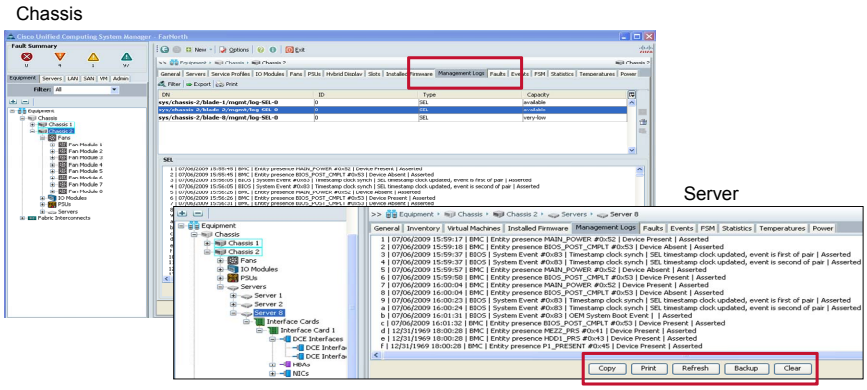


© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco UCS Manager can be used to automatically back up and clear the SEL across all servers in Cisco UCS. The interface also allows for manual backing up of SELs.

SELs as Management Logs

- Make sure that servers are discovered.
- Make sure that the backup destination path is valid.
- This can also be done via CLI.

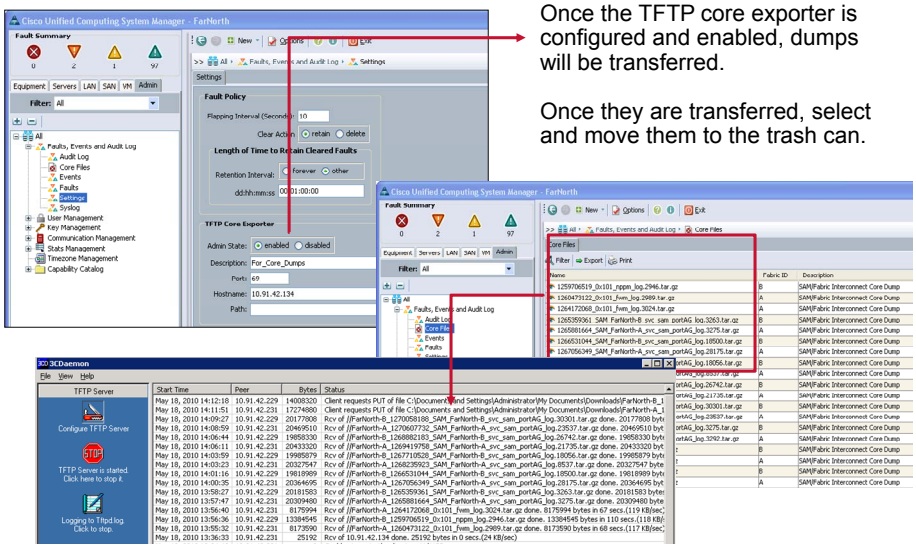


© 2012 Cisco and/or its affiliates. All rights reserved.

Management logs can be viewed from Cisco UCS Manager and from the CLI.

https://t.me/learningnets

Core Dumps



Once the TFTP core exporter is configured and enabled, dumps will be transferred.

Once they are transferred, select and move them to the trash can.

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

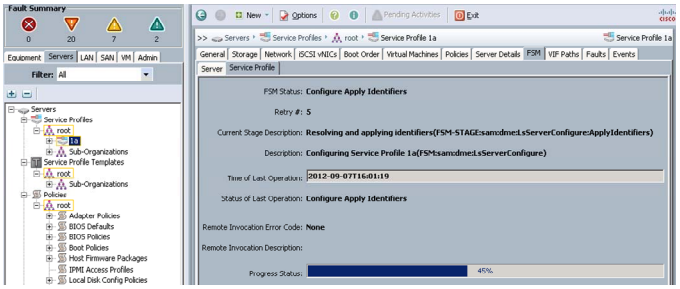
DCUCT v5.0—1-52

Cisco UCS Manager uses Core File Exporter to export core files through TFTP as soon as they occur on a specified location on the network. This functionality allows you to export the .tar file with the contents of the core file.

https://t.me/learningnets

Finite State Machine

- FSM is a workflow model, similar to a flow chart, that is composed of the following:
  - A finite number of stages (states)
  - Transitions between those stages
  - Operations
- Almost every action done by Cisco UCS Manager has an FSM to verify operation and status.



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

A finite state machine (FSM) is a workflow model, similar to a flow chart that is composed of the following: a finite number of stages (states), transitions between those stages, and operations. The current stage in an FSM is determined by past stages and the operations that are performed to transition between the stages. A transition from one stage to another is dependent on the success or failure of an operation.

The Cisco UCS Manager GUI displays FSM information for an endpoint on the FSM tab for that endpoint. You can use the FSM tab to monitor the progress and status of the current FSM task and view a list of the pending FSM tasks. The information about a current FSM task in the Cisco UCS Manager GUI is dynamic and changes as the task progresses. You can view the following information about the current FSM task:

- Which FSM task is being executed
- The current state of that task
- The time and status of the previously completed task
- Any remote invocation error codes that are returned while processing the task
- The progress of the current task

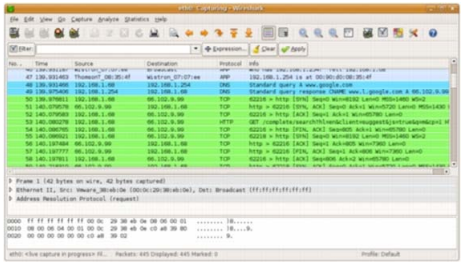
If you want to view the FSM task for an endpoint that supports FSM, navigate to the endpoint in the Navigation pane and click on the FSM tab in the Work pane.

The Cisco UCS Manager CLI can display the FSM information for an endpoint when you are in the command mode for that endpoint. You can use the **show fsm status** command in the appropriate mode to view the current FSM task for an endpoint. The information that is displayed about a current FSM task in the CLI is static. You must reenter the command to see progress updates.

https://t.me/learningnets

Ethanalyzer Overview

- Wrapper over Terminal Wireshark (TShark), the command-line network protocol analyzer of Wireshark
- Utility to view Fabric Interconnect control data and management traffic:
  - Collects frames that are destined to, or that originate from, the Fabric Interconnect control plane
  - Captures traffic: node to Fiber Interconnect as well as Fiber Interconnect to network
- Packet capture file can be either of the following:
  - Read in CLI
  - Exported and viewed in the Wireshark GUI



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

Ethanalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open-source code. Ethanalyzer is a command-line version of Wireshark that captures and decodes packets. You can use Ethanalyzer to troubleshoot your Cisco UCS Fabric Interconnect control and management traffic.

A packet capture file can be read directly on the Cisco NX-OS command line, or the file can be exported. To locally open a capture file, use the Ethanalyzer **local read** command. To export the packet capture file, use the **copy** command. The destination can be any of these options:

- ftp:
- scp:
- sftp:
- tftp:
- usb1:

After it has been exported, the capture file can be opened with Wireshark to allow easier analysis of the capture, as shown here.

https://t.me/learningnets

Capturing Traffic with Ethanalyzer

1. Capture an unlimited detailed number of packets with decoded internal information and save the capture to a file called capture.pcap.
2. Capture a specified maximum number of packets (4).

```
switch# ethanalyzer local interface inbound-hi decode-internal detail limit-captured-
frames 0 write bootflash:capture.pcap
Capturing on eth4
13494
```

```
switch# ethanalyzer local interface inbound-hi limit-captured-frames 4
 Capturing on eth4
2011-05-15 22:01:24.344267 c8:4c:75:4d:52:f4 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP,
OUI 0x00000C (Cisco), PI
D 0x0134

2011-05-15 22:01:24.344345 c8:4c:75:4d:52:f5 -> 01:80:c2:00:00:0e LLC U, func=UI; SNAP,
OUI 0x00000C (Cisco), PI
D 0x0134

2011-05-15 22:01:24.670571 c8:4c:75:5b:25:40 -> 00:05:73:b4:f3:a4 LLC U, func=UI; SNAP,
OUI 0x00000C (Cisco), PI
D 0x0120

2011-05-15 22:01:24.670876 c8:4c:75:5b:25:40 -> 00:05:73:b4:f3:a4 LLC U, func=UI; SNAP,
OUI 0x00000C (Cisco), PI
D 0x0120

4 packets captured
```

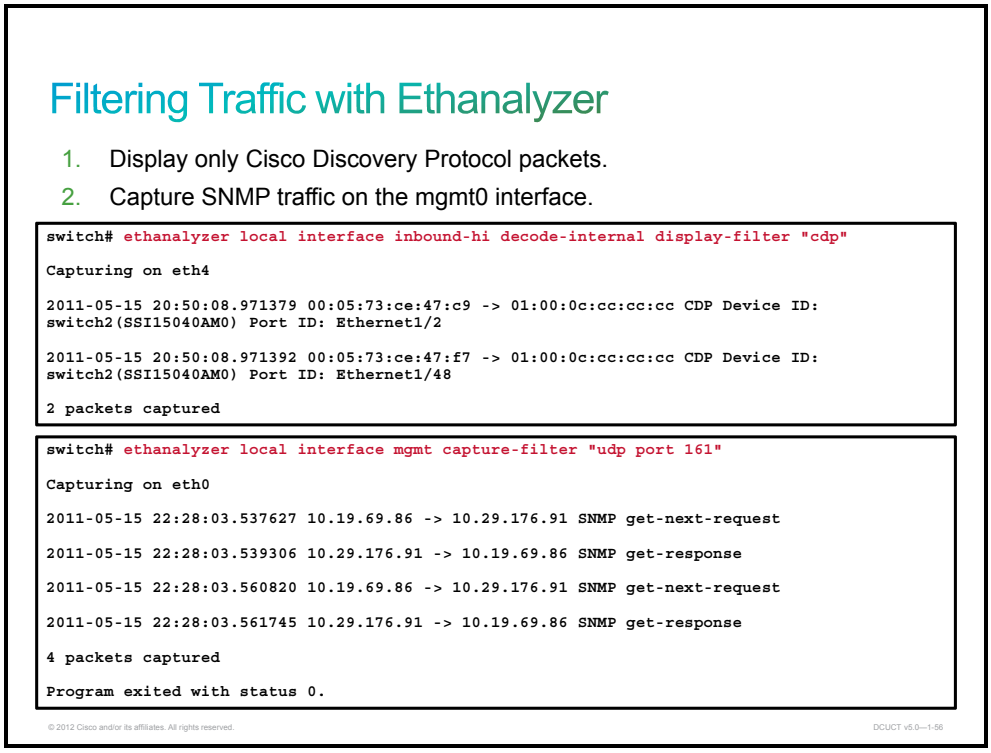
© 2012 Cisco and/or its affiliates. All rights reserved.

Ethanalyzer offers a wide range of packet capture and display options, as shown in this table:

Option	Description
autostop	Capture autostop condition
capture-filter	Filter on Ethanalyzer capture
capture-ring-buffer	Capture ring buffer option
decode-internal	Include internal system header decoding
detail	Display detailed protocol information
display-filter	Display filter on frames captured
limit-captured-frames	Maximum number of frames to be captured (default is 10)
limit-frame-size	Capture only a subset of a frame
write	Filename to which to save capture

By default, Ethanalyzer captures up to 10 frames. The first example shown in the figure illustrates how to capture an unlimited detailed number of packets with decoded internal information and save the capture to a file called “capture.pcap.” The second example shows how to capture a specified maximum number of packets (four in this case).

https://t.me/learningnets

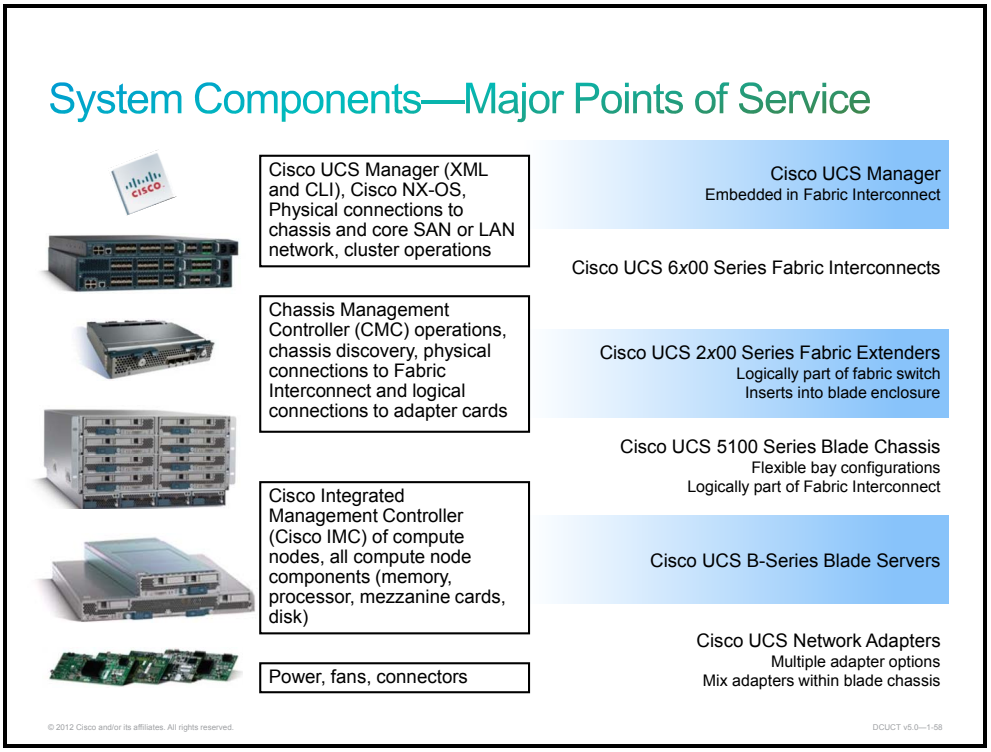


These examples illustrate how to filter packets. In the first example, you display only Cisco Discovery Protocol packets. In the second case you capture SNMP traffic on the mgmt0 interface.

https://t.me/learningnets

Troubleshoot Cisco UCS Hardware Discovery

This topic describes how to troubleshoot Cisco UCS B-Series hardware discovery.



Cisco UCS has many different points of service, including the following:

- Cisco UCS Manager
- Cisco UCS Fabric Interconnects
- Cisco UCS 2100 Fabric Extenders
- Cisco UCS 5100 Series Blade Chassis
- Cisco UCS B-Series Blade Servers
- Cisco UCS Network Adapters

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Viewing Chassis and Blade Discovery

```
FEX-1# show platform software cmcctrl dmclient all
Last scan time                  : 2017842
Chassis-id                      : 1
Fabric-id                       : 1
Cluster-id                      : f1f4d8ac-a0a2-11e0-aca9-000decfde544
Peer IOM                        : PRESENT
Slot id                         : 0
Amber LED Status                : ON
Green LED Status                : OFF
Chassis ok LED Status           : ON
Chassis fault LED Status        : OFF
Locate LED Sattus               : OFF
Locate buttion status           : 0
Backplane status                : 1
Blades present                  : 0 1 2 3 4 5 6 7
Blades powered on               : 0 1 2 3 4 5 6 7
Blades alerted                  : 0 1 2 3 4 5
Fans present                    : 0 1 2 3 4 5 6 7
Fans alerted                    : 0 1 2 3 4 5 6 7
PSs present                     : 0 1 2 3
PSs RMT on                      : 0 1 2 3
PS DC ok                        : 2 3
PS AC ok                        : 2 3
```

Presence and status of the blades

Presence and status of the fans

Presence and status of the power supplies

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

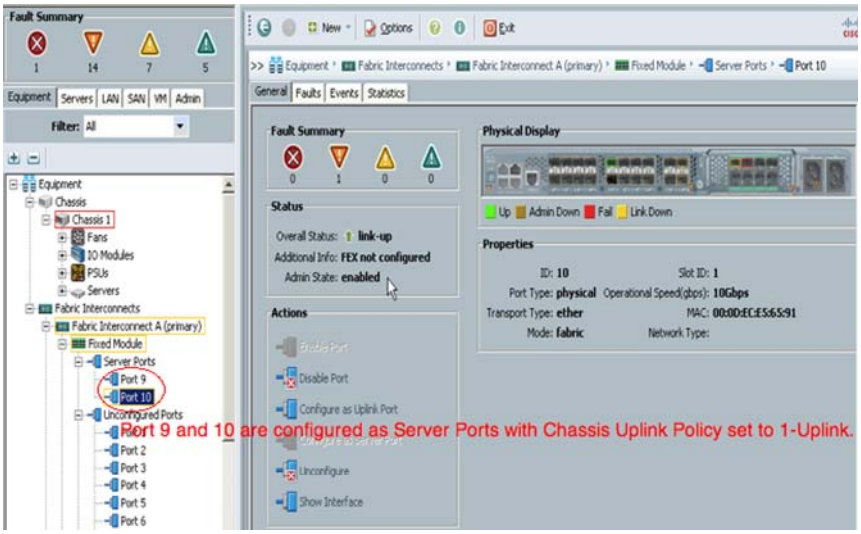
A common problem that results from improper installation and incorrect initial system configuration is the failure of chassis, fabric links, and blades to be properly recognized.

Assuming that Cisco UCS has a two-switch cluster, the **show cluster state** command will help identify whether at least one chassis is recognized by the Fabric Interconnects. If the cluster switches are not in high-availability mode, ensure that the links to the chassis are enabled.

The **show platform software cmcctrl dmclient all** command can be used to quickly determine whether a peer IOM is present, and the number of recognized blades, fans, and power supplies.

https://t.me/learningnets

Server Ports Configuration with Default Chassis Policy



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

With Cisco UCS Manager, it is easy to determine which Fabric Interconnect ports have been designated as server ports (ports that should connect to a chassis IOM). Here you see that port 10 is configured as a server port but that it is not communicating properly with the FEX (IOM).

From Cisco NX-OS, you can use the **show interface brief** command to find the configuration problem with the fabric port Eth 1/1:

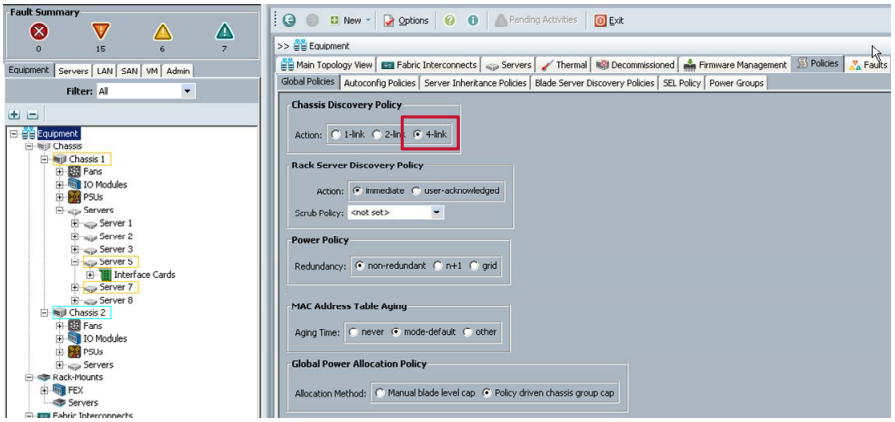
```
T6100-a(nxos)# show interface brief
Interface  Vsan   Admin  Admin  Status  SFP  Oper  Oper Port
           Mode    Trunk           Mode Speed Channel
                Mode                (Gpbs)
fc2/1 1   NP    off   Inlt      swl -    -
fc2/2 1   NP    off   sfpAbsent    -  -    -
fc2/3 1   NP    off   sfpAbsent    -  -    -
fc2/3 1   NP    off   sfpAbsent    -  -    -
fc2/4 1   NP    off   sfpAbsent    -  -    -
fc2/5 1   NP    off   sfpAbsent    -  -    -
fc2/6       1   NP    off   sfpAbsent    -  -    -
fc2/7 1   NP    off   sfpAbsent    -  -    -
fc2/8 1   NP    off   sfpAbsent    -  -    -

Ethernet   VLAN   Type Mode Status Reason    Speed        Port
Interface                                Ch#
Eth1/1     4044   eth trunk up    none         10G(D)-
Eth1/2     1      eth fabric up   none         10G(D)-
Eth1/3     1      eth access down   Administratively down
10G(D)-
```

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Chassis Discovery Policy

- The default chassis discovery policy is one link.
- Change the default discovery policy to the appropriate number of links.
- Reacknowledging overwrites all policies and discovers all links.



The default chassis policy is one link. This means that any chassis with at least one fabric link should be recognized. However, any links in excess of the default of one will not be functional until the chassis is reacknowledged or the default chassis policy is changed.

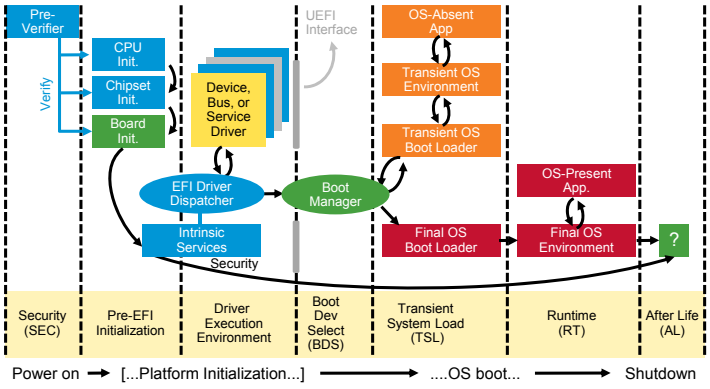
Reacknowledging the chassis is the preferred method for initializing ports that are ignored because of the default chassis policy. Cisco UCS Manager disconnects the server and then builds the connections between the server and the Fabric Interconnect or Fabric Interconnects in the system. The acknowledgment may take several minutes to complete. After the server has been acknowledged, the Overall Status field on the General tab displays an “OK” status.

If the default chassis discovery policy is set to four, then any chassis with fewer than four links will not be recognized.

https://t.me/learningnets

Decoding BIOS POST

- When the BIOS is not booting, how do we understand what is happening?
- Understand the POST process and look for POST codes that indicate the source of the problem. (Consult documentation for meanings.)



OS = operating system; EFI = Extensible Firmware Interface

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

A power-on self-test (POST) behaves differently depending on the platform and BIOS settings.

There are some things to consider when troubleshooting POST failures:

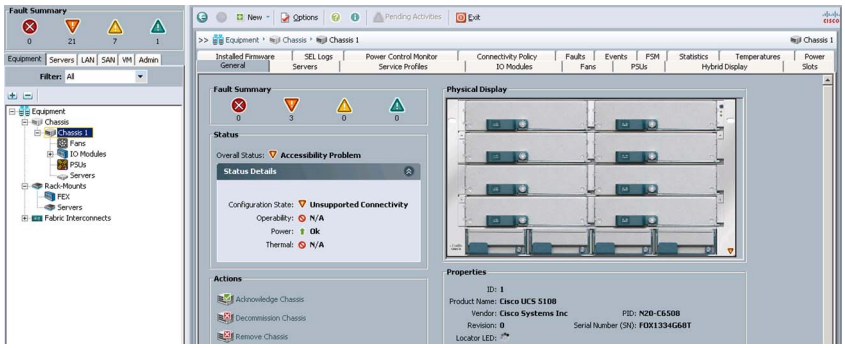
- Save the known default BIOS settings on a good blade and rack. Use it as a good reference with a non-booting POST code sequence.
- If you reached POST code 0x00, this means that the BIOS has finished and that the issue is likely outside of BIOS POST.
- Quickly scan the POST output and look for "[ERROR]." If it is not a duplicate, it is likely the cause of the failure. If it is a duplicate, compare it with your good reference booting sequence.
- It may be most productive to look at the last few POST codes and see where it was stuck.
- If the last POST code is stuck in Memory Reference Code (MRC) at POST code 0xe1, it is likely a Complementary Metal-Oxide Semiconductor (CMOS) Reset bug. Resetting CMOS will fix the issue.

Note The security (SEC), MRC, and CHECKPOINT pieces of the BIOS POST will take longer to execute when you have more memory in the system.

https://t.me/learningnets

Chassis Discovery Failure—Symptom

- The chassis is not discovered correctly.
- The Overall Status field in the General tab reports “Accessibility Problem.”
- The Configuration State reports “Unsupported Connectivity.”



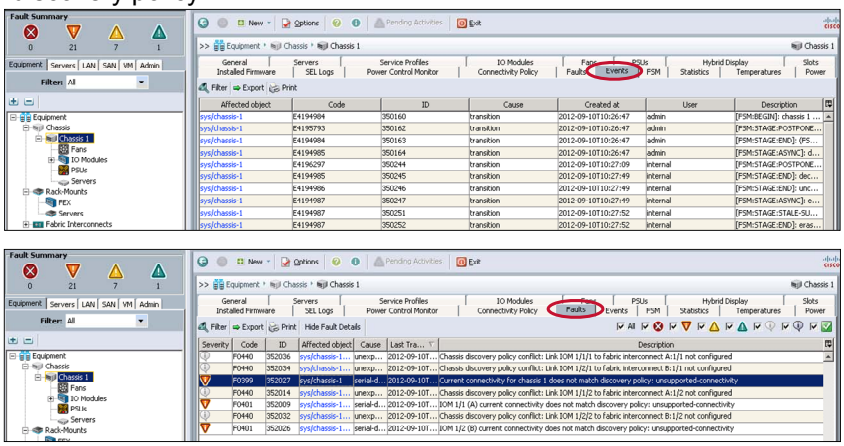
© 2012 Cisco and/or its affiliates. All rights reserved.

This scenario illustrates how to apply a troubleshooting approach to a chassis discovery problem. In Cisco UCS Manager, the problem is seen when you navigate to the chassis and view the General tab. The overall status is reported as “Accessibility Problem.” The Configuration state is displayed as “Unsupported Connectivity.”

https://t.me/learningnets

Chassis Discovery Failure—Gathering Info

- Useful GUI tools include the Faults, Events, and FSM tabs.
- The Fault reports as “Current connectivity for chassis does not match discovery policy.”



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

In the data gathering phase, examine the information that is available in the Cisco UCS Manager GUI. Valuable information is provided in the tabs such as in Faults, Events, and FSM. In this case, the fault description that is displayed reads “Current connectivity for chassis 1 does not match discovery policy.”

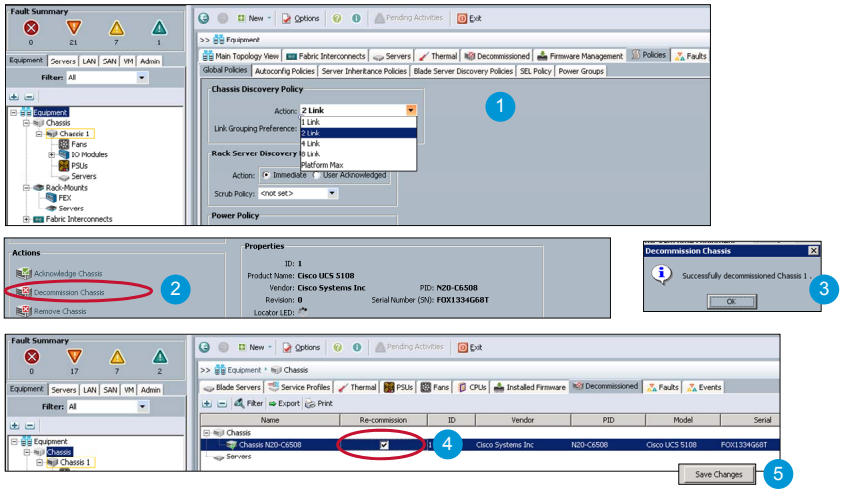
This information helps you identify a problem with the chassis discovery policy.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Chassis Discovery Failure Remediation

- Configure appropriate action in the Chassis Discovery Policy section.
- Decommission and recommission the chassis.



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

The chassis discovery policy determines how the system reacts when you add a new chassis. Cisco UCS Manager uses the settings in the chassis discovery policy to determine the minimum threshold for the number of links between the chassis and the Fabric Interconnect and whether to group links from the IOM to the Fabric Interconnect in a fabric port channel.

This table provides an overview of how the chassis discovery policy works in a multichassis Cisco UCS domain:

Number of Links Wired for the Chassis	1-Link Chassis Discovery Policy	2-Link Chassis Discovery Policy	4-Link Chassis Discovery Policy	8-Link Chassis Discovery Policy	Platform-Max Discovery Policy
1 link between IOM and Fabric Interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS domain.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS domain.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS domain.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link.
2 links between IOM and Fabric Interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 2 links.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS domain.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS domain.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS domain.

https://t.me/learningnets

Number of Links Wired for the Chassis	1-Link Chassis Discovery Policy	2-Link Chassis Discovery Policy	4-Link Chassis Discovery Policy	8-Link Chassis Discovery Policy	Platform-Max Discovery Policy
4 links between IOM and Fabric Interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 2 links. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 4 links.	Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS domain.	If the IOM has 4 links, the chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 4 links. If the IOM has 8 links, the chassis is not fully discovered by Cisco UCS Manager.
8 links between IOM and Fabric Interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 2 links. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 4 links. After initial discovery, reacknowledg e the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 8 links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 8 links.

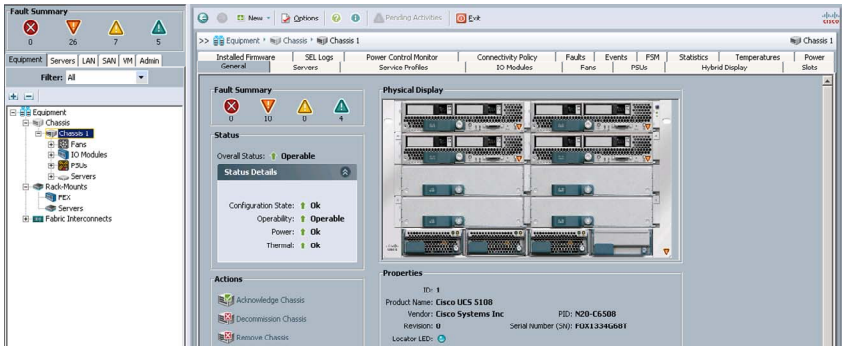
In this case, you modify the Action in the chassis discovery policy to two-link, decommission it, and recommission the chassis to resolve the discovery problem.

Note For Cisco UCS implementations that mix IOMs with different numbers of links, you should use the platform max value. Using platform max ensures that Cisco UCS Manager uses the maximum number of IOM uplinks that are available.

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

Chassis Discovery Failure Resolution Results

- After the number of links has been set correctly, chassis discovery succeeds.
- Alternatively, you could acknowledge the chassis.



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

After you set the Action to the correct link value, and decommission and recommission the chassis, the discovery process will succeed.

You may have used an alternative approach to achieve the same result, to acknowledge the chassis even though it was not discovered properly. Cisco UCS Manager would then recognize the system properly.

https://t.me/learningnets

Issue: HDD Metrics Not Updated in the Cisco UCS Manager GUI

Problem	After hot-swapping, removing, or adding a hard drive, the updated HDD metrics do not appear in the Cisco UCS Manager GUI.
Possible Cause	• Cisco UCS Manager gathers HDD metrics only during a system boot. • If a hard drive is added or removed after a system boot, the Cisco UCS Manager GUI does not update the HDD metrics.
Solution	Reboot the server.

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

After hot-swapping, removing, or adding a hard drive, the updated hard disk drive (HDD) metrics do not appear in the Cisco UCS Manager GUI.

This problem can be caused because Cisco UCS Manager gathers HDD metrics only during a system boot. If a hard drive is added or removed after a system boot, the Cisco UCS Manager GUI does not update the HDD metrics.

To update the HDD metrics, reboot the server.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Issue: Cisco UCS Manager Reports More Disks in Server than Total Slots Available

Problem	Cisco UCS Manager reports that a server has more disks than the total available disk slots in the server.
Possible Cause	This problem is typically caused by a communication failure between Cisco UCS Manager and the server that reports the inaccurate information.
Solution	• Decommission the server. • Recommission the server.

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

You might encounter an issue with Cisco UCS Manager reporting that a server has more disks than the total disk slots that are available in the server. For example, Cisco UCS Manager reports three disks for a server with two disk slots as follows:

```
RAID Controller 1:
           Local Disk 1:
               Product Name: 73GB 6Gb SAS 15K RPM SFF HDD/hot
plug/drive sled mounted
               PID: A03-D073GC2
               Serial: D3B0P99001R9
               Presence: Equipped
           Local Disk 2:
               Product Name:
               Presence: Equipped
               Size (MB): Unknown
           Local Disk 5:
               Product Name: 73GB 6Gb SAS 15K RPM SFF HDD/hot
plug/drive sled mounted
               Serial: D3B0P99001R9
               HW Rev: 0
               Size (MB): 70136
```

This problem is typically caused by a communication failure between Cisco UCS Manager and the server that reports the inaccurate information. To update the server information, decommission the server and then recommission it.

https://t.me/learningnets

Summary

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

Summary

- Cisco UCS B-Series architecture typically uses dual-fabric design for LAN and SAN connectivity.
- Cisco UCS requires three IP addresses for each Fabric Interconnect and at least one IP address for each server within the system for remote KVM access.
- Cisco UCS offers various tools and techniques to troubleshoot complex system issues.
- FSM status and outputs can be used to troubleshoot system and server initialization as well as service profile implementation.
- A common problem that results from improper installation and initial system configuration is the failure of chassis, fabric links, and blades to be properly recognized.

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

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 2

Troubleshooting Cisco UCS B-Series Configuration

Overview

This lesson discusses the skills that are required to understand Cisco Unified Computing System (Cisco UCS) B-Series configuration and normal operation. Many configuration problems in the Cisco UCS environment are related to service profiles and service profile templates. This lesson provides guidelines to troubleshooting the Cisco UCS B-Series service profile and management configuration. It also describes how to perform Cisco UCS B-Series password recovery.

Objectives

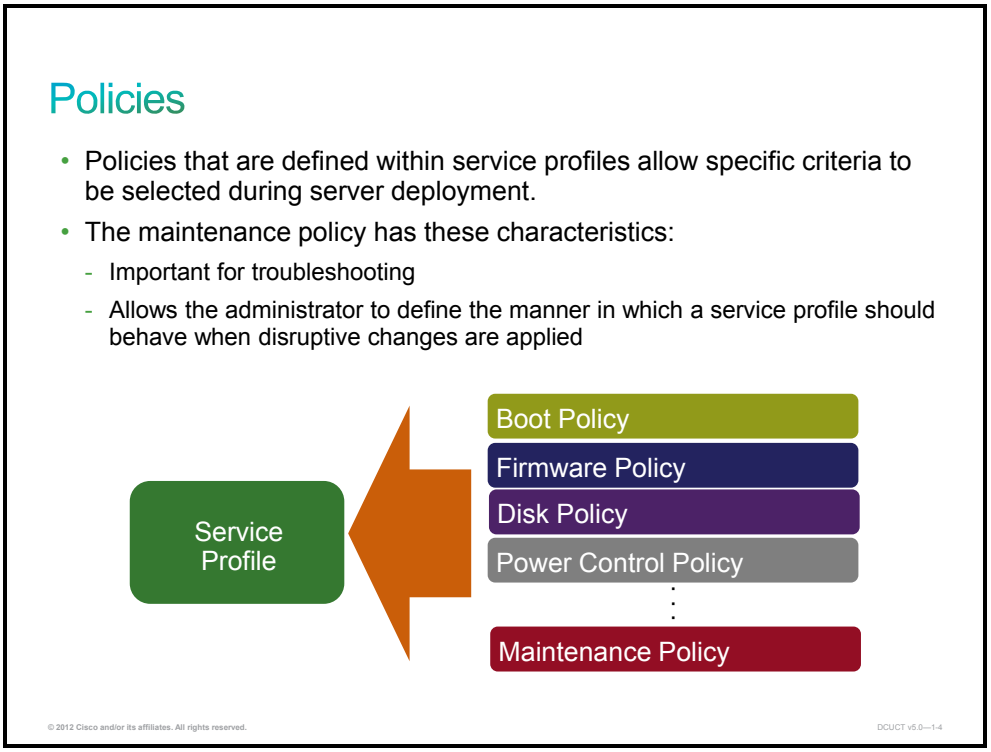
Upon completing this lesson, you will be able to describe Cisco UCS B-Series configuration and troubleshooting of related issues. This ability includes being able to meet these objectives:

- Recognize Cisco UCS B-Series configuration and normal operation
- Recognize Cisco UCS B-Series server deployment configuration
- Troubleshoot Cisco UCS B-Series service profile configuration
- Recognize Cisco UCS B-Series management configuration
- Recognize the steps that are necessary to perform Cisco UCS B-Series password recovery

https://t.me/learningnets

Cisco UCS B-Series Configuration

This topic describes the Cisco UCS B-Series configuration and normal operation.



Policies determine how Cisco UCS components act in specific circumstances. You can create multiple instances of most policies. For example, you might want different boot policies so that some servers can Preboot Execution Environment (PXE) boot, some can SAN boot, and others can boot from local storage.

Policies allow separation of functions within the system. A subject matter expert (SME) can define policies that are used in a service profile, which is created by someone without that subject matter expertise. For example, a LAN administrator can create adapter policies and quality of service (QoS) policies for the system. These policies can then be used in a service profile that is created by someone who has limited or no subject matter expertise with LAN administration.

You can create and use two types of policies in Cisco UCS Manager:

- Configuration policies
- Operational policies

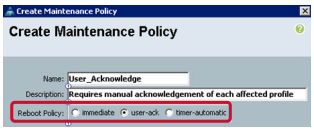
One of the policies that is shown in this figure is the maintenance policy. It has a special significance for the troubleshooting process. The maintenance policy allows the administrator to define the manner in which a service profile should behave when disruptive changes are applied.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Maintenance Policy Actions When Disruptive Change Is Made

- **Immediate**
  - Normal “soft” reboot without confirmation.
  - Standard Advanced Configuration and Power Interface (ACPI) power-button press is sent to the physical node.
  - Operating system should gracefully shut down and the node will reboot.
- **User-ack**
  - Disruptive changes are staged to each affected service profile.
  - The profile is not immediately rebooted.
  - It shows the pending changes and waits for administrator acknowledgement.
- **Timer-automatic**
  - Uses one-time or reoccurring time periods defined as a schedule.
  - Affected nodes are rebooted without administrator intervention.



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

You can define the maintenance policy to react with three different reboot behaviors when a disruptive change is made:

- **Immediate** represents the traditional approach. When a disruptive change is made, the affected service profiles are immediately rebooted without confirmation. A normal “soft” reboot occurs, whereby a standard “power-button press” event is sent to the physical node. If the operating system has a trap for this, the operating system gracefully shuts down and the node reboots.
- **User-ack** is safer in most situations. Disruptive changes are staged to each affected service profile, but the profile is not immediately rebooted. Instead, each profile shows the pending changes in its status field and waits for the administrator to manually acknowledge the changes when it is acceptable to reboot the node.
- **Timer-automatic** allows the maintenance policy to reference the Schedule object. Schedules allow you to define one-time or reoccurring time periods where one or more of the affected nodes can be rebooted without administrator intervention.

https://t.me/learningnets

Configuration Policies

- Configuration policies typically do not need to be modified in a stable environment:
  - Boot Policy
  - Chassis Discovery Policy
  - Ethernet and Fibre Channel Adapter Policies
  - Host Firmware Package
  - IPMI Access Profile
  - Management Firmware Package
  - Management Interfaces Monitoring Policy
  - Network Control Policy
- Suboptimal settings can cause transient problems, such as the following:
  - Jumbo frame drops—settings in Quality of Service Policy
  - Power priority—settings in Power Control Policy

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

Configuration policies typically do not need to be modified in a stable environment and only their understanding and verification are required for successful troubleshooting. In some cases, however, suboptimal settings can cause transient problems, such as from jumbo frame drops, which can be avoided with appropriate configuration of the Quality of Service Policy, or from power priority issues that can be prevented within the Power Control Policy.

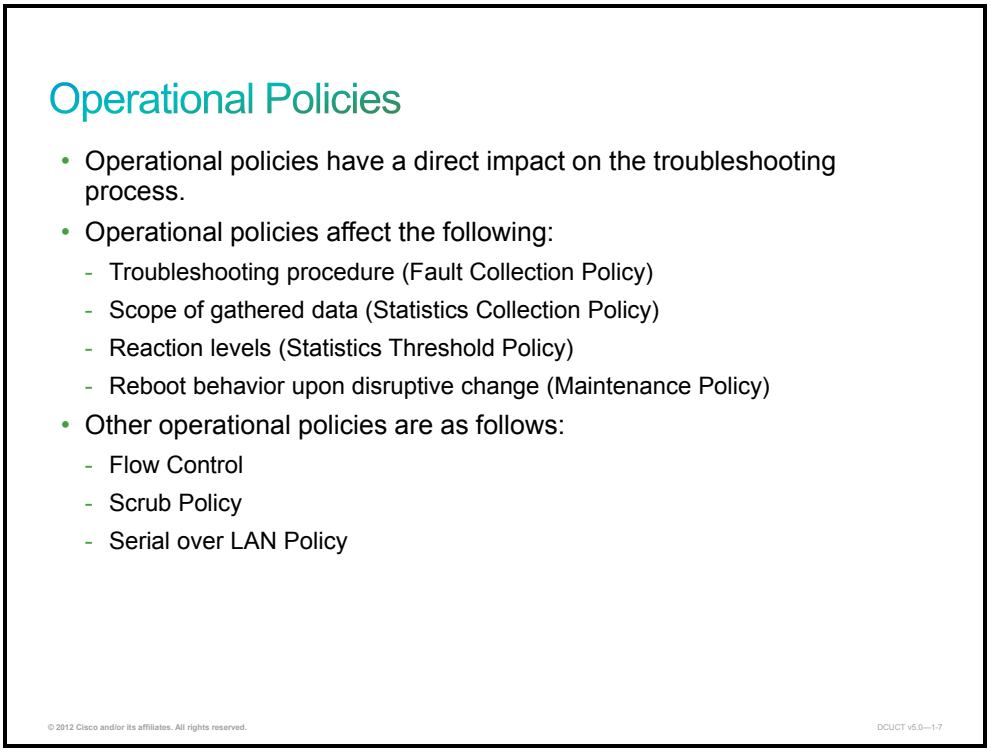
Configuration policies that affect the servers and other components include the following:

- **Boot Policy:** Determines the configuration of the boot device, the location from which the server boots, and the order in which boot devices are invoked
- **Chassis Discovery Policy:** Determines how the system reacts when you add a new chassis
- **Dynamic vNIC Connection Policy:** Determines how the connectivity between virtual machines (VMs) and dynamic virtual network interface cards (vNICs) is configured
- **Ethernet and Fibre Channel Adapter Policies:** Govern the host-side behavior of the adapter, including how the adapter manages traffic
- **Global Cap Policy:** Specifies whether policy-driven chassis group power capping or manual blade-level power capping will be applied to all servers in a chassis
- **Host Firmware Package:** Enables you to specify firmware versions that make up the host firmware package (also known as the host firmware pack)
- **IPMI Access Profile:** Allows you to determine whether Intelligent Platform Management Interface (IPMI) commands can be sent directly to the server, using the IP address
- **Management Firmware Package:** Enables you to specify firmware versions that make up the management firmware package
- **Management Interfaces Monitoring Policy:** Defines how the mgmt0 Ethernet interface on the Fabric Interconnect should be monitored
- **Network Control Policy:** Configures the network control settings for the Cisco UCS domain

https://t.me/learningnets

- **Power Control Policy:** Cisco UCS uses the priority set in this policy, along with the blade type and configuration, to calculate the initial power allocation for each blade within a chassis.
- **Power Policy:** Global policy that specifies the redundancy for power supplies in all chassis in the Cisco UCS domain
- **Quality of Service Policy:** Assigns a system class to the outgoing traffic for a vNIC or virtual host bus adapter (vHBA)
- **Rack Server Discovery Policy:** Determines how the system reacts when you add a new rack-mount server

https://t.me/learningnets



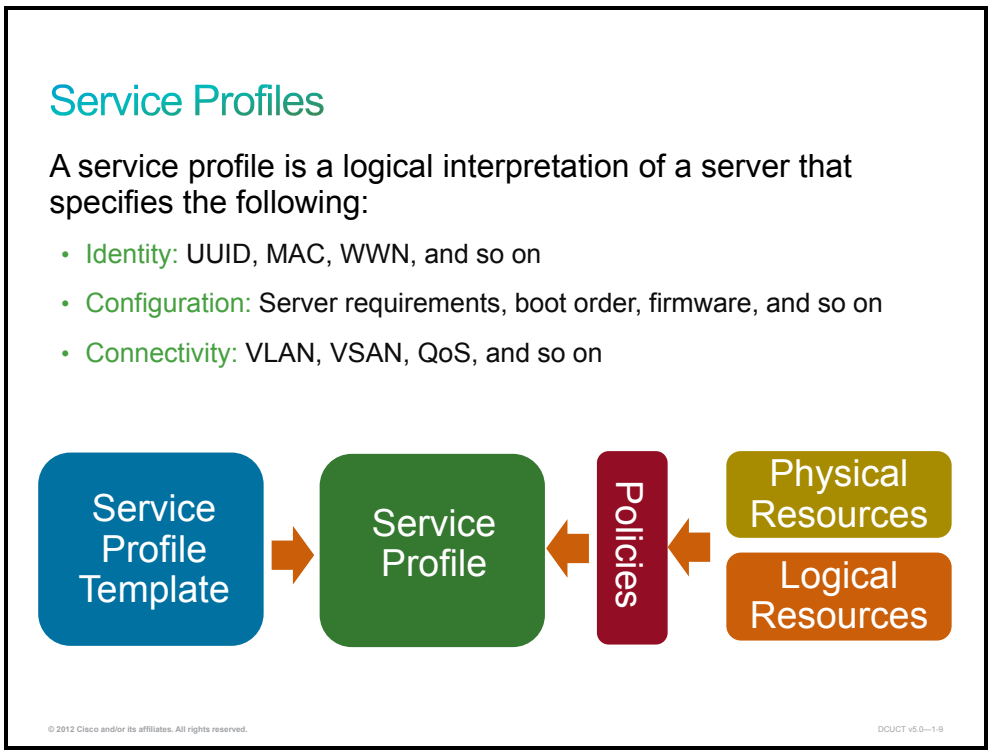
Operational policies fulfill management, monitoring, and access control functions. They have a direct impact on the troubleshooting process. The operational policies influence the troubleshooting procedures, the scope of gathered data, the reaction levels, the reboot behavior upon disruptive change, and so on. You can define these types of operational policies:

- **Fault Collection Policy:** Controls the life cycle of a fault in a Cisco UCS domain, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system)
- **Flow Control Policy:** Determines whether the uplink Ethernet ports in a Cisco UCS domain send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.
- **Maintenance Policy:** Determines how Cisco UCS Manager reacts when a change that requires a server reboot is made to a service profile that is associated with a server or to an updating service profile template that is bound to one or more service profiles
- **Scrub Policy:** Determines what happens to local data and to the BIOS settings on a server during the discovery process and when the server is disassociated from a service profile
- **Serial Over LAN Policy:** Sets the configuration for the serial over LAN (SoL) connection for all servers that are associated with service profiles that use the policy
- **Statistics Collection Policy:** Defines how frequently statistics are to be collected (collection interval) and how frequently the statistics are to be reported (reporting interval)
- **Statistics Threshold Policy:** Monitors statistics about certain aspects of the system and generates an event if the threshold is crossed

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

Cisco UCS Server Deployment Configuration

This topic explains the Cisco UCS B-Series server deployment configuration.



To provide a computing infrastructure that is not tied to physical devices, the Cisco UCS platform separates physical devices from their configurations. This abstraction provides a flexible environment where resources can be provisioned and migrated rapidly between physical devices.

Understanding the service profile concept is critical to understanding server management in Cisco UCS.

The service profile represents a logical view of a single server and does not require you to know exactly on which physical server it might be running. The profile object contains the server personality (identity, network information, and so on) and connectivity requirements. The profile can then be associated with a given physical server.

The concept of profiles is important to the concept of mobility—transferring the identity of a logical server transparently from one physical server to another—as well as to pooling concepts.

Even if you intend to manage the blade server as a traditional individual server, without taking advantage of mobility or pooling, you must create and manage a service profile for the server. While you could theoretically boot a server without a service profile, it would have no network or SAN connectivity.

https://t.me/learningnets

Service Profiles that Inherit Server Identity

- Simplest to use and create
- Uses the default values in the server
- Tied to a specific server and cannot be moved or migrated to another server
- No need to create pools or configuration policies
- Inherits and applies the identity and configuration information that is present at the time of association

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

This hardware-based service profile is the simplest to use and create. This profile uses the default values in the server and mimics the management of a rack-mounted server. It is tied to a specific server and cannot be moved or migrated to another server.

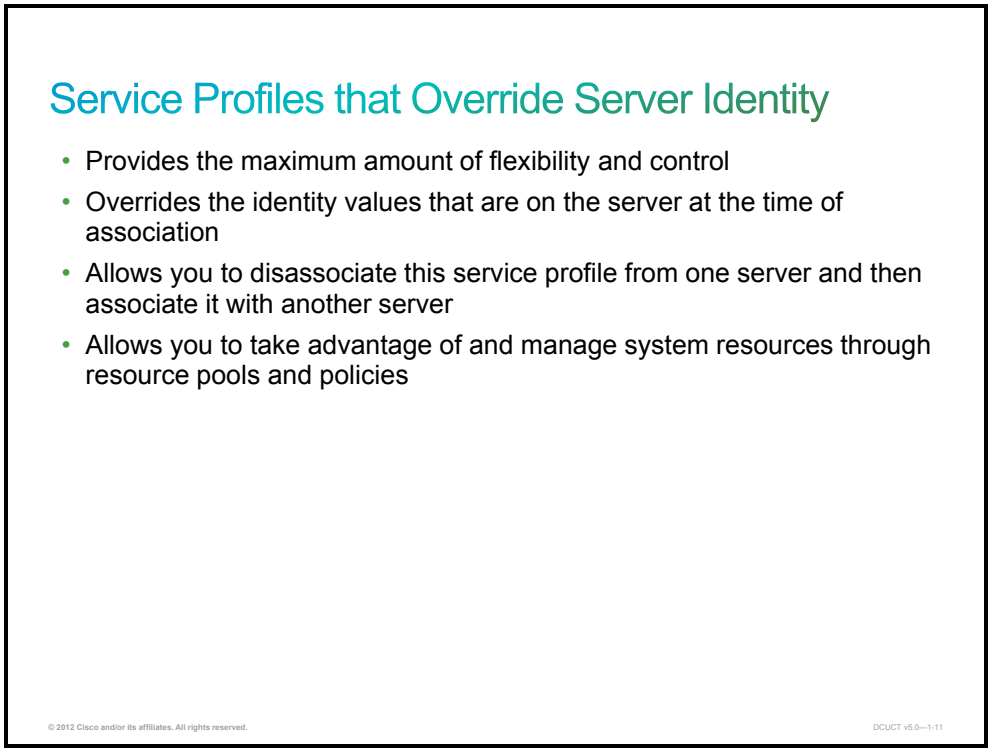
You do not need to create pools or configuration policies to use this service profile.

This service profile inherits and applies the identity and configuration information that is present at the time of association, such as the following:

- MAC addresses for the two network interface cards (NICs)
- For a converged network adapter or a virtual interface card, the world wide name (WWN) addresses for the two host bus adapters (HBAs)
- BIOS versions
- Server universally unique identifier (UUID)

It is important to know that the server identity and configuration information that is inherited through this service profile may not be the values that were burned into the server hardware at time of manufacture if those values were changed before this profile was associated with the server.

https://t.me/learningnets



This type of service profile provides the maximum amount of flexibility and control. This profile allows you to override the identity values that are on the server at the time of association and use the resource pools and policies in Cisco UCS Manager to automate some administration tasks.

You can disassociate this service profile from one server and then associate it with another server. This reassociation can be done either manually or through an automated server pool policy. The burned-in settings on the new server, such as UUID and MAC address, are overwritten with the configuration in the service profile. As a result, the change in server is transparent to your network. You do not need to reconfigure any component or application on your network to begin using the new server.

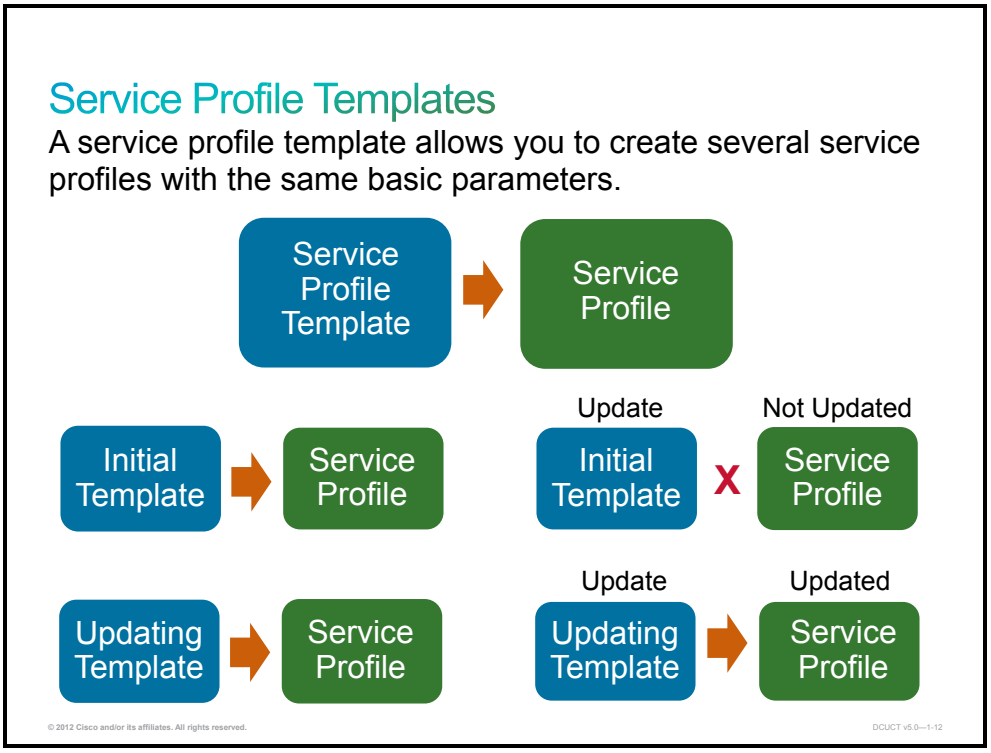
This profile allows you to take advantage of and manage system resources through resource pools and policies, such as the following:

- Virtualized identity information, including pools of MAC addresses, WWN addresses, and UUIDs
- Ethernet and Fibre Channel adapter profile policies
- Firmware package policies
- Operating system boot order policies

Unless the service profile contains power management policies, a server pool qualification policy, or another policy that requires a specific hardware configuration, the profile can be used for any type of server in the Cisco UCS domain.

You can associate these service profiles with either a rack-mount server or a blade server. The ability to migrate the service profile depends upon whether you choose to restrict migration of the service profile.

https://t.me/learningnets



With a service profile template, you can quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools.

If you need only one service profile with similar values to an existing service profile, you can clone a service profile in the Cisco UCS Manager GUI.

For example, if you need several service profiles with similar values to configure servers to host database software, you can create a service profile template, either manually or from an existing service profile. You then use the template to create the service profiles.

Cisco UCS supports the following types of service profile templates:

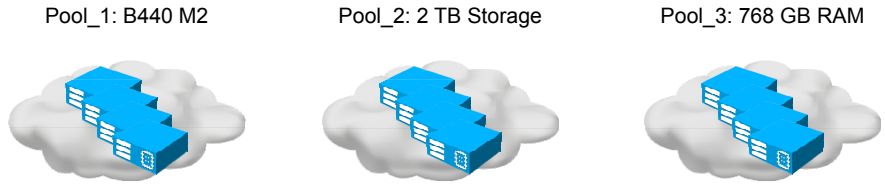
- **Initial template:** Service profiles that are created from an initial template inherit all the properties of the template. However, after you create the profile, it is no longer connected to the template. If you need to make changes to one or more profiles that were created from this template, you must change each profile individually.
- **Updating template:** Service profiles that are created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles that were created from the template.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Pools

- Set of servers with common characteristics, such as:
  - Server type
  - Amount of memory
  - Type of CPU
- Server assignment can be done in two ways:
  - Manual
  - Automated, based on server pool policies and server pool policy qualifications



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

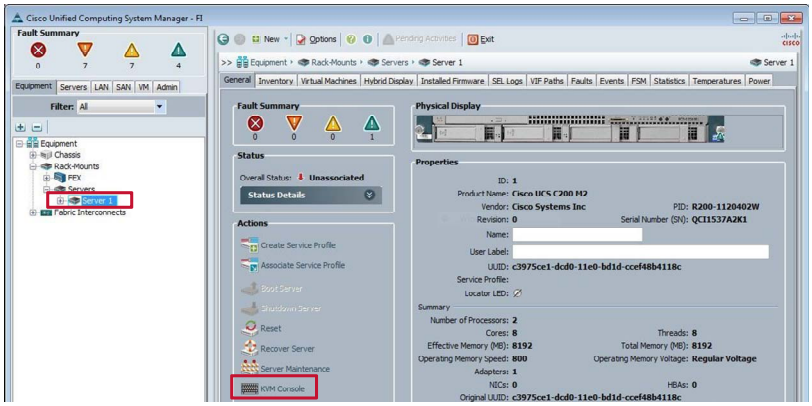
A server pool contains a set of servers. These servers typically share the same characteristics, like their location in the chassis or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If a system implements multitenancy through organizations, you can designate one or more server pools to be used by a specific organization. A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

https://t.me/learningnets

KVM and IP Address Requirements

- Servers require a management IP address assigned to either of the following:
  - Cisco IMC
  - Service profile associated with the server
- This IP address is used for external access that is terminated in Cisco IMC.



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

Each server in a Cisco UCS domain must have a management IP address assigned to its Cisco Integrated Management Controller (Cisco IMC) or to the service profile that is associated with the server. Cisco UCS Manager uses this IP address for external access that terminates in the Cisco IMC. This external access can be through one of the following:

- Keyboard, video, mouse (KVM) console
- SoL
- An IPMI tool

The management IP address that is used to access the Cisco IMC on a server can be one of the following:

- A static IP version 4 (IPv4) address that is assigned directly to the server.
- A static IPv4 address that is assigned to a service profile. You cannot configure a service profile template with a static IP address.
- An IP address drawn from the management IP address pool and assigned to a service profile or service profile template.

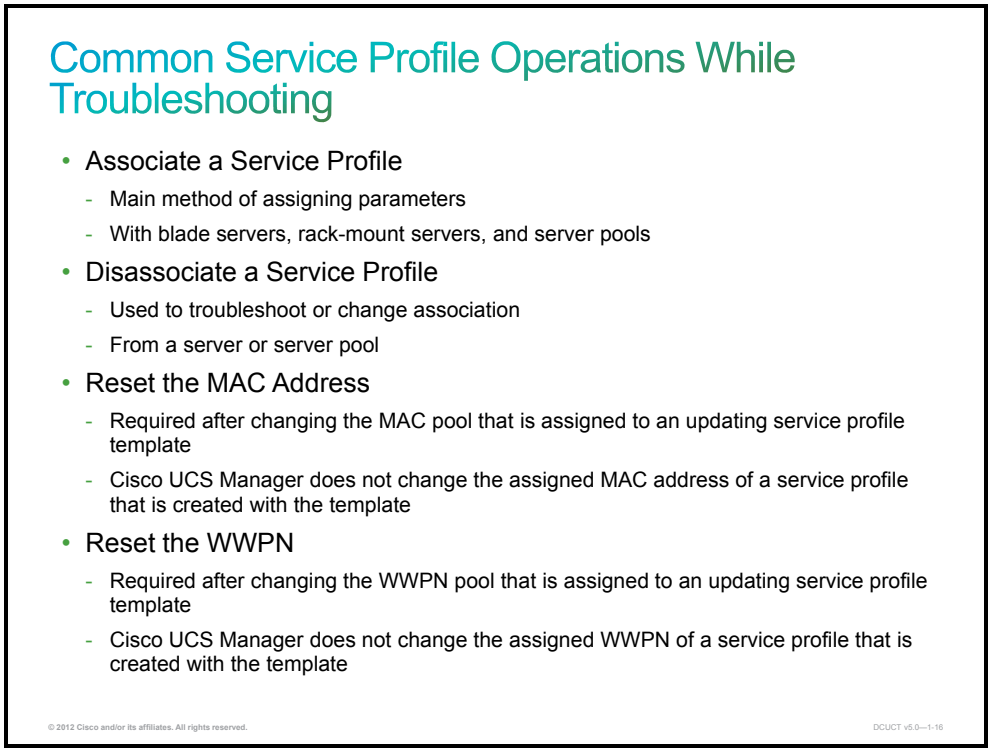
You can assign a management IP address to each Cisco IMC on the server and to the service profile that is associated with the server. If you do so, you must use different IP addresses for each of them.

A management IP address that is assigned to a service profile moves with the service profile. If a KVM or SoL session is active when you migrate the service profile to another server, Cisco UCS Manager terminates that session and does not restart it after the migration is completed. You configure this IP address when you create or modify a service profile.

https://t.me/learningnets

Troubleshoot Cisco UCS Server Deployment

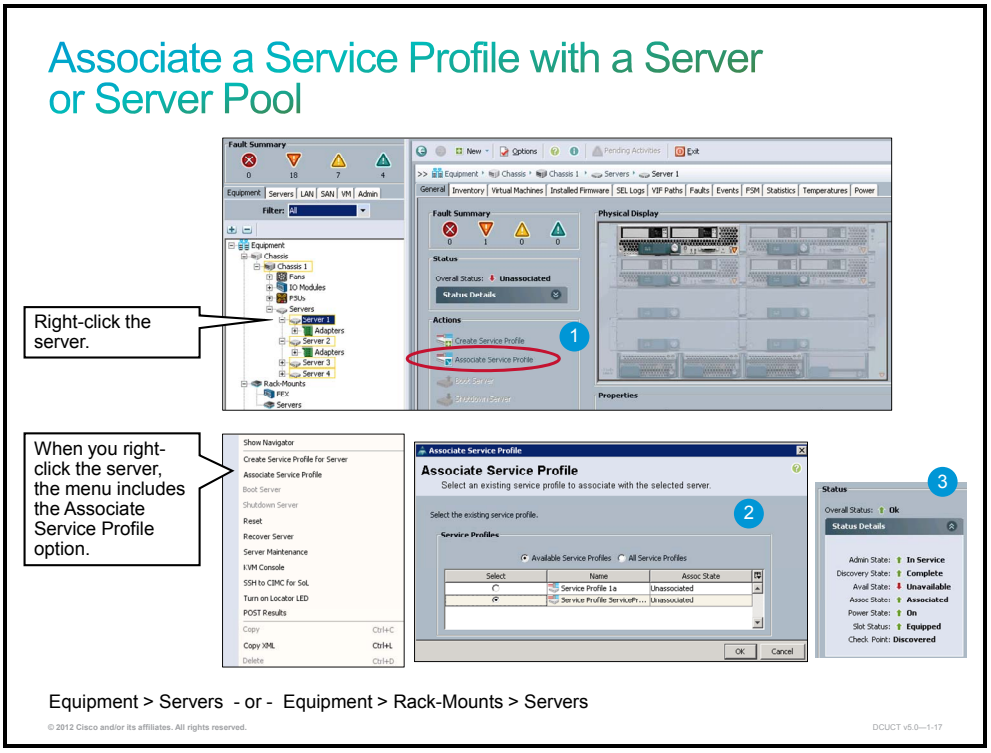
This topic describes how to troubleshoot the Cisco UCS B-Series service profile configuration.



There are several common service profile operations that you must perform when troubleshooting Cisco UCS deployment. These operations include the following:

- **Associating a Service Profile:** This is the main method of assigning parameters to blade servers, rack-mount servers, and server pools.
- **Disassociating a Service Profile:** This action is used to troubleshoot or change association from a server or server pool.
- **Resetting the MAC Address:** This action is required after changing the MAC pool that is assigned to an updating service profile template. Cisco UCS Manager does not change the assigned MAC address of a service profile that is created with the template.
- **Resetting the WWPN:** This operation is required after changing the world wide port name (WWPN) pool that is assigned to an updating service profile template. Cisco UCS Manager does not change the assigned WWPN of a service profile that is created with the template.

https://t.me/learningnets



You can associate a service profile with a server or a server pool using the Cisco UCS Manager GUI or the CLI. You must perform this operation if you did not associate the service profile with a blade server or server pool when you created it, or if you want to change the blade server or server pool with which a service profile is associated. The figure shows the procedure that is performed in the GUI. If you want to perform the procedure in the CLI, follow these steps:

Step 1 Enter organization mode for the specified organization. To enter root organization mode, enter / for the *org-name* argument.
UCS-A# **scope org** *org-name*

Step 2 Enter organization service profile mode for the specified service profile.

UCS-A /org # **scope service-profile** *profile-name*

Step 3 Associate the service profile with a single server or to the specified server pool with the specified server pool policy qualifications.
UCS-A /org/service-profile # **associate** {**server** chassis-id | slot-id | **server-pool** pool-name qualifier}

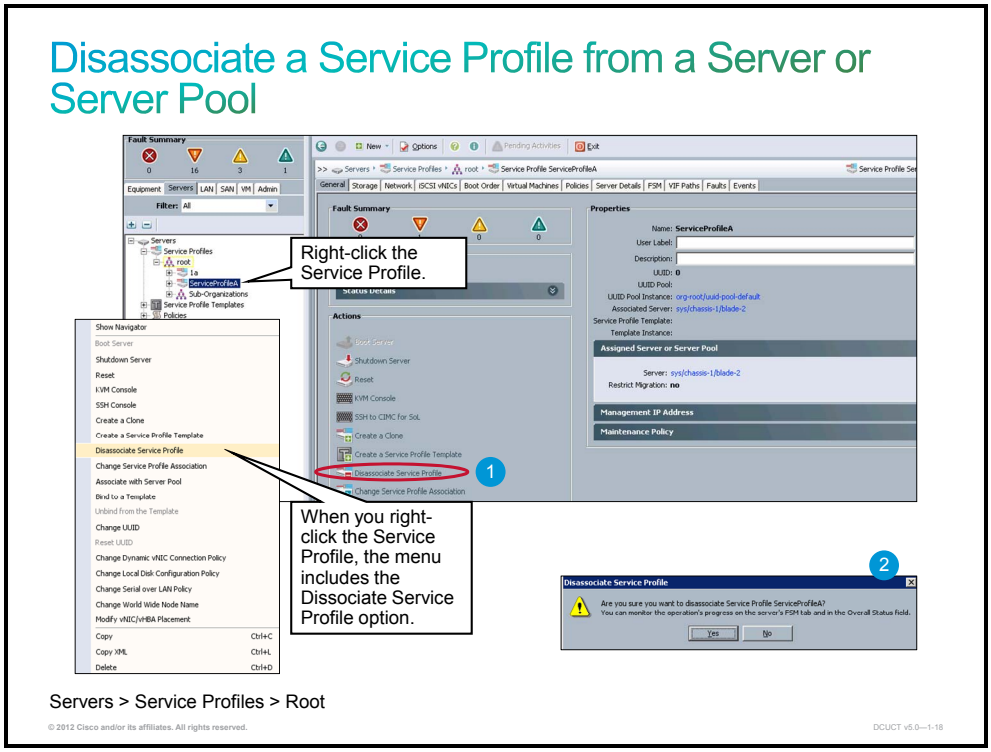
Step 4 Commit the transaction to the system configuration.
UCS-A /org/service-profile # commit-buffer

You can perform a similar procedure to associate a service profile with a rack server. In this case, choose **Equipment > Rack-Mounts > Servers**. The CLI procedure is shown here:

UCS-A# **scope org** *org-name*
UCS-A /org # **scope service-profile** *profile-name*
UCS-A /org/service-profile # **associate server** *serv-id*
UCS-A /org/service-profile # **commit-buffer**

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets



When you disassociate a service profile, Cisco UCS Manager attempts to shut down the operating system on the server. If the operating system does not shut down within a reasonable length of time, Cisco UCS Manager forces the server to shut down.

The figure illustrates the process of disassociating a service profile from a blade server, rack server, or server pool in the Cisco UCS Manager GUI. If you want to perform the procedure in the CLI, follow these steps:

Step 1 Enter organization mode for the specified organization. To enter root organization mode, enter / for the *org-name* argument.
UCS-A# **scope org** *org-name*

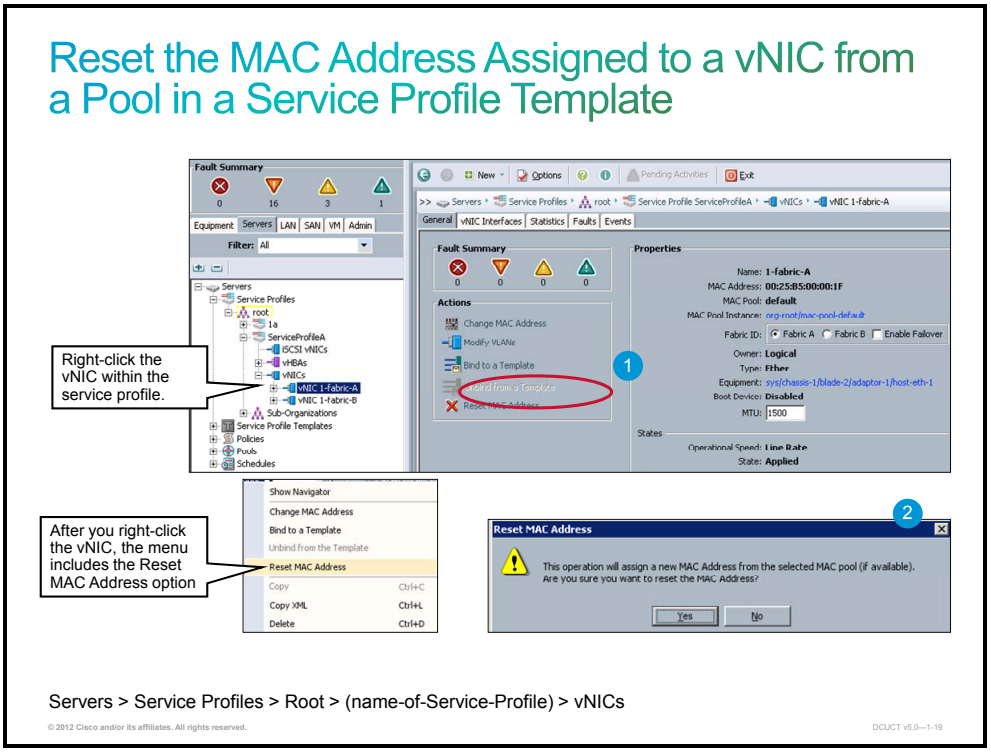
Step 2 Enter organization service profile mode for the specified service profile.

UCS-A /org # **scope service-profile** *profile-name*

Step 3 Disassociate the service profile from the specified server.
UCS-A /org/service-profile # **disassociate**

Step 4 Commit the transaction to the system configuration.
UCS-A /org/service-profile # **commit-buffer**

https://t.me/learningnets



If you change the MAC pool that is assigned to an updating service profile template, Cisco UCS Manager does not change the assigned MAC address of a service profile that was created with the template. If you want Cisco UCS Manager to assign a MAC address from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the MAC address. You can only reset the MAC address that is assigned to a service profile and its associated server under these circumstances:

- The service profile was created from an updating service profile template and includes a MAC address that was assigned from a MAC pool.
- The MAC pool name is specified in the service profile. For example, the pool name is not empty.
- The MAC address value is not 0 and is therefore not derived from the server hardware.

The figure illustrates the process of resetting the MAC addresses in the Cisco UCS Manager GUI. Follow these steps to perform the same process in the CLI:

Step 1 Enter organization mode for the specified organization. To enter root organization mode, enter / for the *org-name* argument.
UCS-A# **scope org** *org-name*

Step 2 Enter command mode for the service profile that requires the MAC address of the associated server to be reset to a different MAC address.

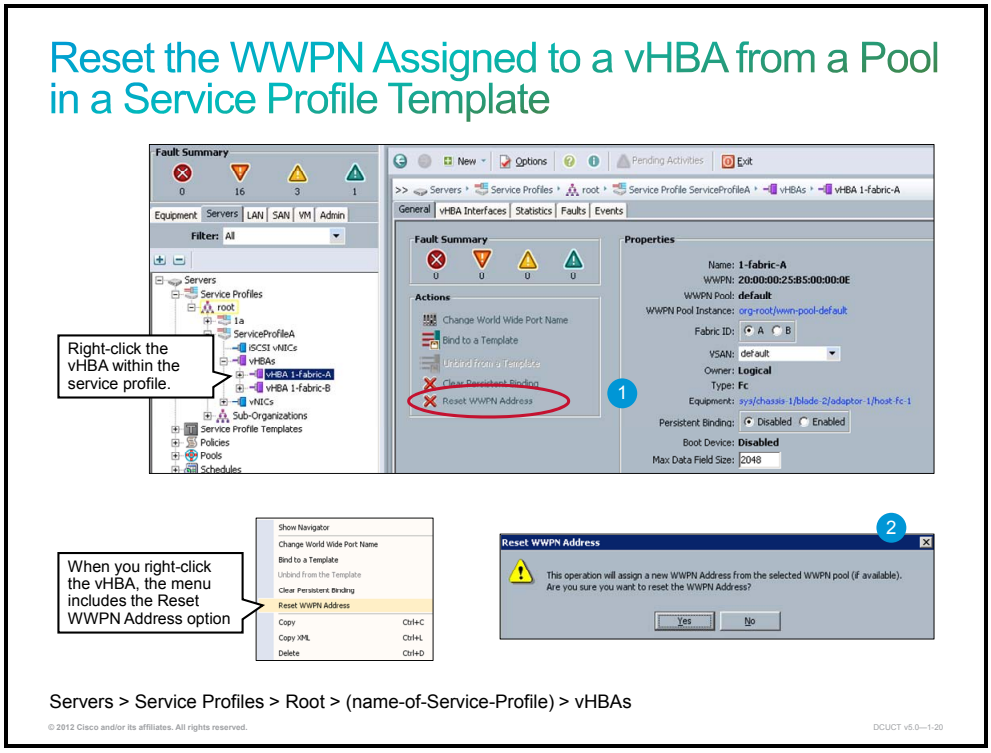
UCS-A /org # **scope service-profile** *profile-name*

Step 3 Enter command mode for the vNIC for which you want to reset the MAC address.
UCS-A /org/service-profile # **scope vnic** *vnic-name*

Step 4 Specify that the vNIC will obtain a MAC address dynamically from a pool.
UCS-A /org/service-profile/vnic # **set identity dynamic-mac derived**

Step 5 Commit the transaction to the system configuration.
UCS-A /org/service-profile # **commit-buffer**

https://t.me/learningnets



If you change the WWPN pool that is assigned to an updating service profile template, Cisco UCS Manager does not change the WWPN that is assigned to a service profile that was created with the template. If you want Cisco UCS Manager to assign a WWPN from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the WWPN. You can only reset the assigned WWPN of a service profile and its associated server under these circumstances:

- The service profile was created from an updating service profile template and includes a WWPN that was assigned from a WWPN pool.
- The WWPN pool name is specified in the service profile. For example, the pool name is not empty.
- The WWPN value is not 0 and is therefore not derived from the server hardware.

The figure illustrates the process of resetting the WWPN in the Cisco UCS Manager GUI. Follow these steps to perform the same process in the CLI:

Step 1 Enter organization mode for the specified organization. To enter root organization mode, enter / for the *org-name* argument.
UCS-A# **scope org** *org-name*

Step 2 Enter organization service profile mode for the vHBA for which you want to reset the WWPN.

UCS-A /org # **scope service-profile** *profile-name*

Step 3 Enter command mode for the vHBA for which you want to reset the WWPN.
UCS-A /org/service-profile # **scope vhba** *vhba-name*

Step 4 Specify that the vHBA will obtain a WWPN dynamically from a pool.
UCS-A /org/service-profile/vnic # **set identity dynamic-wwpn derived**

Step 5 Commit the transaction to the system configuration.
UCS-A /org/service-profile # **commit-buffer**

https://t.me/learningnets

Verifying Service Profile Association Using FSM

```
ucsm1# show service-profile association
Service Profile Name Association    Server Pool
-------------------- -------------- ------ -----------
db05           Associated     2/3
vcb01          Unassociated
!
ucsm1# show service-profile identity name vcb01
Service Profile Name: vcb01
UUID Suffix Pool: UUID_Pool
Dynamic UUID: 11000000-0000-0000-2100-00000000148f
<output omitted>
!
ucsm1# show server association
Server  Association  Service Profile
------- ------------ ---------------
1/1     None
1/3     None
!
ucsm1# scope service-profile dynamic-uuid 11000000-0000-0000-2100-00000000148f
ucsm1 /org/service-profile # associate server 1/3
ucsm1 /org/service-profile* # commit-buffer

ucsm1 /org/service-profile # show fsm status
Service Profile Name: vcb01
    FSM 1:
        <output omitted>
        Progress (%): 45
        Current Task: Configure adapter for pre-boot environment on server 1/3(FSM-
TAGE:sam:dme: ComputeBladeAssociate:NicConfigPnuOS)
```

1. View service profile associations. Profile vcb01 is not associated.
2. View service profile attributes, including UUID.
3. View server associations. Server 1/3 is not associated.
4. Associate service profile with server.
5. FSM status displays the association progress, which is rising and reaches 100%.

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

The finite state machine (FSM) can be used to verify the service profile association with a given blade server. The procedure consists of five steps:

Step 1 Verify the current service profile associations using the **show service-profile association** command. In this example, the service profile vcb01 has not been associated to any servers.

Step 2 View the attributes of the service profiles using the **show service-profile identity name** command. The output includes the UUID of the profile, which you can use to assign to a server.

Step 3 Display the server associations using the **show server association** command. In this case, blade 1/3 is not associated with any service profile.

Step 4 Attach the service profile to the server using the **scope**, **associate-server**, and **commit-buffer** commands.

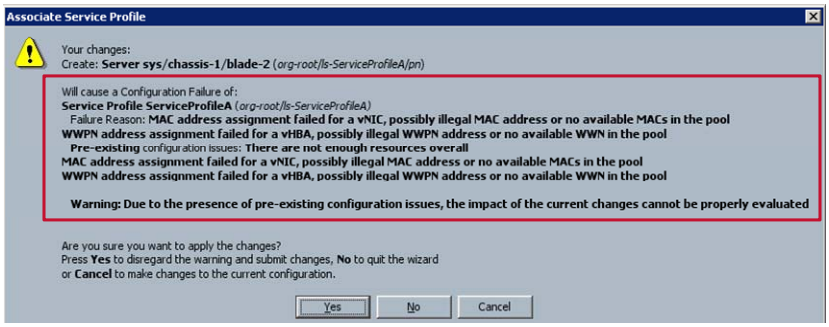
Step 5 Monitor the association progress using the **show fsm status** command. The progress that is displayed should be continuously rising until it reaches 100 percent.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Issue: Service Profile Association Failure

- You encounter this symptom:
  - Attempt to assign service profile to a server produces a warning
- These issues have been reported:
  - MAC address assignment failed
  - WWPN address assignment failed
  - Not enough resources overall



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

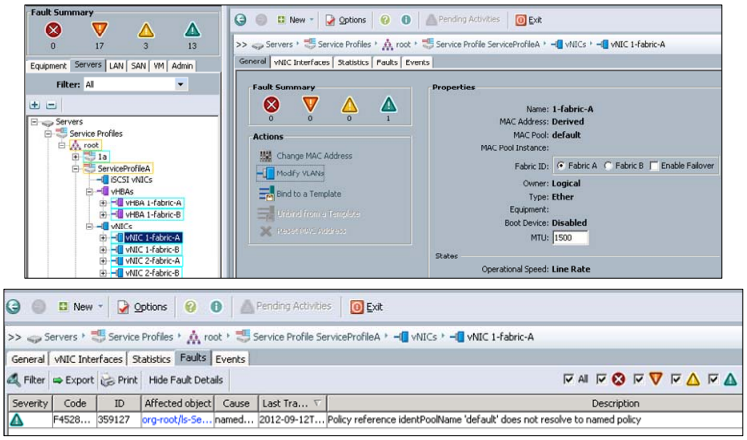
This scenario guides you through the process of troubleshooting a situation in which you attempt to assign a service profile to a server and you get a warning, as shown in this figure. You are warned about these issues:

- Failure of MAC address assignment
- Failure of WWPN address assignment
- Insufficient amount of resources

https://t.me/learningnets

Data Gathering 1: vNIC MAC Addresses

- Examine the MAC address provisioning.
- Fault reports “Policy reference identPoolName ‘default’ does not resolve to named policy.”



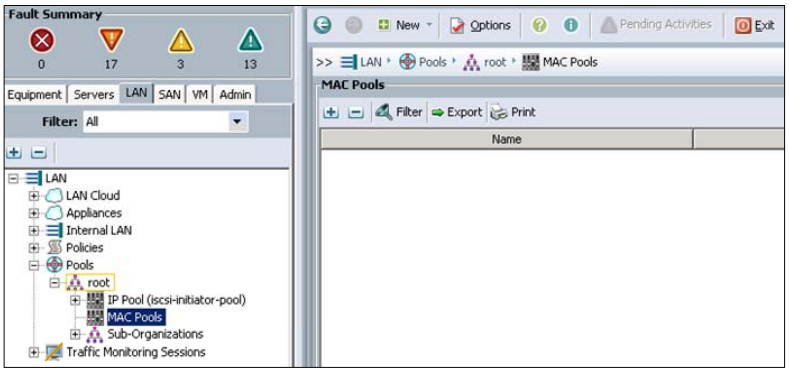
Servers > Service Profiles > Root > ServiceProfileA > vNICs

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

You start to gather data about the problem. Because MAC address assignment was reported as a problem, you check how the MAC addresses are provisioned on the vNICs. The Faults tab offers an explanation of the problem. The fault reads “Policy reference identPoolName ‘default’ does not resolve to named policy.” This message makes you suspect that the configuration of the MAC address pools is incorrect.

Data Gathering 2: vNIC MAC Address Pools

- Check the MAC address pools.
- The problem has been isolated:
  - Address pool missing
  - Service profile does not find a source for obtaining MAC addresses



LAN > Pools > Root > MAC Pools

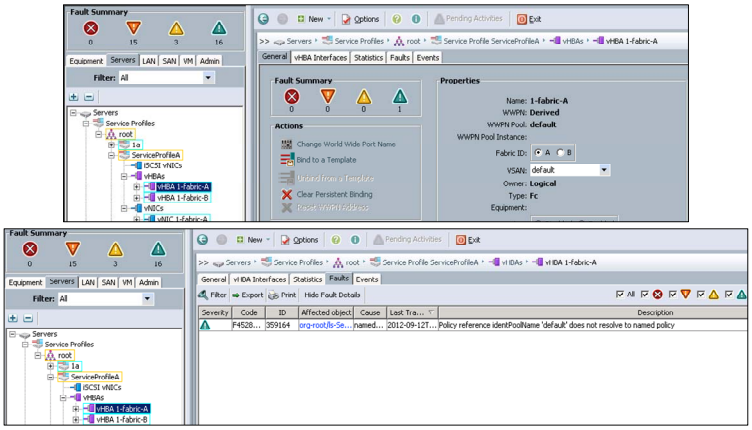
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, you verify the MAC address pool configuration. When you choose LAN > Pools > Root > MAC Pools, you discover that now MAC addresses are configured. This allows you to isolate the problem of the MAC address assignment.

https://t.me/learningnets

Data Gathering 3: vHBA WWPNs

- Investigate the WWPN provisioning.
- Fault reports “Policy reference identPoolName ‘default’ does not resolve to named policy.”



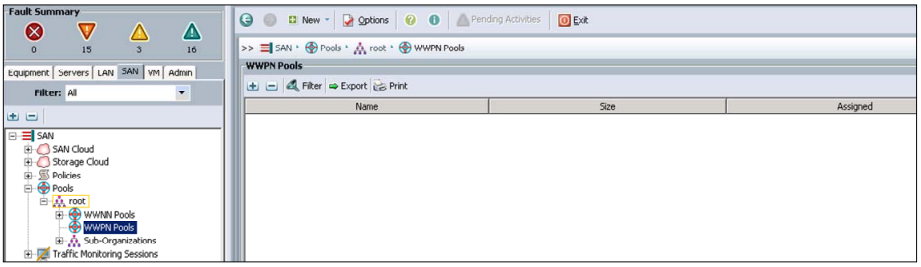
Servers > Service Profiles > Root > ServiceProfileA > vHBAs

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

Now you need to examine the assignment of the WWPNs to the vHBAs. The Faults tab offers an explanation of the problem. The fault reads “Policy reference identPoolName ‘default’ does not resolve to named policy.” This message makes you suspect that the configuration of the WWPN pools is incorrect.

Data Gathering 4: WWPN Pools

- Check the WWPN pools.
- The problem has been isolated:
  - WWPN pool missing
  - Service profile does not find a source for obtaining WWPNs

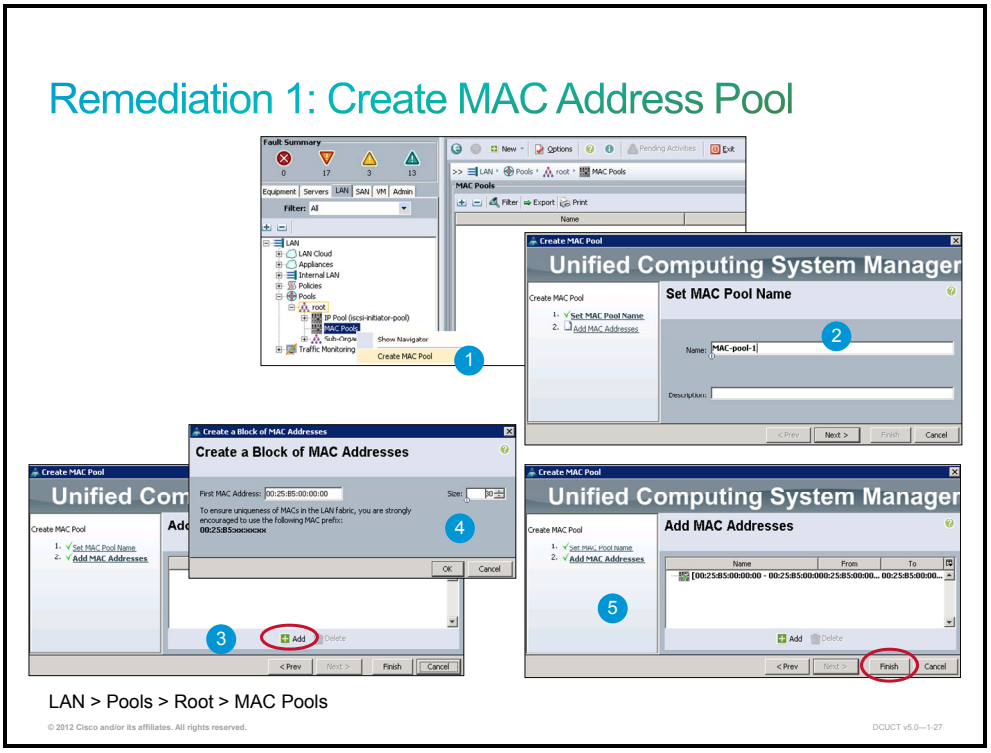


SAN > Pools > Root > WWPN Pools

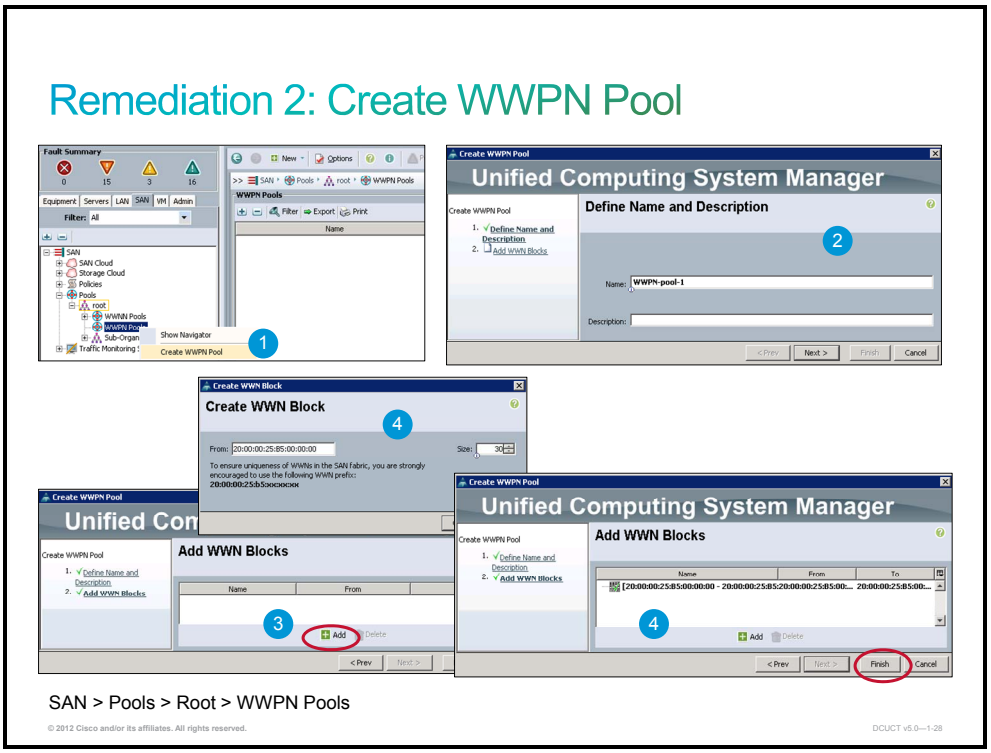
© 2012 Cisco and/or its affiliates. All rights reserved.

When you choose SAN > Pools > Root > WWPN Pools, you see that no configured WWPN pools exist. Now you can isolate the problem of WWPN assignment—there are no WWPN pools to obtain the WWPNs from.

https://t.me/learningnets



You are ready to start the remediation phase. First, you create a MAC address pool.

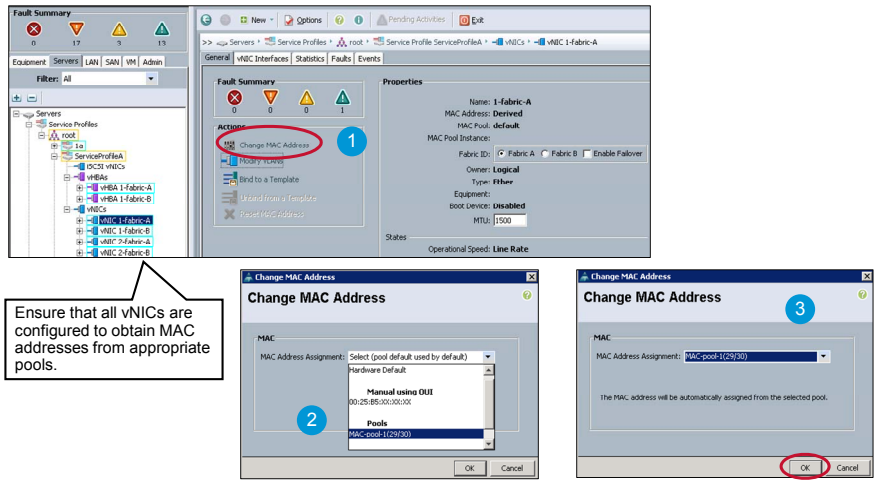


Next, you need to define a WWPN pool.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Remediation 3: Change MAC Address in Service Profile



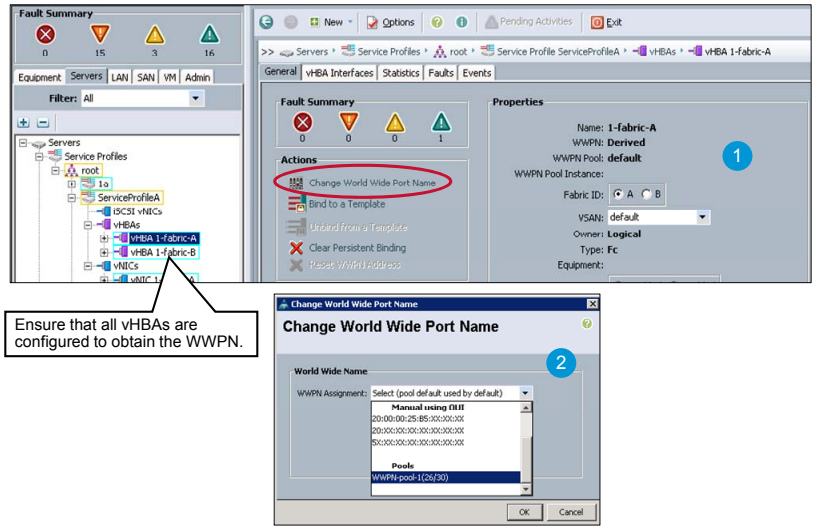
Servers > Service Profiles > Root > ServiceProfileA > vNICs

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

Then you change the MAC addresses of the vNICs in the service profile. Click the **Change MAC address** link, select the MAC address pool from which to obtain the addresses, and confirm the selection.

This procedure must be repeated for all vNICs.

Remediation 4: Change WWPN in Service Profile



Servers > Service Profiles > Root > ServiceProfileA > vHBAs

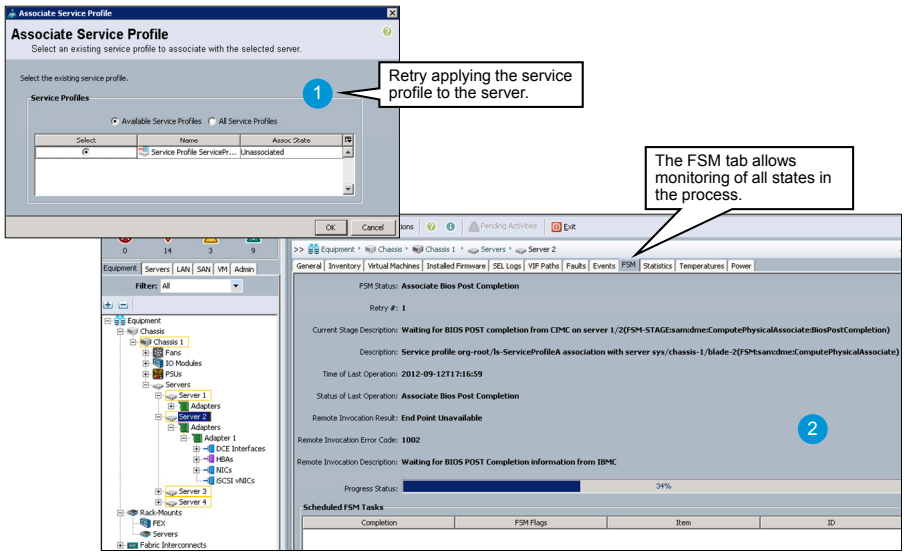
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, you need to change the WWPN of the vHBAs in the service profile.

Click the **Change World Wide Port name** link, select the WWPN pool from which to obtain the WWPNs, and confirm the selection. This procedure must be repeated for all vHBAs.

https://t.me/learningnets

Solution Verification



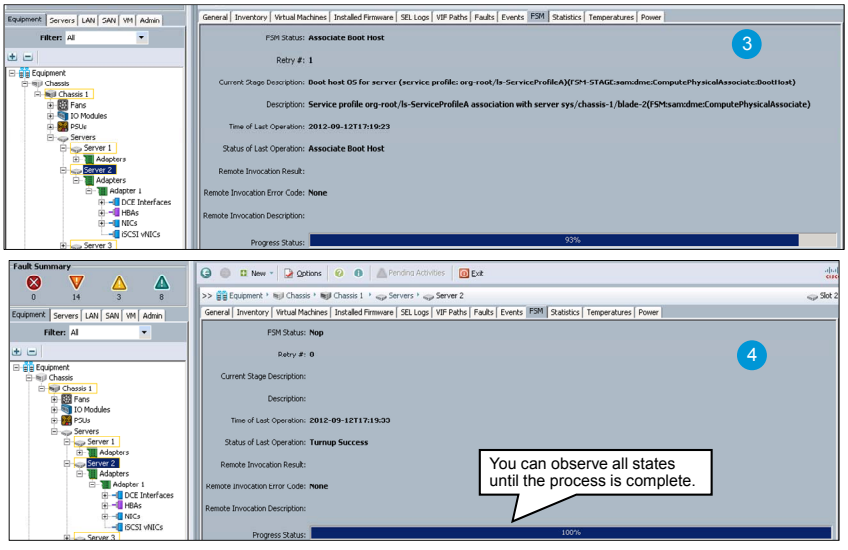
Servers > Service Profiles > Root > ServiceProfileA

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

DCUCT v5.0—1-31

Finally, you verify the effectiveness of the solution and attempt to associate the service profile with the server again. You can use the FSM tab to monitor the progress of the association process.

Solution Verification (Cont.)



Servers > Service Profiles > Root > ServiceProfileA

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

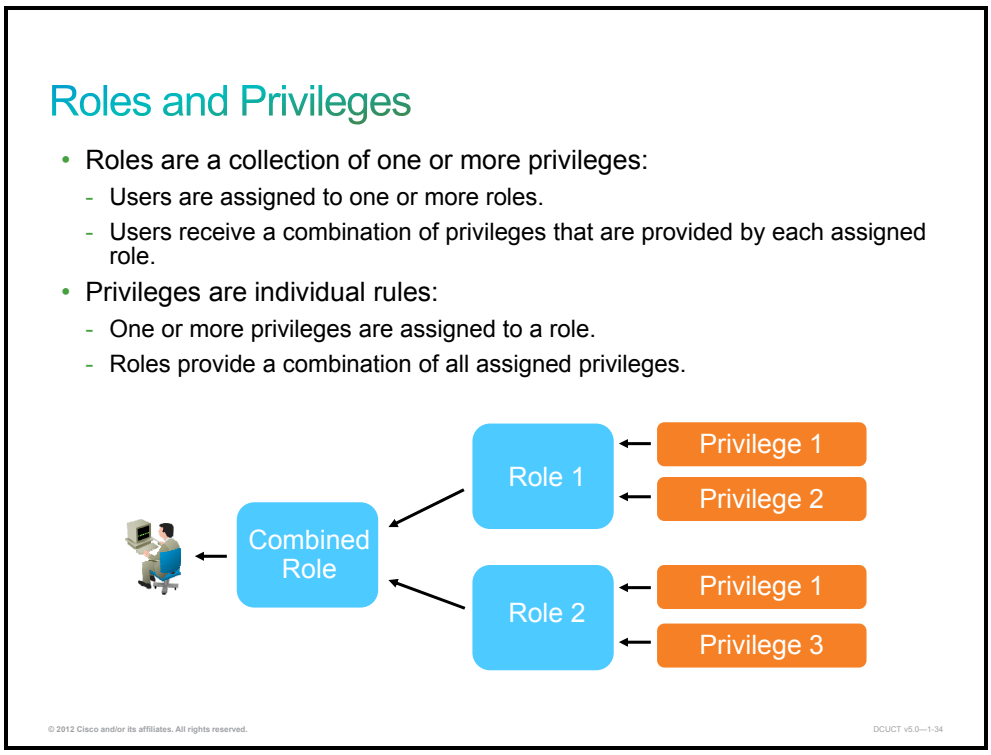
DCUCT v5.0—1-32

The FSM monitoring takes you through all the states of the state machine, until the process is completed and 100 percent is reached. This figure does not show all the states of the FSM.

https://t.me/learningnets

Troubleshoot Cisco UCS Management Configuration

This topic explains Cisco UCS B-Series management configuration.



Role-based access control (RBAC) allows users to be granted granular permission sets, based on their responsibilities. A series of roles is defined by a superuser or system administrator and then assigned to other users. RBAC provides a granular access control.

A potential issue that is related to RBAC results from assigning rights that are too wide or too narrow for a given administrator. A profile that is too permissive gives them the potential to perform undesired operations and exploit their role. Privileges that are too restrictive limit the scope of activities. Cisco UCS automatically performs an audit log.

To effectively capture audit logs for archival purposes, you must script a retrieval process:

```
switch-A# scope security
switch-A /security # show audit-logs
```

This logging, if performed in a reliable fashion, allows you to detect any inappropriate administrator behavior, and may even prevent any wrongdoing.

Privileges are the building blocks of roles. Each role is defined with one or more privileges. Users receive rights or privileges based on assigned roles. A user may be assigned one or more roles. When users are assigned more than one role, they receive a combination of the privileges that are defined in each role. This combination of privileges means that they will have all the privileges that are defined in each assigned role. This fact is important to note because vendor RBAC schemes differ and other products or systems may operate in another fashion.

https://t.me/learningnets

Here are two examples of privileges:

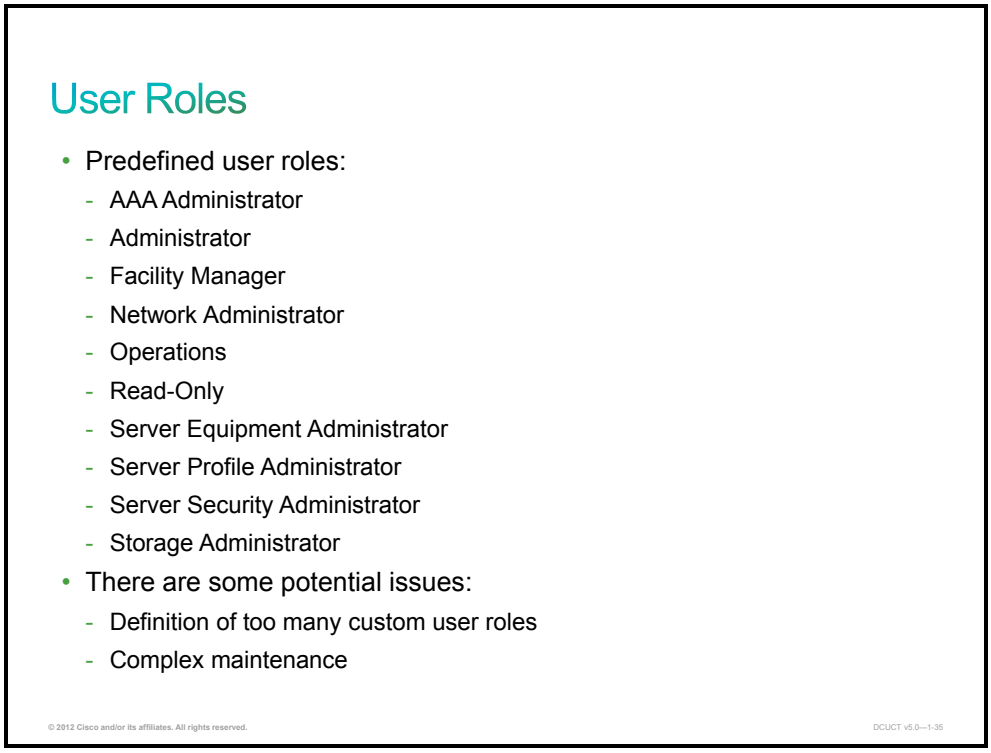
- **Admin:** Can do everything on the system (across all organizations), such as a superuser
- **AAA:** Authentication, authorization, and accounting (AAA), including administration of the RBAC feature itself

Note Neither of these privileges is organization-specific.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

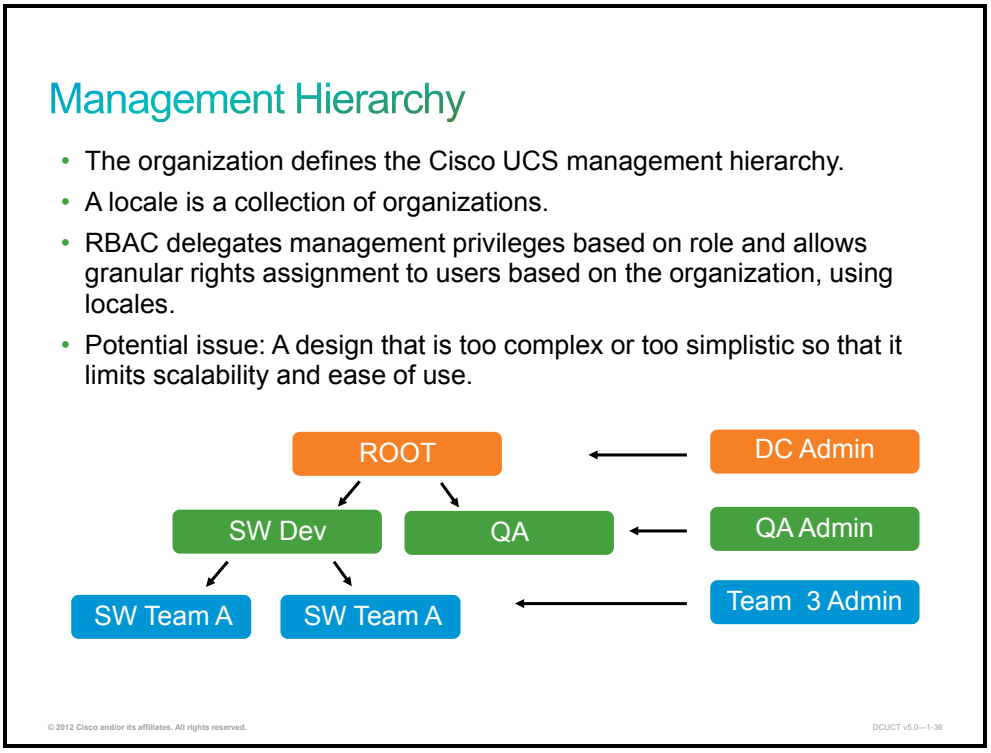


Cisco UCS contains a set of default user roles:

- **AAA Administrator:** Read and write access to users, roles, and AAA configuration. Read access to the rest of the system.
- **Administrator:** Read and write access to the entire system. The "admin" account is assigned this role by default and it cannot be changed.
- **Facility Manager:** Read and write access to power management operations through the power-mgmt privilege. Read access to the rest of the system.
- **Network Administrator:** Read and write access to the Fabric Interconnect infrastructure and network security operations. Read access to the rest of the system.
- **Operations:** Read and write access to systems logs, including the syslog servers, and faults. Read access to the rest of the system.
- **Read-Only:** Read-only access to the system configuration, with no privileges to modify the system state.
- **Server Equipment Administrator:** Read and write access to physical server-related operations. Read access to the rest of the system.
- **Server Profile Administrator:** Read and write access to logical server-related operations. Read access to the rest of the system.
- **Server Security Administrator:** Read and write access to server security-related operations. Read access to the rest of the system.
- **Storage Administrator:** Read and write access to storage operations. Read access to the rest of the system.

A common issue in enterprise environments is the creation of too many user roles. Such a configuration may limit visibility and unnecessarily complicate maintenance. Using the predefined user roles is recommended in most environments.

https://t.me/learningnets



Organization

The organizational structure defines a management hierarchy within Cisco UCS. This hierarchy is used to assist in the management of the resources and logical objects that are used within the system.

Locale

Locale defines the organizations (domains) that a user is allowed to access. A user can be assigned one or more locales. Each locale defines one or more organizations (domains) that the user is allowed to access, and access is limited to the organizations that are specified in the locale.

An exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations.

Role-Based Access Control

RBAC delegates rights to users based on the organization in which the users exist. The RBAC feature allows for fine-grained privilege assignment and restricts user privileges to specific organizations.

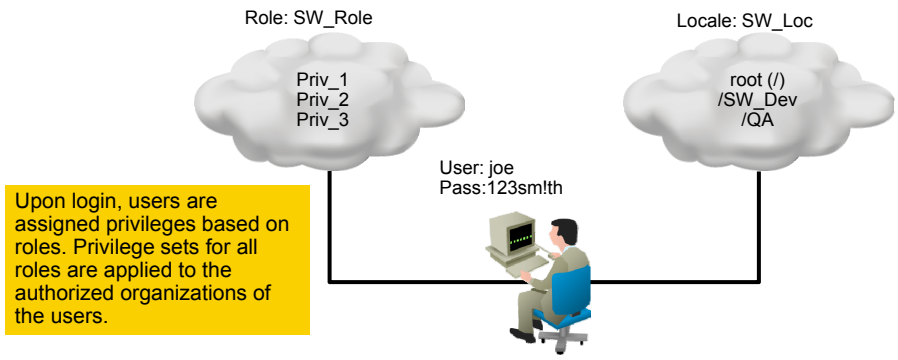
RBAC and organizations are complementary and not dependent on each another. By themselves, organizations provide a logical management hierarchy that allows granular resource assignment. RBAC (without defined organizations) places all defined roles at the default root level to provide role-based resource control to Cisco UCS in its entirety.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

RBAC, TACACS, and RADIUS

- RBAC can be combined with external user databases.
- User and administrator accounts can be stored on external repositories.
- Potential issues can result from communication problems.



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

A role is a set of privileges. There are several predefined roles, and custom roles can be created with user-defined privileges.

Note	A user in two different organizations cannot have different privileges in those two organizations. All privileges are cumulative and applied in combination to all the organizations in the specified locales of the users.

Some privileges are not organization-related. These privileges are applied regardless of the assigned locales of the user.

RBAC can be combined with external user databases. This approach is very common in many enterprises. This method allows you to store the user and administrator accounts on external repositories that act as central databases for multiple systems. Potential issues, however, can result from communication problems between the network devices and the external servers.

Cisco UCS supports RADIUS, TACACS+, and Lightweight Directory Access Protocol (LDAP) for centralized RBAC authentication. These are common authentication systems in current data centers. Using centralized authentication for RBAC requires that the device is configured to pass login requests to a central server or server group. These credentials are checked against a user database on the authentication server and permissions are granted based on matches.

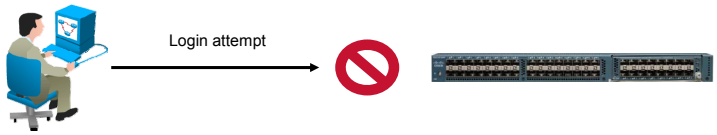
These are best practices for implementing RADIUS and TACACS+ for Cisco UCS products:

- Configure at least one AAA server that is reachable over IP.
- Configure a local AAA policy that can be used by default if no AAA servers are reachable.
- Use AAA server monitoring to automatically detect and remove nonresponsive AAA servers from a server group.
- Mandate complex alphanumeric login passwords. If an all-numeric username exists on an AAA server and is entered during login, the user is not logged in.
- Use passwords of at least eight characters.

https://t.me/learningnets

Issue: Authentication Failure 1

- You encounter this symptom:
  - Administrator fails to log on to the system.
- These issues were reported:
  - Administrator was able to log on earlier.
  - A similar problem was experienced before but, after a while, it disappeared.



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

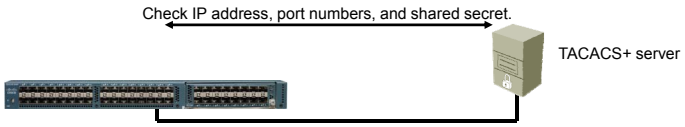
In this troubleshooting scenario, an administrator fails to log in to the system. Authentication failures can have various possible causes. You learn that, in this particular case, the administrator could log in before and that a similar problem was previously experienced but it disappeared after a while.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Data Gathering

- Examination of the AAA configuration shows the following:
  - The TACACS+ server is used as the external authentication source.
  - The AAA configuration is correct on both sides (IP addresses, port numbers, and shared secrets).
  - You cannot ping the TACACS+ server.
- There are two possible causes:
  - There is a connectivity problem to the TACACS+ host.
  - Firewall rules in the path block TACACS+.



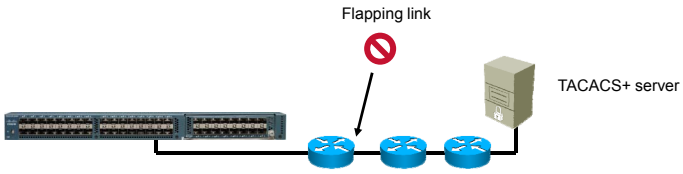
© 2012 Cisco and/or its affiliates. All rights reserved.

You begin gathering additional data about the problem. In this scenario, the administrator authentication is performed on a TACACS+ server. You verify that the AAA communication settings, such as IP addresses, port numbers, and shared secrets are configured correctly. This confirms the statement of the administrator that the authentication worked before. You cannot, however, ping the TACACS+ server from the Cisco UCS system. Your suspicions include connectivity problems or firewall rules that are too restrictive (this could be a result of an administrative change of firewall configuration like blocking TCP port 49) in the path to the AAA server.

https://t.me/learningnets

Problem Isolation

- After approximately 30 seconds, **ping** worked again.
- The firewall configuration was ruled out as a reason for the problem.
- Closer observation of the routing tables and interface statistics reveal the following:
  - A flapping link in the path between Cisco UCS and TACACS+ server



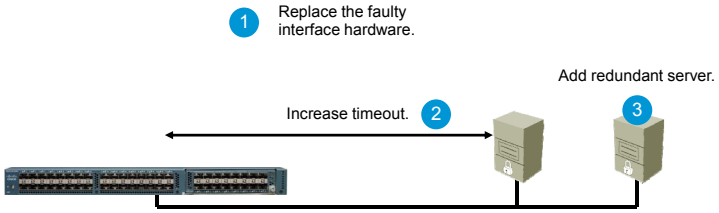
© 2012 Cisco and/or its affiliates. All rights reserved.

After approximately 30 seconds, ping started working. You check the network topology and component settings, and decide that firewall rules could not have caused the problem. A closer examination of the routing tables and interface statistics on the routers in the path between Cisco UCS and the TACACS+ server reveal a flapping link.

https://t.me/learningnets

Remediation

- Replace the hardware on the flapping link.
- Take these proactive measures:
  - Set the timeout to a higher value. This can help bridge transient network connectivity problems.
  - Deploy a redundant server to be used as a backup in case of path or server failure.



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

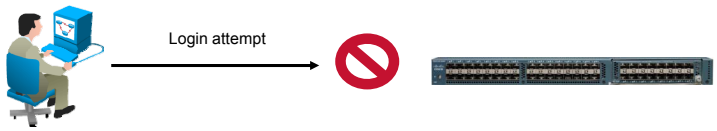
To remediate the problem, you replace the flapping link. In this particular scenario, you want to take some proactive measures to prevent similar problems from happening in the future, if this or another link should flap.

One proactive measure it to increase the server connection timeout to a higher value. More importantly, you decide to add a redundant AAA server that will take over when the primary server fails or becomes unreachable. The latter action reflects the best practice recommendations when deploying external AAA servers.

https://t.me/learningnets

Issue: Authentication Failure 2

- You encounter this symptom:
  - Administrator fails to log on to the system.
- These issues were reported:
  - Administrator was able to log on earlier.
  - The fault management system reports that one of the RADIUS servers is down.



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

This troubleshooting scenario is also focused on an authentication failure. In this case too, the administrator was able to log in to the system before, but cannot now log in.

In this situation, however, the authentication failure coincides with the failure of one of the RADIUS servers. Theoretically, this should not cause a problem, because the network has a pair of redundant RADIUS servers.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Data Gathering

- Examination of the AAA configuration shows the following:
  - Redundant RADIUS servers are used as the external authentication source.
  - The primary RADIUS server is down.
- There are three possible causes:
  - The failover to the secondary server did not work.
  - The connectivity to the secondary server failed.
  - RADIUS authentication port UDP 1812 is blocked in the path to the secondary server.

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

In the data gathering phase, you learn that the primary RADIUS is down. Cisco UCS and other network components are configured to fail over to the secondary RADIUS server when the primary one becomes unavailable. The network devices do not receive any responses from the primary host and attempt communication with the secondary one.

You examine the AAA communication parameters on the secondary RADIUS server, such as port numbers and shared secret, and compare them to the settings on the Cisco UCS. They match, so you rule out incorrect configuration as the reason for the failure.

You identify three potential causes of this problem:

- Failover to the secondary server does not work due to a bug in the AAA client code. You check the release notes and other product documentation but do not find any confirmation.
- Connectivity to the secondary server failed. You verify this assumption using a series of pings and the connectivity between Cisco UCS and the secondary RADIUS is faultless.
- RADIUS authentication port UDP 1812 is blocked in the path to the secondary server. You examine the path and do not find any faulty firewall rules.

https://t.me/learningnets

Problem Isolation

- Network connectivity verification on the backup RADIUS server reveals the following:
  - AAA communication parameters are configured correctly.
  - There is only one-way connectivity between the primary and secondary server networks:
    - Packets from the secondary server reach the primary server default gateway.
    - Packets from the primary server subnet do not reach the secondary server.
- User database verification on the backup RADIUS server shows the following:
  - Some administrator accounts are missing.
- The problem has been found:
  - Database replication failed from the primary to secondary server long before the primary RADIUS server failed.

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

Then you proceed to verify the connectivity between the RADIUS server subnets. You cannot verify the connectivity directly between the servers because the primary server is down, but you can check the communication between the primary server default gateway and the secondary server. You use extended **ping** to send packets from the subnet of the primary server.

You experience a unidirectional connectivity situation in which the traffic from the primary server subnet fails to reach the secondary server, and the traffic from the secondary to the primary server is delivered properly. You examine the routing policies on the routers in the path and discover an update filter that prevents the secondary server subnet from being advertised to the primary server default gateway.

Next, you check the user database on the secondary server and find that some accounts are missing. This indicates that the up-to-date information was not being replicated from the primary to the secondary server.

https://t.me/learningnets

Remediation

- Remove the update filter that prevented the secondary server subnet from being advertised into the network toward the primary server.
- Repair the primary RADIUS server.
- Verify that the secondary server database is being updated.

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

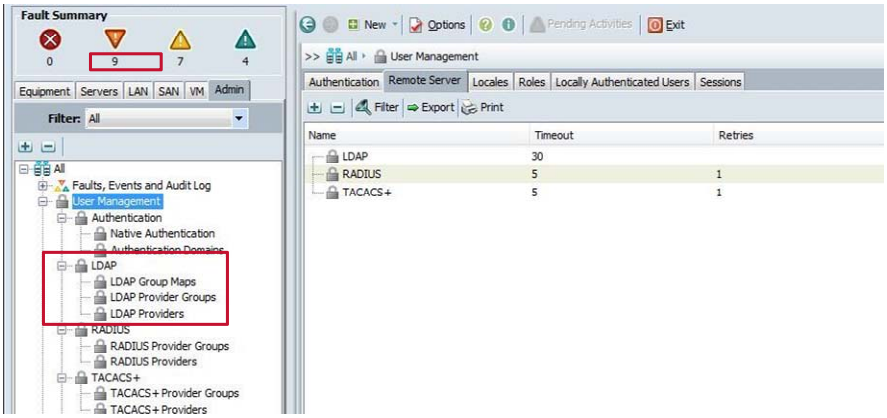
To remediate the problem, you remove the update filter that prevented an appropriate exchange of routing information. At this point, you verify that the communication between the primary server subnet and the secondary server is working bidirectionally.

Next, you repair the primary RADIUS server and restore its current configuration from a backup. When the restore operation is complete, the database is automatically replicated to the secondary RADIUS server and you verify that new user accounts have been added to it.

https://t.me/learningnets

Integration with LDAP

- LDAP, and specifically Active Directory, is the most common user database in enterprise environments.
- Authentication problems result from incorrect settings or connectivity failure.



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

Cisco UCS can be configured to authenticate user logins remotely using LDAP and various remote authentication providers, such as Active Directory. Authentication problems in an environment with an LDAP authentication server can result from wrong settings or a connectivity failure. Both sides must have the same configuration for the authentication to succeed.

Perform these tasks on the Active Directory server to troubleshoot integration with Cisco UCS:

Step 1 Check the organizational unit configuration.

Step 2 Verify groups.

Step 3 Verify a non-administrative bind user account.

Step 4 Verify if users have been added to the Cisco UCS organizational unit.

These troubleshooting tasks must be performed in Cisco UCS Manager:

Step 1 Verify the configuration of a local authentication domain.

Step 2 Check the LDAP provider parameters.

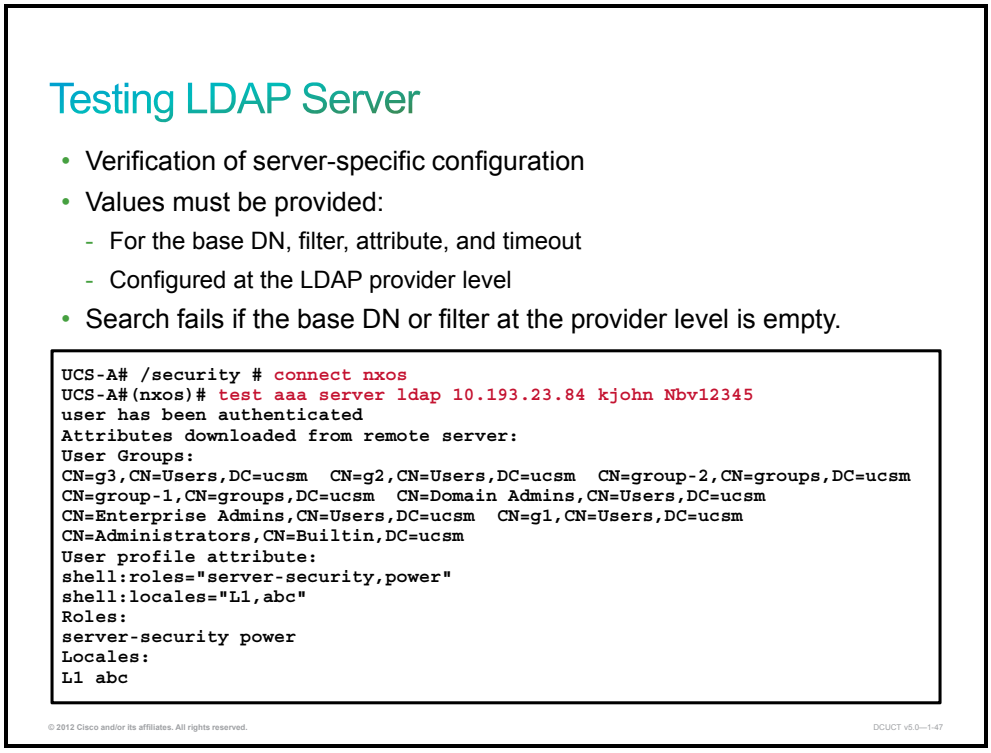
Step 3 View the LDAP group rule.

Step 4 Verify if the LDAP provider group has been created.

Step 5 Verify if the LDAP group map is configured properly.

Step 6 Check the LDAP authentication domain settings.

https://t.me/learningnets



Use the **test aaa server ldap** command to verify the following information if Cisco UCS Manager is able to communicate with the LDAP provider:

- The server responds to the authentication request if the correct username and password is provided.
- The roles and locales that are defined on the user object in the LDAP are downloaded.
- If the LDAP group authorization is turned on, the LDAP groups are downloaded.

The **test aaa server ldap** command verifies the server-specific configuration, irrespective of the LDAP global configurations. This command uses the values for the base distinguished name (DN), filter, attribute, and timeout that are configured at the LDAP provider level. If the base DN or filter at the provider level is empty, the LDAP search fails.

You can also test your configuration using the Cisco UCS Manager GUI:

Step 1 Launch the Cisco UCS Manager GUI.

Step 2 Enter **sampleaaa** in the User Name field.

Step 3 In the Password field, enter the sampleaaa Active Directory password.

Step 4 From the Domain drop-down list, choose your LDAP provider and click **OK**.

Step 5 Choose **All > User Management > User Services > Remotely Authenticated Users** and confirm that your authentication domain and Active Directory username are listed.

https://t.me/learningnets

Testing LDAP Group

- Verification of group-specific configuration
- Server responds to the authentication request.
- Download of the following:
  - The roles and locales defined on the user object in the LDAP
  - LDAP groups, if the LDAP group authorization is turned on

```
UCS-A# /security # connect nxos
UCS-A#(nxos)# test aaa group grp-ad1 kjohn Nbv12345
user has been authenticated
Attributes downloaded from remote server:
User Groups:
CN=g3,CN=Users,DC=ucsm  CN=g2,CN=Users,DC=ucsm  CN=group-2,CN=groups,DC=ucsm
CN=group-1,CN=groups,DC=ucsm  CN=Domain Admins,CN=Users,DC=ucsm
CN=Enterprise Admins,CN=Users,DC=ucsm  CN=g1,CN=Users,DC=ucsm
CN=Administrators,CN=Builtin,DC=ucsm
User profile attribute:
shell:roles="server-security,power"
shell:locales="L1,abc"
Roles:
server-security power
Locales:
L1 abc
```

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

Use the **test aaa group** command to verify the following information if Cisco UCS Manager is able to communicate with the LDAP group:

- The server responds to the authentication request if the correct username and password is provided.
- The roles and locales that are defined on the user object in the LDAP are downloaded.
- If the LDAP group authorization is turned on, the LDAP groups are downloaded.

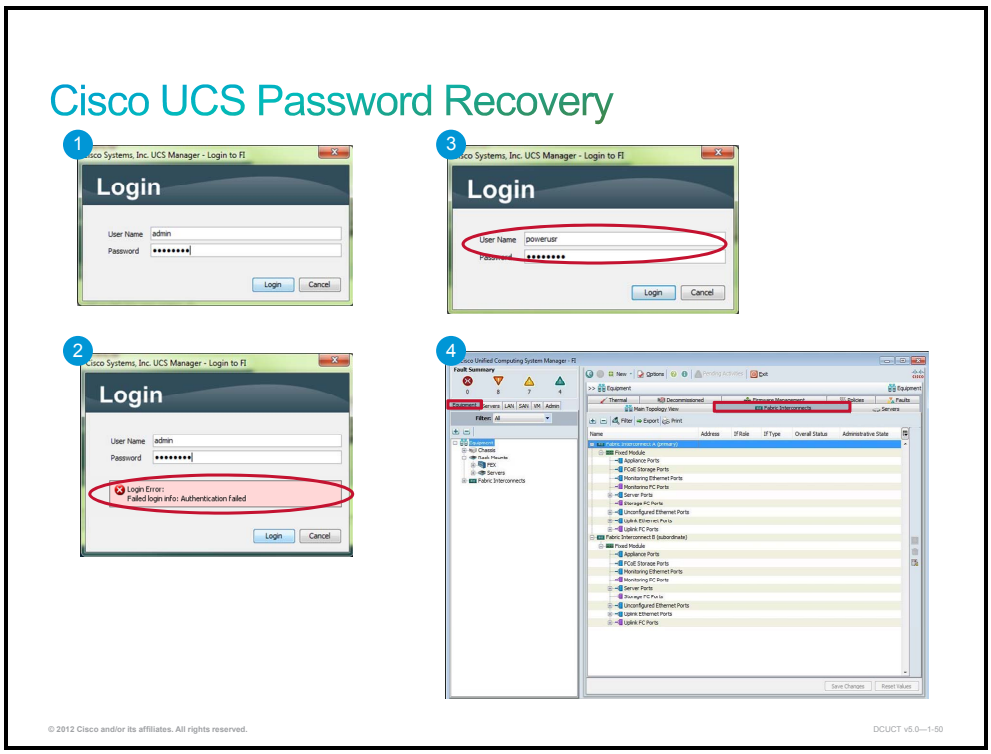
The **test aaa group** command verifies the group-specific configuration, irrespective of the LDAP global configurations.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS Password Recovery

This topic explains the steps to perform Cisco UCS B-Series password recovery.



The “admin” account is the system administrator or superuser account. If an administrator loses the password to this account, you can encounter a serious security issue. As a result, the procedure to recover the password for the “admin” account requires you to power-cycle all Fabric Interconnects in a Cisco UCS domain.

When you recover the password for the “admin” account, you actually change the password for the account. You cannot retrieve the original password for the account.

This procedure requires that you power down all Fabric Interconnects in a Cisco UCS domain. As a result, all data transmission in the Cisco UCS domain is stopped until you restart the Fabric Interconnects. If no other account to log in to Cisco UCS exists, you need to power down, power up the Fabric Interconnects, and follow the password recovery procedure.

If there is another account that can be used to log in to Cisco UCS, use it to verify certain settings (such as Fabric Interconnect roles, current kickstart, and system image) before proceeding with the reset procedure.

To determine the leadership role of a Fabric Interconnect, use these steps:

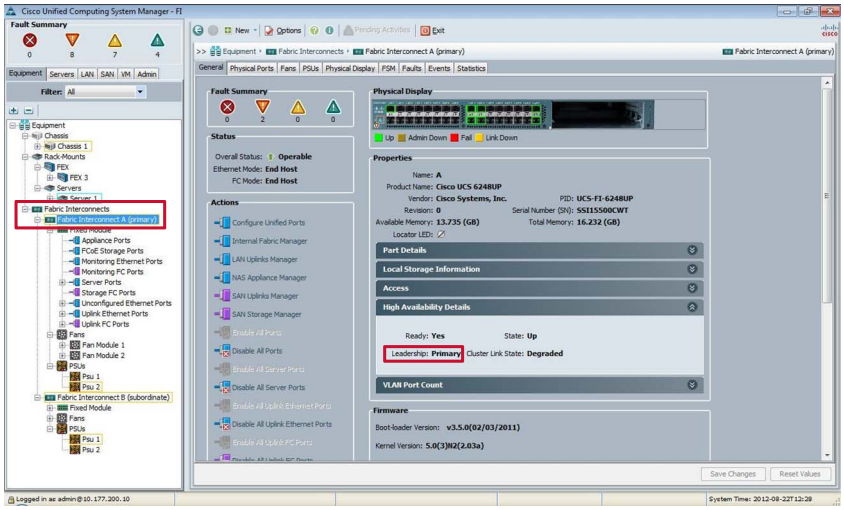
Step 1 In the Navigation pane, select the Equipment tab.

Step 2 In the Equipment tab, expand Equipment > Fabric Interconnects.

Step 3 Select the Fabric Interconnect for which you want to identify the role.

https://t.me/learningnets

Identify Leadership Role



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

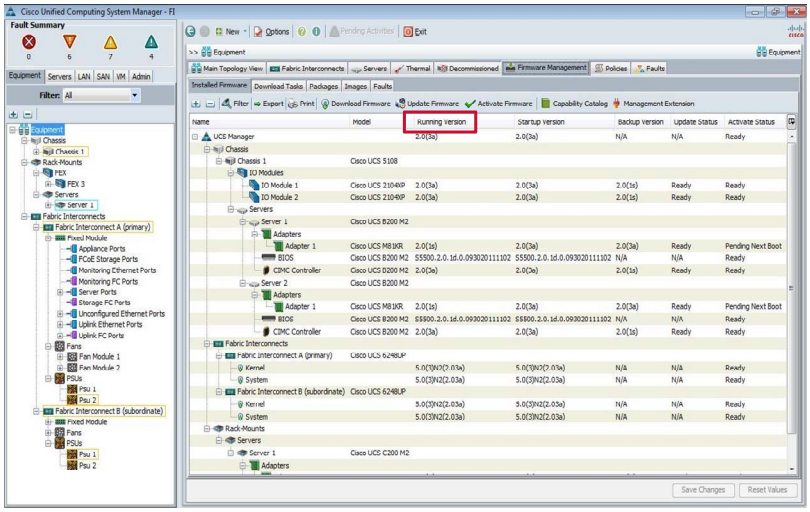
Step 1 In the Work pane, select the General tab.

Step 2 In the General tab, click the down arrows on the High Availability Details bar to expand that area.

Step 3 View the Leadership field to determine whether the Fabric Interconnect is the primary or subordinate.

https://t.me/learningnets

Verify Firmware Version



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

To verify the firmware version, follow these steps:

Step 1 In the Navigation pane, select the Equipment tab.

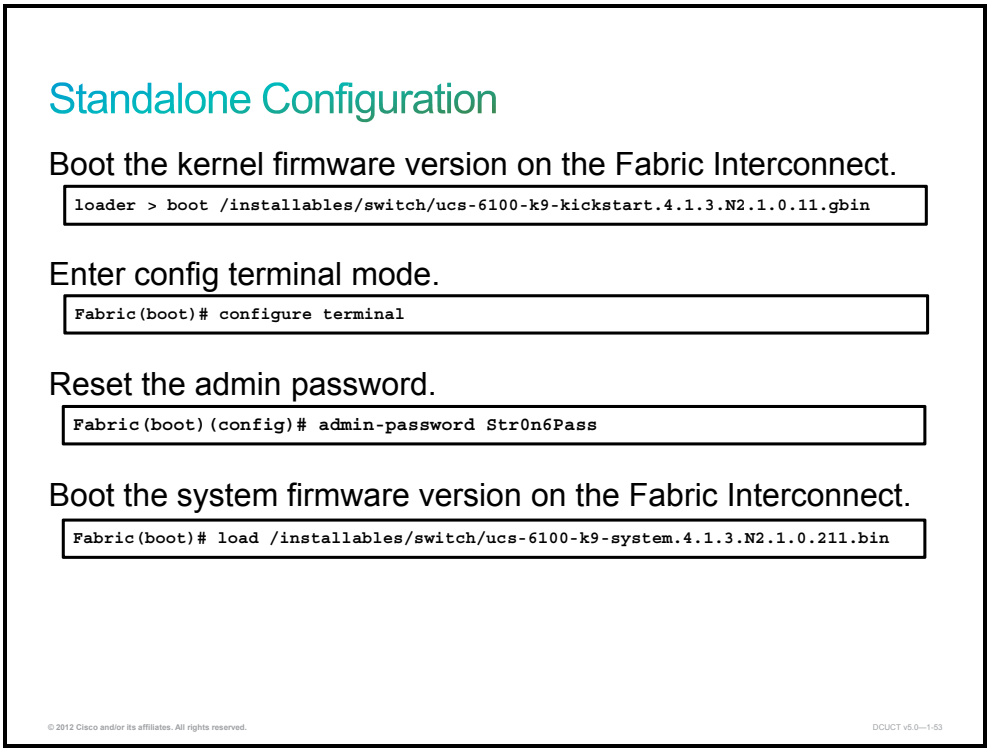
Step 2 In the Equipment tab, select the Equipment node.

Step 3 In the Work pane, select the Firmware Management tab.

Step 4 In the Installed Firmware tab, verify that the following firmware versions for each Fabric Interconnect match the version to which you updated the firmware:
- Kernel version
- Software version

If you are completely locked out of Cisco UCS, the Fabric Interconnects can only be restarted during the boot process. The kickstart and system software versions can only be observed during the boot process, as well.

https://t.me/learningnets



This procedure will help you to recover the password that was set for the "admin" account when you performed the initial system setup on the Fabric Interconnect. Before you begin, you must physically connect the console port on the Fabric Interconnect to a computer terminal or console server, and determine the running versions of the firmware kernel on the Fabric Interconnect and firmware system.

Step 1 Connect to the console port.

Step 2 Power-cycle the Fabric Interconnect.

- Turn off the power to the Fabric Interconnect.
- Turn on the power to the Fabric Interconnect.

Step 3 On the console, press one of the following key combinations as it boots to get the loader prompt:

- **Ctrl-l**
- **Ctrl-Shift-r**

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Step 4 Boot the kernel firmware version on the Fabric Interconnect.

loader > **boot /installables/switch/***kernel_firmware_version*

Here is an example:

loader > **boot /installables/switch/***ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin*

Step 5 Enter config terminal mode.

Fabric(boot)# **config terminal**

Step 6 Reset the "admin" password.

Fabric(boot)(config)# **admin-password** *password*

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

Step 7 Exit config terminal mode and return to the boot prompt.

Step 8 Boot the system firmware version on the Fabric Interconnect.

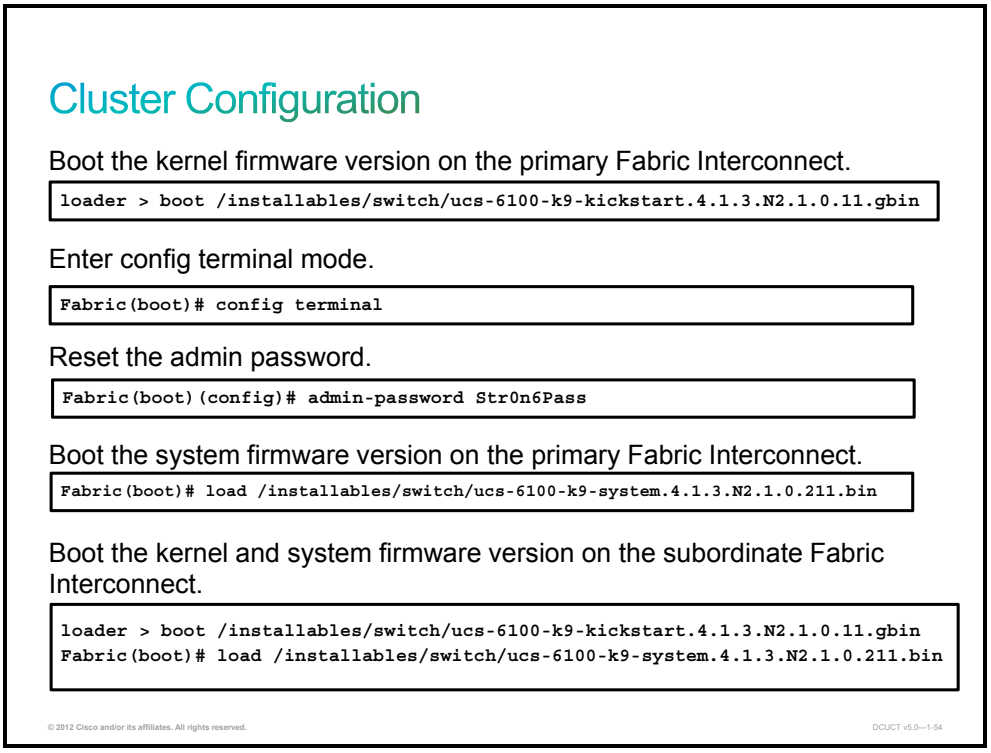
Fabric(boot)# **load /installables/switch/***system_firmware_version*

Here is an example:

Fabric(boot)# **load /installables/switch/***ucs-6100-k9-system.4.1.3.N2.1.0.211.bin*

Step 9 After the system image loads, log in to Cisco UCS Manager.

https://t.me/learningnets



To recover the “admin” account in the cluster configuration, first you must physically connect the console port on the Fabric Interconnect to a computer terminal or console server, and determine the running versions of the firmware kernel on the Fabric Interconnect and firmware system. At the end of the process, you must determine which Fabric Interconnect has the primary leadership role and which is the subordinate.

Step 1 Connect to the console port.

Step 2 Power-cycle the subordinate Fabric Interconnect.

- Turn off the power to the Fabric Interconnect.
- Turn on the power to the Fabric Interconnect.

On the console, press one of the following key combinations as it boots to get the loader prompt:

- **Ctrl-l**
- **Ctrl-Shift-r**

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Step 3 Power-cycle the primary Fabric Interconnect.

- Turn off the power to the Fabric Interconnect.
- Turn on the power to the Fabric Interconnect.

On the console, press one of the following key combinations as it boots to get the loader prompt:

- **Ctrl-l**
- **Ctrl-Shift-r**

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Step 4 Boot the kernel firmware version on the primary Fabric Interconnect.
loader > **boot /installables/switch/***kernel_firmware_version*

Here is an example:

loader > **boot /installables/switch/***ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin*

Step 5 Enter config terminal mode.

Fabric(boot)# **config terminal**

Step 6 Reset the “admin” password.

Fabric(boot)(config)# **admin-password** *password*

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.The new password displays in cleartext mode.

Step 7 Exit config terminal mode and return to the boot prompt.

Step 8 Boot the system firmware version on the primary Fabric Interconnect.

Fabric(boot)# **load /installables/switch/***system_firmware_version*

Here is an example:

Fabric(boot)# **load /installables/switch/***ucs-6100-k9-system.4.1.3.N2.1.0.211.bin*

Step 9 After the system image loads, log in to Cisco UCS Manager.

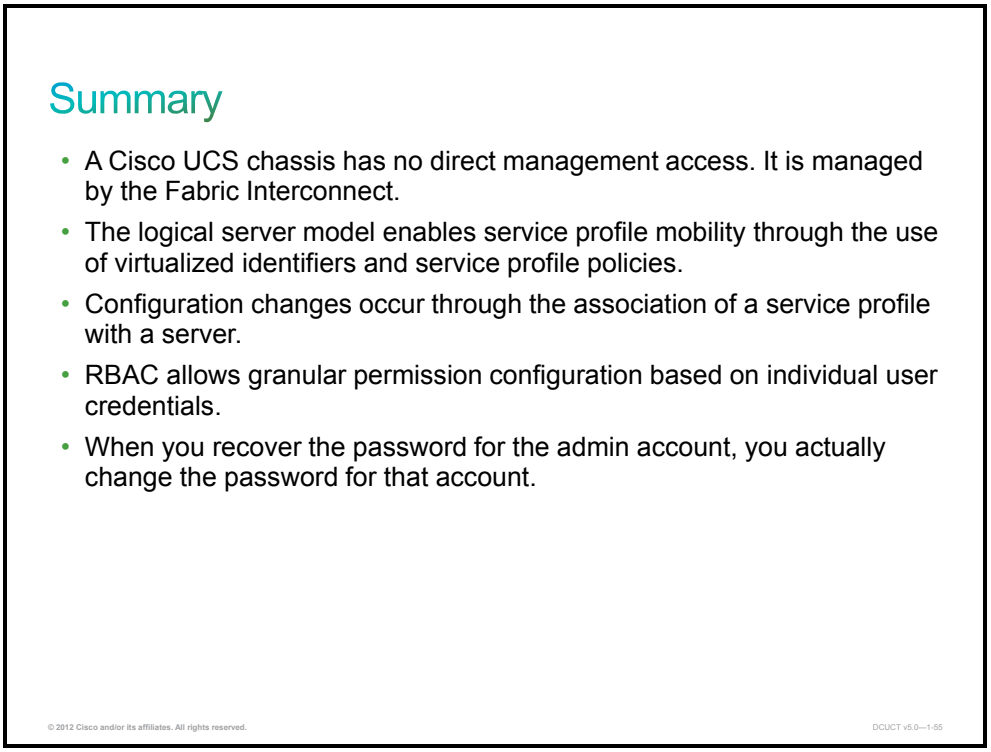
Step 10 On the console for the subordinate Fabric Interconnect, perform the following tasks to bring it up:

- Boot the kernel firmware version on the subordinate Fabric Interconnect.
  loader > **boot /installables/switch/***kernel_firmware_version*
- Boot the system firmware version on the subordinate Fabric Interconnect.
  Fabric(boot)# **load /installables/switch/***system_firmware_version*

https://t.me/learningnets

Summary

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



© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 3

Troubleshooting Cisco UCS B-Series Operation

Overview

In this lesson, you will learn about Cisco Unified Computing System (Cisco UCS) B-Series operation and troubleshooting of related issues.

Objectives

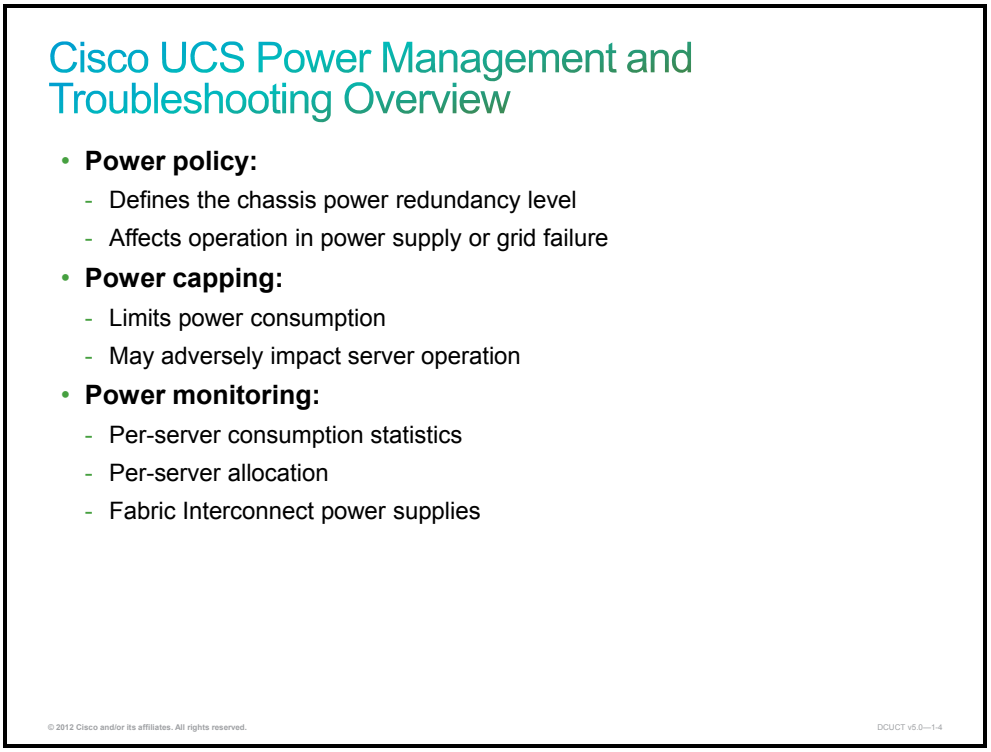
Upon completing this lesson, you will be able to describe Cisco UCS B-Series operation and troubleshooting of related issues. This ability includes being able to meet these objectives:

- Recognize Cisco UCS power consumption, availability, and power policies
- Identify and troubleshoot blade remote access
- Troubleshoot Cisco UCS B-Series server boot
- Identify and troubleshoot operating system driver-related issues

https://t.me/learningnets

Cisco UCS Power Management

This topic describes Cisco UCS power consumption, availability, and power policies.

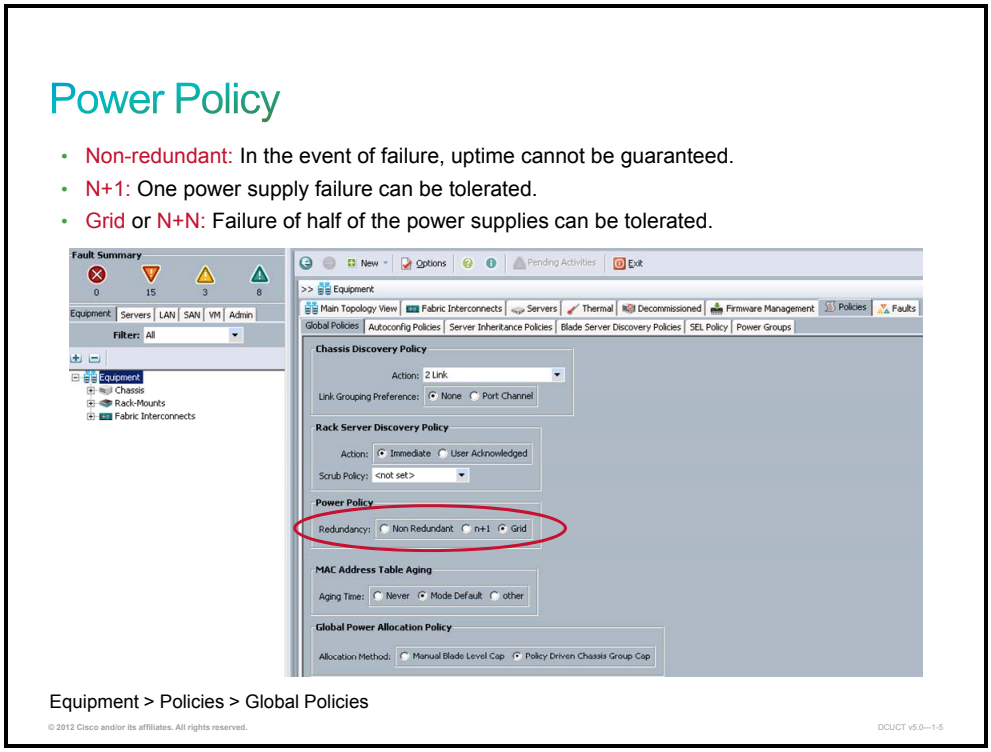


Several areas of Cisco UCS power management require special attention when you are troubleshooting. The areas are as follows:

- **Power policy.** The power policy defines the chassis power redundancy level. There are three modes of power redundancy that can be configured on Cisco USC: nonredundant, N+1, and grid.
- **Power capping.** Power capping is the capability of the system to limit power consumption to some threshold.
- **Power monitoring.** Cisco UCS Manager offers numerous methods to monitor per-server power consumption statistics, per-server power allocation, Fabric Interconnect power supplies, and other power-related information.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



There are three modes of power redundancy that can be configured on the Cisco USC system.

Nonredundant Mode

In a nonredundant or combined mode, all installed power supplies are on and balance the load evenly. Common configurations require two or more power supplies (if requirements are between 2500 W and 5000 W peak) in nonredundant mode.

When using Cisco UCS Release 1.4(1) and later, the chassis requires a minimum of two power supplies.

N+1 Redundancy Mode

The N+1 redundancy configuration implies that the chassis contains a total number of power supplies to satisfy nonredundancy, plus one additional power supply for redundancy. All the power supplies that are participating in N+1 redundancy are turned on and equally share the power load for the chassis. If any additional power supplies are installed, Cisco UCS Manager recognizes these “unnecessary” power supplies and places them on standby.

If a power supply fails, the surviving supplies can provide power to the chassis. In addition, Cisco UCS Manager turns on any “turned-off” power supplies to bring the system back to N+1 status.

To provide N+1 protection, the following number of power supplies is recommended:

- Three power supplies are recommended if the power configuration for the chassis requires more than 2500 W or if the system is using Cisco UCS Release 1.4(1) and later.
- Two power supplies are sufficient if the power configuration for the chassis requires less than 2500 W or if the system is using Cisco UCS Release 1.3(1) or earlier.

Adding an additional power supply to either of these configurations provides an extra level of protection. Cisco UCS Manager turns on the extra power supply in the event of a failure and restores N+1 protection.

https://t.me/learningnets

Grid Redundancy Mode

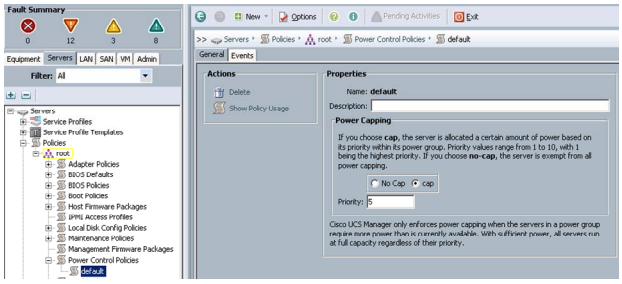
A common reason for using grid redundancy is if the rack power distribution is such that power is provided by two power distribution units (PDUs) and you want grid redundancy protection in case of PDU failure.

To provide grid redundant (or greater than N+1) protection, the following number of power supplies is recommended:

- Four power supplies are recommended if the power configuration for the chassis requires more than 2500 W or if the system is using Cisco UCS Release 1.4(1) and later.
- Two power supplies are recommended if the power configuration for the chassis requires less than 2500 W or if the system is using Cisco UCS Release 1.3(1) or earlier.

Power Capping

- Capability to limit power consumption
- Static power capping:
  - Fixed power consumption limit for each blade
  - Does not take into consideration that the blades may have varying loads
- Dynamic power capping:
  - Designed to allocate pool of power across multiple blades in chassis
  - Servers with higher loads and requirements get more power



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

Power capping is the capability of Cisco UCS to limit power consumption. This feature is particularly useful in large environments, where power oversubscription is likely.

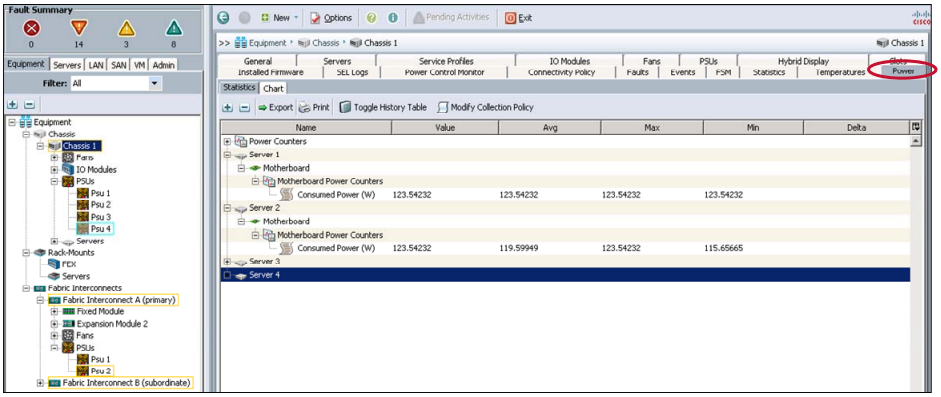
If the maximum power rating of a single blade server is 340 W, and the power that is available to the chassis is 3334 W AC, which is sufficient to supply an average of 300 W per blade server, plus the chassis, each blade can be capped at a maximum of 300 W per blade to avoid oversubscription. This type of capping is known as static power capping. Capping helps ensure that the chassis will never draw more power than it is allowed, but it does not take into consideration that the various blades may have varying loads and a blade may not use its full allotment of power at any given time.

Dynamic power capping allows the power management system to dynamically allocate the total pool of power across multiple blades in a chassis. With dynamic power capping, a server with higher loads get more power, but the whole power budget is in defined limits.

https://t.me/learningnets

Monitoring Power Consumption

- Cisco UCS monitors current power consumption of all blades.
- A chart provides a graphical illustration of power management.
- Information that is needed to remediate power allocation issues is provided.



Equipment > Chassis > Chassis-name > Power > Statistics

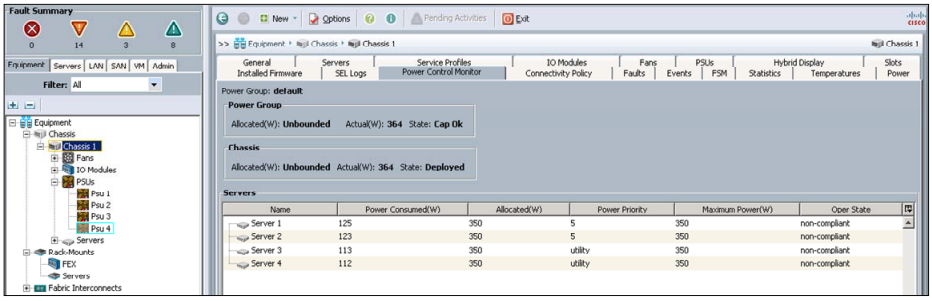
© 2012 Cisco and/or its affiliates. All rights reserved.

The Cisco UCS Manager GUI and CLI can be used to monitor the current power consumption of all blade servers. Choose **Equipment > Chassis > Chassis-name > Power**, and the relevant statistics are displayed in the Statistics tab. The Chart tab offers you a graphical illustration of the current power management state. You require information regarding power consumption to properly configure and troubleshoot power on Cisco UCS.

https://t.me/learningnets

Power Control Monitoring

- Power control provides information on dedicated, consumed, and maximum power.
- The priority defines the order of server shutdown at power shortage.



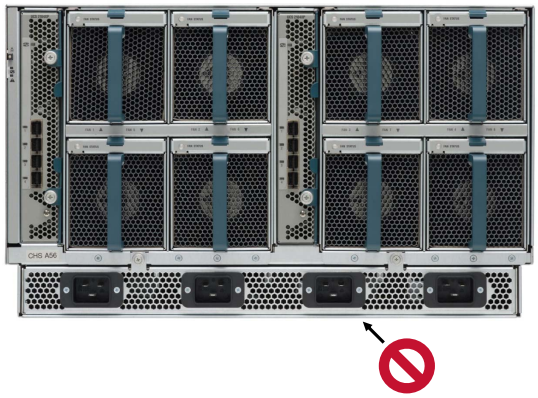
Equipment > Chassis > Chassis-name > Power Control Monitor

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

Choose **Equipment > Chassis > Chassis-name**. Power control monitoring information—such as per-server information about the power consumed, power allocated, power priority, maximum power, and operation state of each server blade—is available in the Power Control Monitor tab. The priority defines the order of server shutdown when there is a power shortage.

Issue: Short Service Interruption at Power Supply Failure

- Symptom: There is a short power interruption at failure of a power supply.
- Blade servers are installed in all slots.
- All four power supplies are connected to grid.



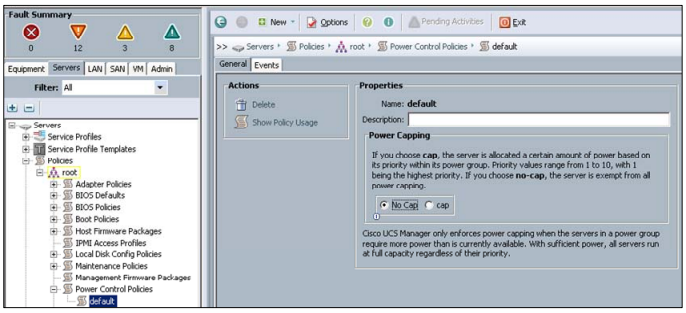
© 2012 Cisco and/or its affiliates. All rights reserved.

In this troubleshooting scenario, you are assigned to a case in which a short service interruption is reported at failure of a power supply. A glimpse at the system reveals that Cisco UCS is fully loaded, with eight blade servers and four power supplies.

https://t.me/learningnets

Data Gathering

- After a short interruption, full service is restored despite the failed power supply.
- No power capping is configured.
- Priorities of all servers are set to the same value.
- Replication on a test chassis:
  - Interruption does not occur with light server loads.
  - Interruption occurs under heavy CPU load.



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

In the data gathering phase, you examine the situation and realize that, after a short interruption, full service is restored despite one failed power supply. You check the Cisco UCS configuration and find that power capping is not configured. The priorities of all servers are set to the same value—5.

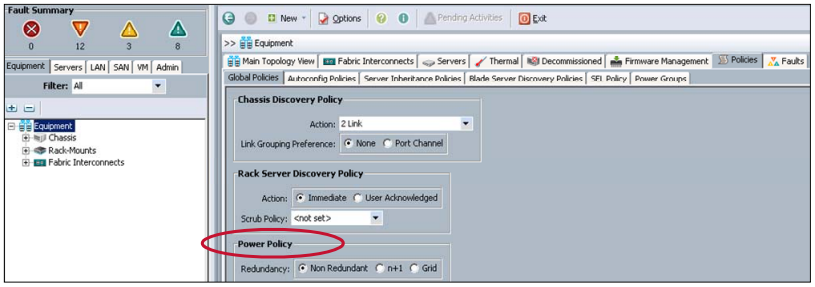
To further investigate the problem, you try to replicate it on a Cisco UCS chassis in the test environment. These are the results:

- Interruption does not occur with light server loads.
- Interruption occurs under heavy CPU load.

https://t.me/learningnets

Fault Isolation

- The current power configuration is in non-redundant mode.
- Supplies not used by the system are placed into standby.
- Installation order, not slot number, affects which supplies are placed into standby.
- Load is balanced across active power supplies.
- Standby power supplies are activated in the event of a failure.
- Failover may not occur fast enough to avoid downtime.



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

After the data gathering phase and cross-checking the results against Cisco documentation, you are able to isolate the fault. The problem results from the configured power policy mode—nonredundant. Nonredundant mode is characterized by the following:

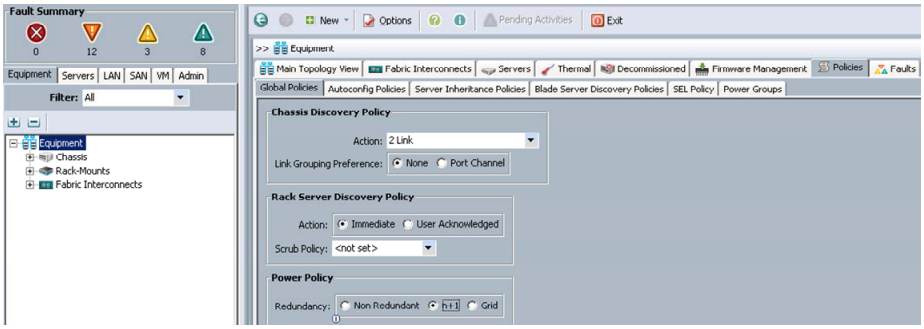
- Power supplies that are not used by the system are placed into standby state.
- The installation order affects which power supplies are placed into standby. The slot number has no impact on the state of the power supply.
- The load is balanced across active power supplies.
- Standby power supplies are activated in the event of a failure.
- Failover may not occur fast enough to avoid downtime.

You experienced the service interruption under a heavy load as a result of the failover time.

https://t.me/learningnets

Remediation

- The redundancy mode is changed to N+1.
- Best practices for all deployments:
  - Use one of the two redundant modes: N+1 or grid.
  - Never deploy Cisco UCS without some level of redundancy.



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

To remediate the problem, you change the power policy mode to redundancy mode. You have two options: N+1 and grid. Select grid mode if you have two separate grids that are available to power your system. In other cases, the N+1 mode is recommended.

In redundant mode, at least one of the power supplies is kept on standby and the failover does not incur any service interruption.

https://t.me/learningnets

Issue: Mission-Critical Server Shutdown at Power Supply Failure

- Server mix in a single chassis:
  - Four mission-critical servers
  - Four medium-impact servers
- Redundancy mode: N+1
- At failure of two power supplies, a mission-critical server is shut down.

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

In this troubleshooting scenario, you have a fully loaded chassis. The eight blade servers are divided into two pools: four mission-critical servers and four medium-impact servers. The power policy is set to N+1 mode.

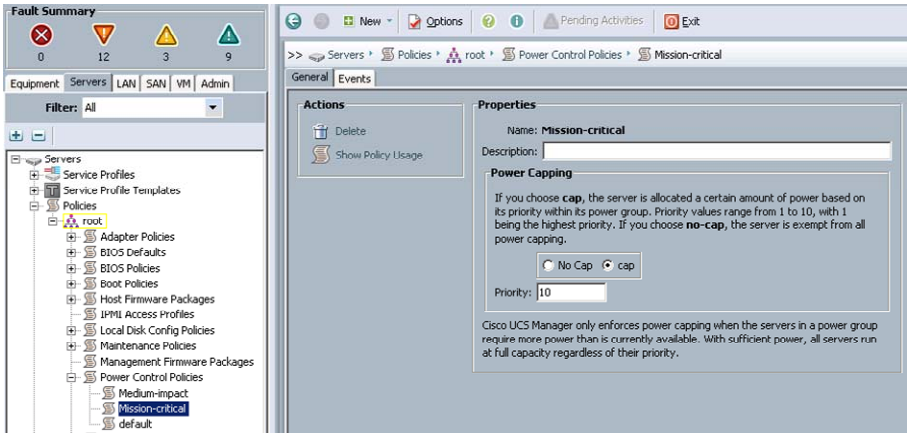
The problem is that when two power supplies fail, one or two of the mission-critical servers are shut down. This situation is in contrast to the required behavior, where the medium-impact servers should be shut down first if there is not enough power in the system.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Data Gathering 1: Mission-Critical Power Control Policy

- Power capping is enabled for mission-critical servers.
- The priority is set to the highest value: 10.

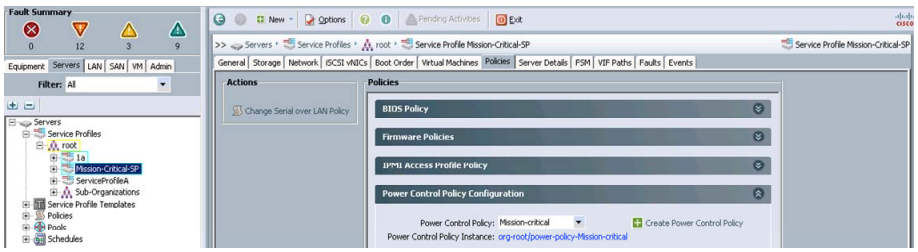


© 2012 Cisco and/or its affiliates. All rights reserved.

You start the data gathering phase and verify the existing power control policies. You find the "Mission-critical" policy, which enables capping of power and sets the priority to the highest value—10.

Data Gathering 2: Mission-Critical Service Profile

- The "Mission-critical" power control policy is applied to the "Mission-Critical-SP" service profile.
- The "Mission-Critical-SP" service profile is associated with mission-critical servers.



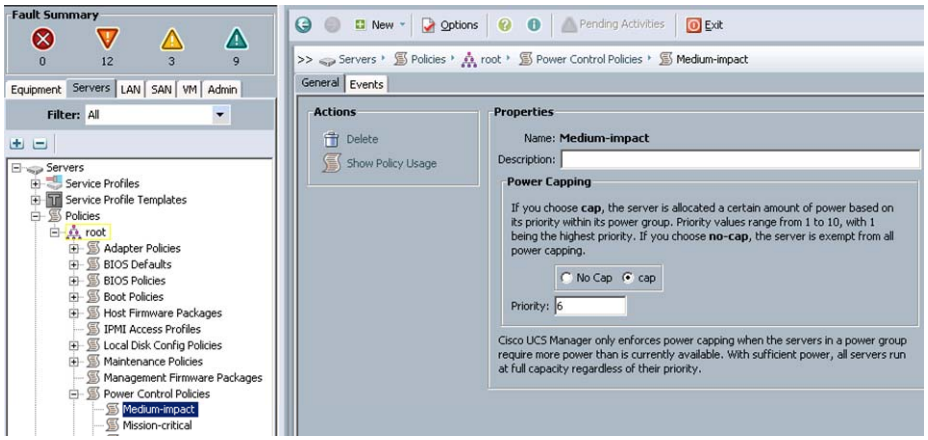
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, you verify that the "Mission-critical" power control policy is applied to the "Mission-Critical-SP" service profile. This service profile is applied to the mission-critical blade servers, although this is not shown in the figure.

https://t.me/learningnets

Data Gathering 3: Medium-Impact Power Control Policy

- Power capping is enabled for medium-impact servers.
- The priority is set to 6.

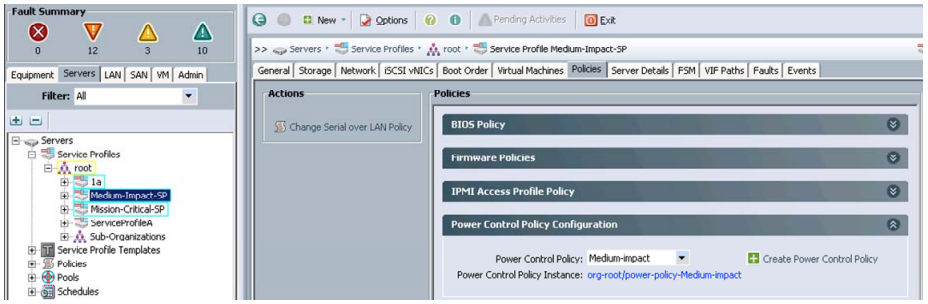


© 2012 Cisco and/or its affiliates. All rights reserved.

Next, you identify the “Medium-impact” policy, which enables capping of power and sets the priority to a medium value—6.

Data Gathering 4: Medium-Impact Service Profile

- The “Medium-impact” power control policy is applied to the “Medium-Impact-SP” service profile.
- The “Medium-Impact-SP” service profile is associated with medium-impact servers.



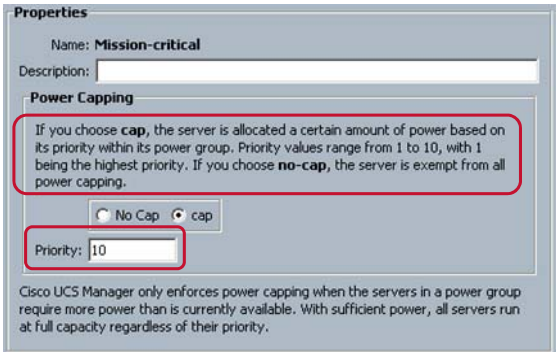
© 2012 Cisco and/or its affiliates. All rights reserved.

Then you verify that the “Medium-impact” power control policy is applied to the “Medium-Impact-SP” service profile. This service profile is applied to the medium-impact blade servers, but this is not shown in the figure.

https://t.me/learningnets

Fault Isolation

- There is an incorrect configuration of current priorities:
  - Mission-critical: 10
  - Medium-impact: 6
- The highest priority is 1.
- With the current settings, mission-critical servers are put out-of-service first.



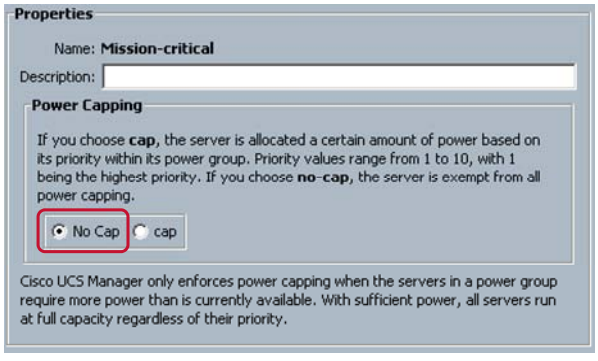
© 2012 Cisco and/or its affiliates. All rights reserved.

With the gathered information, you are able to pinpoint the cause of the problem. The priorities have been incorrectly set. The highest priority (1) is not equal to the numerically highest number (10).

When the mission-critical servers have priority 10, they will be shut down first.

Remediation

- This is a good solution:
  - Change the priority to 1, which is the highest priority.
- This is the best-practice solution:
  - Configure “No Cap” (no power capping) for mission-critical servers.



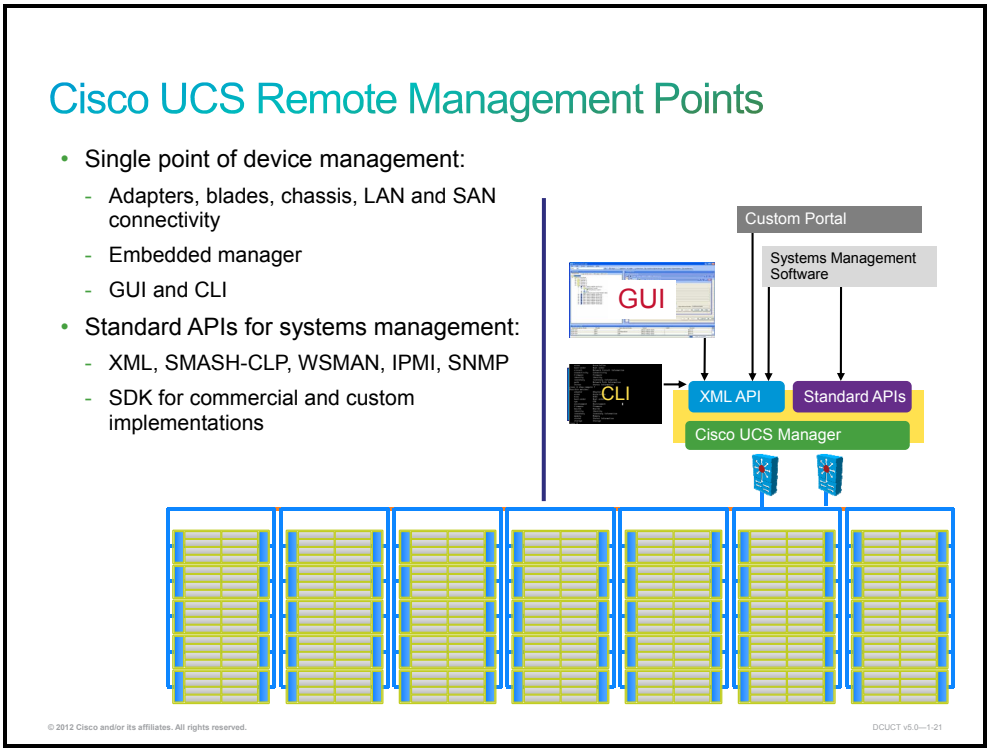
© 2012 Cisco and/or its affiliates. All rights reserved.

To resolve the problem, you can change the priority of the mission-critical servers to 1. This would suffice in this situation but it is not the best solution. Ideally, you should follow the best practice recommendation and disable power capping for mission-critical servers.

https://t.me/learningnets

Troubleshoot UCS Manager Remote Access

This topic describes how to troubleshoot remote access problems.

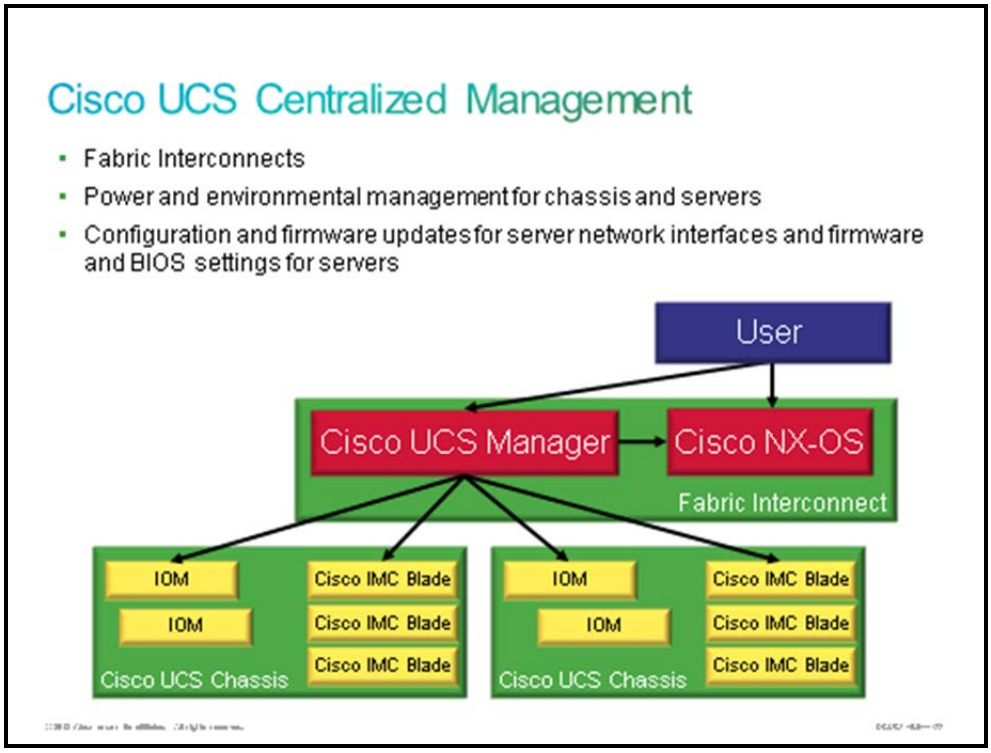


When solving problems that are related to accessing Cisco UCS Manager on the Fabric Interconnect, Cisco Integrated Management Controller (Cisco IMC), and other parts of the Cisco UCS platform, it is important to understand how the elements are connected. It is also important to understand that a GUI and CLI can both perform the same tasks except for some tasks that can only be performed in the GUI *or* the CLI.

The specific tasks change from version to version. Certain tasks, such as the Cisco IMC setup and BIOS configuration, are always GUI-related and some tasks are best suited to the GUI specifically.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



Typically, the system administrator connects directly to Cisco UCS Manager to configure the Fabric Interconnect. Access to all other elements in the Cisco UCS platform are from Cisco UCS Manager, including the switching fabric in the Cisco UCS 6100, the I/O module (IOM) in each chassis, and Cisco IMC on each blade in the chassis.

Cisco UCS Manager runs from the Fabric Interconnect and manages all of the elements of the physical Cisco UCS infrastructure and logical network configuration:

- Fabric Interconnects
- Software switches for virtual servers
- Power and environmental management for chassis and servers
- Configuration and firmware updates for server network interfaces (Ethernet network interface cards [NICs] and converged network adapters)
- Firmware and BIOS settings for servers

Cisco UCS Manager abstracts server state information—including server identity, I/O configuration, MAC addresses and world wide names (WWNs), firmware revision, and network profiles—into a service profile. You can apply the service profile to any server resource in the system, providing the same flexibility and support to physical servers, virtual servers, and virtual machines (VMs) that are connected to a virtual device by a virtual interface card (VIC) adapter.

https://t.me/learningnets

Troubleshooting Administrative Access

- Understand the network flows from the desktop to Cisco UCS Manager.
- Check firewalls, access control lists (ACLs), and routing to Cisco UCS Manager on the Fabric Interconnect.
- Understand the data interaction between the Fabric Interconnect and the Cisco UCS 5108 Blade Server chassis using the FEX modules.
- Understand the communication from the Fabric Interconnect to the Chassis Management Controller (CMC) and Cisco IMC modules for physical status and feedback.

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

If you cannot access Cisco UCS Manager on the Fabric Interconnect, consider the network path between the client and the Fabric Interconnect.

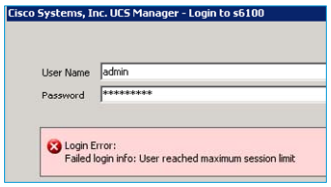
When working in Cisco UCS Manager, consider the interaction between each of the components to help with your troubleshooting process. When establishing hypotheses for the problem cause, it is vital to understand the interaction of each of the components.

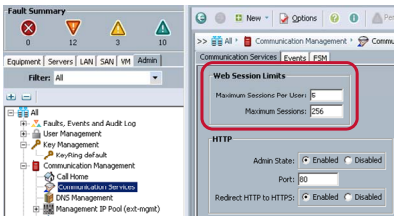
© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Web Session Limits

- When the maximum session limit is exceeded, do one of the following:
  - Close the open GUI sessions.
  - Increase the number in Cisco UCS Manager.
- There are two limits:
  - Per user (default 32)
  - Global (default 256)





Admin > All > Communication Management > Communication Services

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

DCUCT v5.0—1-24

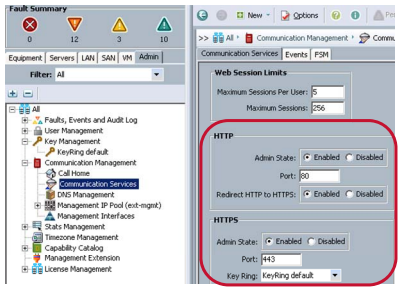
Cisco UCS caps the maximum number of active web administration sessions. There are two limits: per-user with the default value of 32, and per-system with the default value of 256.

You will not be able to log in to the system if any of these thresholds is exceeded. In that situation, you must close some of the open sessions to be able to connect. If the limit is set too low to accommodate your requirements, the maximum session limits can be adjusted in Admin > All > Communication Management > Communication Services.

https://t.me/learningnets

HTTP and HTTPS Access

- Both HTTP (insecure) and HTTPS (secure) are enabled by default.
- Redirection from HTTP to HTTPS is activated by default.
- If a firewall blocks TCP ports 80 or 443, do the following:
  - Change the port numbers in Cisco UCS to ports that are allowed by the firewall.
  - Disable the protocol that is blocked by the firewall.
  - Deactivate redirection if HTTPS is not permitted.



Admin > All > Communication Management > Communication Services

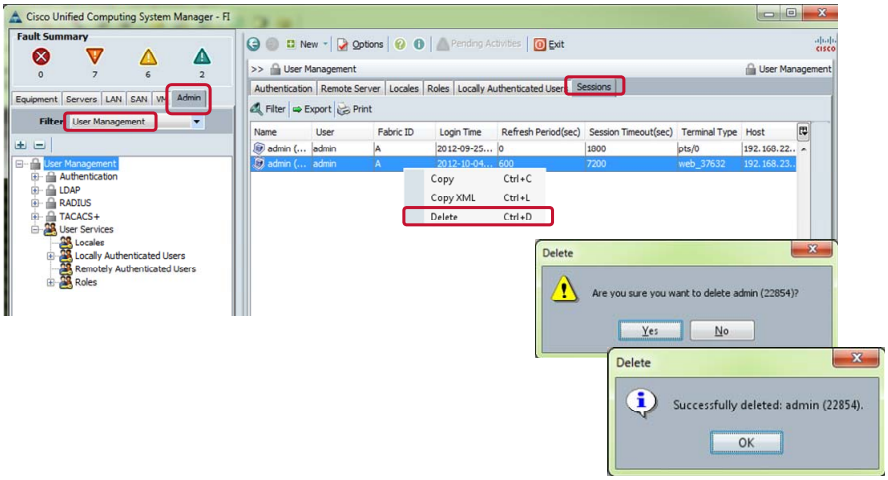
© 2012 Cisco and/or its affiliates. All rights reserved.

By default, Cisco UCS enables both HTTP and HTTPS access, but redirects HTTP-based sessions to HTTPS to provide a more secure access method. Firewalls that are installed in your organization may enforce a security policy that blocks one or both of the default ports 80 and 443. To solve this problem, you can either change the default port numbers to other numbers that are permitted by the firewall or disable one of the access protocols.

https://t.me/learningnets

Managing User Sessions

- Non-active sessions can be cleared to allow management access.



Admin > User Management > Sessions

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

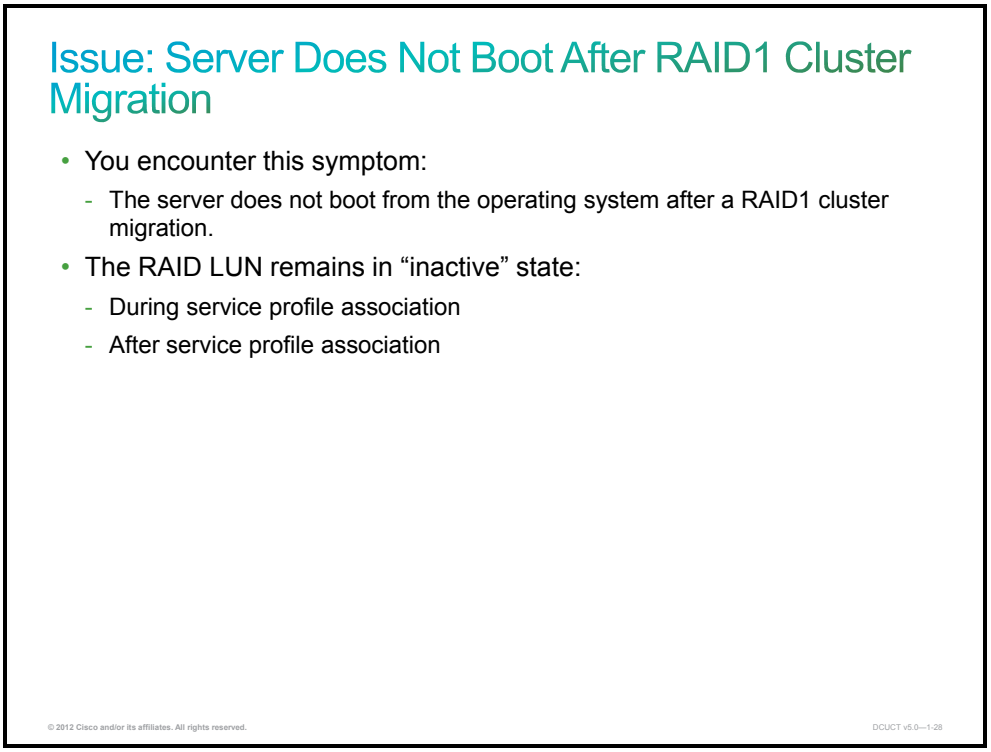
DCUCT v5.0—1-26

When there are too many management sessions open (such as sessions that are not being used but were not properly closed), the session limit prevents any new management sessions to be opened. In this case, the non-active sessions can be cleared by choosing the Session tab under the Admin > User Management options. Right-click to show the menu, where the Delete option can be selected to delete these sessions.

https://t.me/learningnets

Troubleshoot Cisco UCS B-Series Server Boot

This topic describes how to troubleshoot the Cisco UCS B-Series server boot.



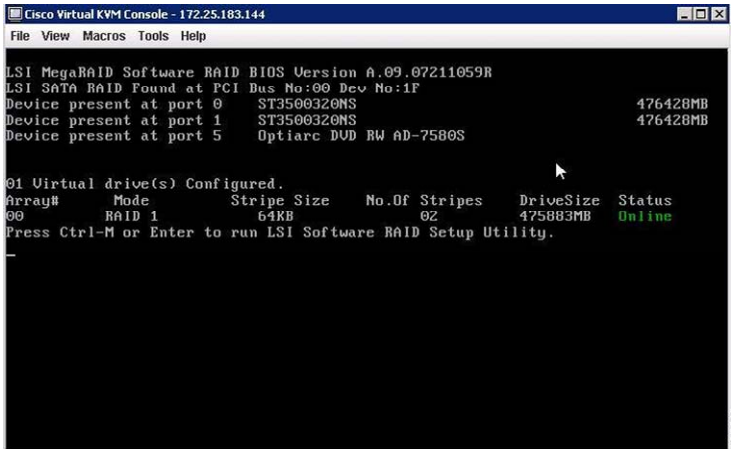
In this troubleshooting scenario, you are confronted with a server boot failure after a RAID1 cluster migration. The server fails to boot the operating system from the RAID1 disk. The RAID logical unit numbers (LUNs) appear as inactive during and after the service profile association.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Data Gathering: RAID Setup Utility

- The RAID setup utility is accessible through KVM.
- Press **CTRL-M** to access ICH10R onboard controller configuration.

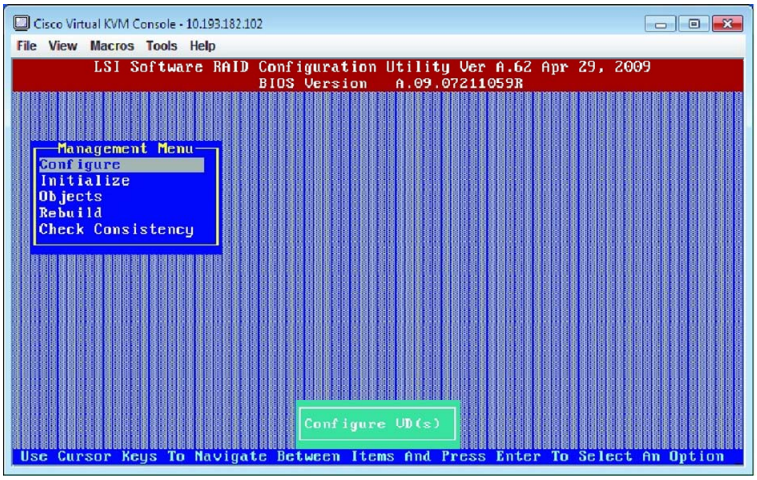


© 2012 Cisco and/or its affiliates. All rights reserved.

To gather additional information, you use the keyboard, video, mouse (KVM) console and observe the boot process. You can invoke the RAID setup utility by pressing the **Ctrl-M** key combination.

Data Gathering: Examine RAID Configuration

- Configuration settings depend on the type of the onboard controller.



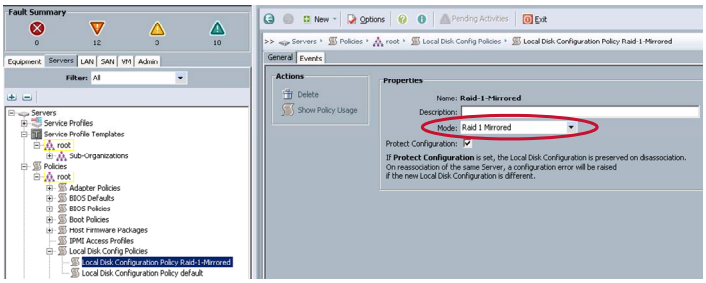
© 2012 Cisco and/or its affiliates. All rights reserved.

Within the RAID configuration utility, you can check the configuration and, if necessary, modify the settings. In this particular case, you do not find any faults.

https://t.me/learningnets

Data Gathering: Local Disk Configuration Policies

- Check the local disk configuration policies that are defined in Cisco UCS Manager.
- The policy with mode “Raid-1 Mirrored” is required for this scenario.



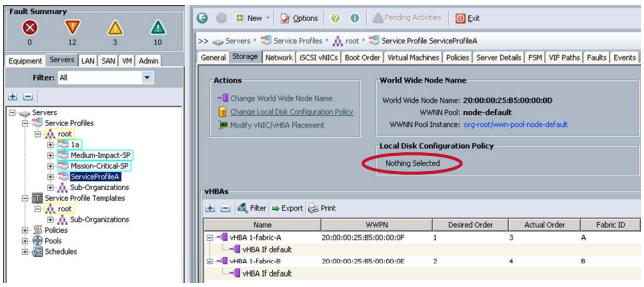
Servers > Policies > Local Disk Config Policies

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

Then you proceed to verify the local disk configuration policies that are defined in Cisco UCS Manager. You find an appropriate policy, called “Raid-1-Mirrored” with “Raid 1 Mirrored” mode, which is suitable for the RAID1 scenario.

Data Gathering: Local Disk Configuration Policy in Service Profile

- Check the service profile that is attached to the server.
- Verify that the correct local disk policy is applied in the Storage tab.
- In this case, “Nothing Selected” is the policy.



Servers > Service Profiles

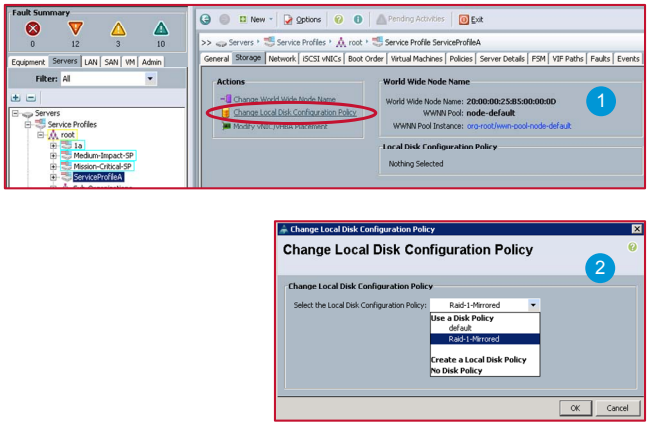
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, you need to verify the local disk configuration policy that is attached to the required service profile. In this case, you find that no policy has been assigned to the service profile “ServiceProfileA,” which is applied to the relevant servers.

https://t.me/learningnets

Remediation

- Apply the “Raid-1-Mirrored” policy to the proper service profile.



Servers > Service Profiles

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

DCUCT v5.0—1-33

To resolve the problem, you apply the appropriate local disk configuration policy to the specific service profile.

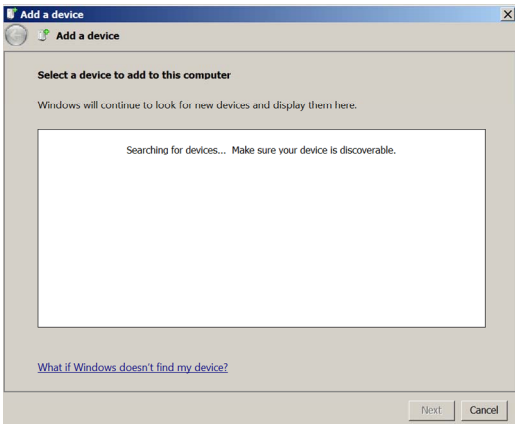
https://t.me/learningnets

Troubleshoot Operating System Software Drivers

This topic describes how to troubleshoot operating system driver-related issues.

Driver Location

- Drivers are included on the Cisco UCS B-Series Drivers DVD, which is provided.
  - However, download the latest versions from Cisco.com.
- You can view the installed devices using the Cisco UCS Manager GUI to decide which drivers are needed.



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

To confirm which devices have been configured on each blade, as well as each device type, you can use the Cisco UCS GUI or CLI and verify the hardware elements for which you need software drivers.

The interface cards that are installed in the target server are displayed. The product identifier (PID) of each card is listed.

You can find more information here:
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/b/os/windows/install/drivers-app.html

All drivers for Cisco UCS B-Series servers are included on the Cisco UCS B-Series drivers DVD that is shipped with the server. Best practice, however, is to download the most recent drivers from Cisco.com.

Viewing Installed Devices Using the KVM Console

To see the names and model numbers of the devices that are displayed on the console screen during server bootup, follow these steps:

1. In the Cisco UCS Manager main window, click the Equipment tab in the Navigation pane.
2. On the Equipment tab, expand **Equipment > Chassis > *Chassis_Number* > Servers**.
3. Select the target server that you want to access through the KVM console.
4. In the Work pane, select the General tab.
5. In the Actions area, click **KVM Console**. The KVM console opens in a separate window.

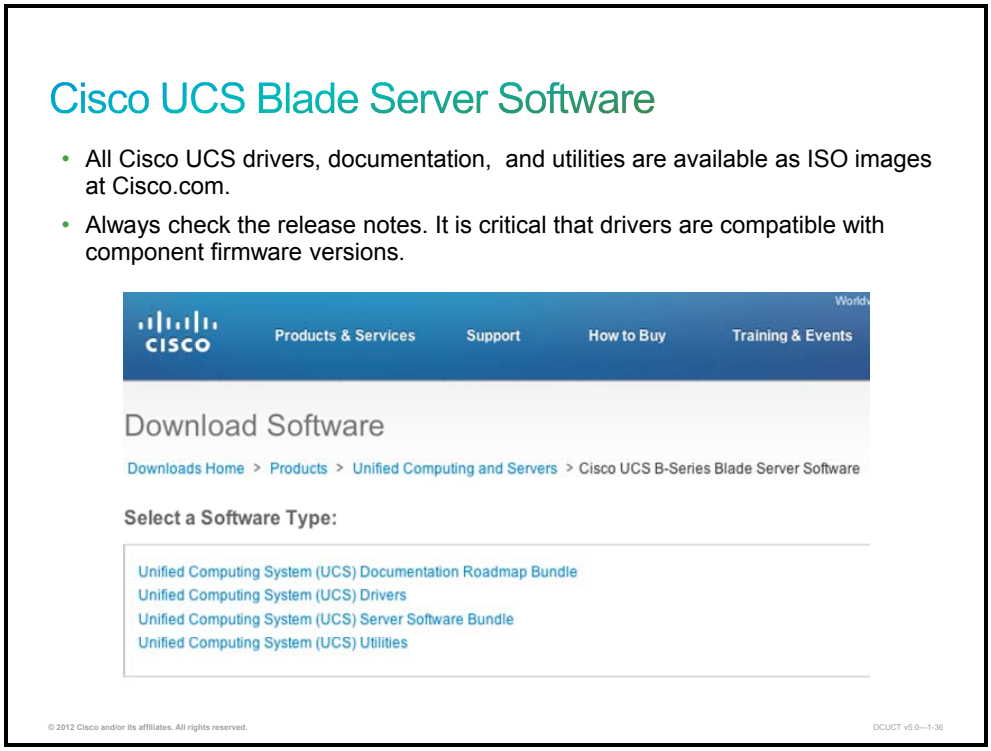
https://t.me/learningnets

6. Reboot the server and observe the information about the installed devices on the console screen during bootup.

Viewing Installed Devices Using the Cisco UCS Manager GUI

To view the installed devices in the server by using the Cisco UCS Manager GUI, follow these steps:

1. In the Cisco UCS Manager main window, click the Equipment tab in the Navigation pane.
2. On the Equipment tab, expand **Equipment > Chassis > *Chassis_Number* > Servers > *Server_Number***, where *Server_Number* is the target server.
3. Select Interface Cards. The interface cards that are installed in the target server are displayed. The PID of each card is listed.



Cisco publishes a single download ISO that contains all the documentation and utilities as an ISO image. This figure shows the four downloads that contain drivers, software, and utilities for the administrator.

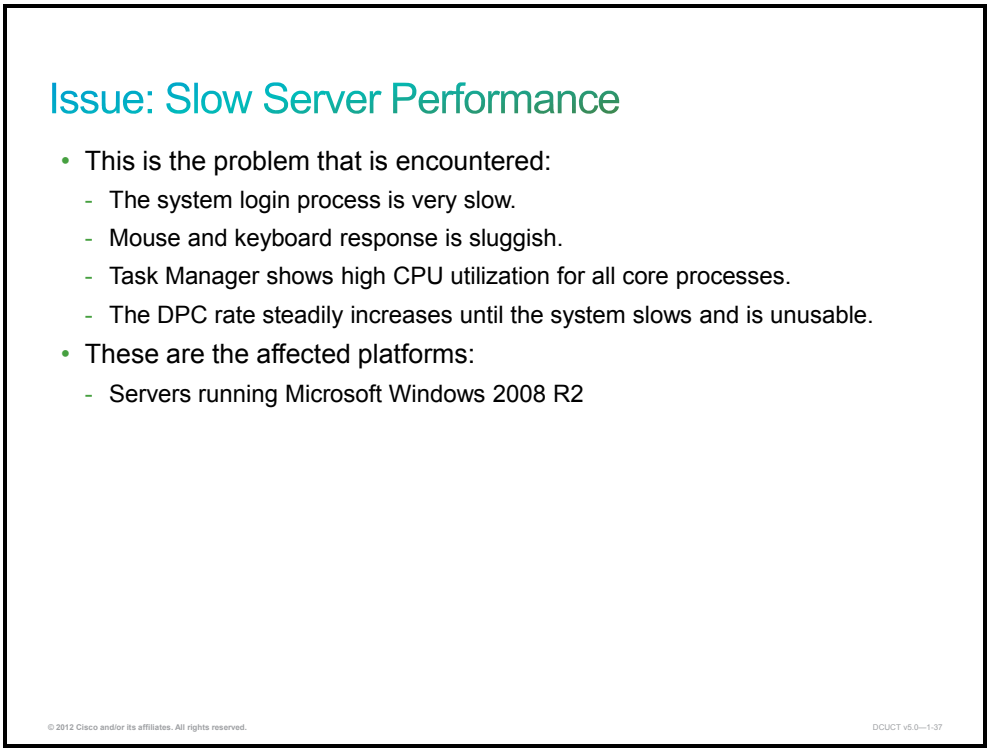
These downloads are currently available here:

http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821

Each download is an ISO that uses suitable mounting as a virtual DVD to update drivers to the operating system as needed. Administrators should keep a copy of the drivers on a local laptop and other ISO files handy for updates to system drivers as needed.

Ensure that you have the ISO version that matches the Cisco UCS Manager version that is deployed to the Fabric Interconnect.

https://t.me/learningnets



In this troubleshooting scenario, you are faced with the performance degradation of servers that are running Microsoft Windows 2008 R2.

There are several aspects to the problem:

- The system login process is very slow.
- The keyboard and mouse response is sluggish.
- Task Manager shows high utilization for all CPU core processes.

When the ports are not electrically “linked” and the embedded driver is loaded, the Deferred Procedure Calls (DPCs) rate steadily increases until the system slows and is unusable.

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

Data Gathering (Slow Server Performance)

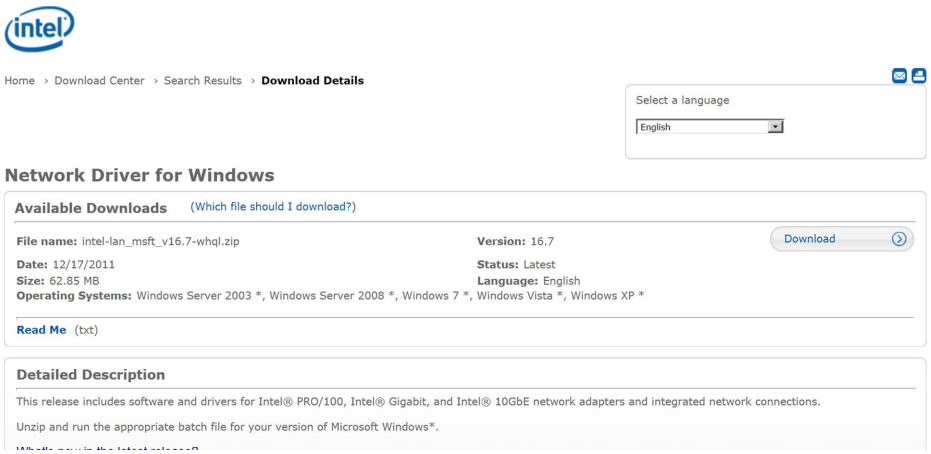
- A search in the documentation reveals the following:
  - There is a known issue with the Intel 82576 driver that is included with Microsoft Windows 2008 R2.

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

In the data gathering phase, you tried to investigate the issue on the server, but no specific results could be obtained. Then you searched for appropriate problem descriptions and found that there is a known issue with the Intel 82576 driver that is included with Microsoft Windows 2008 R2.

Remediation (Slow Server Performance)

- Download and install the latest driver.



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

To remediate the problem, you download the latest driver, install it, and verify that the performance has significantly improved.

https://t.me/learningnets

Issue: Microsoft Windows 2008 R2 Install Failure

- You encounter this symptom:
  - Microsoft Windows 2008 R2 installation is not starting.
- In the data gathering phase, you discover the following:
  - The system is not seeing the virtual installation CD on the server.
  - Outdated drivers cannot be ruled out as the reason for this problem.

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

In this troubleshooting scenario, you are confronted with a failure of a Microsoft Windows 2008 R2 operating system installation.

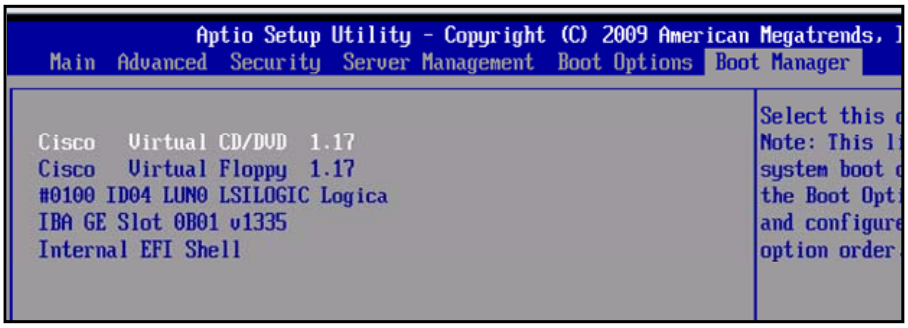
The data gathering phase reveals that the virtual installation CD is not visible on server.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Remediation (Windows Install Failure)

- Make sure that the virtual DVD or CD is mounted.
- Set the boot order in the BIOS so that the server boots from the virtual installation CD.
- Check that the virtual DVD or CD is not corrupted.



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

There are several potential reasons why installation of the operating system is not visible by the boot process:

- The virtual DVD or CD is not mounted.
- The boot order in the BIOS is not correct. Another boot drive has priority.
- The virtual DVD is corrupted.

To remediate the problem, ensure that the virtual DVD or CD is mounted, set the boot order in the BIOS so that the server boots from the virtual installation CD, and check that the virtual DVD or CD is not corrupted.

https://t.me/learningnets

Remediation (Windows Install Failure) (Cont.)

- Download and install required drivers, if necessary.
- Drivers are available at multiple URLs, including here:
  - http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/b/os/windows/install/drivers-app.html

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

Another possible reason for the failure is that the DVD does not have the correct drivers when using slipstreamed operating system builds.

To remediate this issue, download and install the required drivers.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

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

Summary

- Depending on the server model and needs, different power requirements and redundancy modes exist and can be configured.
- Cisco UCS Manager provides a single point of device management for adapters, blades, chassis, and LAN and SAN connectivity.
- Server administration requires access to the BIOS when you configure the server to boot from specific devices, change the onboard RAID configuration, or view the boot options.
- Drivers are included on the Cisco UCS B-Series Drivers DVD and are also provided on Cisco.com.

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

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 4

Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity

Overview

Cisco Unified Computing System (Cisco UCS) components operate in a switched environment where various protocols interoperate to provide optimal system performance. LAN and SAN services are provided over a converged infrastructure. This lesson reviews the major LAN and SAN operation principles of the Cisco UCS B-Series and provides troubleshooting guidance for various problem scenarios.

Objectives

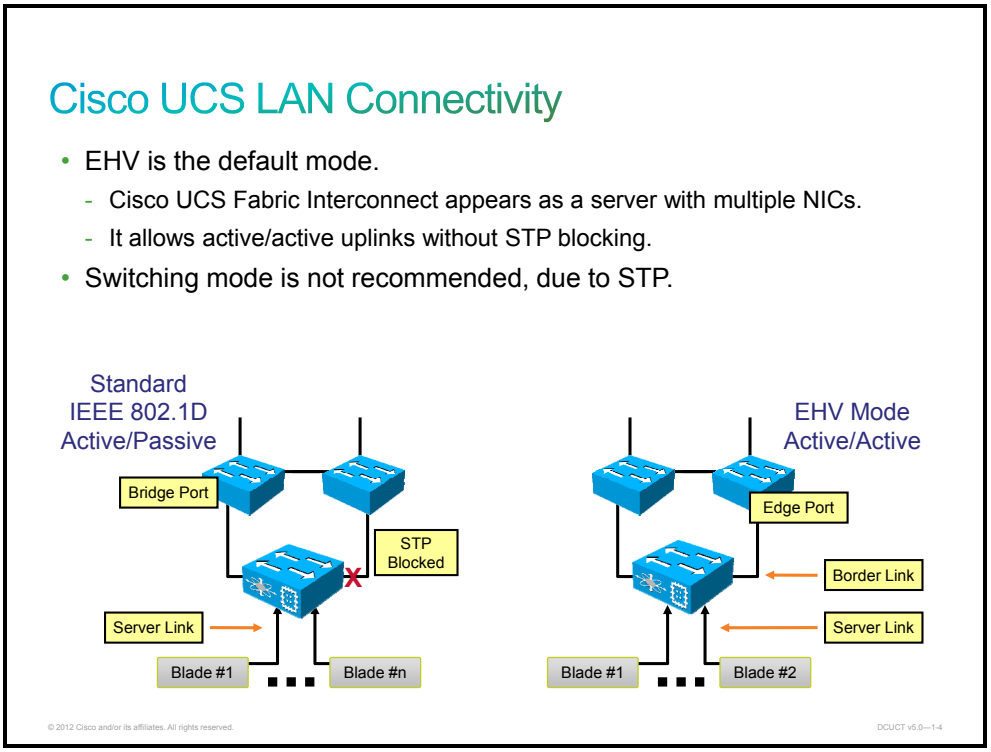
Upon completing this lesson, you will be able to explain LAN, SAN and Fibre Channel operations, including in-depth troubleshooting procedures. This ability includes being able to meet these objectives:

- Recognize Cisco UCS B-Series LAN connectivity
- Troubleshoot Cisco UCS B-Series LAN connectivity
- Troubleshoot Cisco UCS B-Series server redundant connectivity
- Recognize Cisco UCS B-Series SAN connectivity
- Troubleshoot Cisco UCS B-Series SAN connectivity
- Troubleshoot Cisco UCS B-Series SAN boot
- Troubleshoot Cisco UCS B-Series traffic using SPAN
- Troubleshoot Cisco UCS server to fabric packet flow using the GUI or CLI
- Troubleshoot Cisco UCS B-Series integration with the server virtualization platform

https://t.me/learningnets

Cisco UCS B-Series LAN Connectivity

This topic describes Cisco UCS B-Series system LAN connectivity.



The Cisco UCS Fabric Interconnect operates in Ethernet Host Virtualizer (EHV) mode by default, which is also known as “End Host Virtualization.” In EHV mode, Cisco UCS appears, to an external LAN, as an end station with multiple adapters.

There are two types of links in EHV operational mode:

- Server links
- Border links

Border links are Cisco UCS uplinks and can be in the form of a single link or aggregated in a channel. When operating in EHV operational mode, the Cisco UCS Fabric Interconnect does not participate in a Spanning Tree Protocol (STP) topology. Instead, the following is used to achieve a loop-free topology:

- Border links must connect to the Layer 2 network.
- Traffic forwarding between border links is denied.

The benefit of running the Cisco UCS Fabric Interconnect in EHV mode is that the LAN STP topology is simplified and the size of the STP domain is reduced. Additionally, because no links are blocked by STP, the active/active approach uses all redundant links to a Layer 2 network.

In a normal LAN topology, STP takes care of the loops. It does so by disabling some of the links; therefore, the underlying network infrastructure is not fully utilized.

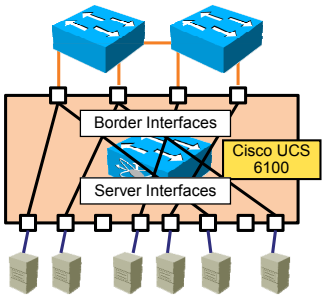
If desired, the Fabric Interconnects can be set to operate in traditional Ethernet switching mode. This introduces the need for STP to avoid broadcast loops. Not all standard Cisco switch options are available in this mode. This deployment method is not typically recommended.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Ethernet Host Virtualizer

- Server interface pinned to border interface:
  - Server-to-network traffic follows pinned uplink.
  - Server-to-server traffic is locally switched.
  - Network-to-server traffic is forwarded to the server if it arrives on a pinned uplink.
  - Server traffic on any uplink, except a pinned uplink, is dropped.



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

In EHV mode, each server link is pinned to one border link. The pinning logic equally distributes server links to various border links.

The server-to-server traffic is locally switched, while server-to-network traffic goes out on the pinned border link. To achieve local switching, the MAC addresses within the chassis are learned.

Network-to-server unicast traffic is forwarded to the server only if it arrives on a pinned border link. A Reverse Path Forwarding (RPF) check is performed as verification. Server traffic that is received on any border link except a pinned border link is dropped (as part of the déjà vu check).

MAC address learning in EHV mode is as follows:

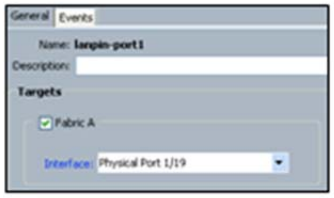
- Learning is disabled on border links. Network MAC addresses are never learned.
- Learning is enabled on server links. Traffic to the server is forwarded based on the destination MAC address.

Learned MAC addresses never age unless the server link goes down or is deleted, in which case server MAC addresses can move (in the event of re-pinning).

https://t.me/learningnets

LAN Pinning

- To identify a specific uplink port or port channel on one or both Fabric Interconnects
- Administrative pinning—using pin groups
  - Pin traffic from the specific blade network adapter to specific uplinks with the service profile.
  - Must use this when LAN uplinks are on different Layer 2 domains.
- Dynamic pinning (default)—not using pin groups
  - Cisco UCS automatically chooses the uplink for the adapter.
  - It could choose incorrectly if LAN uplinks are on different Layer 2 domains.



Cisco UCS allows the use of a mechanism called “pin group.”

With this mechanism, traffic from a specific blade server adapter is tied to a particular uplink port or port channel on each Fabric Interconnect. This is achieved via the service profile configuration.

If pin groups are not used in service profiles, Cisco UCS automatically chooses an uplink port or port channel for the adapter on the blade that is associated with each profile.

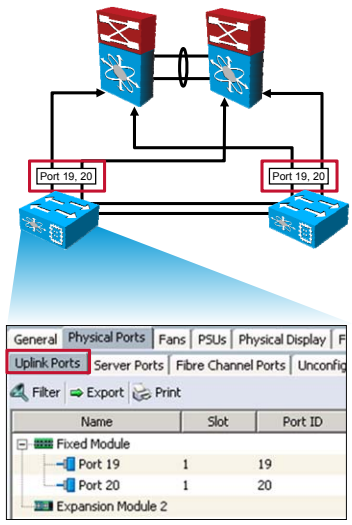
If you need to force a specific blade to use a specific uplink port, the pin group can be used to achieve that when applied via the service profile. This might be necessary when the uplinks are connected to different Layer 2 domains (VLANs). If left to the default, Cisco UCS Manager does not know the correct uplink for the specific blade.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

LAN Connectivity—Uplink Ports

- Connectivity to external LAN devices:
  - Carries Ethernet traffic only
  - Uplink port allowed VLAN list adjusted automatically per configuration
  - Uplink switch must trunk all VLANs that are used in service profiles on that interface
- Port channel can scale bandwidth:
  - Must match uplink switch configuration
- Uplink ports in EHV mode:
  - Appear to be host with many MAC addresses
- Uplink ports in switching mode:
  - Appear to be Ethernet switch



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

Uplink ports in Cisco UCS are the physical ports on the Fabric Interconnects that are dedicated for the connectivity to a LAN device that is external to Cisco UCS (such as for the connectivity to Cisco Nexus 7000).

These ports can be either from the fixed port range or from the expansion module, if present.

The ports only carry VLAN traffic and are configured as IEEE 802.1Q trunk ports to carry VLAN traffic for all the VLANs that are used in the service profiles for a particular fabric. The allowed VLAN list is adjusted automatically based on the Cisco UCS VLAN configuration.

Depending on the Cisco UCS configuration, an uplink port carries VLANs that belong to the fabric it is part of (A or B) and those VLANs that are not fabric-dependent. (The VLANs are defined globally in the LAN cloud.)

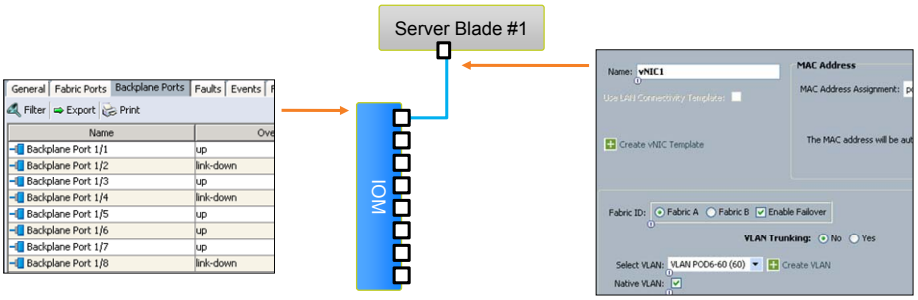
Uplink port bandwidth can be scaled using port channels, which use Link Aggregation Control Protocol (LACP) 802.3ad. The configuration of the port channel must match the other side. (VLANs being trunked must be the same.)

The port channel can be configured using uplink ports from a single Cisco UCS 6100XP Fabric Interconnect in a cluster, that is, from the same fabric.

https://t.me/learningnets

LAN Connectivity—Server Ports

- Server blade to IOM connectivity—vNIC
  - Configured via associated service profile only (no direct configuration of a physical server port)
  - Attributes: VLAN, trunking characteristics, and redundancy settings
  - Native VLAN: Traffic sent untagged



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

The communication between the server blade and the I/O module (IOM) is governed by the service profile configuration. This configuration includes virtual network interface cards (vNICs), which define how the server connects to the LAN network.

A vNIC has various parameters. Some of its more important parameters are VLAN trunking characteristics (trunk versus non-trunk interface) and redundancy settings, which define whether, upon primary fabric failure, the communication fails over to the second fabric (such as from Fabric A to Fabric B or vice versa).

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Server Port—vNIC

- Cisco UCS VIC M81KR adapter:
  - NIC virtualization supports multiple vNIC creation
  - Fabric A or B with failover
  - Number of vNICs depends on the IOM-Fabric Interconnect uplinks

1 x IOM, 8 x Server Blades

Uplinks	vNICs per Adapter
1	13
2	28
4	58

2 x IOM, 8 x Server Blades

Uplinks	vNICs per Adapter
1	26
2	56
4	116

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

You can create up to two vNICs using either Cisco UCS VIC M81KR or Cisco UCS 82598KR-CI adapters.

With Cisco UCS 82598KR-CI, you must match the physical setting (the first adapter goes to Fabric A, the second adapter goes to Fabric B), and you cannot choose to fail over.

The Cisco UCS M81KR Virtual Interface Card (VIC) supports network interface card (NIC) virtualization either for a single operating system or for VMware vSphere. The number of virtual interfaces that are supported on an adapter depends on the number of uplinks between the IOM and the Fabric Interconnect, as well as the number of interfaces that are in use on other adapters that share the same uplinks.

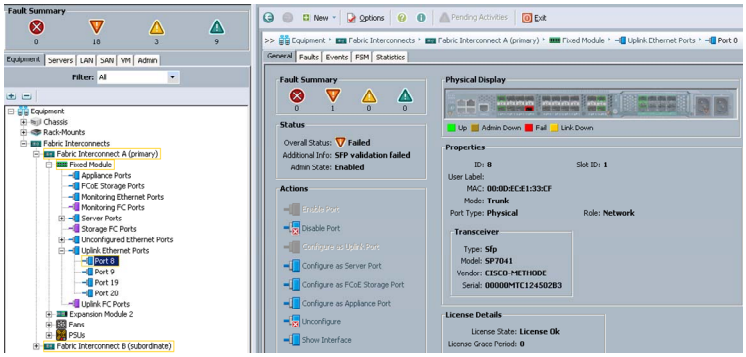
https://t.me/learningnets

Cisco UCS B-Series LAN Connectivity Troubleshooting

This topic describes how to troubleshoot Cisco UCS B-Series system LAN connectivity.

Issue: Failed Uplink

- You encounter this symptom:
  - Failed uplink from Fabric Interconnect to upstream LAN switch
  - Connectivity broken when other uplinks are also down



Equipment > Fabric Interconnects > (Fabric Interconnect A/B) > (Module) > Uplink Ethernet Ports

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

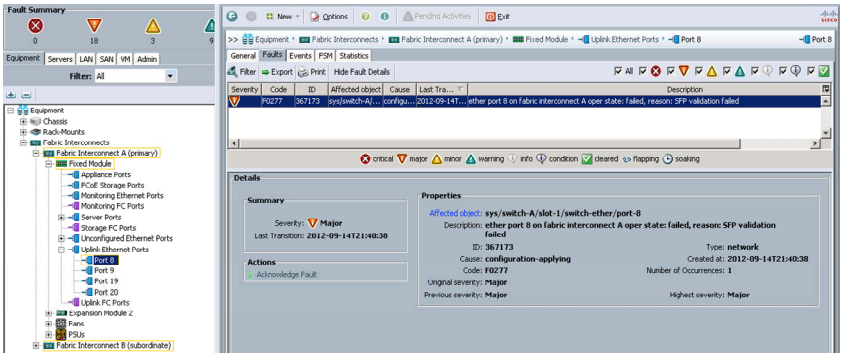
In this LAN troubleshooting scenario, you are faced with the problem of a failed uplink from the Fabric Interconnect to the upstream LAN switch.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Data Gathering: Cisco UCS Manager Faults

- The Faults tab provides a reason description: “SFP validation failed”
- Fault reported with severity “Major”



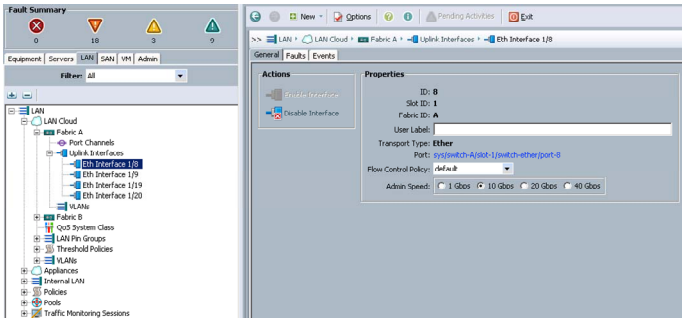
Equipment > Fabric Interconnects > (Fabric Interconnect A/B) > (Module) > Uplink Ethernet Ports

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

In the data gathering phase, you look for hints that are provided by the Cisco UCS Manager embedded tools. The information that is displayed in the Faults tab is useful. In this case, a fault is logged as “SFP validation failed.”

Data Gathering: Cisco UCS Settings

- The faulty uplink is Ethernet 1/8.
- In Cisco UCS Manager, the interface is as follows:
  - Enabled
  - Configured with default control policy
  - Admin Speed set to 10 Gb/s



LAN > LAN Cloud > Uplink Interfaces

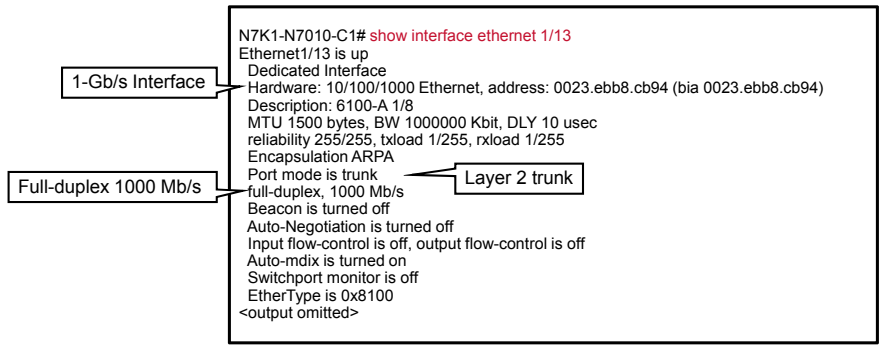
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, you verify the uplink configuration in Cisco UCS Manager. You check the configuration for the Ethernet 1/8 interface, which is the faulty uplink that you are troubleshooting. You find that it is enabled, configured with the default control policy, and set with the interface speed of 10 Gb/s.

https://t.me/learningnets

Data Gathering: Upstream Switch Settings

- An examination of the topology shows that Ethernet 1/13 is the adjacent interface on the uplink switch.
- Verification of the interface settings shows the following:
  - 1-Gb/s interface
  - Layer 2 interface (trunk)
  - Full-duplex, 1-Gb/s speed



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

Next, you proceed to the interface verification on the upstream switch. The uplink is connected to port 1/13, as you found in the network topology data.

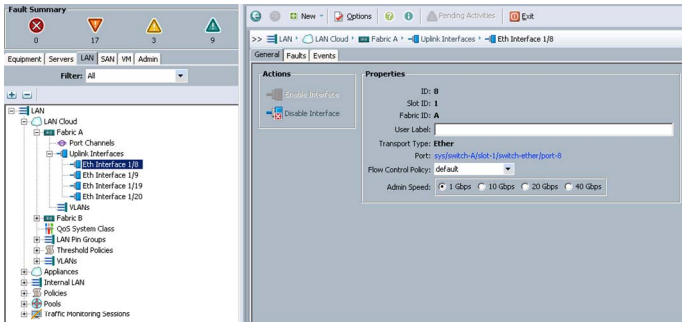
You find that the interface is a 1-Gb/s link that is configured as a Layer 2 interface, in trunking mode, and set to full-duplex communication at 1000 Mb/s.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Remediation

- Speed on the Fabric Interconnect must be downgraded:
  - Set Admin Speed to 1 Gbps
  - Match the upstream interface capabilities
- Other potential issue: The upstream switch interface is configured as a Layer 3 interface or Layer 2 access interface.



LAN > LAN Cloud > Uplink Interfaces

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

You found a mismatch between the interface speeds on each side of the uplink connection. Apart from the configuration settings, the small form-factor pluggable (SFP) and small form-factor pluggable plus (SFP+) hardware must also match (such as when 1-Gb/s Ethernet links are deployed, the 1-Gb/s Ethernet SFP must be used; for 10-Gb/s Ethernet, the 10-Gb/s SFP+ must be used; and so on).

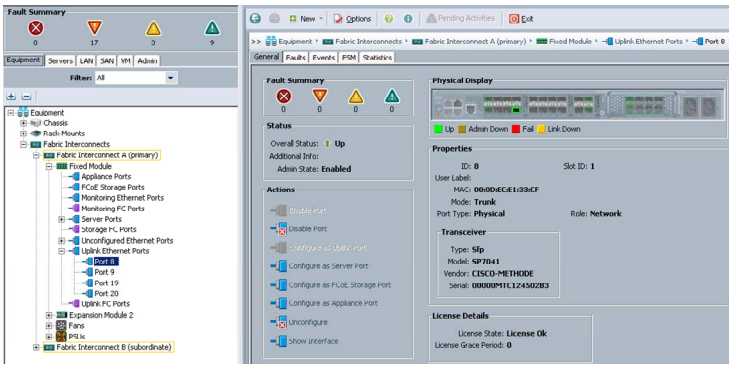
This fault represents one of the common problems that are related to the Layer 1 and Layer 2 functions of the Open Systems Interconnection (OSI) reference model resulting from the mismatch in Ethernet port settings on two adjacent devices. Such a mismatch can prevent or negatively affect Ethernet connectivity between the Fabric Interconnects and the uplink switches. The uplink ports on the Fabric Interconnect should match the settings on the uplink switches in terms of the port speed, duplex mode, Layer 2 port type, and port configured as trunk mode.

You remediate the problem by lowering the interface speed on the Fabric Interconnect, as shown in the figure.

https://t.me/learningnets

Verification

- Overall status: “Up”
- Connectivity can be verified using other methods, such as **ping**.



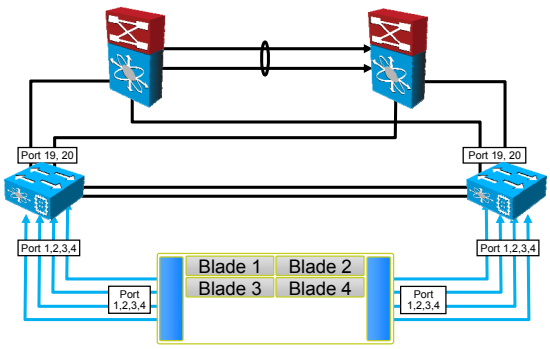
Equipment > Fabric Interconnects > (Fabric Interconnect A/B) > (Module) > Uplink Ethernet Ports

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

After adjusting the interface speed, you can verify that the overall interface status is “UP.” You can also verify, by looking at the interface counters, that the uplink is forwarding traffic, but this is not shown here.

Issue: Broken Network Connectivity for Some Servers

- Some servers do not have network connectivity.
- Other servers in the same chassis have operational network connectivity.



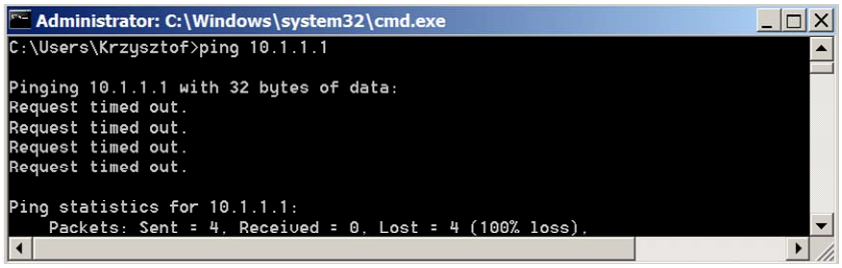
© 2012 Cisco and/or its affiliates. All rights reserved.

In the second LAN troubleshooting scenario, you manage some servers that do not have operational network connectivity, while other servers in the same system do have connectivity. Physical connectivity issues can probably be ruled out, because other servers in the same chassis obtain IP addresses correctly.

https://t.me/learningnets

Data Gathering: Testing IP Connectivity

- First, verify IP connectivity.
- Connectivity to the default gateway does not work.

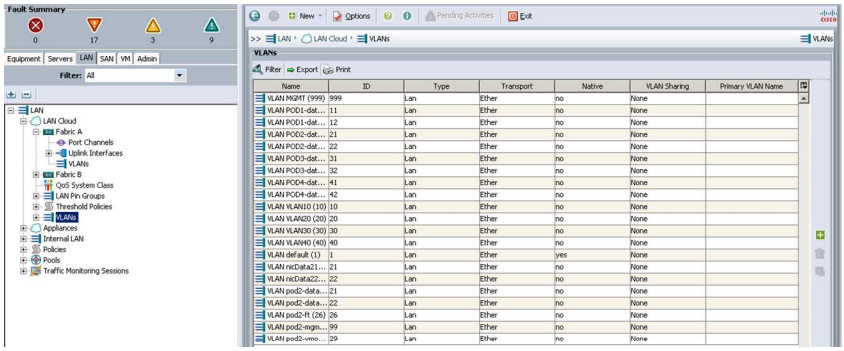


© 2012 Cisco and/or its affiliates. All rights reserved.

First you want to verify if the problem is related specifically to IP connectivity. For that purpose, you use **ping** and **traceroute** to check the IP connectivity. Among other ping checks, you try to ping the default gateway. The ping fails. You are facing a connectivity problem that is manifesting within an IP subnet (that is, this is not an IP routing problem).

Data Gathering: VLANs on Fabric Interconnect

- View the VLANs that are configured on the Fabric Interconnect.
- All existing VLANs are automatically trunked on the uplinks.
- Problematic VLANs are numbered, among others, 30 and 40.



LAN > LAN Cloud > VLANs

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

Next, you verify the VLANs that have been configured on the Fabric Interconnect. You already checked the VLANs to which the servers are connected. The problematic VLANs are numbered, among others, 30 and 40.

https://t.me/learningnets

Data Gathering: VLANs on Upstream Switch

- View the VLANs that are configured on the upstream LAN switch.
- You find all the necessary VLANs. (Not all are shown here.)

```
N7K1-N7010-C1# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Po1, Po100, Po101, Po200, Po201
                                                Eth1/13, Eth1/14, Eth1/24
                                                Eth2/9, Eth2/10, Eth2/11
                                                Eth2/12, Eth2/15, Eth2/16
10   VLAN0010                         active    Po1, Po100, Po101, Po200, Po201
                                                Eth1/13, Eth1/14, Eth2/9
                                                Eth2/10, Eth2/11, Eth2/12
                                                Eth2/15, Eth2/16
11   POD1-data1                       active    Po1, Po100, Po101, Po200, Po201
                                                Eth1/13, Eth1/14, Eth2/9
                                                Eth2/10, Eth2/11, Eth2/12
12   POD1-data2                       active    Po1, Po100, Po101, Po200, Po201
                                                Eth1/13, Eth1/14, Eth2/9
                                                Eth2/10, Eth2/11, Eth2/12
17   POD1-packet                      active    Po1, Po100, Po101, Po200, Po201
                                                Eth1/13, Eth1/14, Eth2/9
                                                Eth2/10, Eth2/11, Eth2/12
18   POD1-control                     active    Po1, Po100, Po101, Po200, Po201
                                                Eth1/13, Eth1/14, Eth2/9
                                                Eth2/10, Eth2/11, Eth2/12
<output omitted>
```

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

Then you verify the VLANs that are configured on the upstream switch. You do not find any inconsistencies with the Fabric Interconnect configuration. The command output in the figure is truncated, and therefore does not show VLANs 30, 40, and others.

Data Gathering: Trunk Parameters

- Verify the trunking parameters on the link to the Fabric Interconnect.
- Interface Eth1/13 connects to the Fabric Interconnect.

```
N7K1-N7010-C1# show interface trunk

--------------------------------------------------------------------------------
Port         Native  Status        Port
             Vlan                  Channel
--------------------------------------------------------------------------------
Eth1/13      1       trunking      --
Eth1/14      1       trunking      --
Eth1/24      1       trunking      --
Eth 2/9      1       trunking      --
Eth2/10      1       trunking      --
--------------------------------------------------------------------------------
Port         Vlans Allowed on Trunk
--------------------------------------------------------------------------------
Eth1/13      1-20
Eth1/14      1-418
Eth1/24      1,99,999
Eth2/9       1-4094
Eth2/10      1-4094
--------------------------------------------------------------------------------
Port         Vlans Err-disabled on Trunk
--------------------------------------------------------------------------------
Eth1/13      none
Eth1/14      none
Eth1/24      none
<output omitted>
```

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

Next, you verify the trunk parameters that are configured on the upstream switch. Most importantly, you pay attention to the configuration of the Ethernet 1/13 interface, which connects to the Fabric Interconnect.

https://t.me/learningnets

Remediation

- Allow all required VLANs to be transported over the trunk.
- In this case, the sufficient range is 1-999.
- Narrow down the ranges for increased security.

```
N7K1-N7010-C1(config)# interface eth 1/13

N7K1-N7010-C1(config-if)# switchport trunk allowed vlan add  30, 40
N7K1-N7010-C1(config-if)# end
```

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

Now you can pinpoint the problem and remediate it. You must allow additional VLANs on the interface that connects to the Fabric Interconnect. This figure illustrates how to allow the additional necessary VLANs 30 and 40 and narrow the allowed VLAN range to include necessary ones only.

Verification

- The required VLAN range is now allowed over the trunk.
- The hosts can connect to their default gateways and beyond.

```
N7K1-N7010-C1# show interface trunk

--------------------------------------------------------------------------------
Port         Native  Status        Port
             Vlan                  Channel
--------------------------------------------------------------------------------
Eth1/13      1       trunking      --
Eth1/14      1       trunking      --
Eth1/24      1       trunking      --
Eth2/9       1       trunking      --
Eth2/10      1       trunking      --
Eth2/11      1       trunking      --
Eth2/12      1       trunking      --
Eth2/15      1       trunking      --
--------------------------------------------------------------------------------
Port         Vlans Allowed on Trunk
--------------------------------------------------------------------------------
Eth1/13      1-999
Eth1/14      1-418
Eth1/24      1,99,999
```

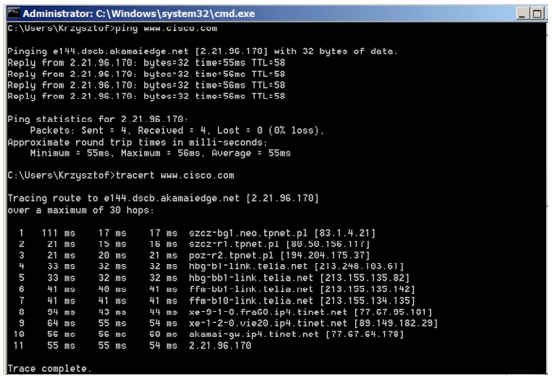
© 2012 Cisco and/or its affiliates. All rights reserved.

To verify the solution, you check the trunking parameters and see that all of the required VLANs are transported over Ethernet 1/13. Then you check that the hosts can now successfully obtain IP addresses and connect to their default gateways.

https://t.me/learningnets

Issue: Intermittent Connectivity

- You encounter this symptom:
  - There is intermittent connectivity.
  - Only some applications seem to be affected.
  - VoIP, for example, is not affected.
- Common connectivity checks do not report any problems.

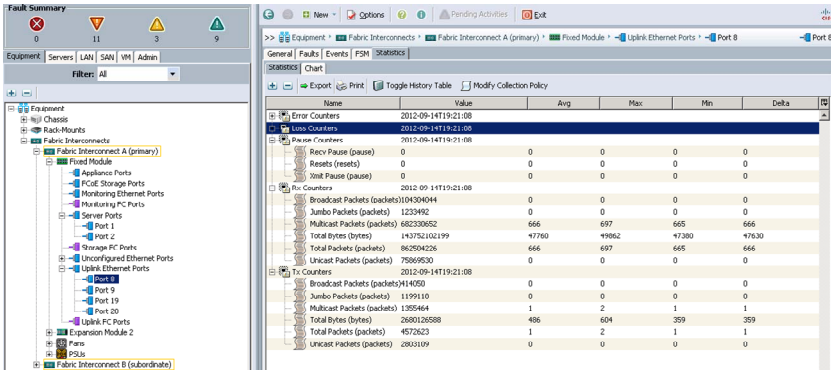


© 2012 Cisco and/or its affiliates. All rights reserved.

In the third LAN troubleshooting scenario, you are faced with reports from users who complain about intermittent connectivity problems. The problem is related to only some applications. VoIP communication, for example, does not experience any problems.

Data Gathering: Interface Counters

- Cisco UCS allows you to view interface statistics for these ports:
  - Server ports
  - Uplink Ethernet ports
- Check the counters for a problem indication.



Equipment > Chassis > Chassis-name > Power Control Monitor

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

In this situation, you decide to start gathering additional information by checking the interface counters. You do not find sufficient information to identify the problem.

https://t.me/learningnets

Data Gathering: Ping with Large Packets

- This is a method to test connectivity with large packet sizes.
- Set the DF bit.
- Large packets are dropped.

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t              Ping the specified host until stopped.
                    To see statistics and continue - type Control-Break;
                    To stop - type Control-C.
    -a              Resolve addresses to hostnames.
    -n count        Number of echo requests to send.
    -l size         Send buffer size.
    -f              Set Don't Fragment flag in packet (IPv4-only).
    -i TTL          Time To Live.
    -v TOS          Type Of Service (IPv4-only. This setting has been deprecated
                    and has no effect on the type of service field in the IP Header).
    -r count        Record route for count hops (IPv4-only).
    -s count        Timestamp for count hops (IPv4-only).
    -j host-list    Loose source route along host-list (IPv4-only).
    -k host-list    Strict source route along host-list (IPv4-only).
    -w timeout      Timeout in milliseconds to wait for each reply.
    -R              Use routing header to test reverse route also (IPv6-only).
    -S srcaddr      Source address to use.
    -4              Force using IPv4.
    -6              Force using IPv6.


C:\Users\Krzysztof>ping 192.168.1.1 -l 8000 -f

Pinging 192.168.1.1 with 8000 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

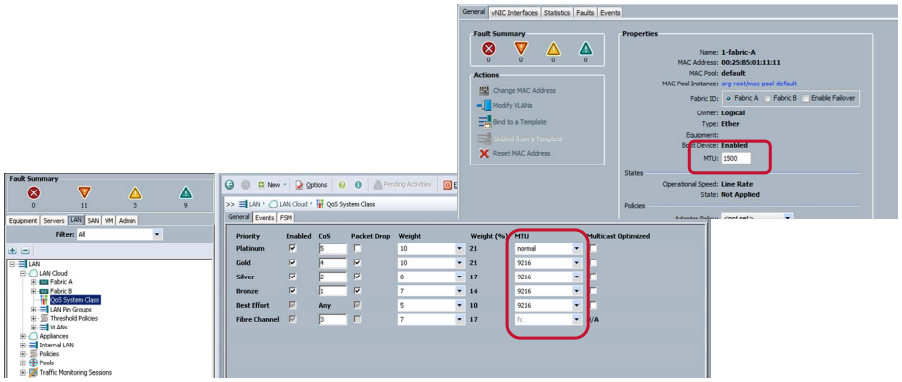
In the process of troubleshooting, you begin to suspect issues with large frame sizes and use the extended **ping** command to identify the problem. The large frames that are marked with the Don't Fragment (DF) bit do not go through.

One of the common causes of intermittent communication problems is related to the maximum transmission unit (MTU) sizes and support for jumbo frames. Jumbo frames are frames whose MTU exceeds the default value of 1500 bytes. The MTU problems occur if the jumbo frames are not supported on some links in the switched environment and are dropped on those ports.

https://t.me/learningnets

Remediation

- Enable jumbo frames in Cisco UCS Manager in the QoS system class.
- The MTU is set on a per-CoS basis.
- The supported MTU size is between 1500 (default) and 9216.
- When there is no QoS policy for the vNIC that is going to the vSwitch, the traffic is “Best-Effort” class.



LAN > LAN Cloud > QoS System Class

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

To remediate the problem, you enable jumbo frames in Cisco UCS Manager.

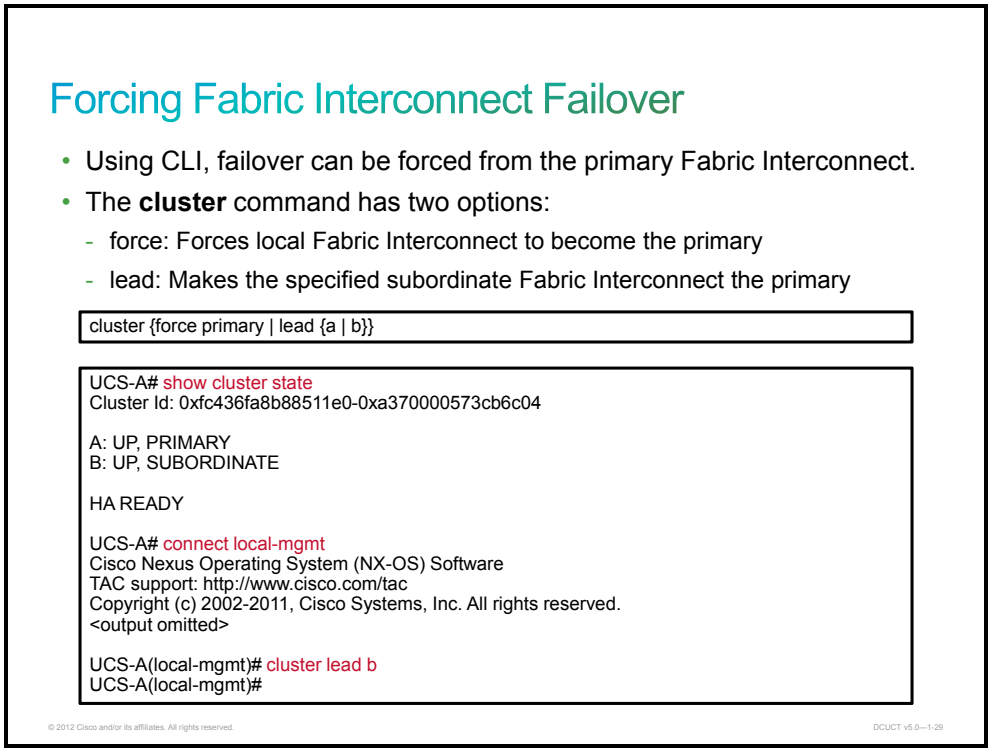
In Cisco UCS Manager, you enable jumbo frames in the quality of service (QoS) system class. The MTU is set on a per-class of service (CoS) basis. When there is no QoS policy for a particular vNIC that is going to the virtual switch (vSwitch), the traffic is classified as “Best-Effort.” Cisco UCS supports MTU sizes between 1500 (the default value for a vNIC MTU) and 9216.

Even when the system class for jumbo frames is enabled, the individual vNIC MTU settings override system class settings. To properly address this issue, the service profile and vNIC configuration must be verified and changed accordingly.

https://t.me/learningnets

Troubleshoot Redundant Connectivity

This topic describes how to troubleshoot Cisco UCS B-Series server redundant connectivity.



While troubleshooting or testing redundant connectivity, you can force a Fabric Interconnect failover. This operation can only be performed in the Cisco UCS Manager CLI. You must force the failover from the primary Fabric Interconnect, which is shown as “UCS-A” in this example.

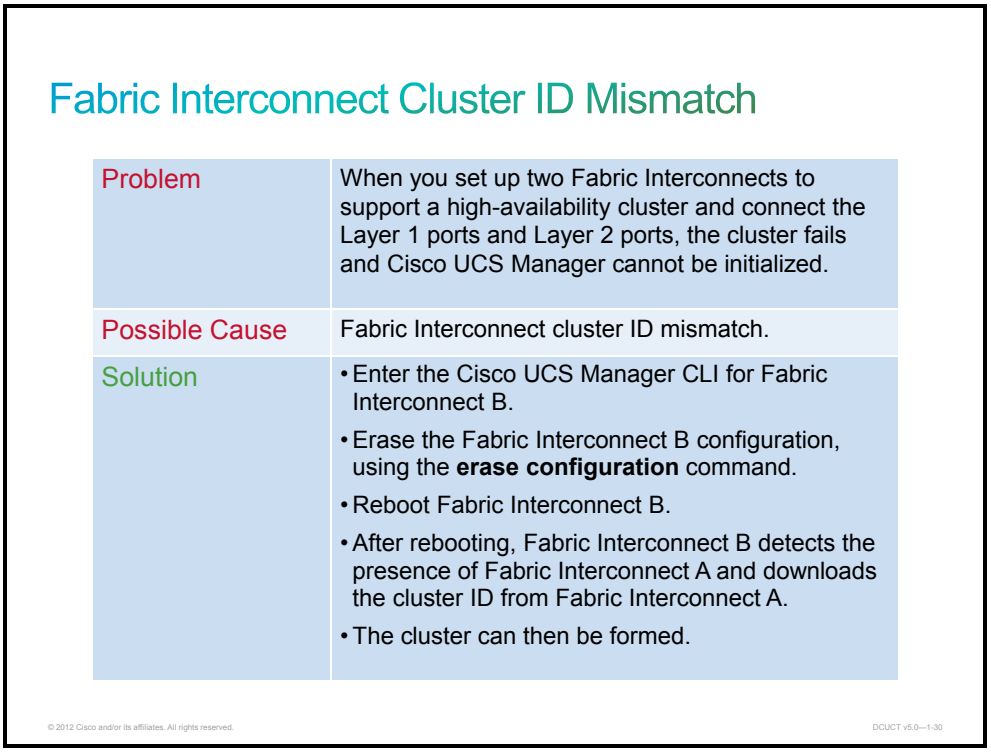
First you can use the **show cluster state** command to display the state of Fabric Interconnects in the cluster and whether the cluster is high-availability-ready. The output shown in this example indicates that both Fabric Interconnects are up, and that “A” is the primary interconnect.

Then you need to enter local management mode for the cluster. This is done with the **connect local-mgmt** command.

Finally, change the subordinate Fabric Interconnect to primary using the **cluster** command with one of the following options:

- **force:** Forces local Fabric Interconnect to become the primary
- **lead:** Makes the specified subordinate Fabric Interconnect the primary

https://t.me/learningnets



When you set up two Fabric Interconnects to support a high-availability cluster and connect the Layer 1 and Layer 2 ports, a Fabric Interconnect cluster ID mismatch can occur. This mismatch could occur if you are building a Cisco UCS cluster using previously deployed Fabric Interconnects (that is, Fabric Interconnects that were used somewhere else and did not have their configuration deleted). This type of mismatch means that the cluster fails and Cisco UCS Manager cannot be initialized.

To resolve a Fabric Interconnect cluster ID mismatch, follow these steps:

Step 1 In Cisco UCS Manager CLI, connect to Fabric Interconnect B and enter the **erase configuration** command. All configuration on the Fabric Interconnect is deleted.

Step 2 Reboot Fabric Interconnect B.

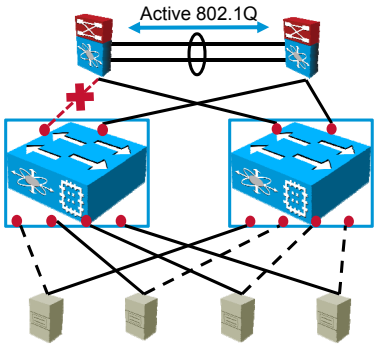
After rebooting, Fabric Interconnect B detects the presence of Fabric Interconnect A and downloads the cluster ID from Fabric Interconnect A. The cluster can then be formed.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Failover Does Not Work Upon Uplink Failure

Problem	Host loses connectivity to external networks when an uplink fails.
Possible Cause	Manual pinning on the Fabric Interconnect and hardware failover are disabled for the server vNIC.
Solution	Depending on the adapter, verify the configuration and either implement automatic pinning or enable hardware failover for the server vNIC.



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

You should have an effective high-availability solution to provide uninterrupted connectivity even if some uplinks fail. A potential problem can result from a suboptimal configuration that includes the following:

- Manual pinning on the Fabric Interconnect
- Hardware failover disabled for the server vNIC

In such a case, you need to verify the requirement and either implement automatic pinning or enable hardware failover for the server vNIC.

With automatic uplink pinning, a link failure causes all servers to be repinned to the remaining uplinks. In this 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.

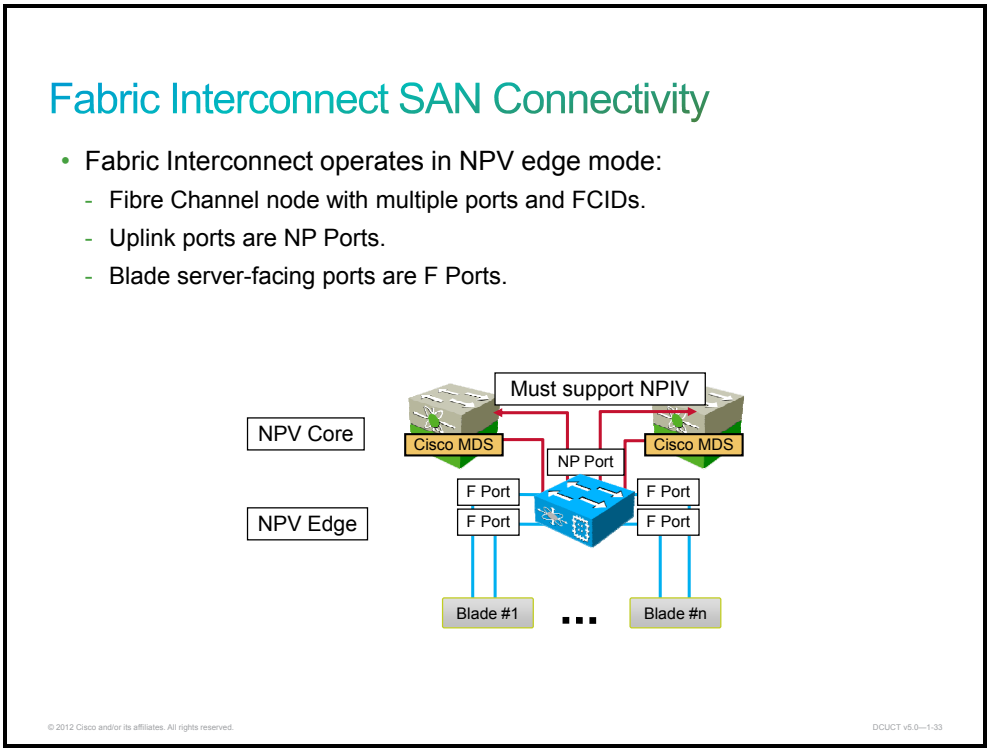
If all uplink ports on the Fabric Interconnect lose connectivity, the IOM instructs the I/O multiplexer (MUX) to shut down all eight of the host ports. The affected servers will use either NIC teaming or hardware failover to re-establish connectivity on Fabric B. If the servers are not configured for high availability in the operating system or service profile, the servers will be down until at least one uplink is restored on Fabric A.

With static pinning, when an uplink interface fails (Ethernet 1/9 in this example), the server fails over to the same 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

Cisco UCS B-Series SAN Connectivity

This topic describes Cisco UCS B-Series SAN connectivity.



The Cisco UCS Fabric Interconnects operate in the Cisco N-Port Virtualizer (Cisco NPV) edge mode.

The upstream Fibre Channel switch (for example, Cisco MDS) must therefore support and be enabled with the N-Port ID Virtualization (NPIV) feature, which allows multiple Fibre Channel IDs (FCIDs) to be assigned a single node port (N Port).

In the NPIV topology, there are two types of interfaces:

- **Server Interface:** The server-facing interface is either physical Fibre Channels or virtual Fibre Channel interfaces operating in fabric port (F Port) mode.
- **Border Interface:** Border interfaces are network-facing and always operate in N Port Proxy (NP Port) mode.

There is no local switching of the Fibre Channel traffic on the Cisco UCS 6100XP. All packets are forwarded to the Cisco NPV core switch.

Fabric login (FLOGI)-related processing is relayed in software (FLOGI, fabric discovery [FDISC], and corresponding LS_ACC, LS_RJT, and so on) to the same uplink interface.

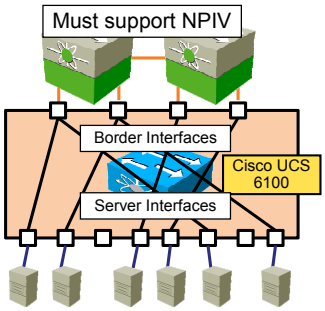
Every uplink can be connected to different Fibre Channel switches and virtual SANs (VSANs).

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco N-Port Virtualizer

- Each server interface is pinned to one border interface.
- Pinning logic distributes server interfaces between border interfaces (round robin).
- All traffic follows the pinned port.
- All traffic is passed to the upstream device for switching.
- Cisco NPV supports nested NPIV.



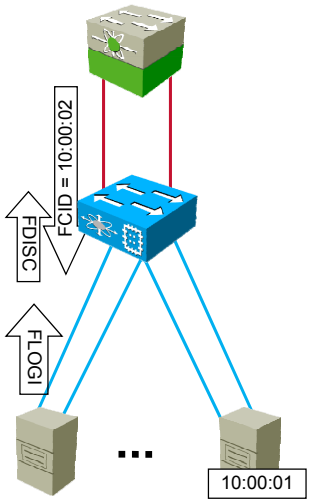
© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco UCS 6100XP in Cisco NPV edge mode pins each server link to one border link. The pinning logic load-balances server links to various border links while all traffic is forwarded to the upstream SAN device for switching.

https://t.me/learningnets

Pinning and Load Balancing

- Server interfaces are pinned to uplink interfaces (not FLOGI).
- Traffic on server interface:
  - Sent to the pinned interface
  - No forwarding lookup
    - NPV switch does not participate in FSPF
  - Binding check performed to verify frame source ID (SID) is on the right server interface
    - Prevent address spoofing
- Traffic on border interface:
  - Forwarding lookup is performed per frame destination ID (DID)
  - DID points to the server interface
  - Packets are discarded on miss



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

In Cisco NPV edge mode, each downstream device (server or blade server) is pinned to an uplink port based on a round-robin algorithm.

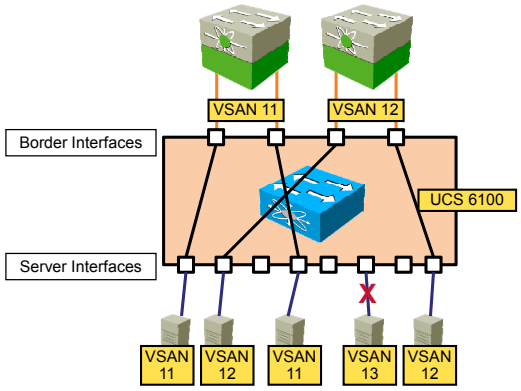
The Cisco UCS 6100XP switch in Cisco NPV edge mode no longer processes FLOGI login requests or makes routing decisions using Fabric Shortest Path First (FSPF). Instead, these operations are passed to the upstream switch that is known as the Cisco NPV core switch. The Cisco NPV core switch uses NPIV to interpret multiple logins from the same port.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Pinning with VSANs

- Pinning based on VSANs:
  - Server interface pinned to border interface with same VSAN
  - Server interface kept down if no interface with same VSAN available

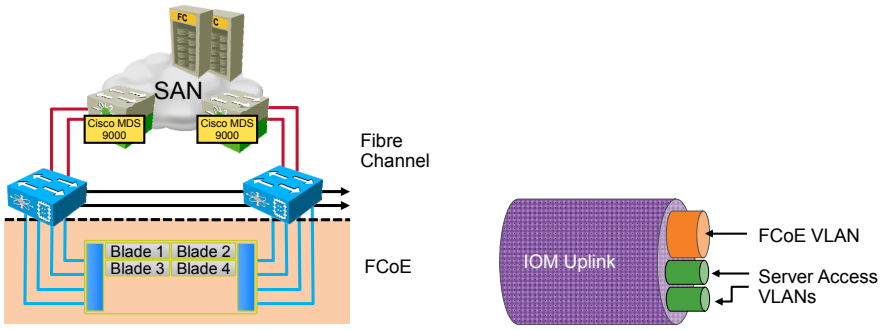


© 2012 Cisco and/or its affiliates. All rights reserved.

With VSANs, the Cisco NPV edge mode pinning also takes the uplink port VSAN into account. The server is pinned to an uplink port based on the uplink interface VSAN membership (still in a round-robin fashion).

SAN Connectivity—FCoE VLAN

- SAN traffic from servers carried via FCoE in dedicated VLANs
- Must not overlap the LAN VLANs



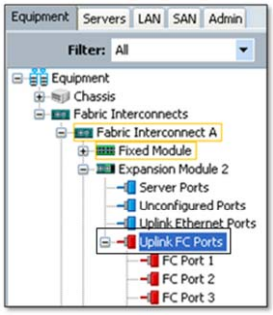
© 2012 Cisco and/or its affiliates. All rights reserved.

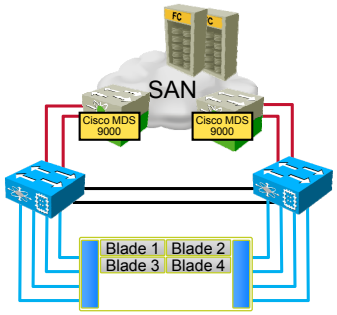
The Fibre Channel over Ethernet (FCoE) VLAN ID should not overlap with regular VLANs that are used for LAN connectivity.

https://t.me/learningnets

SAN Connectivity—Uplink Ports

- Connectivity to external SAN devices
  - Carries Fibre Channel traffic only
- Fibre Channel ports on expansion modules or Fibre Channel SFP in any unified port





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

Uplinks in Cisco UCS are physical Fibre Channel ports on the Fabric Interconnect expansion modules that are used for the connectivity to a SAN device that is external to Cisco UCS (such as for the connectivity to Cisco MDS 9000). A single port can carry traffic for one or multiple VSANs (such as the trunking expansion port [TE Port]).

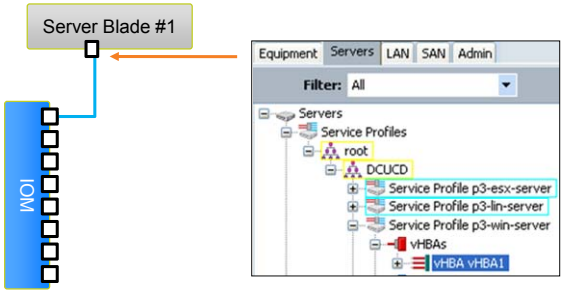
Depending of the Cisco UCS configuration, an uplink port carries VSANs that belong to the fabric to which it is part (A or B).

A single uplink port carries traffic for one or more VSANs, thus being connected to multiple logical fabrics, which are internally mapped to a VSAN number. The same Cisco UCS Fabric Interconnect can be connected via uplinks to multiple separate Fibre Channel fabrics without causing those fabrics to merge. All Fibre Channel services are kept isolated using VSANs and no Inter-VSAN Routing (IVR) is possible.

https://t.me/learningnets

SAN Connectivity—Server Ports

- Defined in a service profile with vHBA:
  - Assigned to a single VSAN
  - VSAN and properties assigned dynamically via the service profile
- VSAN used internally to isolate fabrics even if uplinks connected to switches other than Cisco MDS switches



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

A server SAN port is configured as a virtual host bus adapter (vHBA) that corresponds to a VSAN. The concept is similar to the one used in a LAN, for a VLAN and vNIC.

For the server to be connected to the SAN, the service profile must be configured with the vHBA, where a VSAN must be selected. A vHBA configuration is applied to the Fibre Channel interface on the physical blade when the service profile is associated with the blade server.

Before the VSAN is associated with the vHBA, it must be configured globally in Cisco UCS Manager.

VSANs are supported on Cisco MDS switches, but not by other vendors. Cisco UCS still internally uses VSANs to distinguish between the fabrics and isolates them.

https://t.me/learningnets

Troubleshoot Cisco UCS B-Series SAN Connectivity

This topic describes how to troubleshoot Cisco UCS B-Series SAN connectivity.

Issue: SAN Connectivity Failure

- Symptom: The blade server cannot connect to remote storage.
- The server that is experiencing the problem is installed in blade 2.

```
!!! Emulex OneConnect FCoE BIOS !!!, Version 4.01a0
Copyright (c) 1997-2010 Emulex. All rights reserved.

Press <Alt E> or <Ctrl E> to enter Emulex BIOS configuration
utility. Press <s> to skip Emulex BIOS

Installing Emulex BIOS ......
Bringing the Link up, Please wait...
Link Up  : Physical Link Established.
Bringing the Link up, Please wait...
Link Up  : Physical Link Established.
--Adapter 1 CNAM72KR-E:     S_ID:4D012D  PCI Bus, Device, Function (04,00,03)

--Adapter 2 CNAM72KR-E:     S_ID:53000F  PCI Bus, Device, Function (04,00,02)

Emulex FCoE BIOS is not installed!!!
```

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

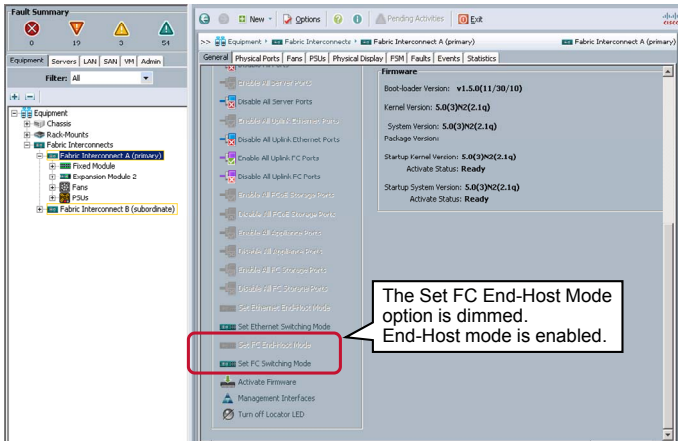
In this troubleshooting scenario, you need to resolve a SAN connectivity problem. The server in the second blade of the Cisco UCS chassis cannot connect to the remote storage.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Data Gathering: Fabric Interconnect Mode

- Verify the Fibre Channel operation mode on the Fabric Interconnects.
- The default mode is End-Host mode, synonymous with NPV.



Equipment > Fabric Interconnects > (Fabric Interconnect A/B) > General

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

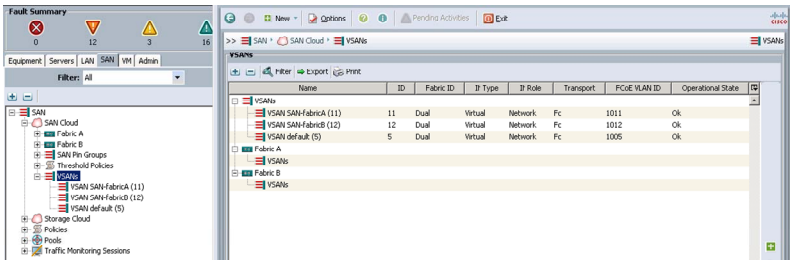
You start the data gathering phase by verifying the Fibre Channel mode in which the Fabric Interconnects operate. There are two options: end-host mode and switch mode. The default mode is end-host. It is synonymous with Cisco NPV mode.

In this case, you verify that both fabrics operate in end-host mode by examining the General tab of each fabric and seeing that “Set FC End-Host Mode” is dimmed, which means that it is activated. The figure shows the verification of Fabric Interconnect A. The second fabric is verified in the same way.

https://t.me/learningnets

Data Gathering: VSANs in Cisco UCS Manager

- Check the VSANs that are defined in Cisco UCS Manager.
- VSANs can be created for both fabrics, or only for a specific one.
- In this example, VSAN 11 is defined for both fabrics (dual-fabric ID).



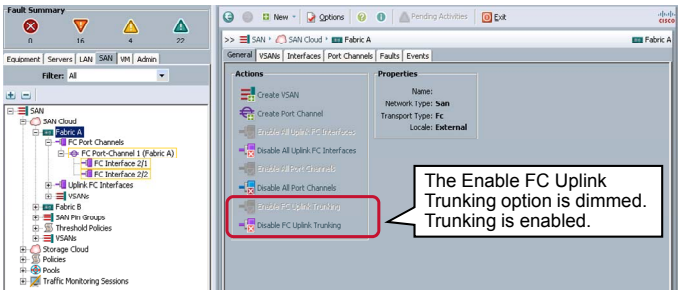
SAN > SAN Cloud > VSANs

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

Then you proceed to the verification of the VSANs that are defined in Cisco UCS Manager. The VSANs can have various scopes: both fabrics or only a specific fabric. In this case, you see that VSANs with IDs 11 and 12 have been configured as dual-fabric.

Data Gathering: Fibre Interconnect Uplinks

- Fibre Channel uplinks can be assigned to VSANs or enabled for trunking.
- If in trunking mode, all VSANs are carried to the Fibre Channel switch.
- In this example, both fabrics have “FC Uplink Trunking” enabled.



SAN > SAN Cloud > (Fabric A/B) > General

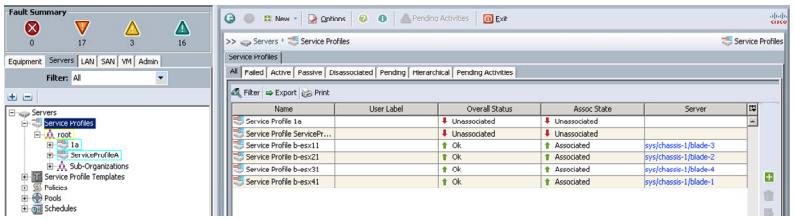
© 2012 Cisco and/or its affiliates. All rights reserved.

Then you examine the Fabric Interconnect “FC Uplinks.” They can be configured as trunk or non-trunk ports. If they were configured as non-trunk ports, you would need to check the pinning of the servers in the respective VSANs. In this scenario, the uplinks have been configured as trunk ports. With trunking, all defined VSANs are automatically transported to the upstream switch.

https://t.me/learningnets

Data Gathering: Service Profile Associations

- Check the service profile association for your blade server.
- Blade 2, in this example, is associated with profile b-esx21.
- Examine this profile to verify the WWPNs that are assigned to the vHBAs.



Servers > Service Profiles > Work pane > All

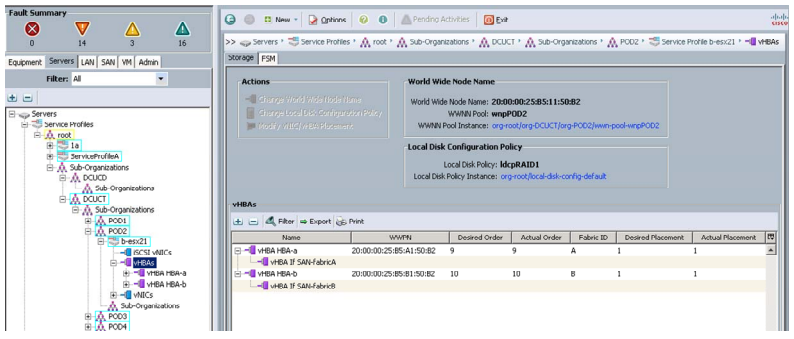
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, you check the service profile association with the server that is experiencing the connectivity problem. The associated service profile provides information on the world wide port names (WWPNs) that are assigned to the virtual adapters.

In this case, you find that the service profile “b-esx21” is associated with the server in slot 2.

Data Gathering: WWPNs on vHBAs

- In the service profile, check the WWPN that is assigned to the vHBAs.
- Look for this WWPN when verifying the databases on the core switch.



Servers > Service Profiles > (Organization path) > (Profile-name) > vHBAs

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

Having identified the appropriate service profile, you can establish the WWPNs that are assigned to the vHBAs. You will use this information when analyzing various databases on the Fibre Channel core switch.

https://t.me/learningnets

Data Gathering: Databases on Core Switch

```
mds# show flogi database
--------------------------------------------------------------------------------
INTERFACE     VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc1/1           11     0xdf0000  20:41:00:0d:ec:b4:45:40 20:02:00:0d:ec:b4:45:41
fc1/1           11     0xdf0001  20:00:00:25:b5:a1:50:b2 20:00:00:00:c9:85:1e:0c
fc1/1           11     0xdf0002  10:00:00:00:c9:85:02:68 20:00:00:00:c9:85:02:68
fc1/2           11     0xdf0100  20:42:00:0d:ec:b4:45:40 20:02:00:0d:ec:b4:45:41
fc1/3           11     0xdf0200  50:06:01:60:4b:a0:31:62 50:06:01:60:cb:a0:31:62
fc1/4           11     0xdf0300  50:06:01:68:4b:a0:31:62 50:06:01:60:cb:a0:31:62

Total number of flogi = 6.

mds# show fcns database

VSAN 11:
--------------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------------
0xdf0000    N     20:41:00:0d:ec:b4:45:40 (Cisco)         npv
0xdf0001    N     20:00:00:25:b5:a1:50:b2 (Emulex)        scsi-fcp
0xdf0002    N     10:00:00:00:c9:85:02:68 (Emulex)        scsi-fcp
0xdf0100    N     20:42:00:0d:ec:b4:45:40 (Cisco)         npv
0xdf0200    N     50:06:01:60:4b:a0:31:62 (Clariion)      scsi-fcp
0xdf0300    N     50:06:01:68:4b:a0:31:62 (Clariion)      scsi-fcp

Total number of entries = 6
```

WWPN of the blade server

WWPN of the blade server

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

Then you proceed to gather information from the Fibre Channel core switch. You can display a list of devices that are logged into the fabric using the **show flogi database** command. The **show fcns database vsan** command is used to display the name server database and statistical information for a specified VSAN.

You can verify that the WWPN of your servers and devices appear in both tables. Along with the WWPN addresses, you can see the FCID addresses that the devices were given by the fabric. This information is used to further explore the operation of the SAN.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Data Gathering: The fcping Command on the Core Switch

- The **fcping** utility allows you to verify connectivity:
  - To the blade server
  - To the storage devices

```
mds# fcping fcid 0xdf0001 vsan 11
28 bytes from  0xdf0001  time = 962 usec
28 bytes from  0xdf0001  time = 863 usec
28 bytes from  0xdf0001  time = 862 usec
28 bytes from  0xdf0001  time = 861 usec
28 bytes from  0xdf0001  time = 861 usec

5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 861/881/962 usec

mds# fcping fcid 0xdf0200 vsan 11
28 bytes from  0xdf0200  time = 893 usec
28 bytes from  0xdf0200  time = 867 usec
28 bytes from  0xdf0200  time = 862 usec
28 bytes from  0xdf0200  time = 865 usec
28 bytes from  0xdf0200  time = 857 usec

5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 857/868/893 usec
```

fcping to the blade server fcid

fcping to the storage device fcid

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

Once you have the FCID of the affected servers and devices, you can verify whether these devices are accessible in the fabric. On a Cisco MDS, you can use the **fcping** utility to verify connectivity to the server and to the storage devices.

Data Gathering: VSANs and Zones on Core Switch

- Check the VSANs, zones, and zone sets on the core switch.

```
mds# show vsan
vsan 11 information
         name:VSAN0011  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 12 information
         name:VSAN0012  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

mds# show zone
mds# show zoneset active
```

No zones have been configured.

No active zone sets.

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

Then you proceed to verify the VSANs, zones, and zone sets that are configured on the core switch. While the VSANs are configured correctly and their IDs match the VSANs that are defined in Cisco UCS Manager, the zone and zone set configuration is missing.

https://t.me/learningnets

Remediation: Zones and Zone Sets on Core Switch

- Add the missing zone and zone set configuration.
- Activate the zone set.
- Verify the results.

```
mds(config)# zone name GOLD vsan 11
mds(config-zone)# member pwwn 20:00:00:25:B5:A1:50:B2
mds(config-zone)# member pwwn 10:00:00:00:c9:85:02:68
mds(config-zone)# member pwwn 50:06:01:60:4b:a0:31:62
mds(config-zone)# member pwwn 50:06:01:68:4b:a0:31:62
mds(config-zone)# exit

mds(config)# zoneset name BINDER vsan 11
mds(config-zoneset)# member GOLD
mds(config-zoneset)# exit

mds(config)# zoneset activate name BINDER vsan 11
Zoneset activation initiated. check zone status

mds(config)# show zoneset active
zoneset name BINDER vsan 11
  zone name GOLD vsan 11
  * fcid 0xdf0001 [pwwn 20:00:00:25:B5:A1:50:B2]
  * fcid 0xdf0002 [pwwn 10:00:00:00:c9:85:02:68]
  * fcid 0xdf0200 [pwwn 50:06:01:60:4b:a0:31:62]
  * fcid 0xdf0300 [pwwn 50:06:01:68:4b:a0:31:62]
```

Define the required zone.

Configure the zone set.

Activate the zone set.

Verify active zone sets.

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

If the zones and zone set database do not include the devices in question, you must add them. To resolve the problem, you must add the zone and zone set configuration, and activate the zone set.

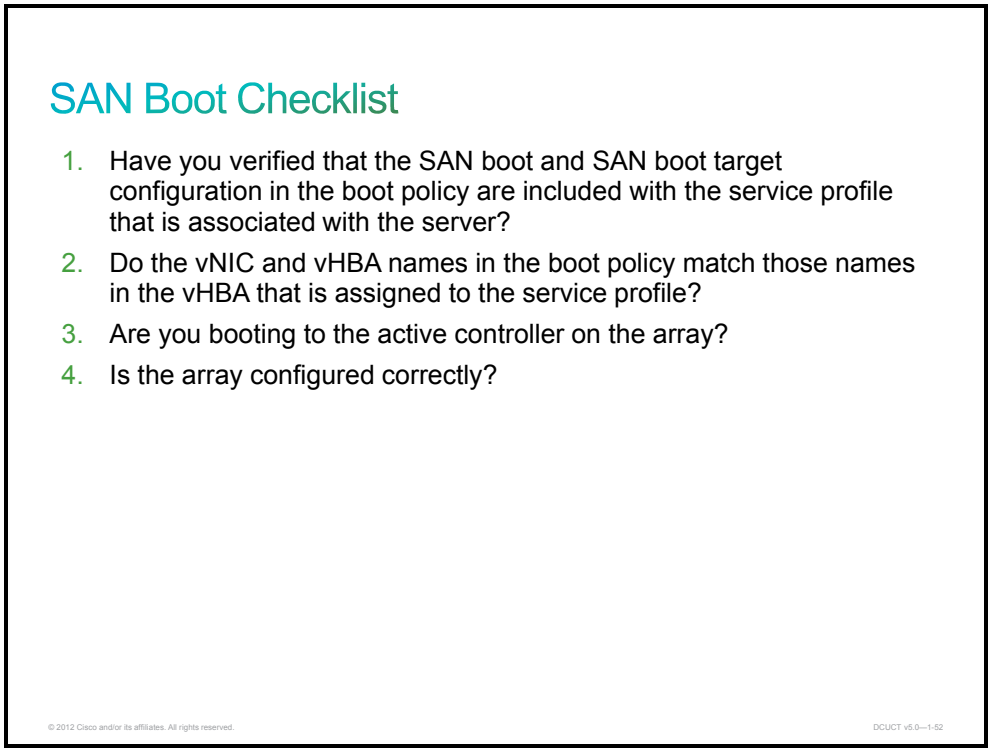
The **show zone set active** command displays the results. When checking the validity of the operational database, you must verify that the * character is listed in addition to the device FCID. The * character denotes that the devices that were added to the zone database are active in the zone. If the * character is missing, the communication will not be active.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Troubleshoot Cisco UCS B-Series SAN Boot

This topic describes how to troubleshoot the Cisco UCS B-Series SAN boot.



SAN boot problems may be caused by generic SAN connectivity issues. However, some additional aspects should be considered when the SAN boot problems persist after SAN connectivity has been confirmed. Use this checklist for easier problem isolation:

Step 1 Have you verified that the SAN boot and SAN boot target configuration in the boot policy is included with the service profile that is associated with the server?

Step 2 Do the vNIC and vHBA names in the boot policy match the names that are assigned to the service profile?

Step 3 Are you booting to the active controller on the array?

Step 4 Is the array configured correctly?

https://t.me/learningnets

SAN Boot Fails Intermittently

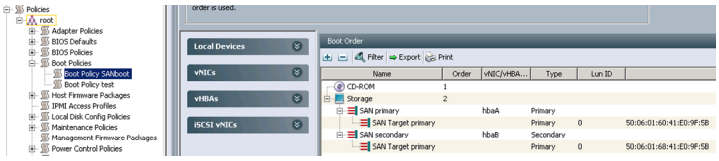
Problem	The SAN boot fails intermittently.
Possible Cause	Misconfigured SAN boot target in the boot policy is included in the service profile.
Solution	Verify that the configuration of the SAN boot target in the boot policy is included in the service profile. For example, make sure that the SAN boot target includes a valid WWPN.

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

If the SAN boot fails intermittently, verify that the configuration of the SAN boot target in the boot policy is included in the service profile. For example, make sure that the SAN boot target includes a valid WWPN.

Server Attempts Local Disk Boot Instead of SAN

Problem	The server attempts to boot from the local disk instead of the SAN.
Possible Cause	Misconfigured boot order in the service profile.
Solution	Verify that the configured boot order in the service profile has SAN as the first boot device. If the boot order in the service profile is correct, verify that the actual boot order for the server includes SAN as the first boot device. If the actual boot order is not correct, reboot the server.



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

If the server tries to boot from the local disk instead of from the SAN, verify that the configured boot order in the service profile has SAN as the first boot device. If the boot order in the service profile is correct, verify that the actual boot order for the server includes SAN as the first boot device. If the actual boot order is not correct, correct it and reboot the server.

https://t.me/learningnets

SPAN for Troubleshooting

This topic describes how to troubleshoot Cisco UCS B-Series traffic using SPAN.

SPAN for Troubleshooting

- SPAN has these characteristics:
  - It is often referred to as port monitoring or mirroring.
  - It selects network traffic for analysis by a network analyzer.
  - It copies interesting traffic from the source port to the destination port.
- Implemented with “Monitoring Port” personalities in Cisco UCS
- Available for Ethernet and Fibre Channel traffic

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

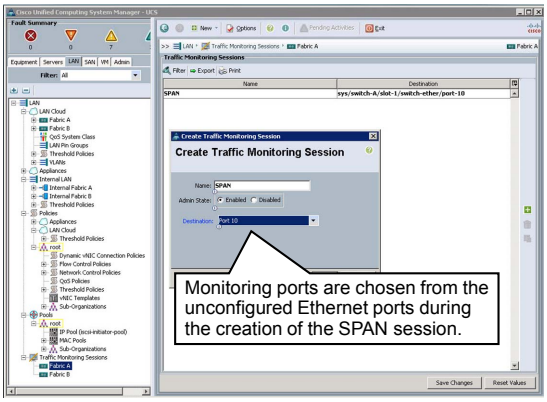
The Switched Port Analyzer (SPAN) feature is sometimes called “port mirroring” or “port monitoring.” The function selects network traffic for analysis by a network analyzer and copies it from the source port to the destination port.

In Cisco UCS, you implement the SPAN feature using “Monitoring Port” personalities. The feature can be deployed both in the Ethernet and in the Fibre Channel environment.

https://t.me/learningnets

Using SPAN for Ethernet Traffic

- 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.

To use SPAN in the LAN environment, you need to create an appropriate monitoring session. To create the session, choose **LAN > Traffic Monitoring Sessions**.

The components of a LAN SPAN monitoring session include the following:

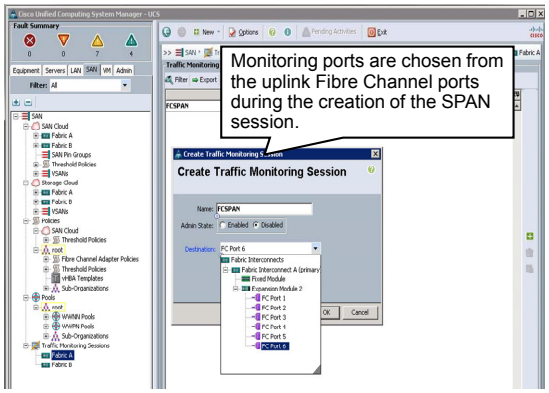
- **SPAN sources**, where traffic will be captured:
  - Uplink Ethernet ports
  - Uplink port channels
  - VLANs
  - vNICs and vHBAs
  - FCoE ports
  - Server ports
  - Fibre Channel uplink ports
- **SPAN destination:** The port to which captured data will be sent for analysis, also called a monitoring port. The destination can be any unconfigured Ethernet port. Select the port during the creation of the monitoring session.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Using SPAN for 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
  - VSANs
  - 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.

You can capture Ethernet or Fibre Channel traffic. To create a Fibre Channel SPAN session, choose **SAN > Traffic Monitoring Sessions**.

The following are components of a Fibre Channel SPAN monitoring session:

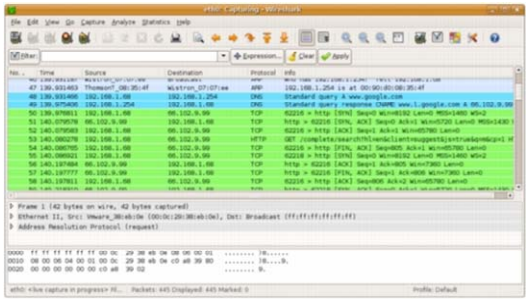
- **SPAN sources**, where traffic will be captured:
  - Uplink Fibre Channel ports
  - Uplink SAN port channels
  - VSANs
  - vHBAs
  - Fibre Channel storage ports
  - Fibre Channel port on Cisco UCS 6248UP cannot be a source port.
- **SPAN destination:** The port to which the captured data will be sent for analysis, also called a 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.

https://t.me/learningnets

SPAN and Ethanalyzer

- Ethanalyzer is a network protocol analyzer of Wireshark.
- Packet capture file can be performed in two ways:
  - Read in CLI
  - Exported and viewed in the Wireshark GUI

```
switch# ethanalyzer local interface inbound-hi decode-internal detail limit-captured-
frames 0 write bootflash:capture.pcap
Capturing on eth4
13494
```



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

When you capture Ethernet or Fibre Channel packets using the SPAN functionality, you typically need a packet analyzer for easier packet examination.

Ethanalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open-source code. Ethanalyzer is a command-line version of Wireshark that captures and decodes packets. You can use Ethanalyzer to troubleshoot your Cisco UCS Fabric Interconnect control and management traffic.

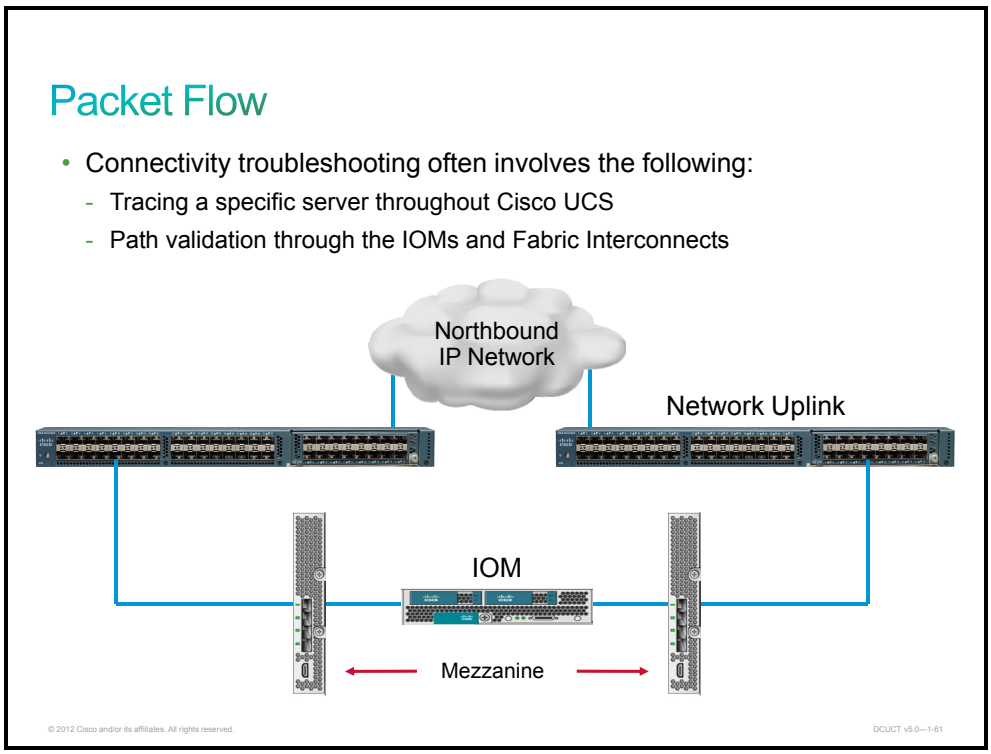
A packet capture file can be read directly on the Cisco NX-OS command line or the file can be exported. To locally open a capture file, use the **ethanalyzer local read** command. To export the packet capture file, use the **copy** command. After it has been exported, the capture file can be opened with Wireshark to allow easier analysis of the capture, as shown here.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Verify Packet Flow

This topic describes how to troubleshoot Cisco UCS server to fabric packet flow.

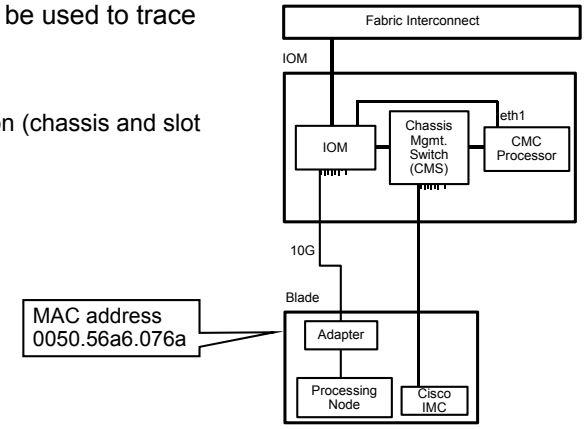


You can perform an end-to-end link-state analysis using various tools. These tools allow you to validate the entire path through the IOMs and Fabric Interconnects.

https://t.me/learningnets

Trace Scenario

- Identify the packet path to and from the VMware host with MAC address 0050.56a6.076a.
- A similar procedure can be used to trace traffic of the following:
  - VMware behind a host
  - Server in specific location (chassis and slot number)



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

In this scenario, you identify the packet path to and from the VMware host with MAC address 0050.56a6.076a.

You can use a similar procedure to trace traffic of the following:

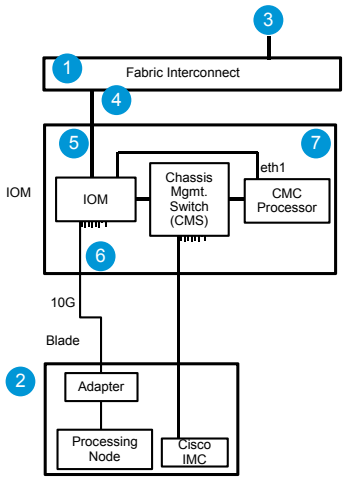
- VMware behind a host
- Server in specific location (chassis and slot number)

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Trace Procedure

1. Identify the Fabric Interconnect serving the host.
2. Identify the blade location.
3. Identify the Fabric Interconnect network port.
4. Identify the Fabric Interconnect server port.
5. Identify the IOM network port.
6. Identify the IOM host port.
7. View the IOM diagram.



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

Follow these steps to identify all links and interfaces that are forwarding traffic:

Step 1 Identify the Fabric Interconnect serving the host.

Step 2 Identify the blade location.

Step 3 Identify the Fabric Interconnect network port.

Step 4 Identify the Fabric Interconnect server port.

Step 5 Identify the IOM network port.

Step 6 Identify the IOM host port.

Step 7 View the IOM diagram.

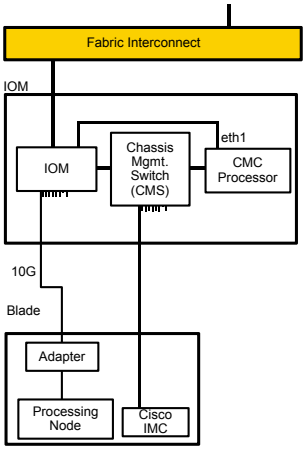
https://t.me/learningnets

Step 1: Identify the Fabric Interconnect Serving the Host

- Check which Fabric Interconnect is forwarding traffic to and from the server.
- Only one Fabric Interconnect should have the server MAC address in the MAC address table.
- If you see the MAC address on both Fabric Interconnects, the following is indicated:
  - Per-flow packet load-balancing at host
  - Not allowed on Cisco UCS B-Series

```
6100-A-B# connect nxos a
6100-A-A(nxos)# show mac-address address 0050.56a6.076a
VLAN      MAC Address       Type    Age       Port
---------+-----------------+-------+---------+---------
503       0050.56a6.076a    dynamic 10        veth928
```

```
6100-A-B# connect nxos b
6100-A-B(nxos)# show mac-address address 0050.56a6.076a
Total MAC Addresses: 0
```



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

First you should verify which Fabric Interconnect is forwarding traffic to and from the server. Only one Fabric Interconnect should have the server MAC address in the MAC address table. If you see that the server MAC address is on both Fabric Interconnects, the server will perform per-flow or per-packet load balancing at the host level, which is not permitted on Cisco UCS B-Series.

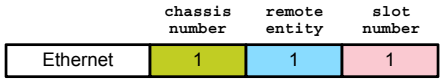
© 2012 Cisco Systems, Inc.

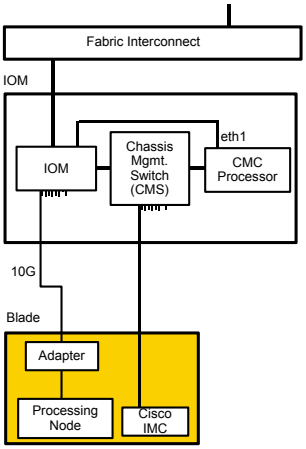
https://t.me/learningnets

Step 2: Identify Blade Location

- Verify the interface to which the server MAC address is connected.
- Perform a check on the Fabric Interconnect that is forwarding traffic to the server.
- In this case, you found chassis 1 and slot number 1.
- Proceed to data path troubleshooting.

```
UCS-6100-A-A(nxos)# show interface veth928
 vethernet928 is up
   Bound Interface is Ethernet1/1/1
 Hardware: VEthernet
 Encapsulation ARPA
 Port mode is trunk
 Last link flapped 1week(s) 5day(s)
 Last clearing of "show interface" counters never
 1 interface resets
```





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

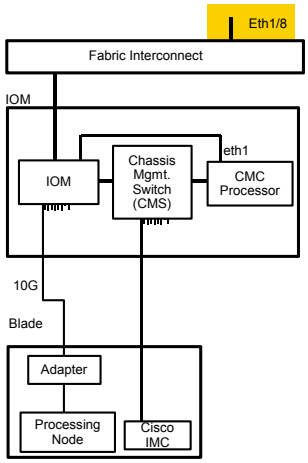
Next, identify the blade location, that is, the interface to which the server MAC address is connected. You need to perform this check on the Fabric Interconnect that is forwarding traffic to the server. In this case, you find the interface notation Ethernet1/1/1. The first digit indicates the chassis number (1). The third digit identifies the slot number (1). You can disregard the second digit, which identifies the remote entity.

https://t.me/learningnets

Step 3: Identify Fabric Interconnect Network Port

- Network port:
  - Connects the Fabric Interconnect to the upstream switch
  - Obtained from the pinning for the virtual Ethernet interface that is associated to the blade
- In this case, the network-facing port is Eth1/8.

```
6100-A-A(nxos)# show interface | begin veth928
vethernet928 is up
   Bound Interface is Ethernet1/1/1
    <output omitted>
   Ethernet1/1/1 is up

6100-A-A(nxos)# show pinning interface veth928

---------------+-----+-----------------------+---
SIF Interface   Sticky  Pinned Border Interface
---------------+-----+-----------------------+---
veth928         No                Eth1/8
```



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

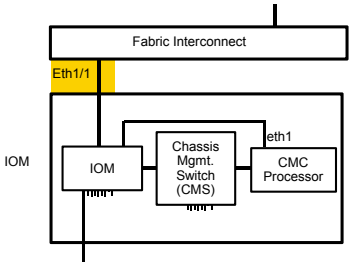
Next, identify the Fabric Interconnect network port. The network port connects the Fabric Interconnect to the upstream switch. You can obtain the network port ID from the pinning information for the virtual Ethernet interface that is associated to the blade. In this case, the network-facing port is Eth1/8.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Step 4: Identify Fabric Interconnect Server Port

- The server port connects the Fabric Interconnect to the IOM.
- The Fabric Interconnect port that is connected to Chassis 1 and Blade 1 is Eth1/1.



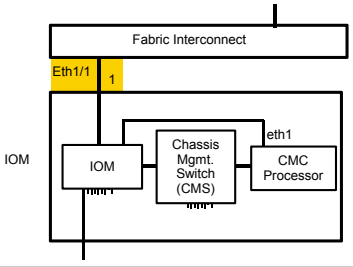

```
6100-A-A(nxos)# show platform software fex info satport ethernet 1/1/1
 Interface-Name  ifindex  State Fabric-if  Pri-fabric Expl-Pinned
        Eth1/1/1 0x1f000000   Up    Eth1/1     Eth1/4     Eth1/1
 Port Phy Up. Port dn req: Not pending
 SDB entry: ifindex(1f000000) fabric if(1a000000)
    Dev: 0 Nif3 Hif7 (Nif:0x20000000 Hif:0x1f000000)
```

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

Next, identify the Fabric Interconnect server port. The server port connects the Fabric Interconnect to the IOM. Use the **show platform software fex info satport ethernet** command for the interface blade interface (Ethernet 1/1/1). From the output, you learn that the Fabric Interconnect port that is connected to Chassis 1/Blade 1 is Eth1/1.

Step 5: Identify IOM Network Port

- The NIF connects the IOM to the Fabric Interconnect.
- The IOM Fabric Interconnect-facing interface is 1.
- It is connected to Fabric Interconnect Eth 1/1.




```
6100-A-A(nxos)# show interface fex-fabric
     Fabric       Fabric        Fex                 FEX
Fex  Port       Port State    Uplink    Model         Serial
------------------------------------------------------------
 1    Eth1/1        Active       1        N20-C6508  QCI132800P2
 1    Eth1/2        Active       2        N20-C6508  QCI132800P2
 1    Eth1/3        Active       3        N20-C6508  QCI132800P2
 1    Eth1/4        Active       4        N20-C6508  QCI132800P2
```

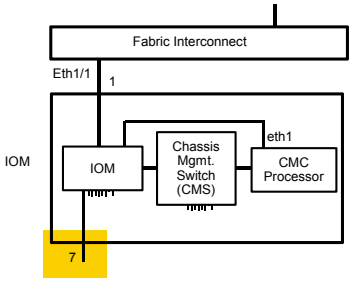
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, identify the IOM network interface (NIF). The NIF connects the IOM to the Fabric Interconnect. You can use the **show interface fex-fabric** command to obtain the NIF. In this case, the IOM Fabric Interconnect-facing interface is 1. It is connected to Fabric Interconnect Eth 1/1.

https://t.me/learningnets

Step 6: Identify IOM Host Port

- The HIF connects the IOM to the server.
- In this case, there are the following results:
  - The NIF is Nif3 (Eth 1/1).
  - The HIF is Hif7.




```
6100-A-A(nxos)# show platform software fex info satport ethernet 1/1/1
 Interface-Name  ifindex  State Fabric-if  Pri-fabric Expl-Pinned
        Eth1/1/1 0x1f000000   Up    Eth1/1     Eth1/4     Eth1/1
 Port Phy Up. Port dn req: Not pending
 SDB entry: ifindex(1f000000) fabric if(1a000000)
    Dev: 0 Nif3 Hif7 (Nif:0x20000000 Hif:0x1f000000)
```

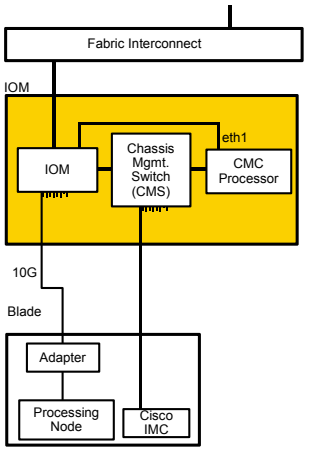
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, identify the IOM host interface (HIF). The HIF connects the IOM to the server. Obtain the required information from the **show platform software fex info satport ethernet** command for the blade-facing interface (Ethernet 1/1/1). From the output, you learn that the NIF is NIF3 (Eth 1/1) and that the HIF is HIF7.

Step 7: View IOM Diagram

```
6100-A-B# connect local-mgmt a
6100-A-A(local-mgmt)# connect iom 1
fex-1# show platform software redwood sts
Board Status Overview:
legend: ' '= no-connect
         X  = Failed
         -  = Disabled
         :  = Dn
         |  = Up
         $  = SFP+ present
         v  = Blade Present
        +---+----+----+----+
 SFP:   |[$]| [$]| [$]| [$]|
        +---+----+----+----+
          |    |    |    |
        +-+----+----+----+-+
        | 0    1    2    3 |
        | I    I    I    I |
        | N    N    N    N |
        |                  |
        |      ASIC 0      |
        |                  |
        | H H H H H H H H  |
        | I I I I I I I I  |
        | 0 1 2 3 4 5 6 7  |
        +-+-+-+-+-+-+-+-+--+
          - - - - | : | |
         +-+-+-+-+-+-+-+-+
         |-|-|-|-|v|v|v|v|
         +-+-+-+-+-+-+-+-+
Blade:     8 7 6 5 4 3 2 1
```

Representation of the IOM ports from the IOM ASIC perspective



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

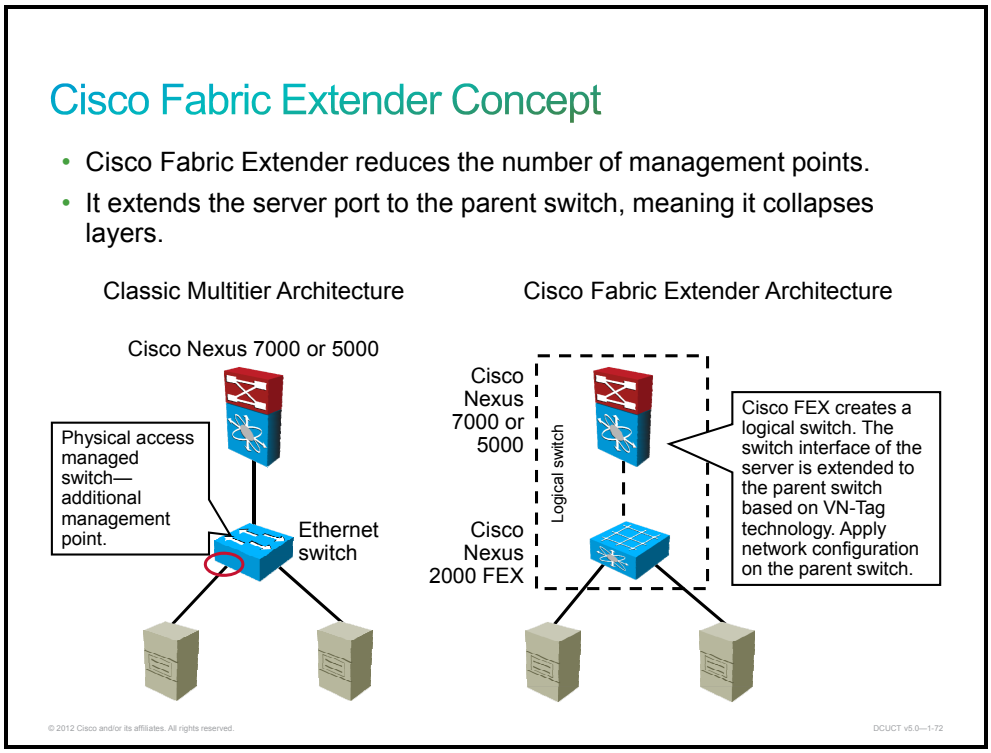
Finally, you can examine the logical diagram of the IOM using the **show platform software redwood iom** command. The output provides a representation of the IOM ports from the IOM ASIC perspective.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Troubleshoot Cisco UCS Integration with Virtualization Platform

This topic describes how to troubleshoot Cisco UCS B-Series integration with the server virtualization platform.

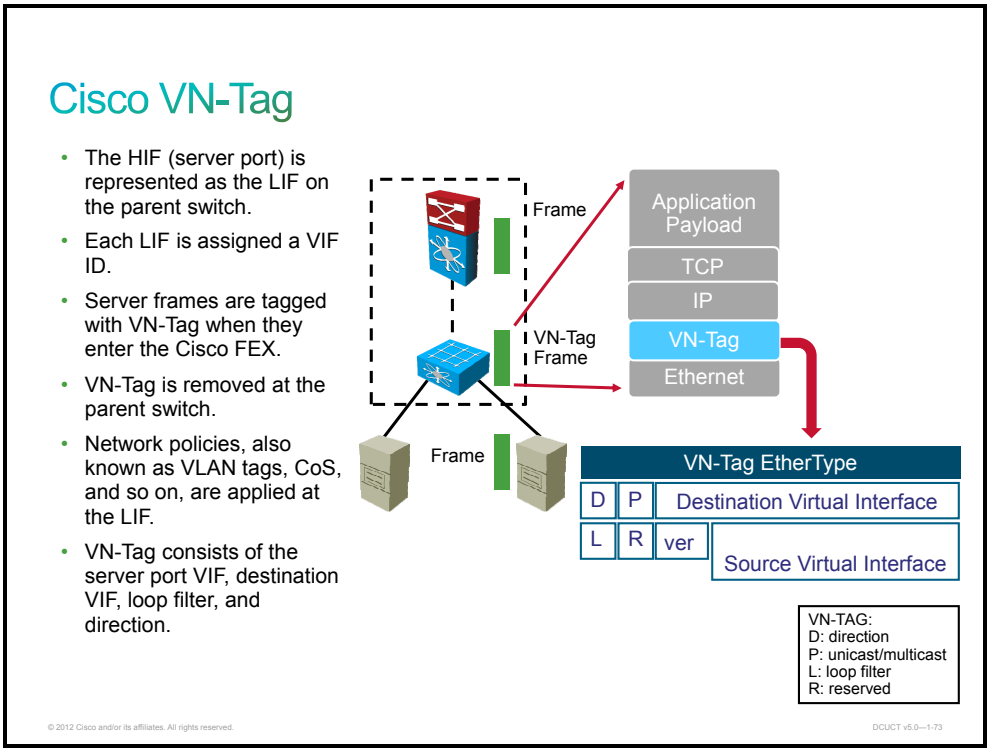


Cisco Fabric Extender technology was introduced along with Cisco Nexus switches and Cisco UCS.

In a classic data center, there are distinct access, aggregation, and core network layers. Each layer consists of switches that must be managed.

With Cisco Fabric Extender technology, which is based on the Cisco VN-Tag, you can collapse network layers. This ability means that the access switches are replaced by unmanaged devices, fabric extenders, such as the Cisco Nexus 2000 or the Cisco UCS IOM and Cisco VICs, and the server port is extended up to the first managed device. This function allows all of the configuration for the server port to be performed on the parent switch. Therefore, you have physical devices forming the access layer, but you manage only the devices from the upper layer.

https://t.me/learningnets



The Cisco Fabric Extender is an unmanaged device to which the server is connected. You use a parent switch on which the Cisco Fabric Extender is installed. From the parent switch, you provision the network configuration for the server. The parent switch must have a way to access, control, and apply configuration to the fabric extender. This configuration is achieved by using VN-Tag technology.

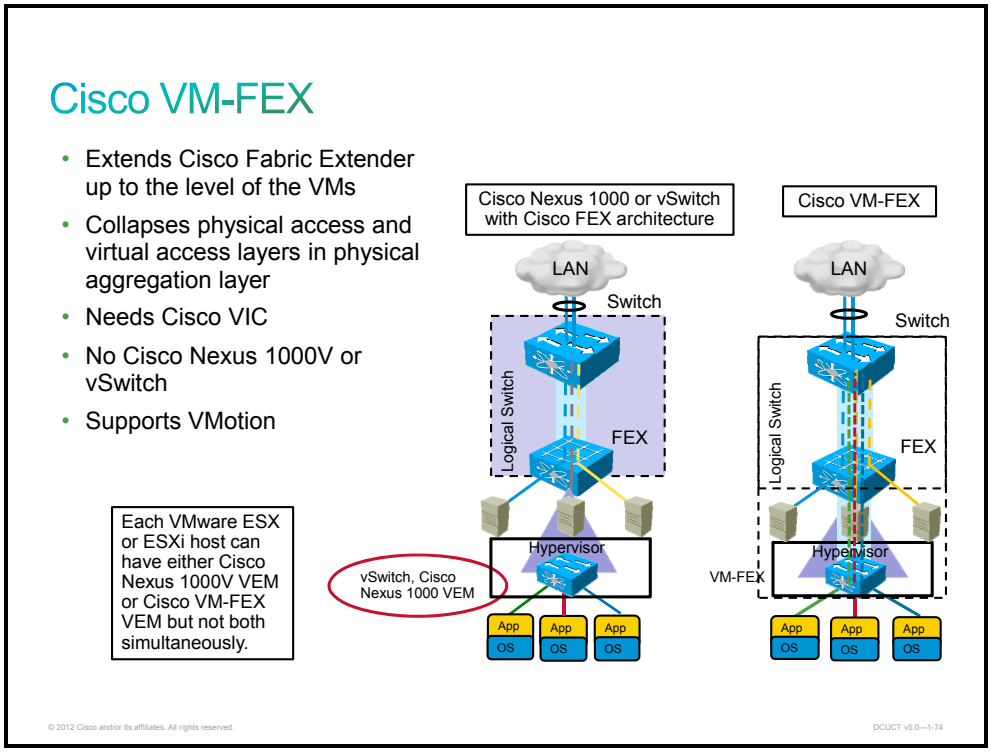
With VN-Tag, each port to which a server is connected on the fabric extender is called a host interface (HIF). The HIF is represented on the parent switch as a logical interface (LIF). Each LIF is identified by a virtual interface (VIF) ID. With the VIFs, each HIF is represented on the parent switch. The HIF can be managed directly at the parent switch.

As network policies and configuration to server traffic are applied to the LIF on the parent switch, there must also be a way to identify traffic from and to multiple servers that are connected to the HIF on the Cisco Fabric Extender. The VN-Tag, an additional tag in the Ethernet frame, is used for this identification. The tag is applied on the HIF of the Cisco Fabric Extender when the frame of the server enters, and the tag is stripped away on the parent switch. This process is an internal process between the Cisco Fabric Extender and the parent switch.

VN-Tag technology allows remote, unmanaged interfaces to be visible and managed on a parent device. Additionally, this technology allows segmentation of traffic from different servers that are connected in this manner.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



The Cisco Virtual Machine Fabric Extender (VM-FEX) extends the Cisco Fabric Extender up to the level of the virtual machines (VMs). This extension allows collapsing both the virtual access network layer and the physical access network layer in the aggregation network layer.

The Cisco Fabric Extender is the Cisco Virtual Interface Card (VIC). The VM vNICs are connected to the Peripheral Component Interconnect Express (PCIe) devices that are created in the Cisco VIC dynamic vNICs. The VN-Tag is used between the dynamic vNICs and the Fabric Interconnects, on which LIFs are created, called virtual Ethernet (vEth) interfaces.

With Cisco VM-FEX, there is no software switch. Switching is performed on the Cisco UCS Fabric Interconnects.

Because there is no Cisco Nexus 1000V Virtual Supervisor Module (VSM), the network configuration is created on Cisco UCS Manager.

https://t.me/learningnets

Cisco VM-FEX Verification Checklist: VMware ESX Host Side

1. Check the VEM switch status on the VMware ESX host.
2. Check if the VEM module is loaded by the VMware ESX kernel.
3. View information regarding Cisco VM-FEX maximum number of ports, connectivity status, used ports IDs that are mapped to virtual machine dynamic vNICs, vmkernel, and so on.
4. Check the virtual machine dynamic vNIC network connectivity from the VMware ESX host side.

```
~ # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.1.4.1.0-3.0.4
Build 4
Date Thu Aug 25 10:47:10 PDT 2011
Number of PassThru NICs are 15
VEM modules are loaded
DVS Name Num Ports Used Ports Configured Ports MTU Uplinks
DVS-PTS-VNFEX 256 17 256 1500 vmnic0,vmnic1

 <further steps omitted>
```

The number of passthrough NICs are dynamic vNICs.

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

Here is a checklist that guides you through a sample Cisco VM-FEX troubleshooting scenario. The first section explains how to check the Cisco VM-FEX switch status on the VMware ESX host:

Step 1 Check the Virtual Ethernet Module (VEM) switch status on the VMware ESX host. Here is an output example:

```
~ # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.1.4.1.0-3.0.4
Build 4
Date Thu Aug 25 10:47:10 PDT 2011
Number of PassThru NICs are 15
VEM modules are loaded
DVS Name Num Ports Used Ports Configured Ports MTU Uplinks
DVS-PTS-VNFEX 256 17 256 1500 vmnic0,vmnic1
Number of PassThru NICs are 15
```

Step 2 Check if the VEM module is loaded by the ESX kernel.

```
# vmkload_mod -l | grep vem
vem-v132-svs-mux 12 32
vem-v132-pts 1 144
```

Step 3 View the information regarding Cisco VM-FEX maximum number of ports, connectivity status, used port IDs that are mapped to virtual machine dynamic vNICs, vmkernel, and so on.

```
esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports MTU Uplinks
vSwitch0 128 2 128 1500
PortGroup Name VLAN ID Used Ports Uplinks
Service Console 0 0
VM Network 0 0 DVS Name Num Ports Used Ports Configured Ports
MTU Uplinks
```

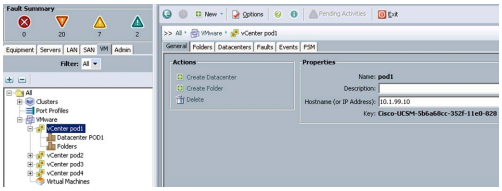

https://t.me/learningnets

```
UPT_DVS 256 5 256 1500 vmnic0,vmnic1
DVDV Port ID 1500 In Use Client
1516 0
1523 1 vmnic1
1539 1 vmnic0
1 1 vmk0
1500 1 Windows2K8R2 ethernet0
```

Step 4 Check the virtual machine dynamic vNIC network connectivity issues from the ESX host side.

Cisco VM-FEX Verification Checklist: Cisco UCS VM-FEX and VMware vCenter

1. Connect to Cisco UCS VM tab:
   - View all available Cisco VM-FEX switches that are defined in the Fabric Interconnect.
   - View all virtual machine dynamic vNICs with the corresponding Cisco VM-FEX DV Port ID connectivity information.
2. Verify that the dynamic port names of the virtual interfaces are displayed on the Cisco UCS service profile:
   - Cisco VM-FEX creates active and standby VIFs.
   - These interfaces are placed on Fabric Interconnect A and B.
3. Display all the available Cisco VM-FEX DVSs from different data centers in the VMware vCenter Networking tab.



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

Perform the following verifications on Cisco UCS VM-FEX and VMware vCenter:

Step 1 The Cisco UCS VM tab allows you to view all available Cisco VM-FEX switches that are defined in the Fabric Interconnect and also allows you to define port profiles with network settings. You can apply the port profiles to multiple Cisco VM-FEX switches that are running on the Fabric Interconnect. The Cisco UCS VM tab provides a logical view of all virtual machine dynamic vNICs with the corresponding Cisco VM-FEX DV Port ID connectivity information.

Step 2 To support automatic fabric-based failover on virtual machine dynamic vNICs, Cisco VM-FEX creates active and standby VIFs. These interfaces are placed on Fabric Interconnect A and B. The corresponding dynamic port names of the virtual interfaces are displayed on the Cisco UCS service profile. The Cisco UCS CLI view provides information on virtual interface of virtual machine dynamic vNIC mapping to the Cisco UCS vEthernet interface. You can verify the mapping information using the **show vnic** and **show virtual-machine Virtual Machine:** commands.

Step 3 The VMware vCenter Networking tab displays all the available Cisco VM-FEX distributed virtual switches (DVSs) from different Data Centers. The tab also provides the corresponding virtual machine dynamic vNICs DV Port ID, which is a part of Cisco VM-FEX DVSs across the data center.

https://t.me/learningnets

Cisco VM-FEX Verification Checklist: Cisco VIC Adapter

- Connect to the corresponding adapter.
- Verify the dynamic vNIC MAC address that is associated with the vNIC on the adapter.
- In this example, blade 1 is connected on chassis 2, which has the Cisco VIC adapter 1.

```
UCS-A# connect adapter 2/1/1
 adapter 2/1/1 # connect
 adapter 2/1/1 (top):1# attach-mcp
adapter 2/1/1 (mcp):1# vnic vif uif : bound uplink 0 or 1, =:primary, -
:secondary, >:current
-------------------------
vnic lif vifid name type bb:dd.fstate lifstate uif ucsm idx vlanstate
-------------------------
5vnic_1 enet 08:00.0 UP 2 UP =>0 1326 187 1 UP
- 1 1327 181 1 UP
6vnic_2 enet 08:00.1 UP 3 UP - 0 1329 186 1 UP
=>1 1328 180 1 UP
7vnic_3 enet_pt08:00.2 UP 4 UP =>0 1330 189 1 UP
-1 1331 183 1 UP

 <further steps omitted>
```

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

To see the corresponding dynamic vNIC “vf_vmnic0” MAC address that is associated with the vNIC on the adapter, you need to connect to the corresponding adapter. In this example, blade 1 is connected on chassis 2, which has the Cisco VIC adapter 1.

```
UCS-A# connect adapter 2/1/1
adapter 2/1/1 # connect
adapter 2/1/1 (top):1# attach-mcp
adapter 2/1/1 (mcp):1# vnic vif uif : bound uplink 0 or 1,
=:primary, -:secondary, >:current
-------------------------
vnic lif vifid name type bb:dd.fstate lifstate uif ucsm idx
vlanstate
-------------------------
5vnic_1 enet 08:00.0 UP 2 UP =>0 1326 187 1 UP
- 1 1327 181 1 UP
6vnic_2 enet 08:00.1 UP 3 UP - 0 1329 186 1 UP
=>1 1328 180 1 UP
7vnic_3 enet_pt08:00.2 UP 4 UP =>0 1330 189 1 UP
- 1 1331 183 1 UP

adapter 1/7/1 (mcp):14# vnic 7
vnicid : 7
name : vnic7
type : enet_pt
state : UP
adminst : UP
slot : 0
bdf : 03:00.2
mac : 00:00:00:00:00:00
vifid : 1330
```

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

```
vifcookie : 1297761
uif : 0
stby_vifid : 1331
profile :
stdby_profile :
```

In this command output, “devName vf_vmnic 0 08:00.2 MAC: 00:0c:29:b7:8c:95” has two VIF DV Port ID 1500s—1330 and 1331—created on both the Fabric Interconnects. VIF ID 1330 is active and created on Fabric Interconnect A (UP =>0 1330). VIF ID 1331 is standby (stby_vifid :1331) and created on secondary Fabric Interconnect B (-1 1331).

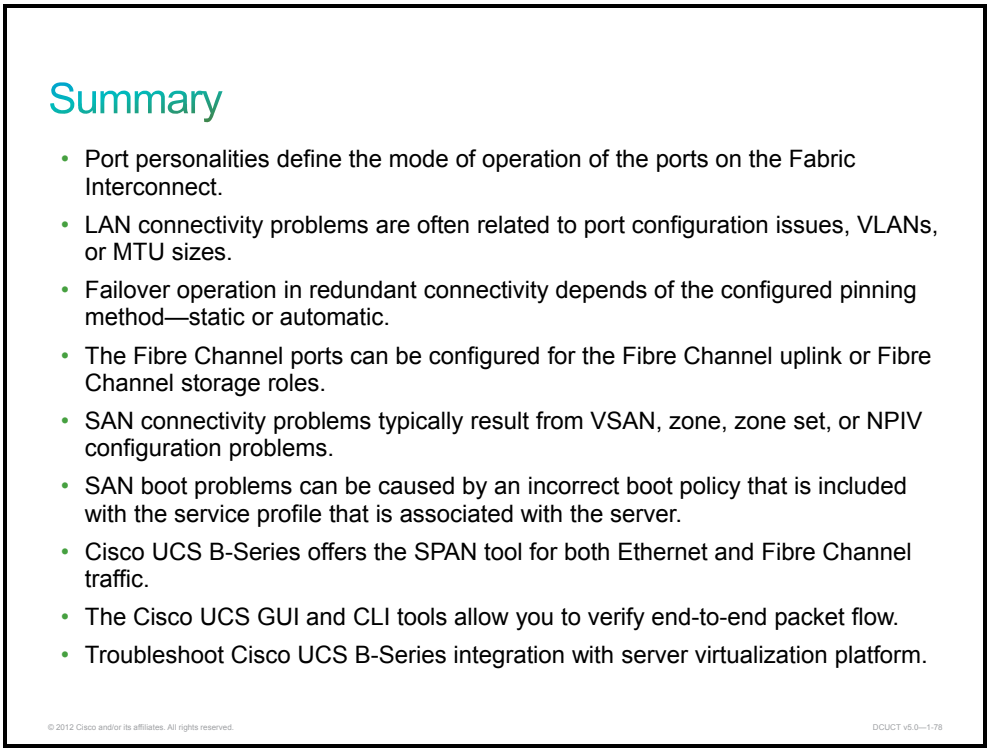
In the output shown here, guest VM dynamic vNIC MAC address “00:0c:29:b7:8c:95” (VIF ID 1330) is registered on the active Fabric Interconnect A and VIF ID 1331 is in standby and becomes active when there is a fabric failover event.

```
Fabric-Cus1-A(nxos)# show mac address-table address
000c.29b7.8c95
VLAN MAC Address Type age Secure NTFY Ports
---------+-----------------+--------+---------+------+----+--
* 1 000c.29b7.8c95 static 0 F F Veth32769
```


https://t.me/learningnets

Summary

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



References

For additional information, refer to these resources:

- *Cisco UCS Manager B-Series Troubleshooting Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/ts/guide/UCSTroubleshooting.html
- *Cisco VM-FEX Using VMware ESX Environment Troubleshooting Guide* at http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns944/basic_troubleshooting_vm_fex_ns1148_Networking_Solutions_White_Paper.html

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 5

Troubleshooting and Upgrading Cisco UCS Manager

Overview

Issues that are introduced through improper firmware upgrades generate a large percentage of Cisco Unified Computing System (Cisco UCS) support calls. The ramifications of an improper firmware upgrade can be loss of valuable system uptime, loss of user data, and even corruption of hardware components necessitating a physical replacement. The release notes of each version provide a definitive guide on how to safely upgrade firmware with minimal disruption.

This lesson introduces general concepts that will help you quickly identify and resolve firmware upgrade problems.

Objectives

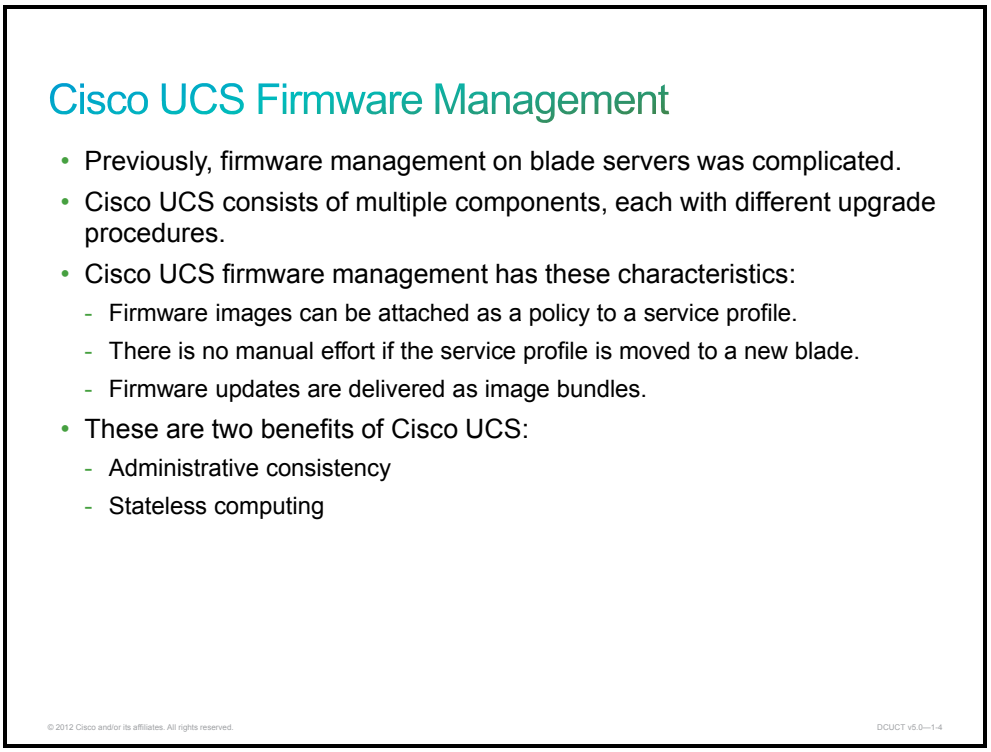
Upon completing this lesson, you will be able to identify best practices that are associated with upgrading Cisco UCS components, and describe how to identify and resolve upgrade failures. This ability includes being able to meet these objectives:

- Distinguish between individual component firmware and firmware bundles
- Install catalogs and management extensions to add support for new hardware
- Identify running and startup firmware on all Cisco UCS components
- Define the general upgrade process for all Cisco UCS components

https://t.me/learningnets

Firmware Packaging Identification

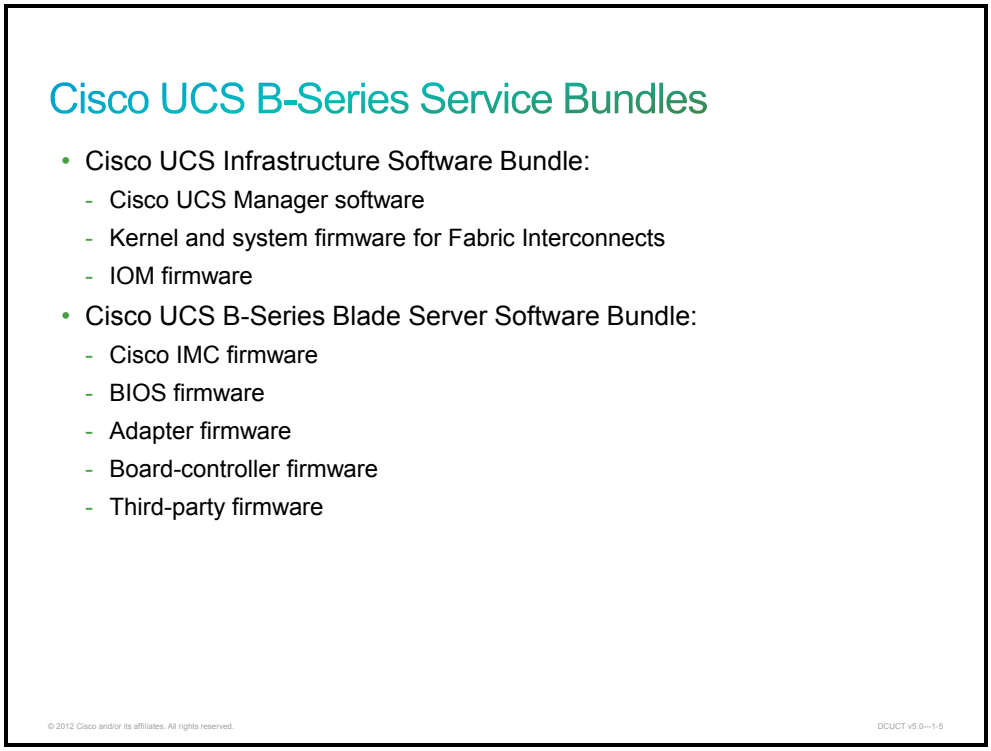
This topic describes how to distinguish between individual component firmware and firmware bundles.



Before the introduction of Cisco 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.

© 2012 Cisco Systems, Inc.

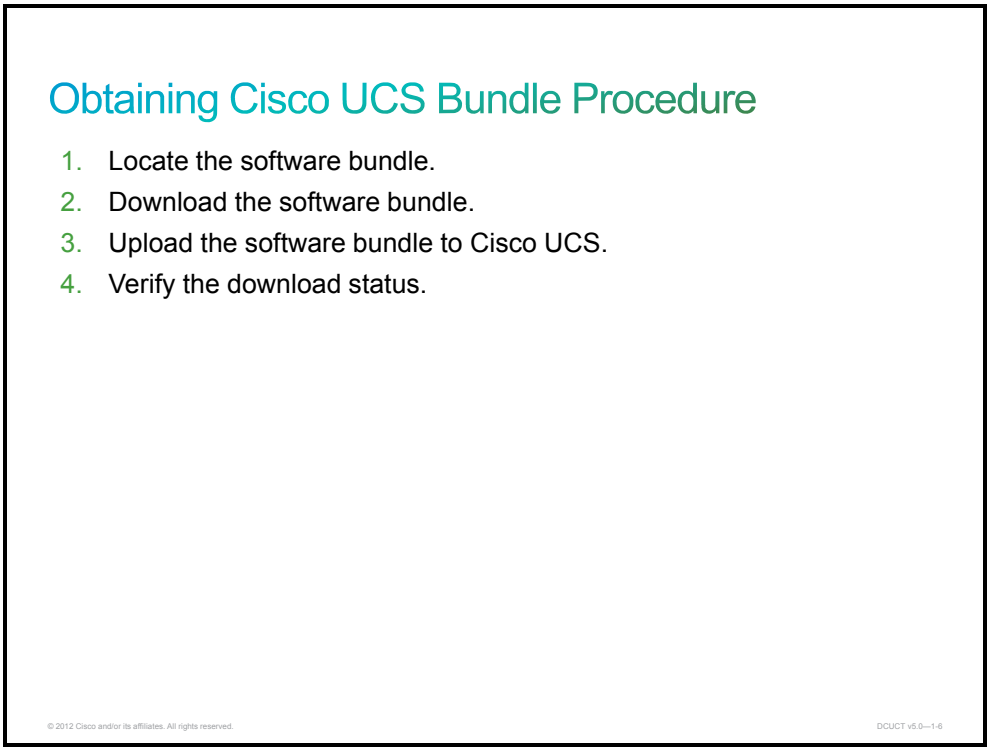
https://t.me/learningnets



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 of the components. Because 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 bundles. There are two bundles that are available for the Cisco UCS B-Series:

- Cisco UCS Infrastructure Software Bundle:
  - Cisco UCS Manager software
  - Kernel and system firmware for Fabric Interconnects
  - I/O Module (IOM) firmware
- Cisco UCS B-Series Blade Server Software Bundle:
  - Cisco Integrated Management Controller (Cisco IMC) firmware
  - BIOS firmware
  - Adapter firmware
  - Board-controller firmware
  - Third-party firmware

https://t.me/learningnets



Follow this procedure to obtain the software bundle and prepare for the Cisco UCS deployment of the firmware update:

Step 1 Locate the software bundle.

Step 2 Download the software bundle.

Step 3 Upload the software bundle to Cisco UCS.

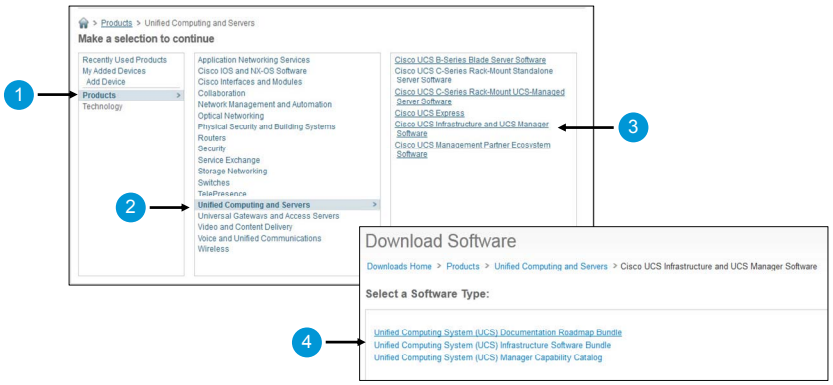
Step 4 Verify the download status.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Step 1: Locate Software Bundle

- Browse to the software navigator.
- Log in with your Cisco.com account.
- Select Unified Computing System (UCS) Infrastructure Software Bundle.



http://www.cisco.com/cisco/software/navigator.html

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

You can download the software bundles from here: http://www.cisco.com/cisco/software/navigator.html.

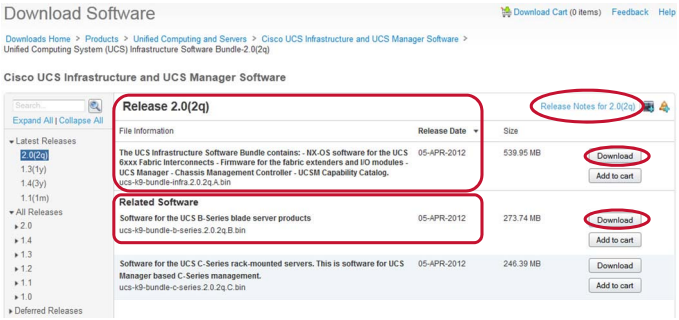
After you log in with your Cisco.com account, choose **Products > Unified Computing and Servers > Cisco UCS Infrastructure and UCS Manager Software** from the download options.

Select **Unified Computing System (UCS) Infrastructure Software Bundle**.

https://t.me/learningnets

Step 2: Download Software Bundle

- Select the version and download the bundle or bundles.
- Read and follow the release notes.



http://www.cisco.com/cisco/software/navigator.html

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

You will receive the Cisco UCS infrastructure bundle and the related software downloads. This process is an easy way to get the three software bundles from one place.

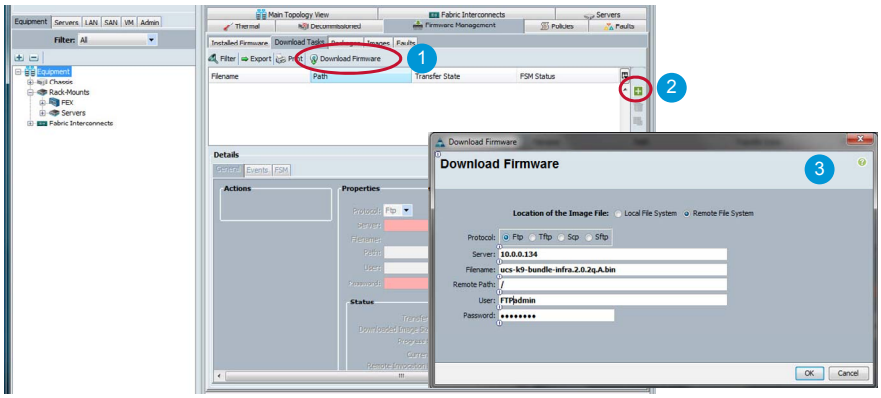
Select the appropriate version of the Cisco UCS software and download the bundles.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Step 3: Transfer Software Bundle to Cisco UCS

- Most firmware operations are performed under the Equipment tab in Cisco UCS Manager.
- Click **Download Firmware** and check the Local File System radio button to use HTTP copy.
- Check the **Remote File System** radio button to copy with FTP, TFTP, SCP, or SFTP.



Equipment > Firmware Management > Download Tasks

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

DCUCT v5.0—1-9

After the bundle image is obtained, you must transfer it 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.

Choose **Equipment** > **Firmware Management** > **Installed Firmware** and then click **Download Firmware**.

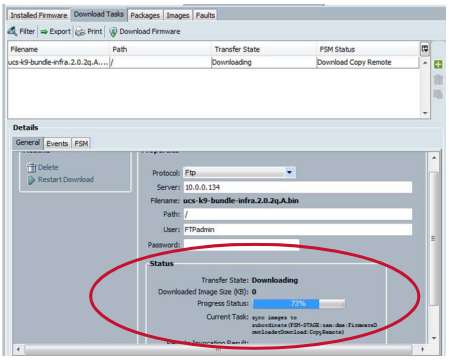
Select how to transfer the bundle image:

- **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 must 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

Step 4: Verify Download Status

- Progress can be observed in the Download Tasks tab.
- Upon successful transfer, the Fabric Interconnect does the following:
  - Expands the individual files from the archive
  - Installs files in the correct flash file system partition
- Files are displayed as individual packages or images.



Equipment > Firmware Management > Download Tasks

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

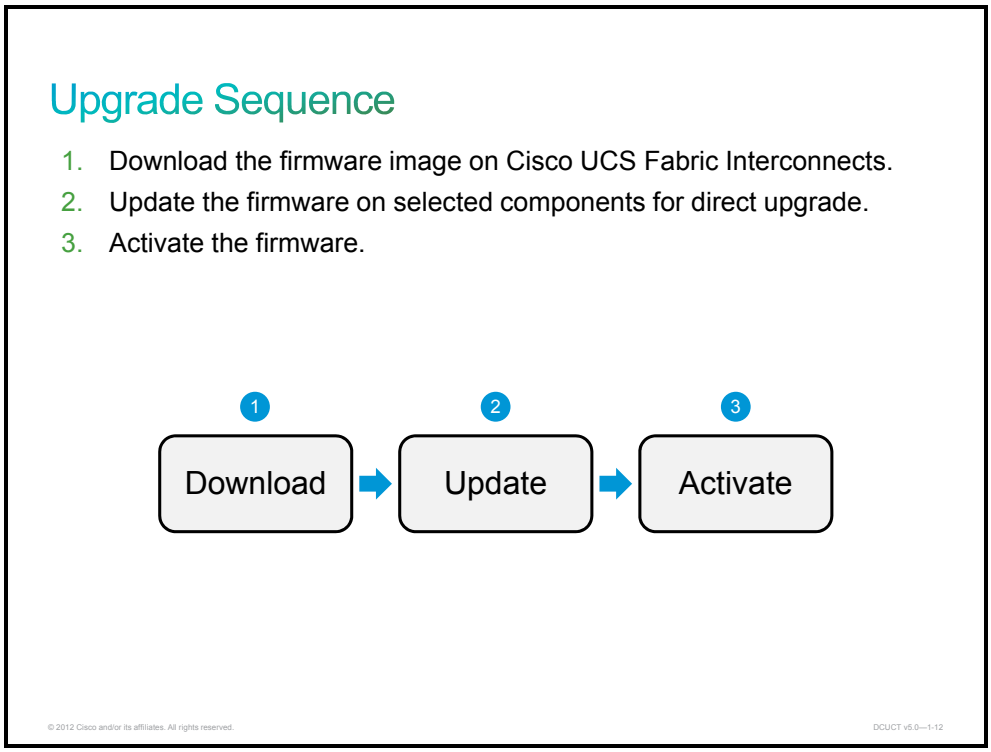
The download starts immediately. The progress can be observed in the Download Tasks tab. When the download is successful, the Fabric Interconnect expands the individual files from the archive and installs them in the correct flash file system partition. The files are then viewable as individual packages or images. The new firmware can be used to update components immediately.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Cisco UCS Firmware Installation Plan

This topic describes how to install catalogs and management extensions to add support for new hardware.



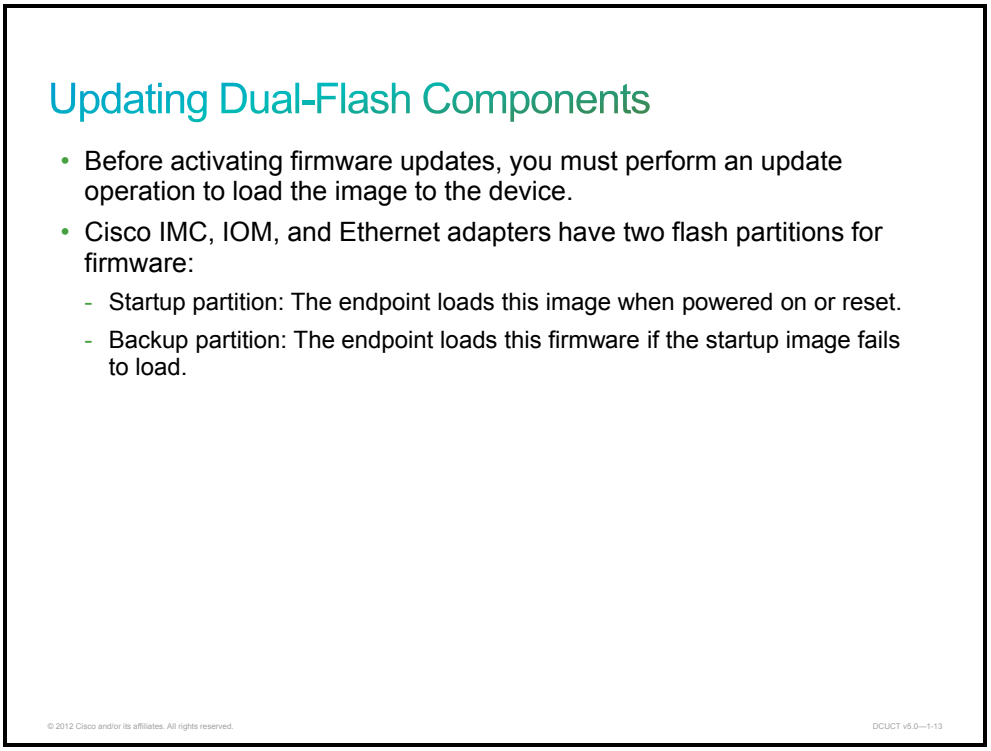
You update the firmware of most hardware components using the same approach. There are three main steps in the upgrade sequence:

Step 1 **Download:** With this operation, you copy the files that are 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..

https://t.me/learningnets



IOMs, Cisco IMC, and converged network adapters (CNAs) have two flash partitions for firmware images. They 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.

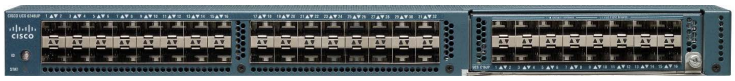
Before the startup image can be activated on a new version, the backup image must be updated with the desired version.

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

Fabric Interconnect Firmware Types

- Cisco Nexus Operating System (Cisco NX-OS) Kernel:
  - Boot loader
  - Low-level operating system
  - Loads Cisco NX-OS
- Cisco NX-OS System:
  - Binary image of Cisco NX-OS
  - Loads Cisco UCS Manager
- Cisco UCS Manager:
  - Runs as a process on dedicated management processors in the Fabric Interconnects
  - Uses separate firmware



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

DCUCT v5.0—1-14

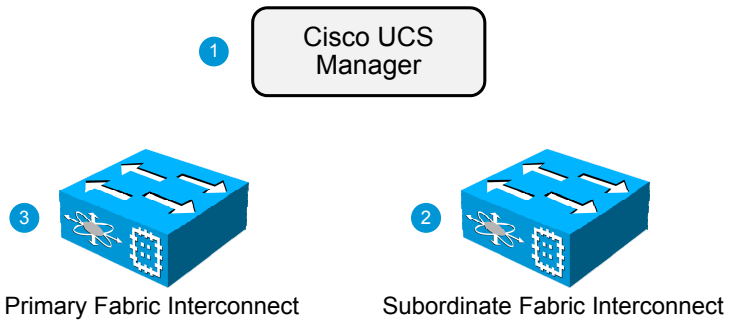
The Fabric Interconnects require three distinct firmware updates:

- **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.

https://t.me/learningnets

Updating Fabric Interconnect Firmware

1. Upgrade Cisco UCS Manager software.
2. Activate the new version on the subordinate Fabric Interconnect.
3. Activate the new version on the primary Fabric Interconnect.



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

Because the Fabric Interconnects operate in a cluster, it is possible to update them 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 nonusable 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 allows 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.

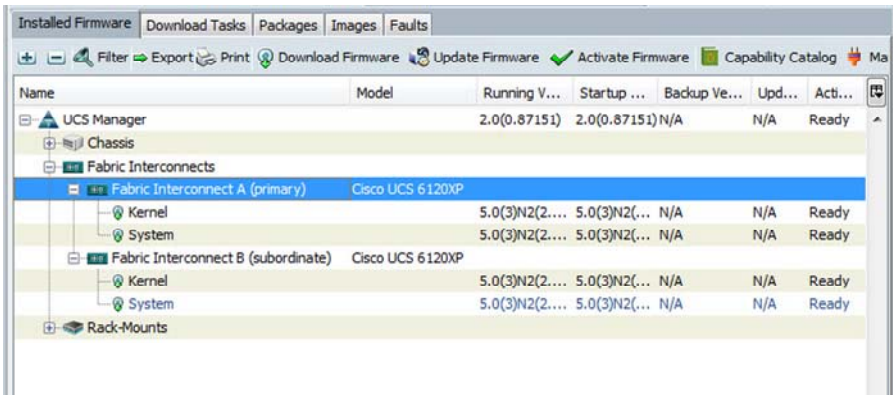
https://t.me/learningnets

Firmware Levels on Cisco UCS Components

This topic describes how to identify running and startup firmware on all Cisco UCS components.

Display Running Fabric Interconnect Firmware Version

- The current firmware can be viewed in the Installed Firmware tab of Cisco UCS Manager.
- Information categories are per hardware components.



Equipment > Firmware Management > Installed Firmware

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

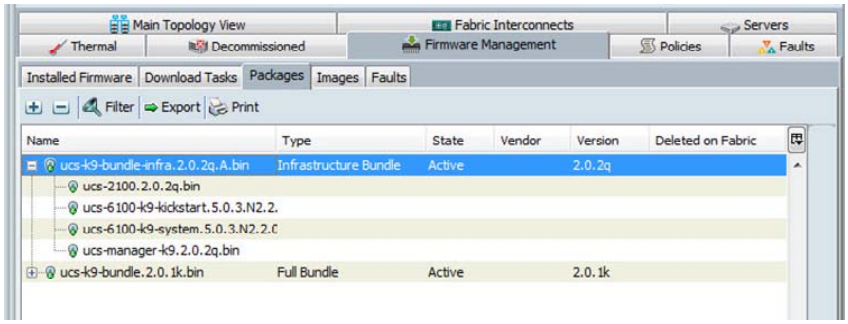
DCUCT v5.0—1-17

You can easily identify the firmware version that is running on your Fabric Interconnects in Cisco UCS Manager. Choose **Equipment** > **Firmware Management** > **Installed Firmware** to view the running version of firmware on both Fabric Interconnects.

https://t.me/learningnets

View Installable Packages

- Installable images and packages can be viewed in the Packages tab of Cisco UCS Manager.
- Packages are displayed after they are uploaded to the Fabric Interconnect.



Equipment > Firmware Management > Packages

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

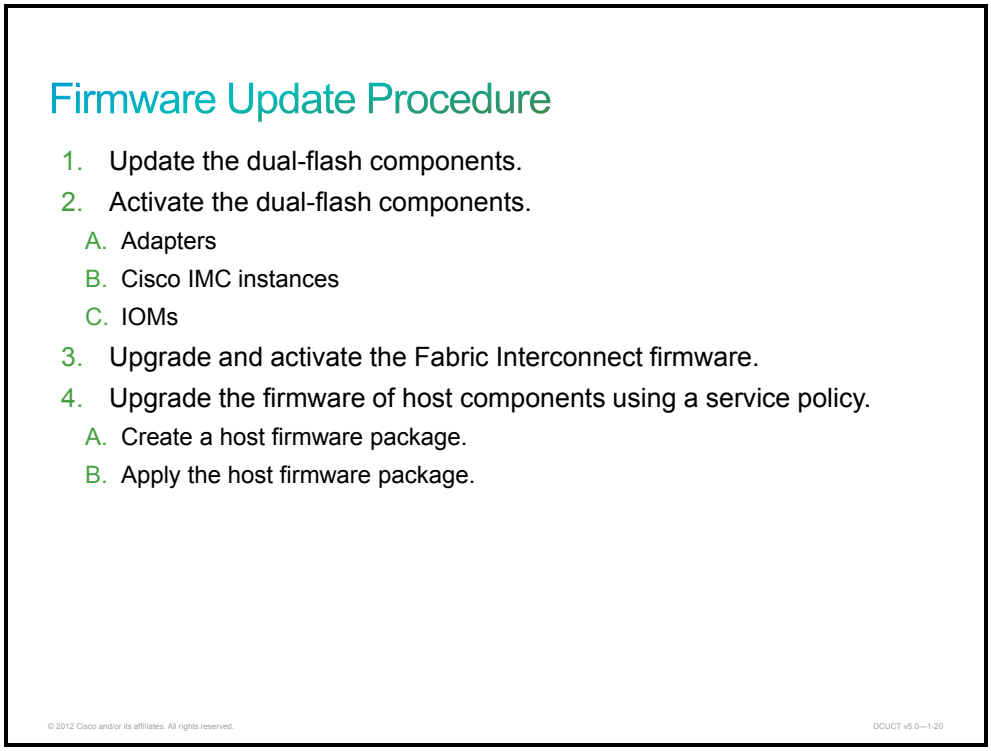
The Firmware Management section of Cisco UCS Manager also contains the Packages tab, which lists the images and packages that can be installed on the individual components.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Firmware Upgrade Process

This topic describes the general upgrade process for all Cisco UCS components.



These tasks form the firmware update process of the Cisco UCS deployment:

Step 1 Update the dual-flash components (adapters, Cisco IMC instances, IOMs).

Step 2 Activate the dual-flash components.

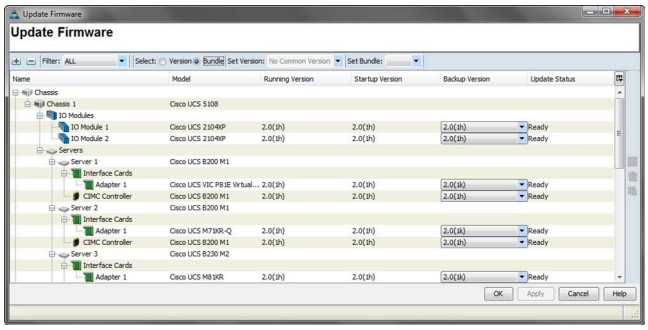
Step 3 Upgrade and activate the Fabric Interconnect firmware.

Step 4 Upgrade the firmware of host components using a service policy. This step includes the creation of a host firmware package and applying the host firmware package to a service policy.

https://t.me/learningnets

Step 1: Update Dual-Flash Components

- The update process affects only the backup firmware partition and is safe to perform during production (subject to change control policy).
- Cisco IMC, IOM, and adapter must be updated before they can be activated on the new version.



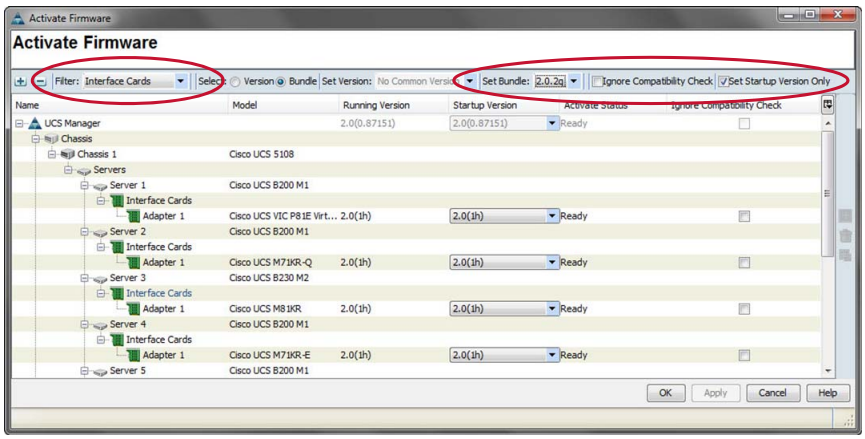
Equipment > Firmware Management > Update Firmware

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

For each dual-flash component, the update process operates on the backup partition. You can safely update the backup partition of any component during regular business hours. Performing this step now will save time during the maintenance window for activating the new firmware.

Step 2A: Activate Adapters

- Activating firmware on the interface card causes a server reboot.
- Plan for a maintenance window.



Equipment > Firmware Management > Activate Firmware

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

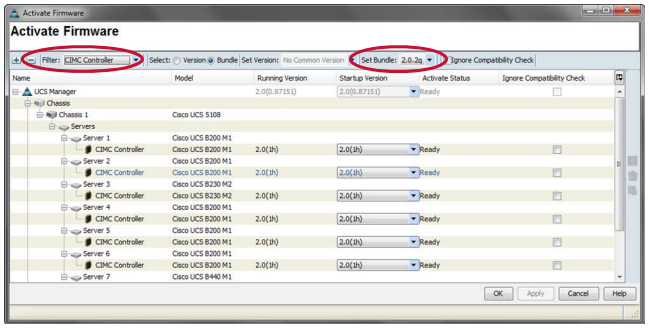
Updating the backup flash on the adapter is a safe operation at any time, but activating new firmware on the adapter causes the associated server to reboot. This activation should be performed only during a change control window or if all virtual machines (VMs) have been moved safely off a hypervisor that runs on the host.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Step 2B: Activate Cisco IMC Instances

- Cisco IMC can be activated without disruption to the operating system on the blade server.
- During firmware activation, KVM, SoL, and IPMI will be lost.



Equipment > Firmware Management > Activate Firmware

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

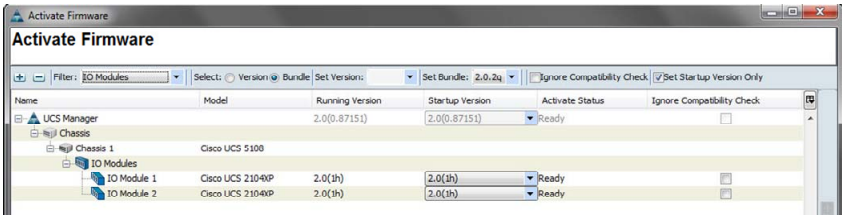
The safest firmware upgrade that an administrator can perform on Cisco UCS is that of updating and activating Cisco IMC instances. As discussed earlier, updating the backup partition of Cisco IMC has no impact on communications. Activating the new startup version to the eight servers that are shown in this 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).

https://t.me/learningnets

Step 2C: Activate IOMs

- Set the filter to select the IOMs and select a common version or bundle from the drop-down list.
- 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 Technical Assistance Center (TAC) recommendation.



Equipment > Firmware Management > Activate Firmware

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

Choose **Equipment > Firmware Management > Installed Firmware** and click **Activate Firmware**. In the Activate Firmware pop-up window, choose **IO Modules** from the Filter drop-down list. Choose the common version or bundle that the IOMs should share from the Set Version drop-down list. Click **Apply** to start the 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 startup. When the activation is complete, the old startup version becomes the backup version.

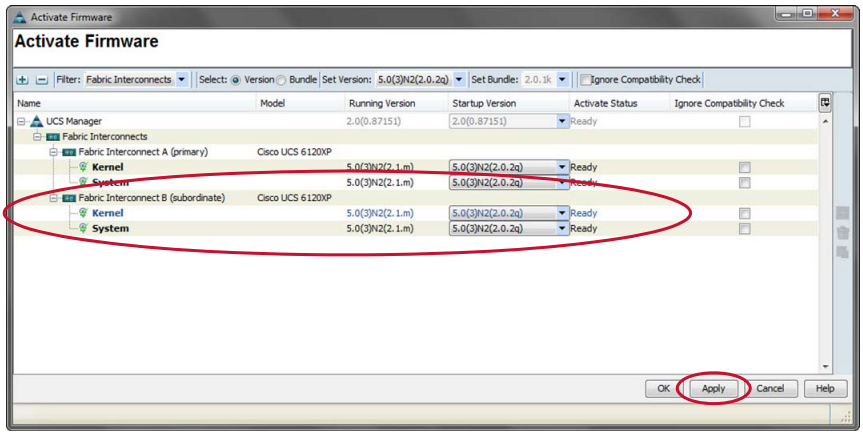
The best practice is to check the Set Startup Version Only check box when activating new firmware on IOMs. This setting causes the IOM to wait until its associated Fabric Interconnect reboots.

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

Step 3: Upgrade and Activate Fabric Interconnect Firmware

- First, activate the subordinate Fabric Interconnect.
- The kernel and system image versions must be the same.



Equipment > Firmware Management > Activate Firmware

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

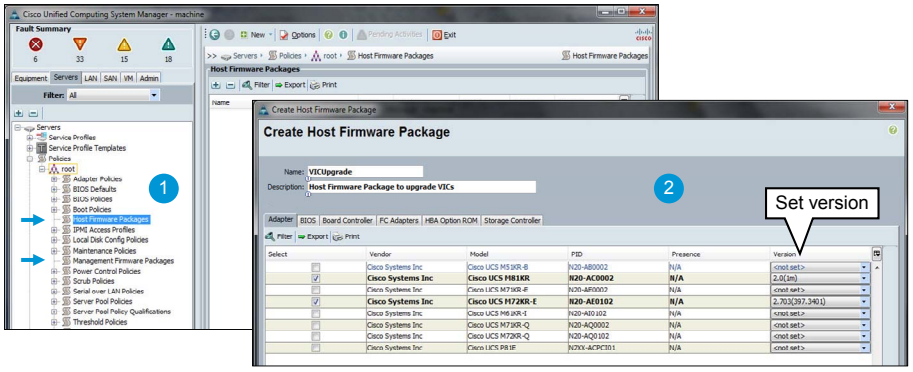
Choose **Equipment** > **Firmware Management** > **Installed Firmware** and click **Activate Firmware**. A dialog box opens for you to select the desired firmware versions from drop-down lists. After you have chosen the correct version of kernel and system images for each Fabric Interconnect, click **Apply** to begin the upgrade.

Note	The kernel and system must use the same major version.

https://t.me/learningnets

Step 4A: Create Host Firmware Package

- There are two types of firmware packages for server policies:
  - Host
  - Management
- There are multiple tabs for the different components.



Servers > Policies > root > Host Firmware Packages

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

A few upgradable components cannot be updated through direct firmware updates. The server BIOS, host bus adapter (HBA), HBA option ROM, and 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.

Under the Policy category of the navigation pane Server tab, choose **Host Firmware Packages**. Right-click the policy or click the small plus sign (+) in the content pane to start the host firmware package creation wizard.

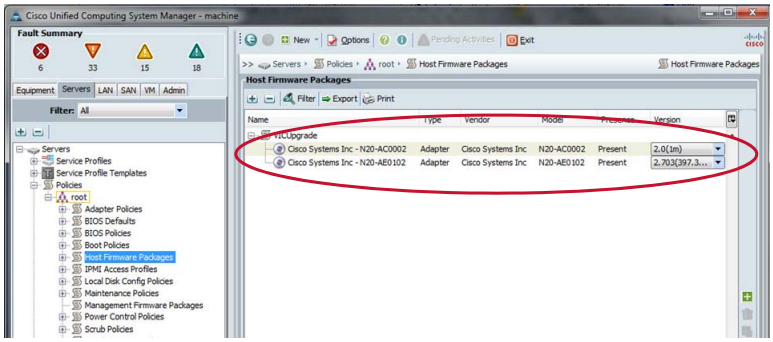
A unique name for the host firmware package must be defined. Optionally, a description can be provided.

In the host firmware package creation window, the hardware components are divided in separate tabs. For the components that must be upgraded, you must select the corresponding tab, select the model from the list, and set the version.

https://t.me/learningnets

Step 4B: Apply Host Firmware Package

- The “VICUpgrade” host firmware package can now be applied to a service policy.



Servers > Policies > root > Host Firmware Packages

© 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

Issue: Upgrade Failure on Fabric Interconnect

- Symptom: There has been a failed upgrade attempt of the Fabric Interconnect.
- The Fabric Interconnect boots with the loader> prompt.
- The upgrade procedure has not been followed.
- Remediation is required:
  - Requires access to console and TFTP server from which to boot.
  - Remediation requires system recovery.

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

In this troubleshooting scenario, you are facing a Fabric Interconnect that has failed a software upgrade and boots with the loader> prompt.

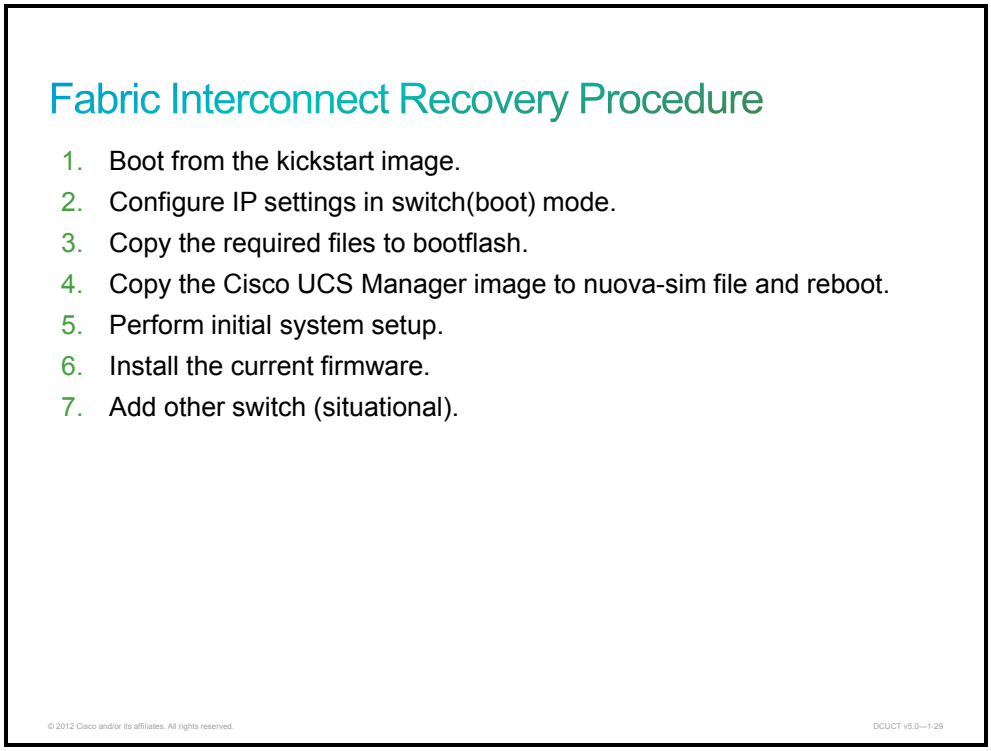
The Fabric Interconnects enable you to perform a system recovery procedure like the one that is available on Cisco NX-OS switches.

On a normal Cisco UCS Fabric Interconnect, the kickstart, system, and Cisco UCS Manager boot files are located in the /bootflash/installables/switch directory. Additionally, there is a symbolic link from /bootflash/nuova-sim-mgmt-ngs.0.1.0.001.bin to the Cisco UCS Manager boot file that is located in the /bootflash/installables/switch directory.

To repair the Fabric Interconnect, you must perform system recovery.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets



This procedure summarizes the system recovery process on a Fabric Interconnect. This is not a common process, but certain firmware upgrade failures may require this procedure to rebuild the affected Fabric Interconnect. You must perform these steps, starting with one switch in the deployment:

Step 1 Boot from the kickstart image.

Step 2 Configure IP settings in switch(boot) mode.

Step 3 Copy the required files to bootflash.

Step 4 Rename the Cisco UCS Manager image and reboot.

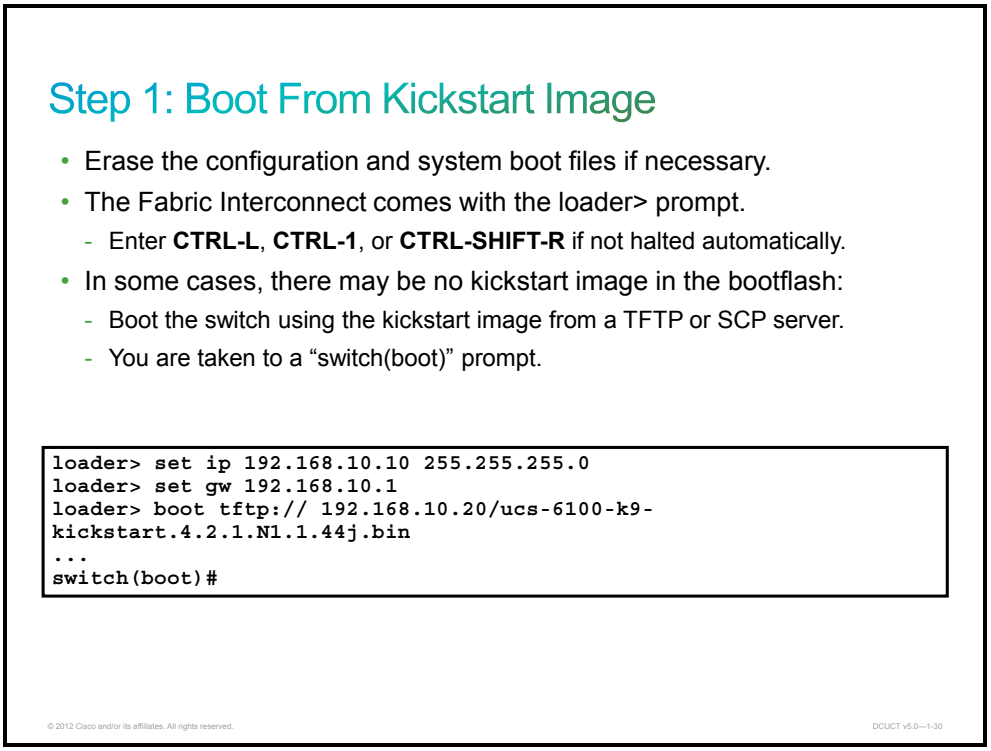
Step 5 Perform initial system setup.

Step 6 Install the current firmware.

Step 7 Add other switch (situational).

Note	Some verifications should be performed during this procedure. The verification steps have been omitted for brevity.

https://t.me/learningnets



To perform the system recovery process, you may have to erase the configuration and system boot files. A Fabric Interconnect without any boot files boots with the loader> prompt. You can also enter the loader> by interrupting the boot process using the **CTRL-L**, **CTRL-1**, or **CTRL-SHIFT-R** key sequence. This key combination may be required if the system does not halt automatically and you want to replace the boot files.

If there is no kickstart image in the bootflash, you can boot the switch using the kickstart image from a TFTP or SCP server. When this external boot is complete, the switch will show the switch(boot)# prompt.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Step 2: Configure IP Settings in Switch(boot) Mode

- The configuration in performed in switch(boot) mode:
  - IP address and subnet mask of the mgmt 0 interface
  - Default gateway information

```
switch(boot)#configure terminal
switch(boot)(config)#interface mgmt 0
switch(boot)(config-if)#ip address 192.168.10.10 255.255.255.0
switch(boot)(config-if)#no shutdown
switch(boot)(config-if)#exit
switch(boot)(config)#ip default-gateway 192.168.10.1
switch(boot)(config)#exit
switch(boot)#
```

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

In the switch(boot)# mode, you must configure the IP address on the mgmt0 interface and set the default gateway. These parameters should enable IP connectivity with other systems.

Step 3: Copy Files to Bootflash

- There are some files that must be copied to bootflash:
  - Kickstart image
  - System image
  - Cisco UCS Manager image
- There are various transfer methods: FTP, SCP, and TFTP.

```
switch(boot)#copy ftp://user1@[192.168.10.30/ucs-6100-k9-
kickstart.4.2.1.N1.1.44j.bin bootflash:

switch(boot)#copy ftp://user1@ 192.168.10.30/ucs-6100-k9-
system.4.2.1.N1.1.44j.bin  bootflash:

switch(boot)#copy ftp://user1@ 192.168.10.30/ucs-manager-
k9.1.4.4j.bin bootflash:
```

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

When the IP connectivity is assured, you must copy three files to the Fabric Interconnect bootflash. The required files are the kickstart image, the system image, and the Cisco UCS Manager image. You can transfer the files using FTP, SCP, or TFTP. This figure illustrates an FTP-based example.

https://t.me/learningnets

Step 4: Copy Cisco UCS Manager Image and Reboot

- Copy the Cisco UCS Manager image.
  - Reserved target name "nuova-sim-mgmt-nsg.0.1.0.001.bin”
- Exit switch(boot) mode to reboot the Fabric Interconnect.
  - The switch boots in the loader screen.
  - Enter **CTRL-L**, **CTRL-1**, or **CTRL-SHIFT-R** if necessary.
- Boot with the kickstart and system images at the same time.

```
switch(boot)#copy bootflash:ucs-manager-k9.1.4.4j.bin
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

switch(boot)#exit

…
loader>
loader> boot ucs-6100-k9-kickstart.4.2.1.N1.1.44j.bin ucs-
6100-k9-system.4.2.1.N1.1.44j.bin
```

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

Next, you must rename the Cisco UCS Manager image to the reserved name "nuova-sim-mgmt-nsg.0.1.0.001.bin”. The name of the nuova-sim file is exactly as shown and does not change from one release to the next.

Then, exit switch(boot)# mode, which causes the Fabric Interconnect to automatically reboot. The switch boots in the loader screen. You can use the **CTRL-L**, **CTRL-1**, or **CTRL-SHIFT-R** key combination, if necessary.

When the switch enters the loader> mode, you must boot with the kickstart and system images at the same time.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Step 5: Perform Initial System Setup

- Initial system setup can be performed in either of these two methods:
  - CLI
  - Started in CLI and completed in GUI
- Difference between standalone and cluster setup

```
Enter the installation method (console/gui)?  console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch.  Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 IPv4 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Virtual IPv4 address : 192.168.10.12
Configure the DNS Server IPv4 address? (yes/no) [n]: yes
  DNS IPv4 address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
...
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

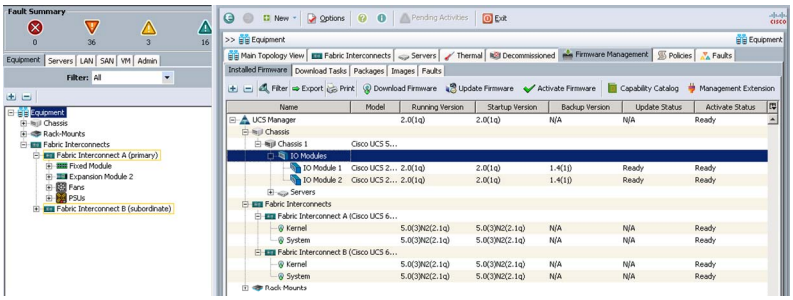
© 2012 Cisco and/or its affiliates. All rights reserved.

Next, the switch boots and enters the initial system setup wizard. You can choose the method of setup: GUI or CLI. If you choose GUI, you need to enter only basic settings using the CLI and complete the setup in the GUI. If you choose CLI, you can enter all of the parameters that are shown in this figure, and then connect to the Cisco UCS Manager GUI to configure the system. The initial system setup varies depending on whether you have a backup from which to restore the configuration, and whether this is a standalone switch or a cluster.

https://t.me/learningnets

Step 6: Install Current Firmware

- Download, update, and activate firmware.
- This can be done in the Cisco UCS Manager GUI or CLI.
- Perform the process CLI if you cannot connect to the Cisco UCS Manager GUI.



Equipment > (Work pane) > Firmware Management > Installed Firmware

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

An important step after the system recovery is to download, update, and activate the current firmware. These operations can be performed in the Cisco UCS Manager GUI or CLI. If you experience problems connecting to the GUI, update the firmware in the CLI and try launching the Cisco UCS Manager GUI again.

Step 7: Add Cluster Peer

- Perform this step depending on the situation in the cluster.
- Disconnect the second switch.
- Perform full or partial system recovery.
- Reconnect the second switch and join the cluster.

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

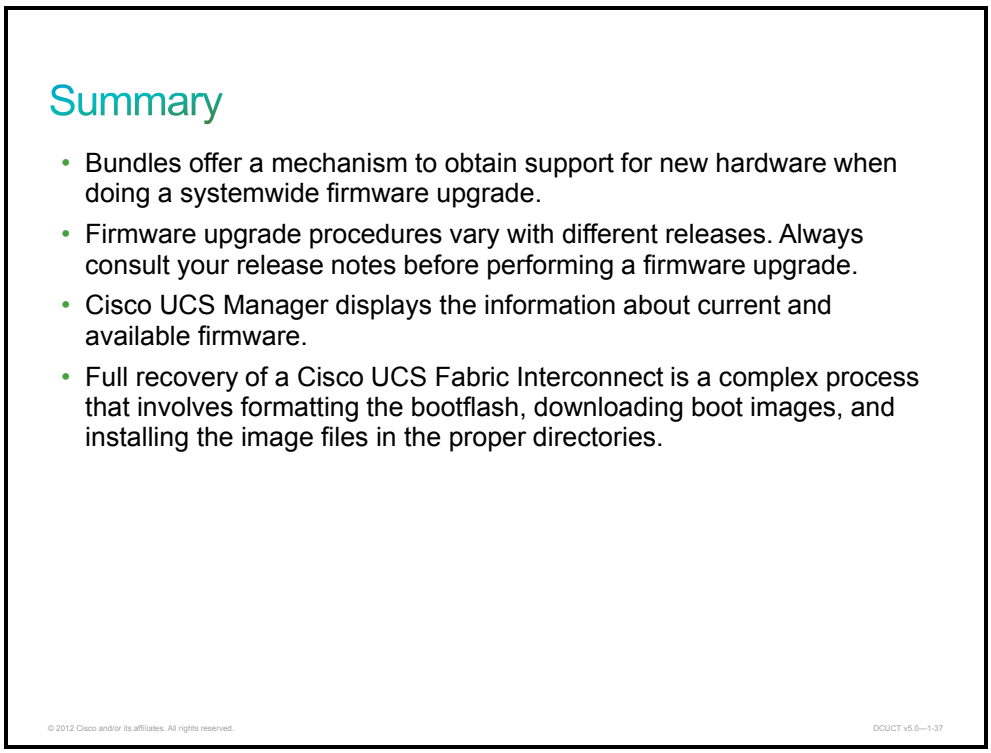
Depending on your environment, you may or may not want to perform system recovery on the second switch in the cluster. If you do, you should first disconnect the second switch from the first one, and then perform system recovery. When the system is recovered, reconnect the second switch and join the cluster.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

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



https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Lesson 6

Troubleshooting Cisco UCS B-Series Hardware

Overview

Cisco Unified Computing System (Cisco UCS) blade memory errors can be difficult to troubleshoot and they account for a high percentage of support calls. Return Materials Authorization (RMA) costs are high and, in many cases, replacing a DIMM does not fix the problem. This lesson describes the sources of troubleshooting information in the Cisco UCS environment. It discusses various hardware failure scenarios and provides solutions that will help a support engineer to correctly identify and fix hardware and memory issues.

Objectives

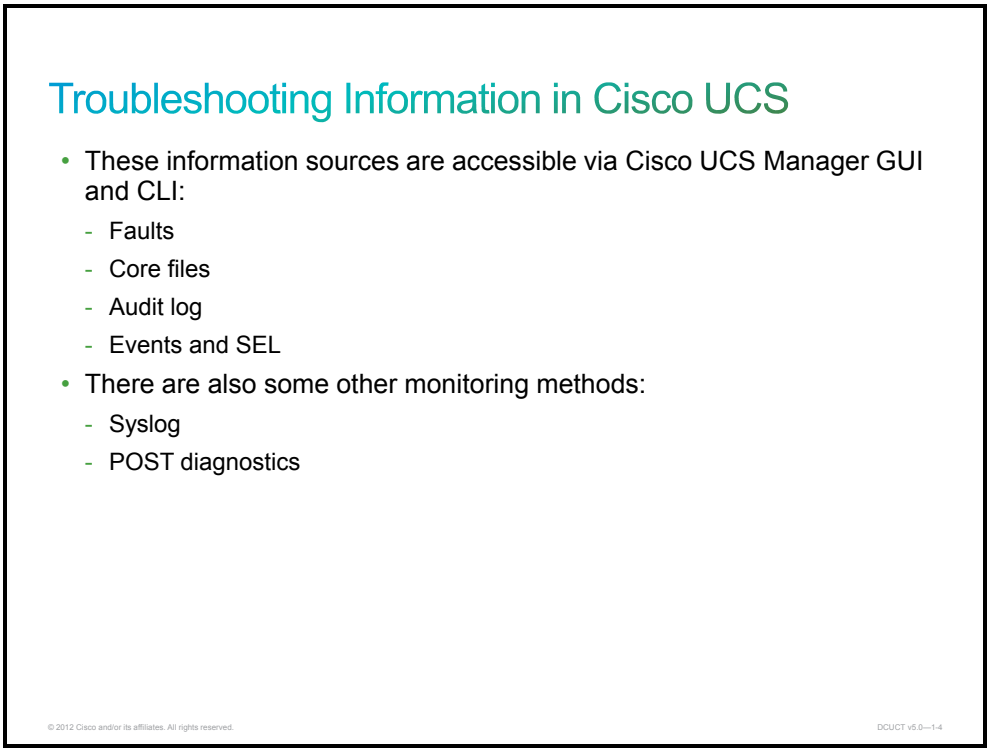
Upon completing this lesson, you will be able to identify best practices for troubleshooting Cisco UCS B-Series hardware. This ability includes being able to meet these objectives:

- Use Cisco UCS CLI and GUI to detect failed hardware
- List tools and techniques that are used to identify memory configuration errors and memory failures

https://t.me/learningnets

Defective Hardware

This topic describes how to use Cisco UCS CLI and GUI to detect failed hardware.



The Cisco UCS Manager GUI provides several tabs and other areas that you can use to find troubleshooting information for a Cisco UCS domain. For example, you can view faults and events for specific objects or for all objects in the system.

You can also use the Cisco UCS Manager CLI to obtain troubleshooting information. The CLI includes several **show** commands that you can use to find troubleshooting information for a Cisco UCS domain. These **show** commands are scope-aware. For example, if you enter the **show fault** command from the top-level scope, it displays all of the faults in the system. If you scope to a specific object, the **show fault** command displays faults that are related to that object only.

In general, these information sources are accessible via Cisco UCS Manager GUI and CLI:

- Faults
- Core files
- Audit log
- Events and System Event Log (SEL)

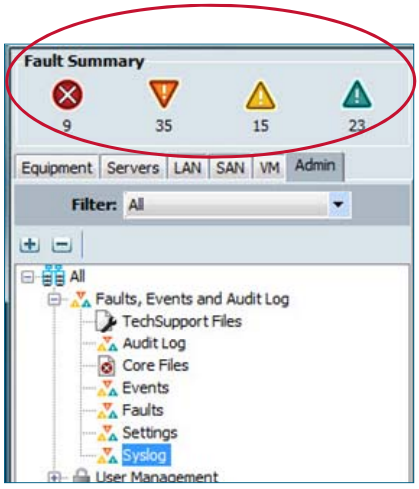
Further monitoring methods include syslog and power-on self-test (POST) diagnostics.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Faults

- Represent a failure or that an alarm threshold has been raised
- Can change from one state or severity to another
- Remain in Cisco UCS Manager until the fault is cleared and deleted
- Fault Summary bar is displayed above the configuration tabs
- Color images represent severity levels of faults:
  - Critical
  - Major
  - Minor
  - Warning



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

In Cisco UCS, a fault is a mutable object that is managed by Cisco UCS Manager. Each fault represents a failure in the Cisco UCS domain or an alarm threshold that has been raised. During the life cycle of a fault, it can change from one state to another or from one severity to another.

Each fault includes information about the operational state of the affected object at the time that the fault was raised. If the fault is transitional and the failure is resolved, the object transitions to a functional state.

A fault remains in Cisco UCS Manager until the fault is cleared and deleted according to the settings in the fault collection policy.

This figure shows the global fault summary, which 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 Severities

Severity Level	Description
Critical	• Requires immediate corrective action • Might indicate that object is out of service and must be restored
Major	• Requires urgent corrective action • Might indicate a severe degradation in the capability of the object
Minor	• Requires corrective action to prevent a more serious fault • Condition may not be degrading the object capacity
Warning	• Potentially or impending service-affecting fault • Has no significant effects in the system • Action should be taken to further diagnose
Condition	• Message about a condition • Possibly independently insignificant
Info	• Basic notification or informational message • Possibly independently insignificant

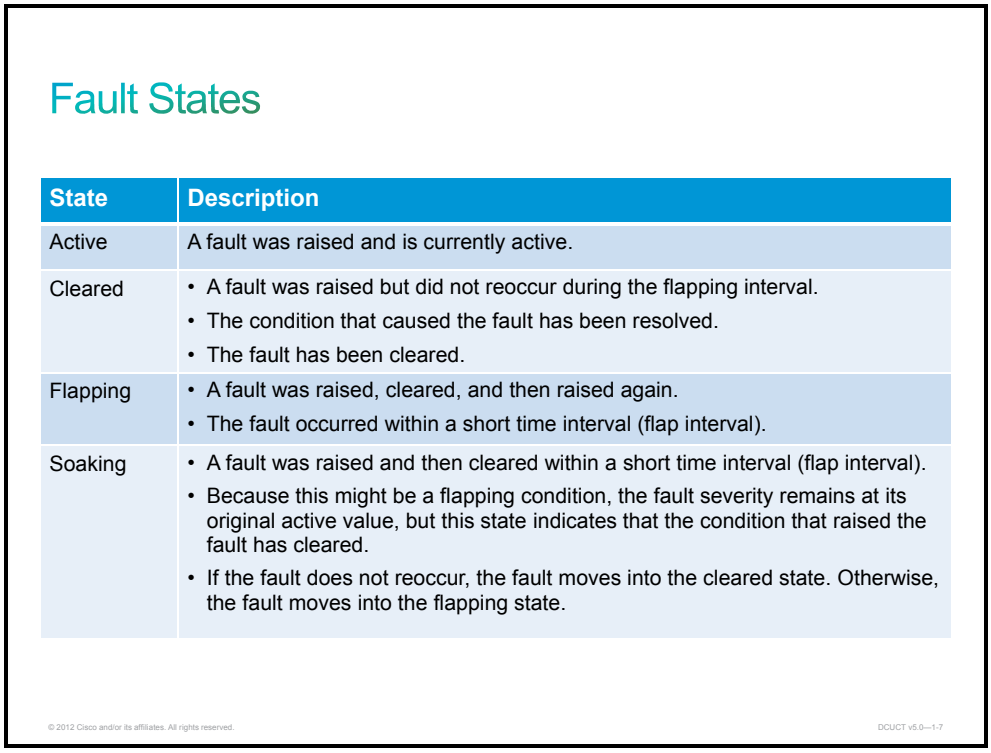
© 2012 Cisco and/or its affiliates. All rights reserved.

A fault that is raised in a Cisco UCS domain can transition through more than one severity level during its life cycle. This table describes the fault severities that you may encounter.

Severity	Description
Critical	Service-affecting condition that requires immediate corrective action. For example, this severity could indicate that the managed object is out of service and its capability must be restored.
Major	Service-affecting condition that requires urgent corrective action. For example, this severity could indicate a severe degradation in the capability of the managed object and that its full capability must be restored.
Minor	Non-service-affecting fault condition that requires corrective action to prevent a more serious fault from occurring. For example, this severity could indicate that the detected alarm condition is not degrading the capacity of the managed object.
Warning	Potential or impending service-affecting fault that has no significant effects on the system. You should take action to further diagnose, if necessary, and correct the problem to prevent it from becoming a more serious service-affecting fault.
Condition	Informational message about a condition, possibly independently insignificant.
Info	Basic notification or informational message, possibly independently insignificant.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



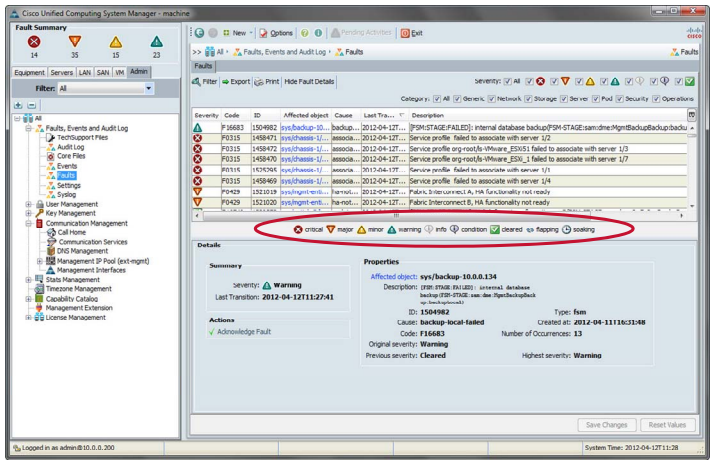
A fault that is raised in a Cisco UCS domain transitions through more than one state during its life cycle. This table describes the possible fault states in alphabetical order.

State	Description
Cleared	Condition that has been resolved and cleared.
Flapping	Fault that was raised, cleared, and raised again within a short time interval, known as the flap interval.
Soaking	Fault that was raised and cleared within a short time interval, known as the flap interval. Because this state may be a flapping condition, the fault severity remains at its original active value, but this state indicates the condition that raised the fault has cleared.

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.



Admin > All > Faults, Events and Audit Log > Faults

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

Choose **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.

A fault has the following life cycle:

Step 1 A condition occurs in the system and Cisco UCS Manager raises a fault. This is the active state.

Step 2 When the fault is alleviated, it enters a flapping or soaking interval that is designed to prevent flapping. Flapping occurs when a fault is raised and cleared several times in rapid succession. During the flapping interval, the fault retains its severity for the length of time that is specified in the fault collection policy.

Step 3 If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared.

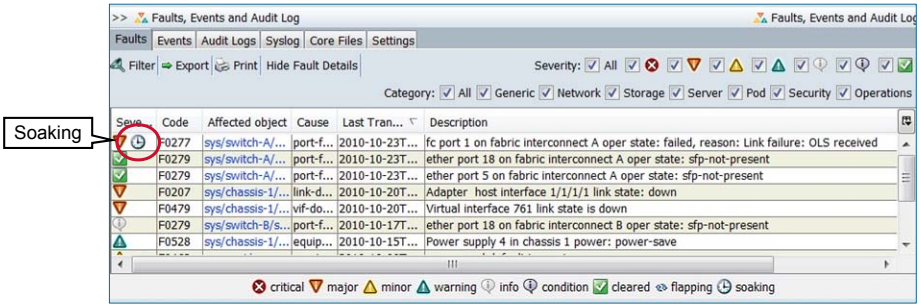
Step 4 The cleared fault enters the retention interval. This interval ensures that the fault reaches the attention of an administrator even if the condition that caused the fault has been alleviated and the fault has not been deleted prematurely. The retention interval retains the cleared fault for the length of time that is specified in the fault collection policy.

Step 5 If the condition reoccurs during the retention interval, the fault returns to the active state. If the condition does not reoccur, the fault is deleted.

https://t.me/learningnets

Fault in Soaking State

- An interface has transitioned between operational and nonoperational within the 10-second flapping interval.



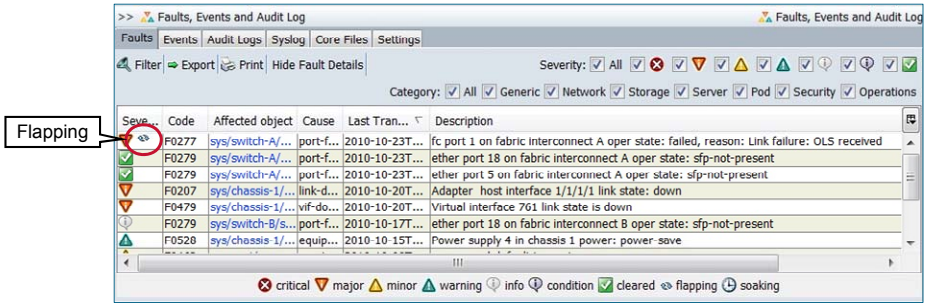
Admin > All > Faults, Events and Audit Log > Faults

© 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.

Fault in Flapping State

- An interface has transitioned between operational and nonoperational for longer than the 10-second flapping interval.



Admin > All > Faults, Events and Audit Log > Faults

© 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 greater than the flapping interval. The default flapping interval is 10 seconds.

https://t.me/learningnets

Faults in Cisco UCS Manager CLI

```
s6200-A# show fault
Major     F0637    2012-06-07T14:21:00.185    333097 Power cap application failed for
server ½
Major     F0637    2012-05-30T14:07:41.957    319033 Power cap application failed for
server 1/4
Major     F0637    2012-05-29T15:37:12.533    319182 Power cap application failed for
server 1/3
Major     F0637    2012-05-29T15:23:57.274    227716 Power cap application failed for
server 1/1
Minor     F0463    2012-03-23T15:57:42.324    232532 server pool default is empty
Major     F0369    2012-03-10T23:38:38.805    226411 Power supply 2 in fabric interconnect
A power: error
Major     F0374    2012-03-10T23:38:38.805    226412 Power supply 2 in fabric interconnect
A operability: inoperable
<output omitted>

s6200-A# show fault ?                                  Various display options
  0-9223372036854775807  ID
  <CR>
  >                      Redirect it to a file
  >>                     Redirect it to a file in append mode
  cause                  Cause
  detail                 Detail
  severity               Severity
  |                      Pipe command output to filter

s6200-A# show fault  cause ?                           Display faults with a specific cause
<output omitted>
  wait-for-conn-ready-failed                              Wait For Conn Ready Failed
  wait-for-maint-permission-failed                       Wait For Maint Permission
Failed
  wait-for-maint-window-failed                            Wait For Maint Window Failed
  wait-foribmcfw-update-failed                            Wait Foribmcfw Update Failed
  wait-on-phys-failed                                          Wait On Phys Failed
```

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

If you want to view the faults for all objects in the system, enter the **show fault** command from the top-level scope. If you want to view the faults for a specific object, scope to that object and then execute the **show fault** command.

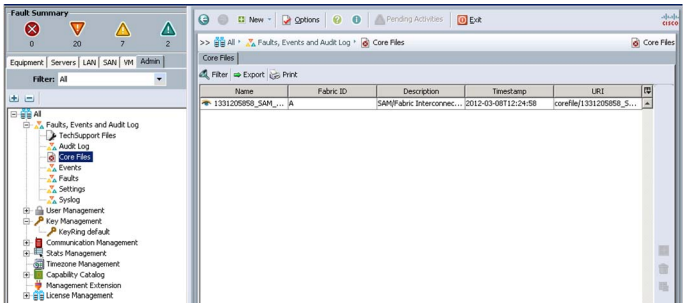
If you want to view all available details about a fault, enter the **show fault detail** command.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Core Files

- Critical failures in Cisco UCS Manager and some of the Cisco UCS components can cause the system to create a core file.
- Each core file contains a large amount of data about the system and the component.
- You can export a copy of a core file to a TFTP location.



Admin > All > Faults, Events and Audit Log > Core Files

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

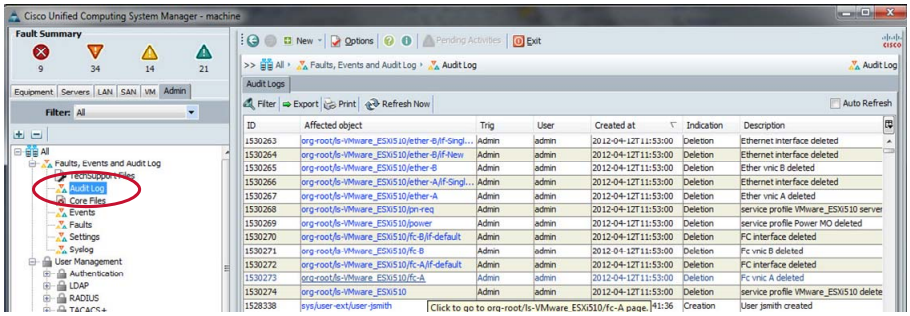
Critical failures in Cisco UCS Manager and in some of the Cisco UCS components, such as a Fabric Interconnect or an I/O module (IOM), can cause the system to create a core file. Each core file contains a large amount of data about the system and the component at the time of the failure.

Cisco UCS Manager manages the core files from all of the components. You can configure Cisco UCS Manager to export a copy of a core file to a location on an external TFTP server as soon as that core file is created. The core file is not a file that the administrator will interpret but rather a file that Cisco Technical Assistance Center (TAC) engineers will utilize.

https://t.me/learningnets

Audit Log

- The audit log records the following:
  - Login events for all users
  - Actions that they performed in the Cisco UCS Manager interface
- This information is useful if an unapproved change has been made.



Admin > All > Faults, Events and Audit Log > Audit Log

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

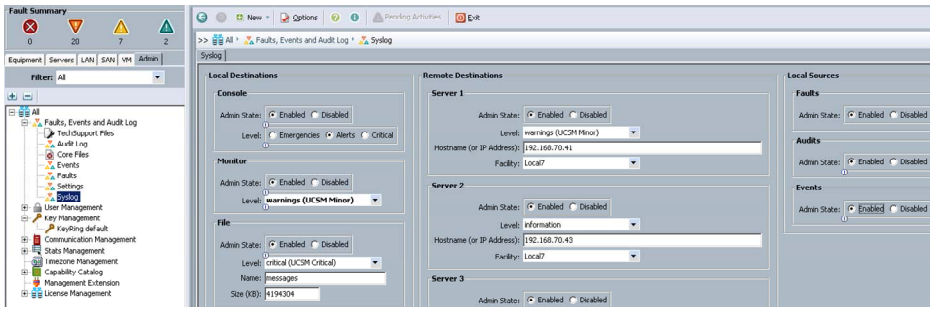
The audit log records actions that are performed by users in Cisco UCS Manager, including direct and indirect actions. Each entry in the audit log represents a single, nonpersistent action. For example, if a user logs in or logs out, or creates, modifies, or deletes an object such as a service profile, Cisco UCS Manager adds an entry to the audit log for that action. This information is useful if an unapproved change has been made.

The audit log can be accessed from the Admin tab. Expand **Faults, Events and Audit Log**, and then choose **Audit Log**.

https://t.me/learningnets

Events and Logging Options

- This example represents nonpersistent conditions in the Cisco UCS domain.
- Events remain in Cisco UCS until the event log fills up.
- When the log is full, Cisco UCS Manager purges the log and all events.
- Logging data is available in several places.
- All logging is disabled by default.



Admin > All > Faults, Events and Audit Log > Syslog

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

In Cisco UCS, an event is an immutable object that is managed by Cisco UCS Manager. Each event represents a nonpersistent condition in the Cisco UCS domain. After Cisco UCS Manager creates and logs an event, the event does not change. For example, if you power on a server, Cisco UCS Manager creates and logs an event for the beginning and the end of that request.

You can view events for a single object, or you can view all of the events in a Cisco UCS domain from either the Cisco UCS Manager CLI or the Cisco UCS Manager GUI. Events remain in Cisco UCS until the event log fills up. When the log is full, Cisco UCS Manager purges the log and all of the events in it.

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.

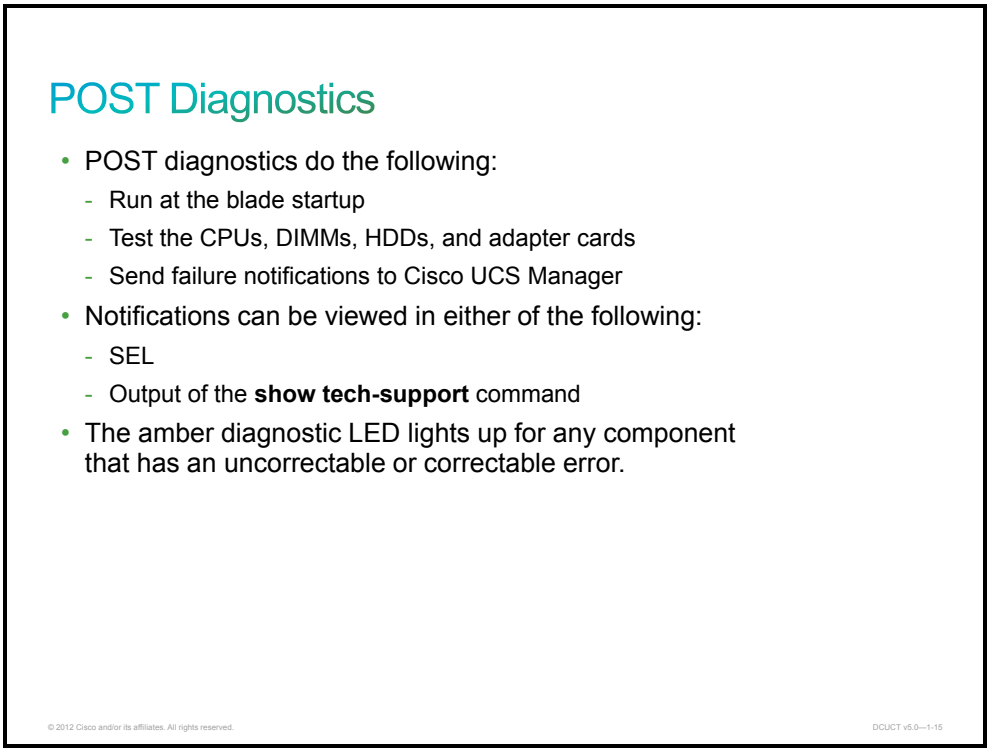
The Monitor option allows logging messages to be copied via Secure Shell (SSH) to Remote Terminal (RT) sessions. Be conservative when setting the logging level. If enough messages per second are transmitted over the remote session, the connection can easily be overloaded.

The File option allows logging messages to be stored in local flash memory. The default file size of more than 4 GB is not a wise choice. 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



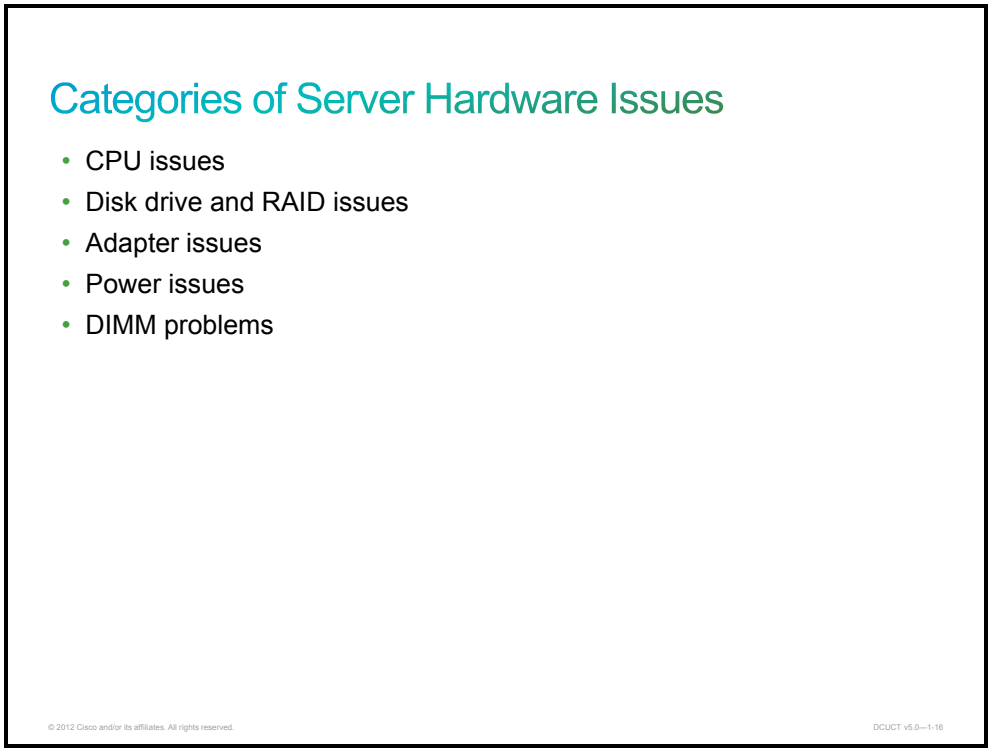
At the blade startup, the POST diagnostics test the CPUs, DIMMs, hard disk drives (HDDs), and adapter cards. Any failure notifications are sent to Cisco UCS Manager. You can view these notifications in the SEL or in the output of the **show tech-support** command. If errors are found, an amber diagnostic LED lights up next to the failed component. During run time, the blade BIOS, component drivers, and operating system monitor for hardware faults. The amber diagnostic LED lights up for a component if an uncorrectable error occurs, or if a correctable error over the allowed threshold—such as a host error checking and correction (ECC) error—occurs.

The LED states are saved. If you remove the blade from the chassis, the LED values persist for up to 10 minutes. Pressing the LED diagnostics button on the motherboard causes the LEDs that currently show a component fault to illuminate for up to 30 seconds. The LED fault values are reset when the blade is reinserted into the chassis and booted.

If any DIMM insertion errors are detected, they can cause the blade discovery to fail, and errors are reported in the server POST information. You can view these errors in either the Cisco UCS Manager CLI or the Cisco UCS Manager GUI. The blade servers require specific rules to be followed when populating DIMMs in a blade server. The rules depend on the blade server model. Refer to the documentation for a specific blade server for those rules.

The HDD status LEDs are on the front of the HDD. Faults on the CPU, DIMMs, or adapter cards also cause the server health LED to light up as solid amber for minor error conditions or blinking amber for critical error conditions.

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



The issues that you may experience on Cisco UCS server blades can be classified into these main categories:

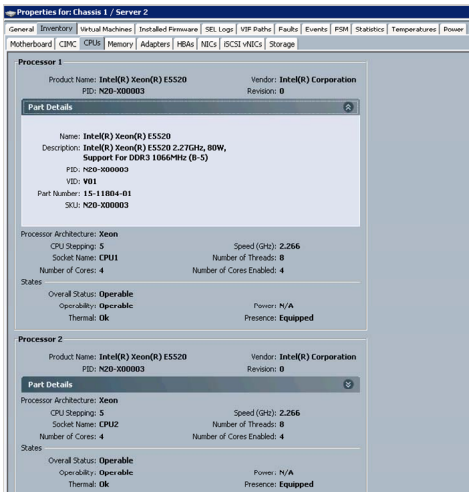
- CPU issues
- Disk drive and RAID issues
- Adapter issues
- Power issues
- DIMM memory problems

https://t.me/learningnets

Troubleshooting CPU Issues

- All Cisco UCS servers support 1 to 2 or 1 to 4 CPUs.
- A problem with a CPU can cause any of the following situations:
  - A server can fail to boot.
  - Performance can slow down.
  - Serious data loss or corruption can occur.

```
UCS-A# scope server 1/5
UCS-A /chassis/server # show cpu

CPU:
   ID Presence  Architecture  Socket Cores  Speed(GHz)
   -- --------- ------------- ------ ------ ----------
   1  Equipped      Xeon         CPU1    6     3.333000
   2  Equipped      Xeon         CPU2    6     3.333000
```



Server > Inventory > CPUs

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

All Cisco UCS servers support 1 to 2 or 1 to 4 CPUs. A problem with a CPU can cause a server to fail to boot, run very slowly, or cause serious data loss or corruption. If CPU issues are suspected, consider the following:

- All CPUs in a server should be the same type, running at the same speed, and populated with the same number and size of DIMMs.
- If the CPU was recently replaced or upgraded, make sure that the new CPU is compatible with the server and that a BIOS that supports the CPU was installed. Refer to the server documentation for a list of supported Cisco models and product IDs. Use only CPUs that are supplied by Cisco. The BIOS version information can be found in the software release notes.
- The CPU speed and memory speed should match. If they do not match, the server runs at the slower of the two speeds.
- If a CPU fails, the remaining active CPU or CPUs do not have access to memory that is assigned to the failed CPU.
- If a CPU in a multi-CPU system is replaced, the stepping level must match on all CPUs or the operating system and hypervisor will crash.

https://t.me/learningnets

Troubleshooting Adapter Issues

- All adapters are unique Cisco designs.
- Adapters that are not from Cisco are not supported.
- A problem with the Ethernet or FCoE adapter can cause the following situations:
  - A server can fail to connect to the network.
  - The server can become unreachable from Cisco UCS Manager.

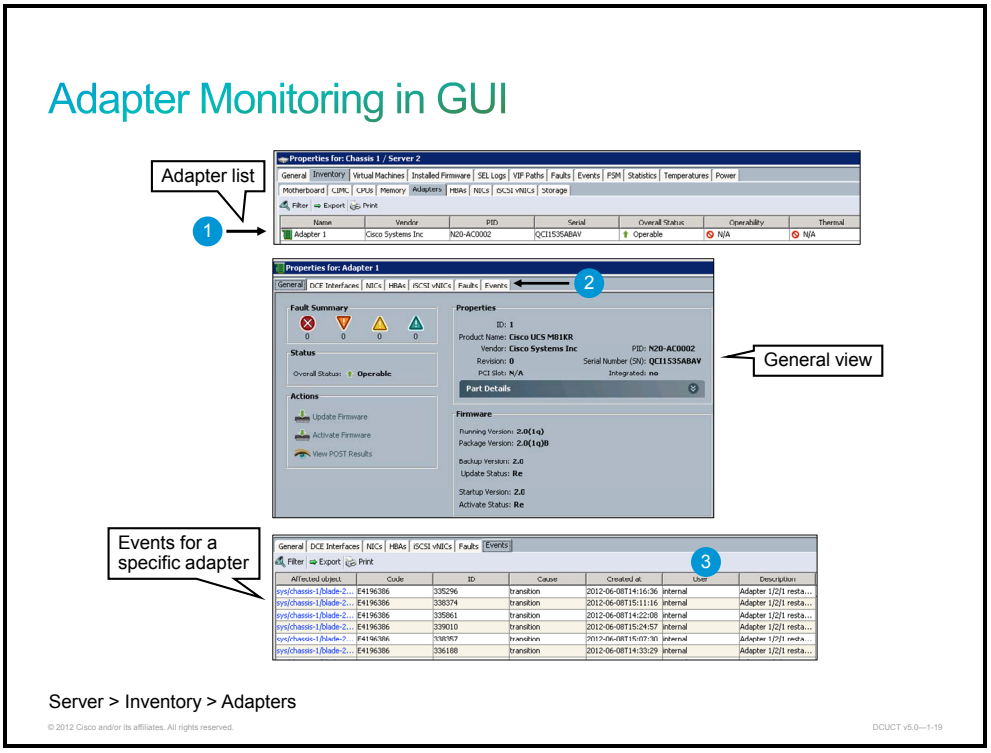
```
UCS-A# scope server 1/5
UCS-A /chassis/server # show adapter detail

Adapter:
    Id: 2
    Product Name: Cisco UCS 82598KR-CI
    PID: N20-AI0002
    VID: V01                          Various adapter details
    Vendor: Cisco Systems Inc
    Serial: QCI132300GG
    Revision: 0
    Mfg Date: 2009-06-13T00:00:00.000
    Slot: N/A
    Overall Status: Operable
    Conn Path: A,B
<output omitted>
```

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

A problem with the Ethernet or Fibre Channel over Ethernet (FCoE) adapter can cause a server to fail to connect to the network and make it unreachable from Cisco UCS Manager. All adapters are unique Cisco designs. Adapters that are not from Cisco are not supported. If adapter issues are suspected, consider the following:

- Check if the Cisco adapter is genuine.
- Check if the adapter type is supported in the software release that you are using. The Internal Dependencies table in the Cisco UCS Manager Release Notes provides minimum and recommended software versions for all adapters.
- Check if the appropriate firmware for the adapter has been loaded on the server.
- If the software version update was incomplete, and the firmware version no longer matches the Cisco UCS Manager version, update the adapter firmware as described in the appropriate Cisco UCS Manager configuration guide for your installation.
- If you are migrating from one adapter type to another, ensure that the drivers for the new adapter type are available. Update the service profile to match the new adapter type. Configure appropriate services to that adapter type.
- If you are using dual adapters, be aware that there are certain restrictions on the supported combinations.

https://t.me/learningnets



The Cisco UCS Manager GUI allows you to monitor the server adapters in the Server > Inventory > Adapters menu.

Select an adapter to display its general parameters and choose any tab for its details. This figure illustrates how to view events for the selected adapter.

https://t.me/learningnets

Bad or Inoperable Adapter

Problem	Server connectivity failure
Monitoring Information	• Adapter is reported as bad in the SEL and POST • Adapter is reported as inoperable in Cisco UCS Manager
Possible Cause	• Incorrect model or unsupported firmware • Adapter incorrectly seated
Solution	• Verify that the adapter is supported on that server model. • Verify that the adapter has the required firmware version. • Reseat it to ensure a good contact, reinsert the server, and rerun POST. • Verify that the adapter is the problem by trying it in a server that is known to be functioning correctly and that uses the same adapter type.

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

If you have connectivity problems on your blade server and if the adapter is reported as bad in the SEL or POST, or reported as inoperable in Cisco UCS Manager, the adapter may not have the required firmware or it may be incorrectly installed. In this case, perform these verification tasks:

- Verify that the adapter is supported on that server model.
- Verify that the adapter has the required firmware version.
- Reseat it to ensure a good contact, reinsert the server, and rerun POST.
- Verify that the adapter is the problem by trying it in a server that is known to be functioning correctly and that uses the same adapter type.

https://t.me/learningnets

Issue: Server Performance Degradation

- You discover this symptom:
  - The performance of one server is lower than that of the other servers in the chassis.
- The system environment is as follows:
  - All blade servers have the same hardware.
  - All blade servers run the same operating system, patches, and applications.

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

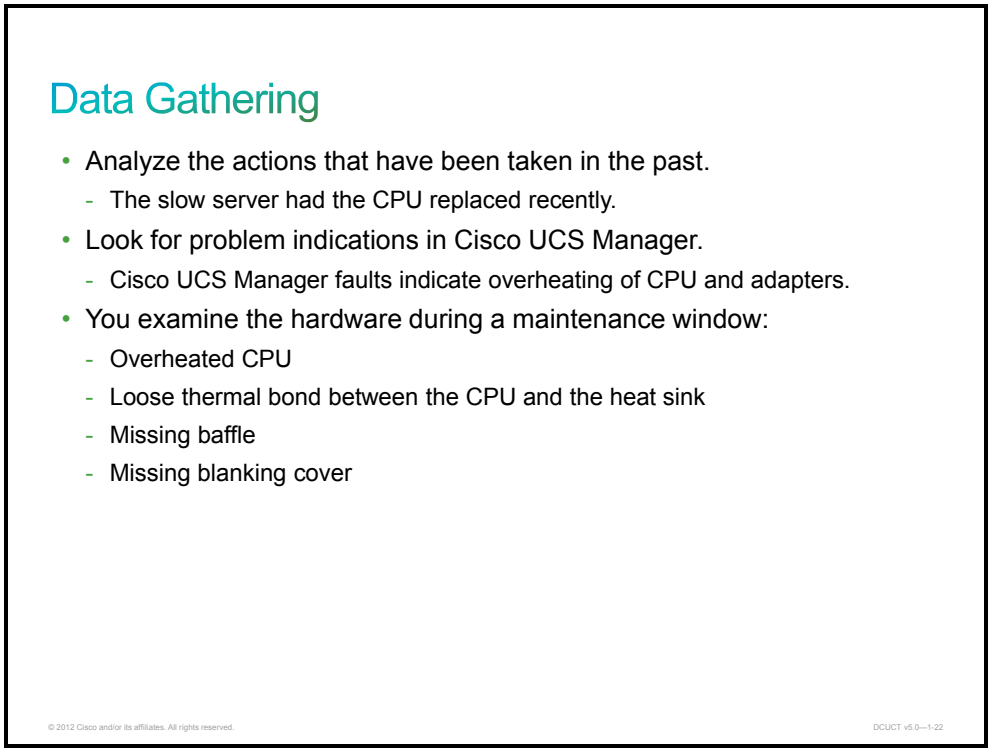
In this troubleshooting scenario, you have a server with significantly degraded performance compared to other servers in the chassis. When you investigate the issue, you find that all the blade servers have the same hardware components and run the same operating system, patches, and applications.

If Cisco UCS Manager displays faults that report an adapter overheating problem, the physical server setup may be faulty and prevent proper air flow. Possible causes include missing blanking covers or air baffles. In this situation, perform the following tasks:

- Verify that the adapter is seated correctly in the slot.
- Reseat the adapter to assure a good contact and rerun POST.
- Verify that all empty HDD bays, server slots, and power supply bays use blanking covers to ensure that the air is flowing as designed.
- Verify that the server air baffles are installed to ensure that the air is flowing as designed.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets



In the data gathering phase, you analyze the actions that have been taken in the past. You discover that the CPU of the affected server was replaced a few weeks before. Then you search for problem indications in Cisco UCS Manager and find that several faults have been logged that indicate the overheating of the CPU and an adapter. These faults have been overlooked so far because the administrators found that overheating is unlikely.

You decide to examine the server hardware during a maintenance window and discover that the CPU is indeed overheated. Upon a closer check, you find a loose thermal bond between the CPU and the heat sink, a missing baffle, and a missing blanking cover.

https://t.me/learningnets

Remediation

- Thermally bond the CPU and the heat sink.
- Adjust the baffles to improve air flow.
- Verify that the adapters are seated correctly in the slot.
  - Reseat the adapters to ensure good contact.
  - Rerun POST.
- Install blanking covers.
  - For all empty HDD bays, server slots, and power supply bays
  - To ensure that the air is flowing as designed

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

These findings enable you to identify that overheating is the most likely cause of the server performance degradation.

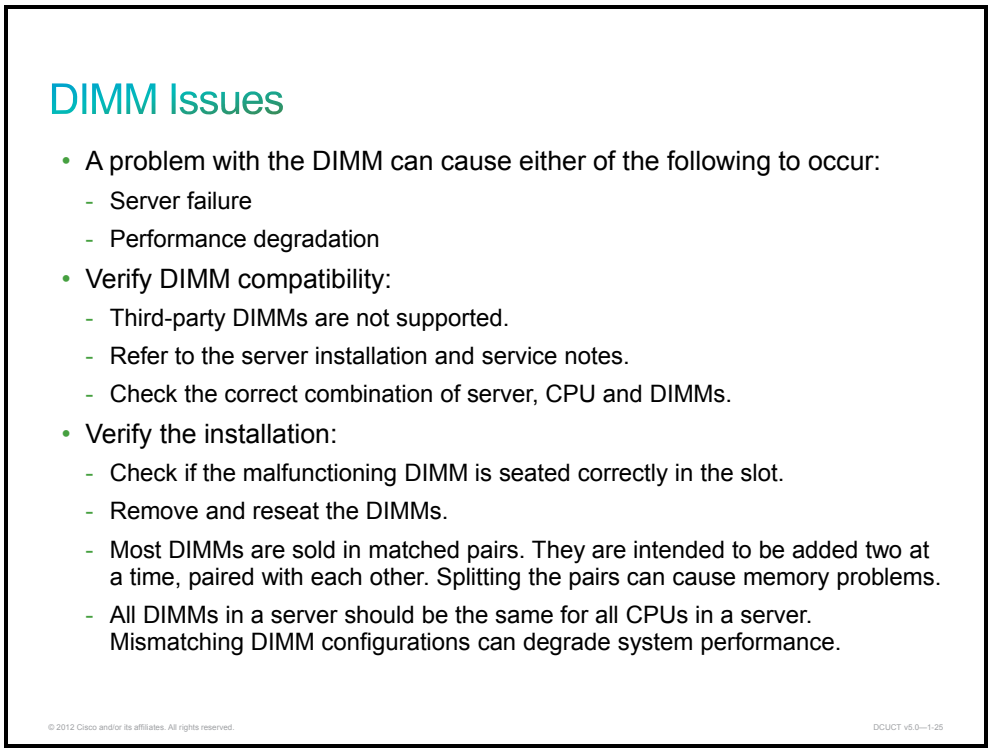
To remediate the problem, you thermally bond the CPU and the heat sink, and adjust the baffles to improve air flow. You verify that the adapters are seated correctly in the slot. You reseat the adapters to assure a good contact and rerun POST. You install the missing blanking cover in the empty HDD to ensure that the air is flowing as designed.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Memory Troubleshooting

This topic describes the tools and techniques that are used to identify memory configuration errors and memory failures.



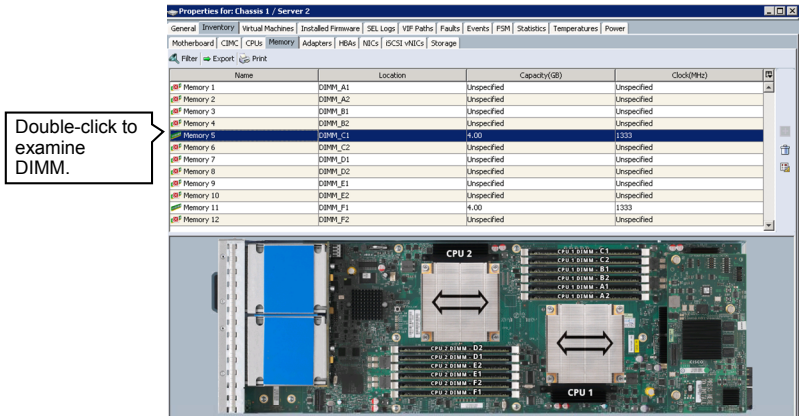
A problem with a DIMM can cause a server to fail to boot or cause the server to run below its capabilities. If DIMM issues are suspected, consider the following:

- DIMMs tested, qualified, and sold by Cisco are the only DIMMs that are supported on your system. Third-party DIMMs are not supported, and if they are present, Cisco technical support will ask you to replace them with Cisco DIMMs before continuing to troubleshoot a problem.
- Check if the malfunctioning DIMM is supported on that model of server. Refer to the server installation and service notes to verify whether you are using the correct combination of server, CPU, and DIMMs.
- Check if the malfunctioning DIMM is seated correctly in the slot. Remove and reseat the DIMMs.
- All Cisco servers have either a required or recommended order for installing DIMMs. Refer to the server installation and service notes to verify that you are adding the DIMMs appropriately for a given server type.
- Most DIMMs are sold in matched pairs. They are intended to be added two at a time, paired with each other. Splitting the pairs can cause memory problems.
- If the replacement DIMMs have a maximum speed lower than those previously installed, all DIMMs in a server run at the slower speed or do not work at all. All of the DIMMs in a server should be of the same type.
- The number and size of DIMMs should be the same for all CPUs in a server. Mismatching DIMM configurations can degrade system performance.

https://t.me/learningnets

Monitoring Memory in GUI: General

- List of DIMMs and their parameters
- Graphical illustration of the server board
- Double-click a specific DIMM for details



Double-click to examine DIMM.

Server > Inventory > Memory

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

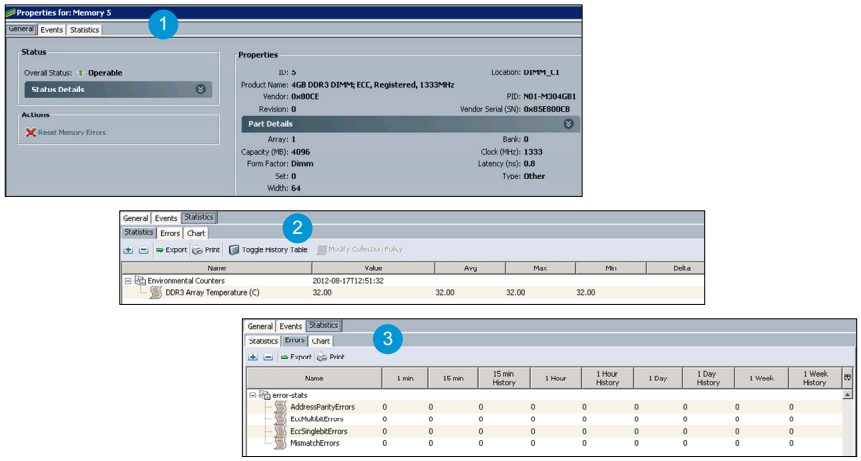
You can determine the type of DIMM errors using the Cisco UCS Manager GUI.

In the navigation pane, expand the correct chassis and select the server. On the Inventory tab, choose the Memory tab. The Memory tab displays the DIMMs that are installed on the server. The GUI presents a graphical illustration of the motherboard and marks the slots where the DIMMs are installed. You can select and double-click a DIMM to investigate its operational details.

https://t.me/learningnets

Monitoring Memory in GUI: DIMM

- Various details are available for each DIMM.
- The Statistics tab has three sub-tabs: Statistics, Errors, and Chart.



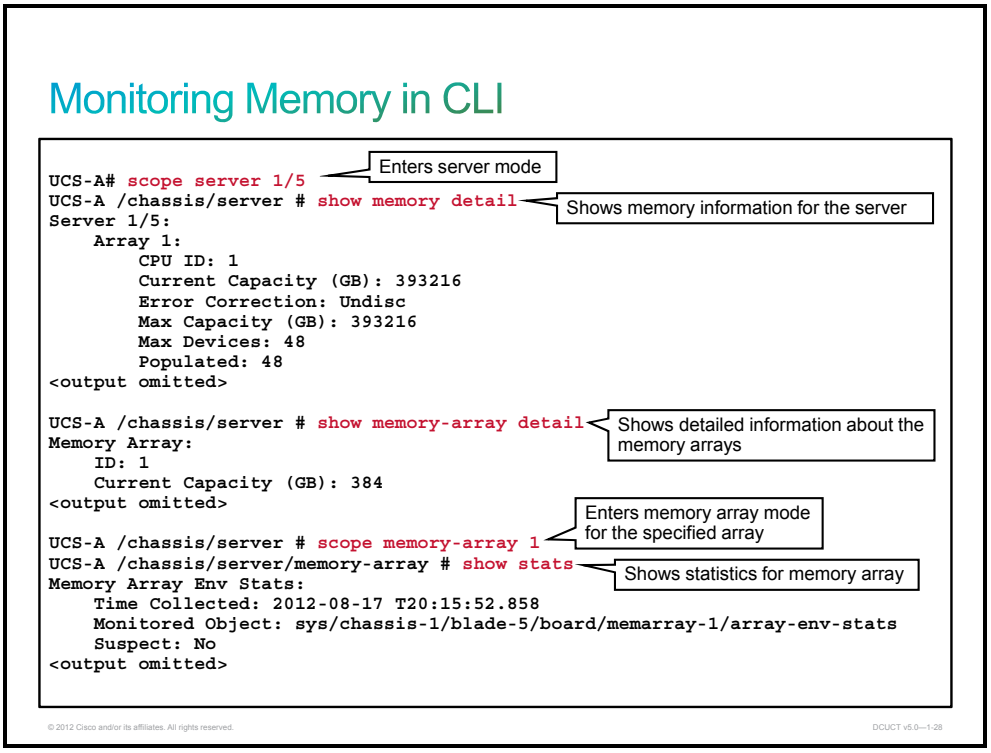
Server > Inventory > Memory

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

If you double-click on a specific DIMM, you are presented with a Properties page. The Properties page has three tabs: General, Events, and Statistics. The General tab describes the status, required actions, parameters, and part details. The Statistics tab has three sub-tabs:

- **Statistics:** This tab displays the statistical values for various parameters, such as the temperature. An example is shown in this slide.
- **Errors:** This tab contains the errors that are related to the DIMM. A sample screenshot is presented in this figure.
- **Chart:** This tab provides a graphical representation of the memory utilization. It is not shown here for brevity purposes.

https://t.me/learningnets



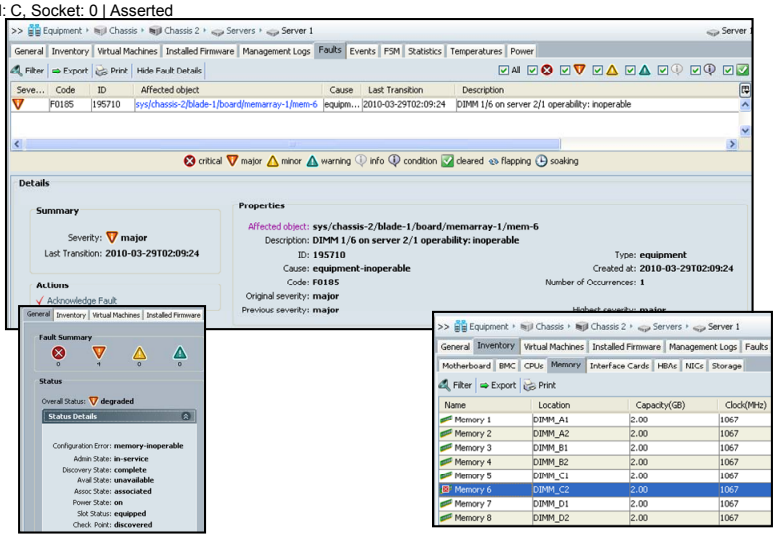
The Cisco UCS Manager CLI offers an alternative method of examining memory information to identify possible DIMM errors. This scenario illustrates the use of the most common CLI commands that you can use for memory troubleshooting:

Command	Purpose
UCS-A# scope server x/y	Enters server mode for the specified server.
— **UCS-A /chassis/server # show memory detail**	Shows memory information for the server.
— **UCS-A /chassis/server # show memory-array detail**	Shows detailed information about the memory arrays.
— **UCS-A /chassis/server # scope memory-array x**	Enters memory array mode for the specified array.
— **UCS-A /chassis/server/memory-array # show stats**	Shows statistics for memory array.

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

Identifying Memory Faults

System Event Log:
5ed | 03/29/2010 02:20:50 | Memory 0x02 | Uncorrectable ECC/other uncorrectable memory error | Rank: 0, DIMM Socket: 1, Channel: C, Socket: 0 | Asserted



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

You can identify memory faults using either the Cisco UCS Manager GUI or CLI. In this scenario, a problem is reported for the Memory 6 DIMM in the first memory array on blade 1. The fault is visible both in the GUI and in the system event log CLI.

You can examine the problem using various other methods:

- Examine the output of the **show tech-support** command and check the memory inventory.
- Capture the BIOS version and the memory configuration.
- Use the **show memory detail** command.

https://t.me/learningnets

DIMM Not Recognized, Does Not Fit, or Overheated

Problem	Server failure or performance degradation
Possible Cause	DIMMs installed incorrectly
Solution	• Verify that the DIMM is supported on that server model. • Verify that the DIMM is in a slot that supports an active CPU. • Verify that the DIMM is sourced from Cisco. • Verify that the DIMM is oriented correctly in the slot. • Reseat it to assure good contact and rerun POST. • Verify that any needed CPU air blockers, blanking covers, and air baffles are installed and that the air is flowing as designed.

Caution: Do not operate a blade in the chassis with the top cover removed.

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

The most fundamental issues that are related to server memory are the DIMMs not being recognized, not fitting into the slots, or being overheated. The possible causes are that the DIMMs are not supported or are installed incorrectly.

In all of these cases, you should consider taking these corrective actions:

- Verify that the DIMM is supported on that server model.
- Verify that the DIMM is oriented correctly in the slot. DIMMs and their slots are keyed and only seat in one of the two possible orientations.
- Verify that the DIMM is seated fully and correctly in its slot. Reseat it to assure a good contact and rerun POST.
- Verify that all empty HDD bays, server slots, and power supply bays use blanking covers to assure that the air is flowing as designed.
- Verify that the server air baffles are installed to assure that the air is flowing as designed.
- Verify that any needed CPU air blockers are installed to assure that the air is flowing as designed.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Issue: Server Performance Degradation

- You encounter this symptom:
  - The performance of one server is lower than that of the other servers in the chassis.
- The system environment is as follows:
  - All blade servers have the same hardware.
  - All blade servers run the same operating system, patches, and applications.

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

In this troubleshooting scenario, you have a server performance degradation problem. One server runs slower than the other servers in the chassis. All blade servers have the same hardware and run the same operating system, patches, and applications.

https://t.me/learningnets

Data Gathering

- Analyze the actions that have been taken in the past.
  - The degraded server had the DIMMs replaced recently.
- Check the cooling of the server components.
  - The cooling works properly.
  - No faults indicate an overheating problem.
- Look for problem indications in Cisco UCS Manager.
  - Cisco UCS Manager reports “Degraded DIMM Error.”
  - DIMMs are not disabled and are available for the operating system to use.
- Verify that the DIMM is supported on that server model.
  - Compliance is assured.
- Verify that the DIMM is populated in its slot according to the population rules for that server model.
  - This is verified successfully.
- Verify that all DIMMs can run at the same speed.
  - If a slower DIMM is added to a system that had used faster DIMMs previously, all DIMMs on a server run at the slower speed.

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

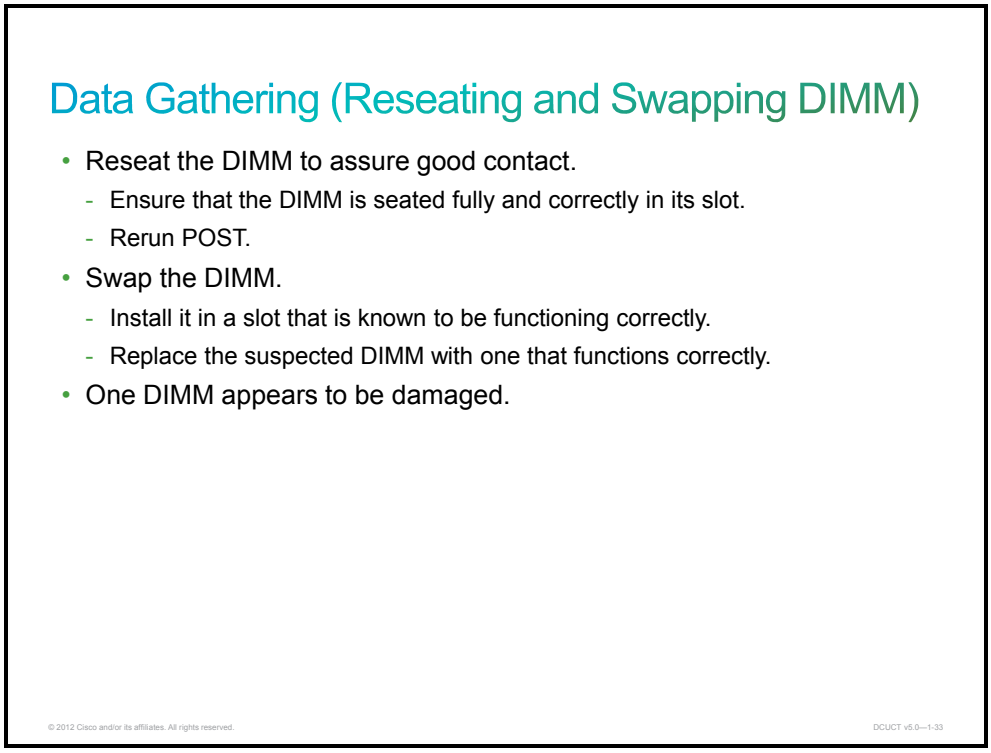
In the data gathering process, you analyze the actions that have been taken in the past and find that the DIMMs of the degraded server were replaced two weeks before. You check the cooling of the server components, but it seems to function properly and no faults indicate an overheating problem.

You look for problem indications in Cisco UCS Manager and discover a fault that says “Degraded DIMM Error.” This message did not receive enough attention, because the DIMMs were not disabled and the operating system continued to use the entire system memory.

You verify that the DIMM is supported on that server model and that the DIMM is populated in its slot according to the population rules for that server model. You check that all of the DIMMs can run at the same speed, knowing that if a slower DIMM was added to the system that had used faster DIMMs previously, all DIMMs would run at the slower speed.

© 2012 Cisco Systems, Inc.

https://t.me/learningnets



Then you take these steps to further isolate a particular failed part:

Step 1 Remove all DIMMs from the system.

Step 2 Install a single DIMM (preferably a tested good DIMM) or a DIMM pair in the first usable slot for the first processor (minimum requirement for POST success). Refer to the published memory population rules to determine which slot to use.

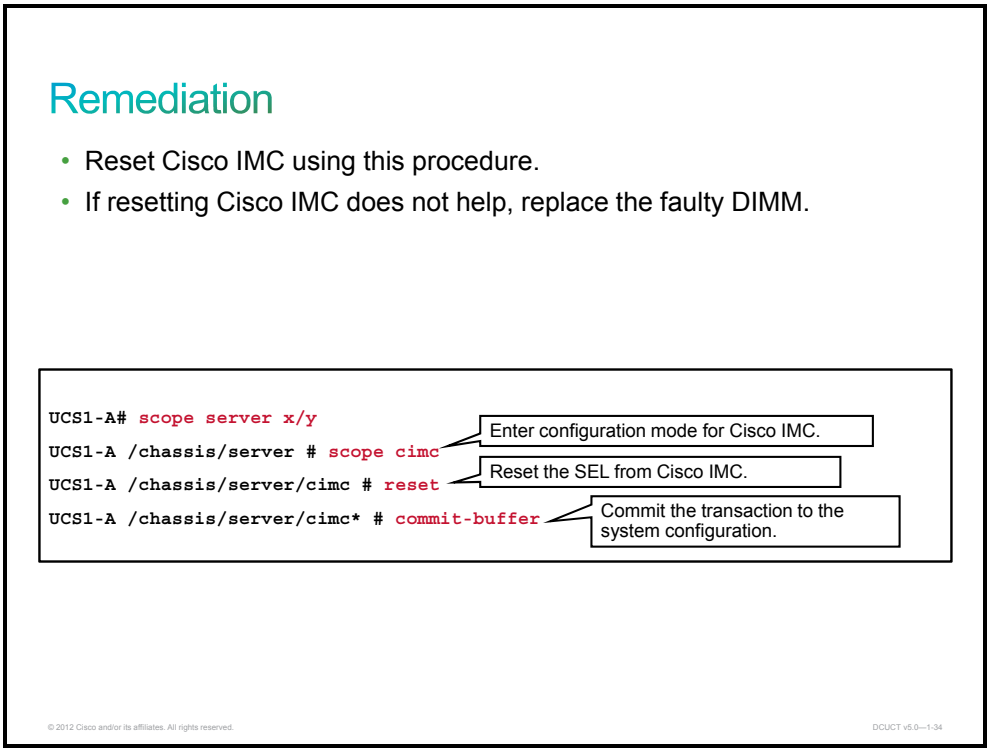
Step 3 Try to boot the system.

Step 4 If the BIOS POST is still unsuccessful, repeat the first three steps using a different DIMM.

Step 5 If the BIOS POST is successful and the blade can associate to a service profile, continue adding memory. Follow the population rules for that server model. If the system can successfully pass the BIOS POST in some memory configurations but not in others, use that information to help isolate the source of the problem.

The result of these tests is that one DIMM appears to be damaged.

https://t.me/learningnets



If you found a reported correctable error that matches the information here, the problem can be corrected by resetting Cisco Integrated Management Controller (Cisco IMC) instead of reseating or resetting the blade server. Use the following Cisco UCS Manager CLI commands:

Command	Purpose
UCS1-A# scope server x/y	Enters server configuration mode.
— **UCS1-A /chassis/server # scope cimc**	Enters configuration mode for Cisco IMC.
— **UCS1-A /chassis/server/cimc # reset**	Resets the Cisco IMC server.
— **UCS1-A /chassis/server/cimc* # commit-buffer**	Commits the transaction to the system configuration.

If this procedure does not help, you may have an uncorrectable memory error. DIMMs with uncorrectable errors are usually disabled and the operating system on the server does not see that memory. If a DIMM or DIMMs fail while the system is up, the operating system could crash unexpectedly. Cisco UCS Manager shows the DIMMs as inoperable in the case of uncorrectable DIMM errors. These errors are not correctable using the software. You can identify a bad DIMM and remove it to allow the server to boot. For example, the BIOS fails to pass the POST due to one or more bad DIMMs.

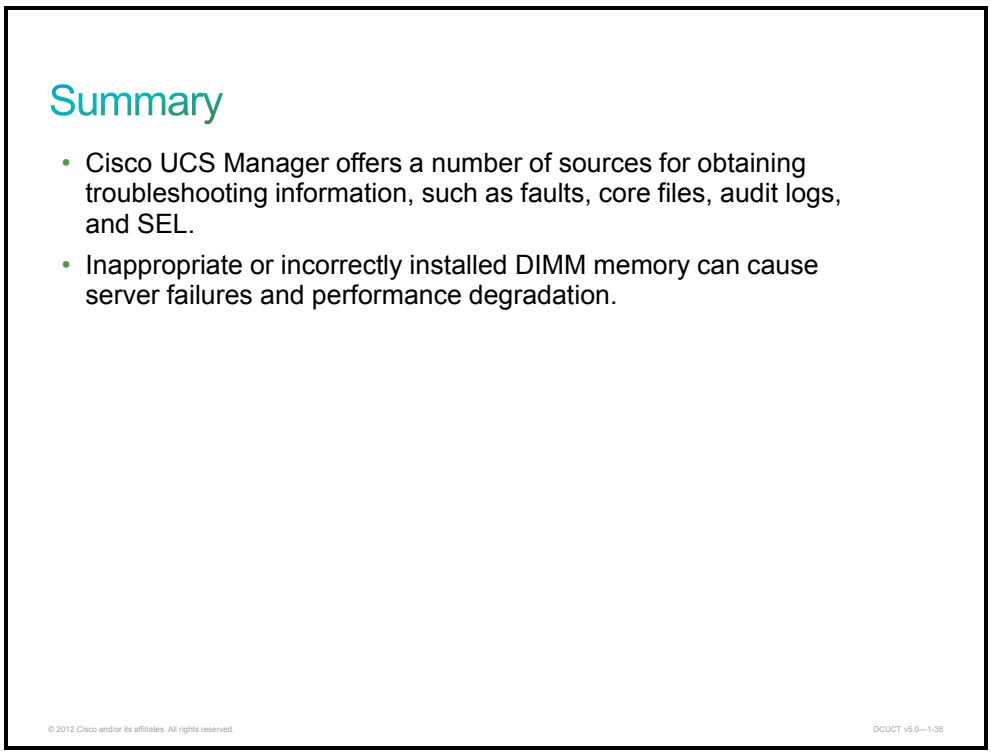
In this case, you decide to implement the only remaining solution to remediate the problem and replace the faulty DIMM.

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Summary

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



References

For additional information, refer to these resources:

- To learn more about troubleshooting server hardware issues, refer to *Cisco UCS Manager B-Series Troubleshooting Guide* at this URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ts/guide/UCSTroubleshooting.html

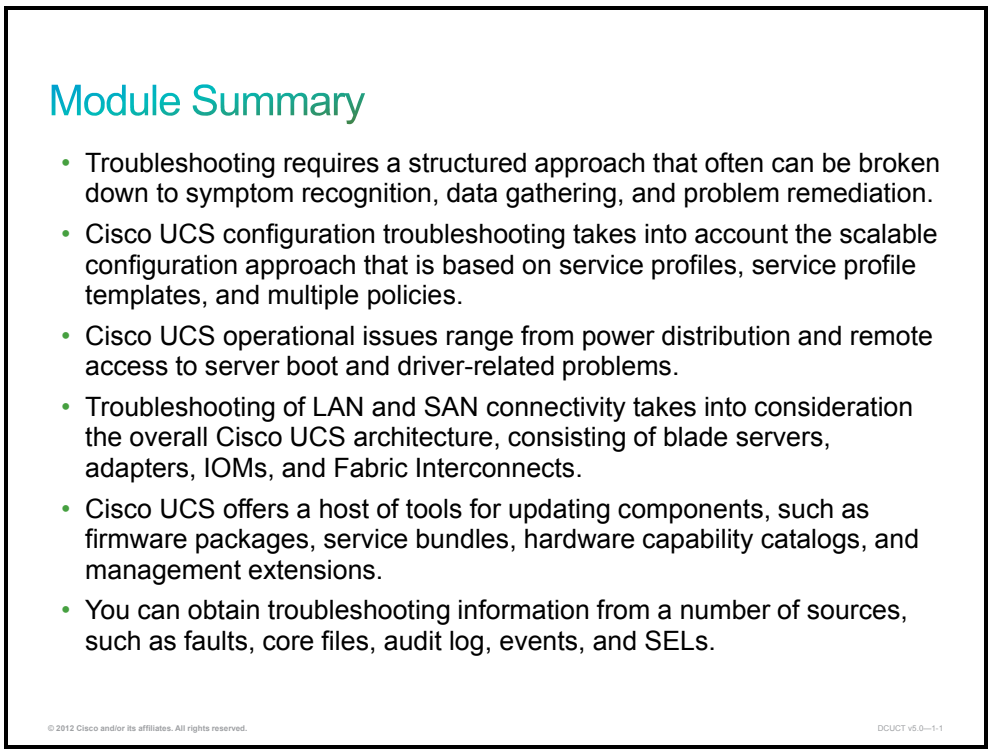
https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module Summary

This topic summarizes the key points that were discussed in this module.



References

For additional information, refer to these resources:

- *Cisco UCS Manager B-Series Troubleshooting Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/ts/guide/UCSTroubleshooting.html

https://t.me/learningnets

 © 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 Cisco UCS connectivity topology is correct? (Source: Troubleshooting Cisco UCS B-Series Architecture and Initialization)

A) standalone FI with single uplink from IOM to Fabric Interconnect
B) standalone FI with dual uplinks from IOM to Fabric Interconnect
C) dual FIs without Layer 1-Layer 1 and Layer 2-Layer 2 connections
D) IOM bypass

Q2) List at least three phases of a structured troubleshooting process. (Source: Troubleshooting Cisco UCS B-Series Architecture and Initialization)

Q3) How can you resolve the problem of an IP address shortage in the management subnet? (Source: Troubleshooting Cisco UCS B-Series Architecture and Initialization)

A) Place the FI management and virtual IP addresses in separate subnets.
B) Keep the FI management and virtual IP addresses in the same subnet, and put the KVM addresses in a separate subnet.
C) Put mgmt0 and mgmt1 addresses in separate subnets.
D) Split the cluster in separate standalone deployments.

Q4) What should you check when troubleshooting KVM launch problems? (Source: Troubleshooting Cisco UCS B-Series Architecture and Initialization)

A) connectivity between the primary FI and the KVMs
B) personal firewall settings
C) Java settings
D) ActiveX settings

Q5) Ethanalyzer helps you capture and decode traffic, and you can use it to examine packets of mission-critical applications on the blade servers. (Source: Troubleshooting Cisco UCS B-Series Architecture and Initialization)

A) true
B) false

Q6) Which two options best describe an FSM? (Choose two.) (Source: Troubleshooting Cisco UCS B-Series Architecture and Initialization)

A) hardware component of Cisco UCS
B) workflow model
C) specialized ASIC
D) ordered number of stages
E) representation of structured troubleshooting
F) monitoring process

Q7) In Cisco UCS, you can assign privileges directly to administrator accounts. (Source: Troubleshooting Cisco UCS B-Series Architecture and Initialization)

A) true
B) false

https://t.me/learningnets

Q8) In Cisco UCS, you can assign server addresses from _____. (Source: Troubleshooting Cisco UCS B-Series Architecture and Initialization)

Q9) What can cause a problem when associating a service profile with a blade server? (Source: Troubleshooting Cisco UCS B-Series Configuration)

A) incorrect service profile template
B) server down
C) lack of available WWPNs
D) unreachable KVM

Q10) What can cause an authentication failure in an environment with a remote RADIUS server? (Source: Troubleshooting Cisco UCS B-Series Configuration)

A) missing administrator account in the Cisco UCS user database
B) accounting port blocked by a firewall
C) incorrect authorization profile on the RADIUS server
D) password entered in capital letters

Q11) What technology should you employ if you have problems with controlled power distribution among the blade servers? (Source: Troubleshooting Cisco UCS B-Series Operation)

Q12) What is a likely reason for connection problems to the Cisco UCS Manager GUI? (Source: Troubleshooting Cisco UCS B-Series Operation)

A) There is a high delay in the connection path.
B) Port 8080 is blocked by a firewall.
C) There is unsupported redirection from HTTP to HTTPS.
D) There is unsupported redirection from HTTPS to HTTP.
E) SSL port TCP/443 is blocked by a firewall.

Q13) What should you check when a Microsoft Windows 2008 R2 installation is not starting? (Source: Troubleshooting Cisco UCS B-Series Operation)

A) the boot order in the BIOS so that the server boots from SAN
B) if the virtual DVD or CD is mounted
C) that power redundancy mode is set to N+1 or grid
D) if the service profile template has not been changed

Q14) Which two LAN switching modes can you use to avoid STP-related problems? (Choose two.) (Source: Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity)

A) switching mode
B) Ethernet Host Virtualizer
C) FabricPath
D) the default mode
E) Rapid Spanning Tree Protocol (IEEE 802.1D) mode

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Q15) What can cause a failure of an FI uplink to the upstream switch? (Source: Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity)

A) duplex mismatch at speed 10 Gb/s
B) speed mismatch
C) Cisco Discovery Protocol mismatch
D) IP address mismatch

Q16) What can prevent a blade server from obtaining the IP address automatically? (Source: Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity)

A) boot order
B) firewall blocking ICMP packets
C) mismatched configuration of allowed VLAN range
D) insufficient resources available for the service profile

Q17) Which Cisco UCS Manager configuration element is used to enable jumbo frames? (Source: Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity)

A) service profile
B) network policy
C) QoS server class
D) QoS system class

Q18) The SAN end-host operation mode of the fabric interconnect is synonymous with _____. (Source: Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity)

Q19) The trunking SAN uplink interfaces of the fabric interconnect transport all VSANs that are defined in the system automatically. (Source: Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity)

A) true
B) false

Q20) What are the two supported SPAN destinations? (Choose two.) (Source: Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity)

A) Ethernet ports
B) Port channels
C) Fibre Channel storage ports
D) FCoE ports
E) Fibre Channel ports

Q21) How can you identify the blade location when tracing server traffic? (Source: Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity)

A) by checking the MAC address table
B) by performing Cisco Discovery Protocol checks on the fabric interconnect
C) by using the trace utility
D) by examining the interface to which the server MAC address is connected

https://t.me/learningnets

Q22) Which two commands can you use on the SAN core switch to identify the server WWPN that is assigned through the service profile? (Choose two.) (Source: Troubleshooting Cisco UCS B-Series LAN and SAN Connectivity)

A) **show interface**
B) **show flogi database**
C) **show wwpn database**
D) **show fcns database**
E) **show server**

Q23) Which three Cisco UCS components have dual partitions for firmware loading? (Choose three.) (Source: Troubleshooting and Upgrading Cisco UCS Manager)

A) Fabric Interconnect
B) Cisco IMC
C) IOM
D) BIOS
E) Ethernet adapters
F) RAID controllers

Q24) What are the three firmware types of Cisco UCS Fabric Interconnect? (Source: Troubleshooting and Upgrading Cisco UCS Manager)

_____

Q25) What is the purpose of the Cisco UCS hardware compatibility catalog? (Source: Troubleshooting and Upgrading Cisco UCS Manager)

A) provide information on element compatibility and compliance
B) provide an API to compliant applications
C) enable support for new hardware
D) simplify the selection process of compatible components

Q26) Which three files must be copied into the Fabric Interconnect bootflash as a result of the system recovery procedure? (Source: Troubleshooting and Upgrading Cisco UCS Manager)

_____

Q27) Which two states are valid Cisco UCS Manager fault states? (Choose two.) (Source: Troubleshooting Cisco UCS B-Series Hardware)

A) dried
B) soaking
C) critical
D) cleared
E) processed

Q28) The core files are small files that contain the core data of the troubleshooting information and are therefore requested by Cisco TAC when troubleshooting Cisco UCS problems. (Source: Troubleshooting Cisco UCS B-Series Hardware)

A) true
B) false

© 2012 Cisco Systems, Inc.

https://t.me/learningnets

Module Self-Check Answer Key

Q1) A

Q2) define, gather, analyze, test, eliminate, remediate, solve

Q3) C

Q4) C

Q5) B

Q6) B, D

Q7) B

Q8) pools

Q9) C

Q10) D

Q11) Power capping

Q12) B

Q13) B

Q14) B, D

Q15) B

Q16) C

Q17) D

Q18) NPV

Q19) A

Q20) A, E

Q21) D

Q22) B, D

Q23) B, C, E

Q24) NX-OS kernel, NX-OS system, and Cisco UCS Manager

Q25) C

Q26) Kickstart image, system image, Cisco UCS Manager image

Q27) B, D

Q28) A

https://t.me/learningnets

 © 2012 Cisco Systems, Inc.

https://t.me/learningnets