

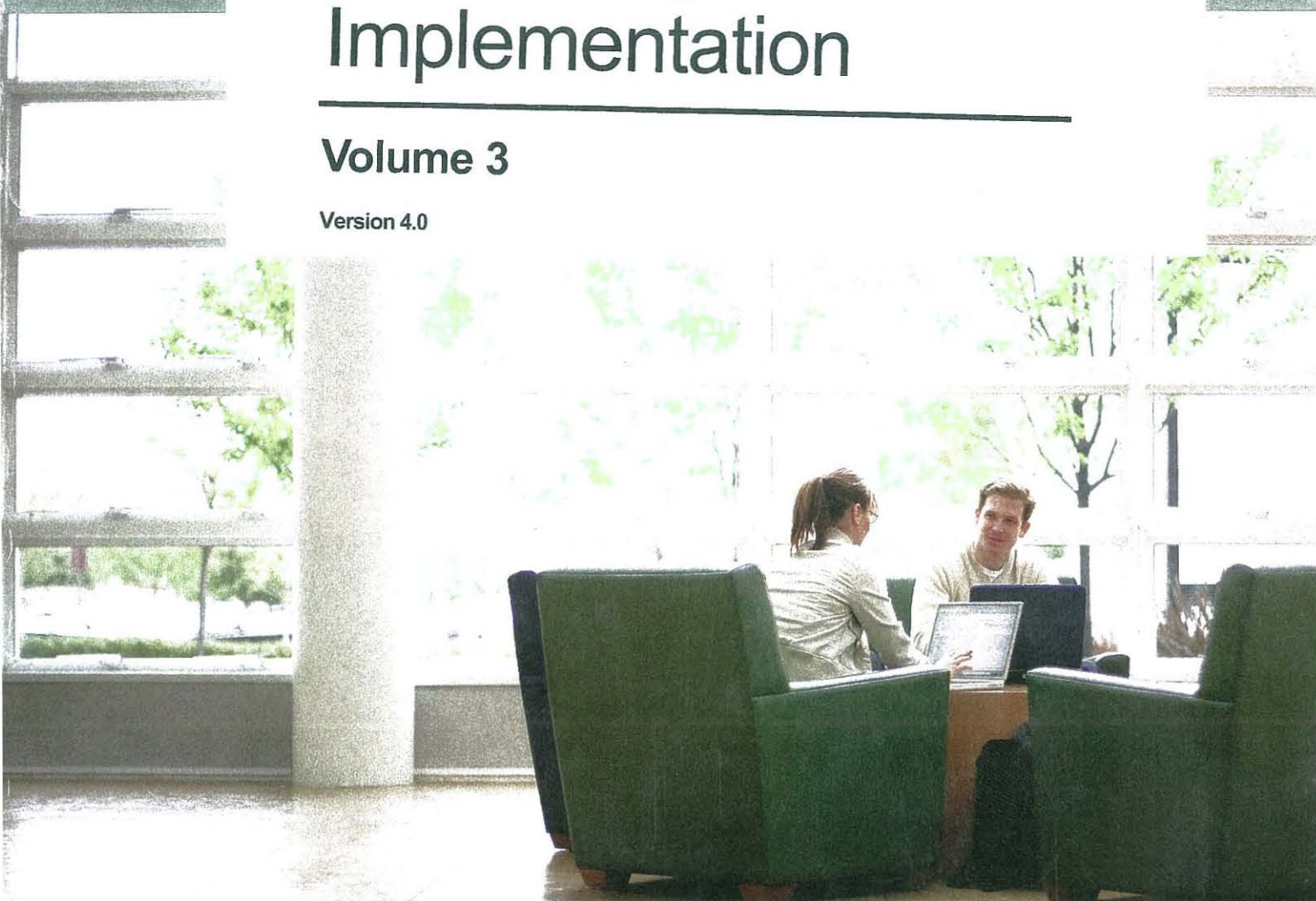


Cisco Learning Product

Data Center Unified Computing Implementation

Volume 3

Version 4.0



Data Center Unified Computing Implementation

Volume 3

Version 4.0

Student Guide

Text Part Number: 97-3022-01



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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Table of Contents

Volume 3

<i>Cisco Unified Computing System Management and Maintenance</i>	8-1
Overview	8-1
Module Objectives	8-1
Implementing Cisco Unified Computing System Startup and Shutdown Procedures	8-3
Overview	8-3
Objectives	8-3
Cisco UCS 6100 Series Fabric Interconnect Startup and Shutdown Procedures	8-4
Fabric Interconnect Startup and Shutdown	8-4
Effects of Shutting down or Rebooting a Cisco UCS 6100 Series Fabric Interconnect on the High-Availability Cluster	8-5
Effect of Active Fabric Interconnect Shutdown	8-5
Effect of Subordinate Fabric Interconnect Shutdown	8-6
Startup and Shutdown Procedures for Cisco UCS B-Series Blade Servers	8-7
Booting a Compute Node	8-7
Shutting down a Compute Node	8-8
Compute Node Hardware Restart	8-9
Procedures for Power State Verification	8-10
IOM Power Options	8-10
Power State Verification—Chassis Rear	8-11
Power State Verification—Chassis Front	8-12
Summary	8-13
Configuring Role-Based Access Control	8-15
Overview	8-15
Objectives	8-15
Overall Framework of RBAC in Cisco UCS B-Series	8-16
RBAC and Organizations	8-16
Role-Based Access Control	8-17
Organization Basics	8-18
Organizational Hierarchy Example	8-19
Scope of Organizations	8-20
What Can Be Configured in an Organization?	8-21
Configuring Local Users, Roles, and Privileges	8-22
Cisco UCS Implementation of Local AAA	8-22
Cisco UCS Authorization	8-23
Structure of a Role	8-24
Create a Role—Start the New Role Wizard	8-25
Name Role and Define Privileges	8-26
Create a Local User—Start the New User Wizard	8-27
Create Local User with Custom Role	8-28
Configuring Organizations and Locales	8-29
Create a New Organization	8-29
Actions in New Organization	8-30
Start the New Locale Wizard	8-31
Name the Locale	8-32
Drag and Drop the Organization onto the Locale Name	8-33
Locale Available to Restrict User Rights	8-34
Modify Local User Rights to Apply Locale	8-35
Effective Rights of a User, as an Intersection of Mapped Roles and Locales	8-36
Determination of Effective Rights	8-36
Effective User Rights for Admin	8-37
Effective User Rights for crhaynes	8-38
Configuring LDAP and Active Directory as an External Authentication and Authorization Service	8-39
Cisco UCS User Security Features	8-39
User Database	8-40
LDAP Statistics	8-41

Create an LDAP and Active Directory Provider	8-42
Change Authorization to LDAP and Active Directory	8-43
Mapping Cisco Unified Computing System Roles to LDAP and Active Directory Attributes	8-44
LDAP Attribute Mapping	8-44
Summary	8-45
Backing up and Restoring the Cisco UCS Manager Database	8-47
Overview	8-47
Objectives	8-47
Supported Backup Types and Functions	8-48
FULL State Backup	8-48
Configuration Backup	8-49
Use of Configuration Backups	8-50
Import Operations and Disaster-Recovery Restore Operations	8-51
Import vs. Restore	8-51
Backup and Import Jobs	8-52
Configuring a Backup Job	8-53
Create a Backup Job	8-53
Execute a Backup Job	8-54
Verifying Backup Creation and Execution	8-55
Verify Backup Job in Cisco UCS Manager	8-55
Verify Backup Job on Remote FTP Server	8-56
Configuring an Import Job to Restore the AAA User Database	8-57
Import Test—Delete a Local User	8-57
Import Test—Local User Deleted	8-58
Create Import Job to Restore AAA Database	8-59
Run Import Job to Restore AAA Database	8-60
Verify Import Job in Cisco UCS Manager	8-61
Verifying Restoration of the AAA User Database	8-62
Confirm that AAA Database Was Restored	8-62
Configuring the Backup Job to Preserve Abstracted Identities	8-63
Preserve Abstracted Identities	8-63
Configuring the Cisco UCS 6100 Series Fabric Interconnect for Disaster-Recovery Restore	8-64
Importing FULL State Backup	8-64
Summary	8-66
Managing High Availability	8-67
Overview	8-67
Objectives	8-67
High-Availability Cluster Connection Requirements for Cisco UCS B-Series Blade Servers	8-68
Cluster Peers Must Be Identical	8-68
Cluster Peers Can Be Different to Upgrade Cluster	8-69
Cluster Cabling	8-70
Intercluster Communications and Cisco UCS Manager Database Synchronization	8-71
Process Management	8-71
Local and Chassis Data	8-72
Primary Cluster Node Election	8-73
Monitor Cluster Status—GUI	8-75
Monitor Cluster Status—CLI	8-76
Cluster Control	8-77
How the Cisco UCS 5108 Chassis Serial EEPROM Resolves Split-Brain Issues in the High-Availability Cluster	8-78
Split Brain	8-78
Cluster Partition in Space and Partition in Time Conditions	8-79
Partition in Space	8-79
Partition in Time	8-80
Modifying Cluster IP Addressing	8-81
Modify Management IP Addressing—GUI	8-81
Modify Management IP Addressing—CLI	8-82
Summary	8-83

Monitoring System Events	8-85
Overview	8-85
Objectives	8-85
Fault Management System and Fault Severity Levels	8-86
Global Fault Summary	8-86
Fault Severity	8-87
Fault States	8-88
Admin Fault Console	8-89
Fault in Soaking State	8-90
Fault in Flapping State	8-91
Admin Fault Console Detail	8-92
Using the Audit Log to Track Administrative Changes to the Cisco UCS Manager Database	8-93
Audit Log	8-93
Filter Audit Log Output	8-94
Filtered Audit Log Output	8-95
Export Audit Log	8-96
Areas of Operation that Are Subject to FSM Validation and FSM Output Interpretation	8-97
Operations Subject to FSM Validation	8-97
Reset IOM—Discovery Process in FSM	8-98
Reset IOM—Discovery Successful	8-99
FSM Discovery Details	8-100
Configuration and Validation of Logging Options	8-101
Logging Options	8-101
Configuring the Smart Call Home Feature	8-102
Call Home	8-102
Contact Configuration	8-103
Email Notification	8-104
Call Home Profiles	8-105
Profile Configuration	8-106
Call Home Policies	8-107
System Inventory	8-108
Validating the Smart Call Home Feature	8-109
Send System Inventory to Validate Call Home	8-109
Settings for Logs, Events, and Faults	8-110
Fault Settings and Retention Policy	8-110
Summary	8-111
Managing and Upgrading Cisco UCS B-Series Firmware	8-113
Overview	8-113
Objectives	8-113
Where to Find Cisco UCS B-Series Firmware Packages on Cisco.com	8-114
Locate Firmware on Cisco.com	8-114
Locate Cisco Unified Computing System Firmware on Cisco.com	8-115
Locate Cisco UCS B-Series Firmware on Cisco.com	8-116
Choose Cisco Unified Computing System Bundle Image	8-117
Copy Cisco Unified Computing System Bundle Image to Fabric Interconnect	8-118
Updating Cisco UCS B-Series Firmware	8-119
Suggested General Upgrade Practices	8-119
Upgrade Overview	8-120
Image Versions	8-121
Displaying Installable Images	8-122
Direct Upgrade of Cisco IMC, IOM, and Mezzanine Adapter Firmware	8-123
Update Dual-Flash Components	8-123
Update Components	8-124
Activate All Adapters	8-125
Activate All Cisco IMC Instances	8-126
Activate Both IOMs	8-127
Software Updates on the Fabric Interconnect	8-128
Fabric Interconnect Firmware Update	8-128
Display Running Fabric Interconnect Firmware Version	8-129

Upgrade the Fabric Interconnect Software	8-130
Firmware Updates via Service Profile	8-131
Host Firmware Package Mandatory	8-131
Host Firmware Package Creation	8-132
Host Firmware Categories	8-133
Host Firmware Selection	8-134
Host Firmware Drag and Drop	8-135
Select Firmware Version	8-136
Host Firmware Package Ready to Apply	8-137
Differences Between Firmware Processes of Cisco UCS 61x0 Fabric Interconnects and Cisco IMC, IOM, and Adapter	8-138
Component Firmware Update Differences	8-138
Summary	8-139
Module Summary	8-141
References	8-142
Module Self-Check	8-143
Module Self-Check Answer Key	8-149

Survey of Cisco Data Center Unified Computing Implementation E-Learning **A-1**

Overview	A-1
Objectives	A-1
Review the Benefits of Cisco UCS	A-2
Differentiate Between Stages of Data Center Evolution	A-2
Select Four Management Challenges in a Blade Server Environment	A-4
Review of Cisco UCS	A-5
List Two Benefits Made Possible by Unified I/O	A-5
Name the Components of Cisco UCS	A-6
Differentiate Between IEEE Standards of Data Center Bridging	A-7
Select Four Features of FCoE	A-8
Review of Cisco UCS C-Series Hardware Components	A-9
Select Two Chassis That Can Support at Least 256-Mb RAM and RAID 50	A-9
Select Five Configurable Options for C-Series BIOS	A-11
Select Two C-Series Chassis That Allow for RAID 10	A-12
Select C-Series LAN, SAN, and Management Connectivity Options	A-14
Which C-Series Chassis Support More Than Two Power Supplies?	A-16
Review of Installing Cisco UCS C-Series Hardware	A-17
Select Two C-Series Rack-Mounting Requirements for Physical Enclosure	A-17
Select Four Steps in the Process of Opening the Server Enclosure	A-18
Select Two ESD Precautions	A-19
Select Minimum Cabling Required to Access Cisco IMC Console	A-20
Review of Cisco UCS B-Series Hardware Components	A-21
Select Six Components of the Cisco UCS 6100 Series Fabric Interconnect	A-21
Define the Purpose of Internal Components of the Cisco UCS 2104 IOM	A-22
Describe Implementation Rationale for the Cisco UCS B-Series Mezzanine Cards	A-24
Select Five Field-Installable Component Options of the Cisco UCS B-Series Blade Servers	A-25
Review of B-Series Architecture and Features	A-26
Select Three Primary Methods to Access Cisco UCS B-Series Blade Server Management Interface	A-26
Select Three B-Series Hardware Redundancy Components for Data and Management Planes	A-27
Review of Cisco UCS Use Cases	A-28
Select Four Challenges of Deploying Microsoft Exchange 2010	A-28
Select Four Microsoft Exchange 2010 Server Roles	A-29
Review of Server Virtualization	A-30
Select Four Benefits of Server Virtualization	A-30
Select Four Benefits of Storage Virtualization	A-31
Select Three Benefits of Network Virtualization	A-32
Introduction to the Data Center Access Layer	A-33
Select Two Basic Designs for Data Center Access Layer	A-33
Review of VMware Ethernet Networking	A-34

Select Three Characteristics of the VMware vSwitch	A-34
Select Three Limitations of the VMware vSwitch	A-35
Select Two VMware DVS Features That Are <i>Not</i> Available in vSwitch	A-36
Select Three Features of VMware Port Groups	A-37
Review of Cisco Nexus 1000V Series Architecture	A-38
Select Three Features of VN-Link in Software	A-38
Select Three Examples Where VNTag Is Implemented	A-39
Summary	A-40

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

Overview	B-1
Objectives	B-1
Cisco UCS B-Series Fault Color Coding Scheme	B-2
Cisco UCS B-Series Fault Summary	B-2
Cisco UCS B-Series Fault Summary: Cluster	B-3
Cisco UCS B-Series Fault Summary: Core Files	B-4
Cisco UCS B-Series Fault Summary: Events	B-5
Cisco UCS B-Series Fault Summary: Settings	B-6
Cisco UCS B-Series Fault Summary: Syslog	B-7
Cisco UCS B-Series Hardware Discovery Common Errors	B-8
Cisco UCS B-Series: Server Discovery	B-8
Cisco UCS B-Series: Server Discovery FSM	B-9
Cisco UCS B-Series: Chassis Discovery FSM	B-11
Cisco UCS B-Series Hardware LED Error Codes	B-12
LED Indicators (Rear View)	B-12
LED Indicators (Front View)	B-13
Interpret LED Indicators	B-14
Beaconing	B-19
Cisco UCS B-Series Core Files	B-20
Displaying Core Dumps	B-20
Managing Core Dumps	B-21
Cisco UCS B-Series Local Management	B-22
show tech-support Commands	B-22
Summary	B-32

Troubleshooting Cisco UCS B-Series Service Profiles ***C-1***

Overview	C-1
Objectives	C-1
Troubleshooting Resource Assignment Issues	C-2
Overview of FSM	C-2
“Good” FSM State in the GUI	C-3
“Bad” FSM State in the GUI	C-4
Examining FSM State at the CLI	C-5
Common Service Profile Configuration Issues Preventing Association	C-6
Configuration Example	C-7
Configuration Issues Before Association: vNIC Assignment	C-8
Configuration Issues Before Association: Insufficient Identities	C-10
Association Issues: Insufficient Identities	C-11
Association Issues: First Server Associated	C-13
Association Issues: Insufficient Identities (Cont.)	C-14
Association Issues: Insufficient WWNN Identities	C-15
Association Issues: Second Server Associating	C-17
Troubleshooting Service Profile Issues After Association	C-18
Service Profile Issues After Association	C-18
Summary	C-24

Overview	D-1
Objectives	D-1
Troubleshoot Communications from Server to Ethernet or SAN Switch	D-2
Server Adapter View of Internal Backplane Ports	D-2
View of Fabric Uplink Ports (I/O Module)	D-3
View of Server Ports from Fabric Interconnect	D-4
Validate Northbound LAN Connectivity	D-5
Troubleshooting Ethernet Connectivity	D-6
Fabric Interconnect Port Display	D-6
Fabric Interconnect FSM Display	D-7
View of Northbound LAN Uplink Ports from Fabric Interconnect	D-8
Validating VLAN Assignments	D-9
Troubleshooting Fibre Channel Connectivity	D-10
Fabric Interconnect Fibre Channel Interface Validation	D-10
Fibre Channel Connectivity from SAN Switch View	D-11
Fibre Channel Switch Device Aliases	D-12
Troubleshooting FCoE Connectivity	D-14
Validate VSAN Assignments	D-14
Summary	D-15

Cisco Unified Computing System Management and Maintenance

Overview

When component physical connectivity is completed, attention shifts to system security and creating a solid administrative procedure framework on which to base operations. Implementers must understand how to configure access control, how to back up and restore the Cisco Unified Computing System Manager (UCS Manager) configuration database, and how to update component firmware.

Module Objectives

Upon completing this module, you will be able to articulate how to secure Cisco UCS Manager against unauthorized access, organize resources, and perform important system management and monitoring functions. This ability includes being able to meet these objectives:

- Implement Cisco Unified Computing System startup and shutdown procedures
- Configure role-based access control
- Back up and restore the Cisco UCS Manager database
- Manage high availability
- Monitor system events
- Manage and upgrade Cisco UCS B-Series firmware

Implementing Cisco Unified Computing System Startup and Shutdown Procedures

Overview

Implementers periodically need to power down and restart elements of Cisco Unified Computing System. Proper startup and shutdown procedures must be followed to prevent data corruption and communication failure. Cisco Unified Computing System is designed to operate in a high-availability configuration with few single points of failure. The fabric interconnect cluster can survive the complete failure of one cluster element and continue to forward on the fabric B data plane.

The Cisco Unified Computing System B-Series (UCS B-Series) Blade Server can survive the loss of one fabric interconnect and continue to operate if the other fabric interconnect is operational. If the server needs to be removed from the chassis for maintenance, then proper shutdown procedures need to be followed.

Objectives

Upon completing this lesson, you will be able to follow correct procedures to start up and shut down fabric interconnects and blade servers. This ability includes being able to meet these objectives:

- Describe the Cisco UCS 6100 Series Fabric Interconnect startup and shutdown procedures
- Describe the effects of shutting down or rebooting a Cisco UCS 6100 Series Fabric Interconnect on the high-availability cluster
- Implement startup and shutdown procedures for Cisco UCS B-Series Blade Servers
- List the procedures for power state verification

Cisco UCS 6100 Series Fabric Interconnect Startup and Shutdown Procedures

This topic discusses the procedures to start up and shut down a Cisco UCS 6100 Series Fabric Interconnect.

Fabric Interconnect Startup and Shutdown

Fabric Interconnect Startup and Shutdown

- The Cisco UCS 6100 begins power-up when power is applied to at least one power supply.
- To reboot a fabric interconnect, log in to the Cisco UCS Manager CLI, connect to the local management shell, and issue the **reboot** command.

```
s6100-A# connect local-mgmt
Cisco UCS 6100 Series Fabric Interconnect
s6100-A(local-mgmt)# reboot
```

Cisco UCS 6100 Series Fabric Interconnects were designed for continuous operation; therefore, they have no power switch. A fabric interconnect power-up assumes that power is applied to one or both of the power supplies.

If the fabric interconnect needs to be rebooted, then open a connection to the Cisco UCS Manager command-line interface (CLI), connect to the local management shell, and issue the **reboot** command.

Effects of Shutting down or Rebooting a Cisco UCS 6100 Series Fabric Interconnect on the High-Availability Cluster

This topic discusses the impact on the cluster and hosts if the active fabric interconnect is rebooted or shut down.

Effect of Active Fabric Interconnect Shutdown

Effect of Active Fabric Interconnect Shutdown

Effects on the cluster:

- The subordinate cluster node becomes the active management node.
- The data plane on the subordinate node becomes the only active data path.

Effects on the hosts:

- If hardware failover is configured in the service profile, then fabric failover prevents loss of connectivity.
- If NIC teaming is configured in the operating system or hypervisor, then fabric failover prevents loss of connectivity.
- For Fibre Channel or FCoE communication, a multipath I/O driver is required in the operating system or hypervisor to reroute around path failure.

If the active management node in the cluster is rebooted or taken out of service, then the subordinate node detects the absence of its peer and becomes the active management node. The data plane of the newly promoted fabric interconnect becomes the only active data path.

Fabric failover can occur only when hardware failover is configured in the service profile or when network interface card (NIC) teaming occurs at the operating system or hypervisor level. Assuming that fabric failover is successful for Ethernet communications, Fibre Channel over Ethernet (FCoE) communication continues only if there is a multipath I/O driver in the operating system or hypervisor.

If neither hardware failover nor NIC teaming is configured, then all Ethernet and Fibre Channel communications are halted on that host. FCoE depends on Ethernet communications to establish initiator connections to a Fibre Channel target.

Effect of Subordinate Fabric Interconnect Shutdown

Effect of Subordinate Fabric Interconnect Shutdown

Effects on the cluster:

- The active fabric interconnect detects the loss of its peer and does not attempt to synchronize configuration or firmware objects until the peer rejoins the cluster.

Effects on the hosts:

- Ethernet hosts are not affected by the loss of the subordinate fabric interconnect.
- A multipath I/O driver in the operating system or hypervisor detects path failure.
- Fibre Channel or FCoE communication continues over the primary path.

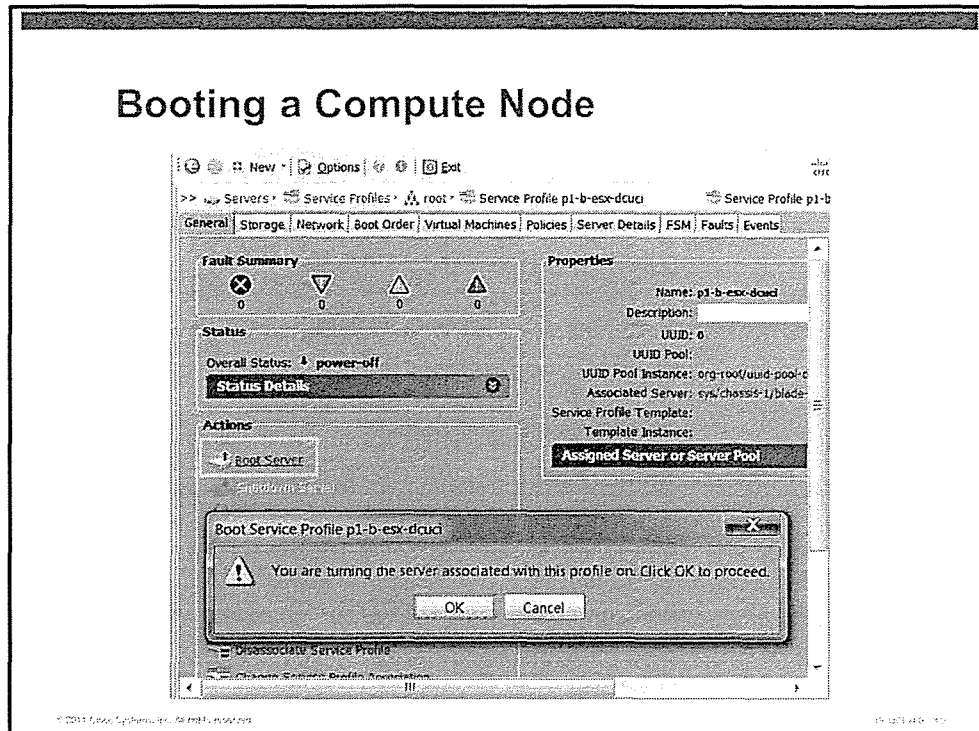
If the subordinate management node in the cluster is rebooted or taken out of service, then the active node detects the absence of its peer. The active node discontinues configuration and former replication to its peer.

Ethernet and FCoE hosts continue using the primary data path. Multipath I/O drivers detect the loss of the path that is provided by the subordinate peer.

Startup and Shutdown Procedures for Cisco UCS B-Series Blade Servers

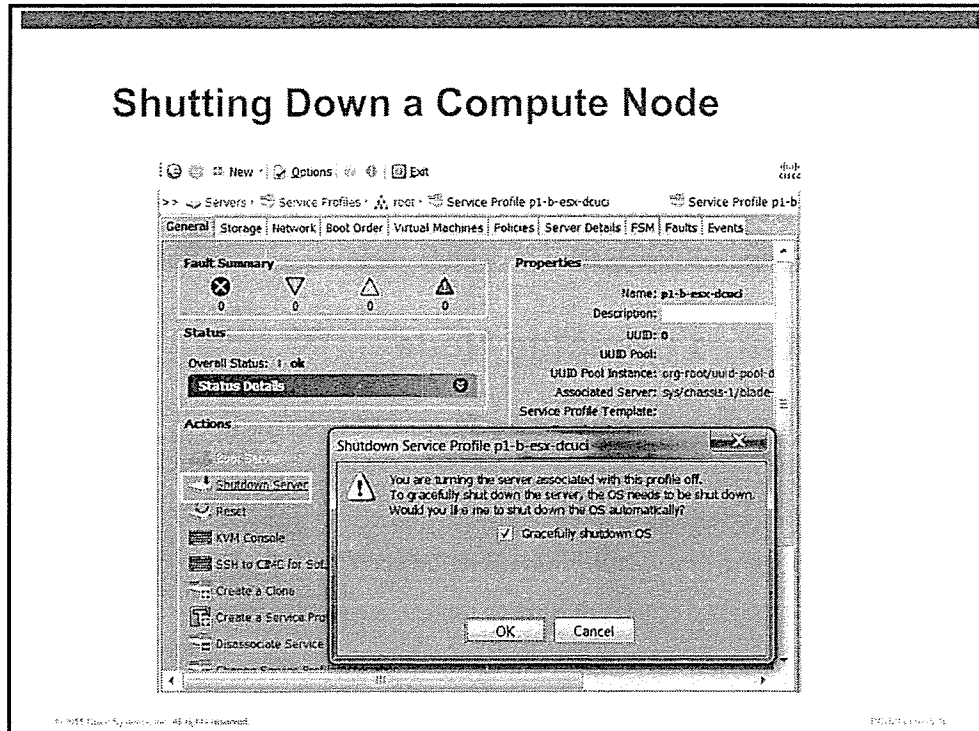
This topic discusses the process to boot, restart, or shut down a Cisco UCS B-Series Blade Server.

Booting a Compute Node



Boot a blade server from the Servers tab of the navigation pane. In the Actions section of the content pane, click the **Boot Server** link. To observe the boot sequence, click the KVM console link.

Shutting down a Compute Node

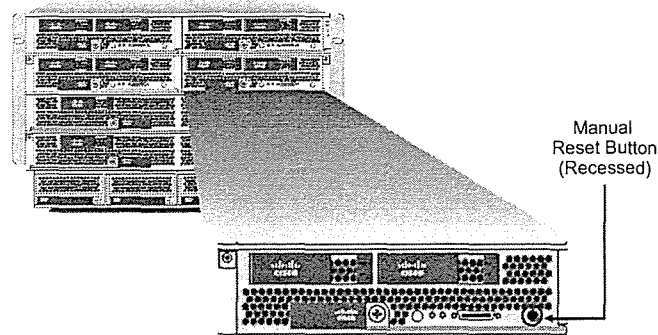


Best practice is to shut down a computing node from within the operating system or hypervisor. However, if the server must be shut down without access to the operating system or hypervisor, the server can be shut down from its service profile. The check box for graceful shutdown tries to signal the operating system or hypervisor that the server needs to shut down via an Advanced Configuration and Power Interface (ACPI) call.

Compute Node Hardware Restart

Compute Node Hardware Restart

- Each blade has a reset button on the front panel. This button should be used only when a software reset through the Cisco UCS Manager is not possible.



A compute node can also be restarted from the front panel of the blade server. Refer to the figure for the location of the recessed button. When you press the button, it sends an ACPI call to the operating system or hypervisor, stating that the system is going down. If the button is pressed and held for 4 seconds or more, then the system powers off immediately.

The hardware reset button should be used as a last resort to reset the compute node, because the use of this button can result in data corruption. The hardware reset button can be disabled in BIOS.

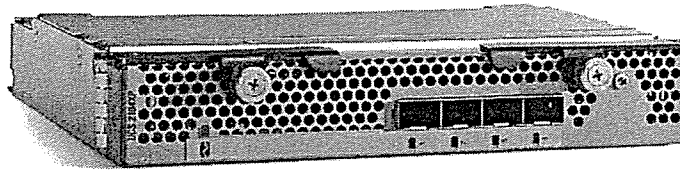
Procedures for Power State Verification

This topic discusses power state verification.

IOM Power Options

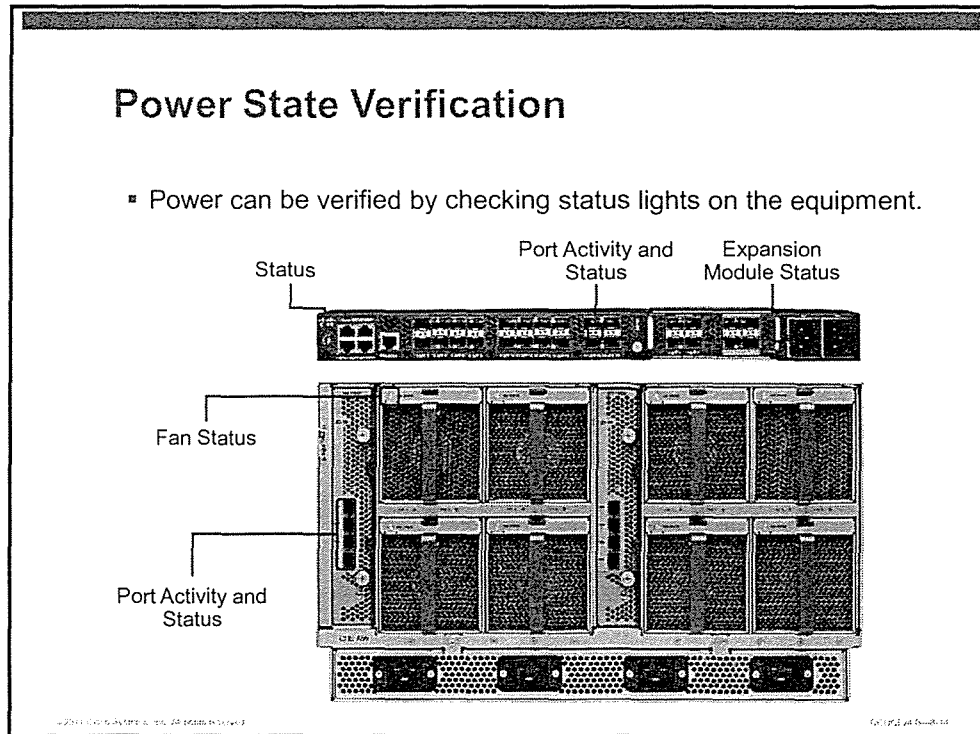
IOM Power Options

- IOMs in the server chassis have no independent power options. These devices act as an extension of the Cisco UCS 6100 Fabric Interconnect.
- Cisco UCS 2104 modules are powered on when power is applied to the Cisco UCS 5108 server chassis.



The Cisco UCS 2104 I/O module (IOM) is passive, from a power state perspective. This module is powered on or off when power is supplied or removed from the Cisco UCS 5108 server chassis.

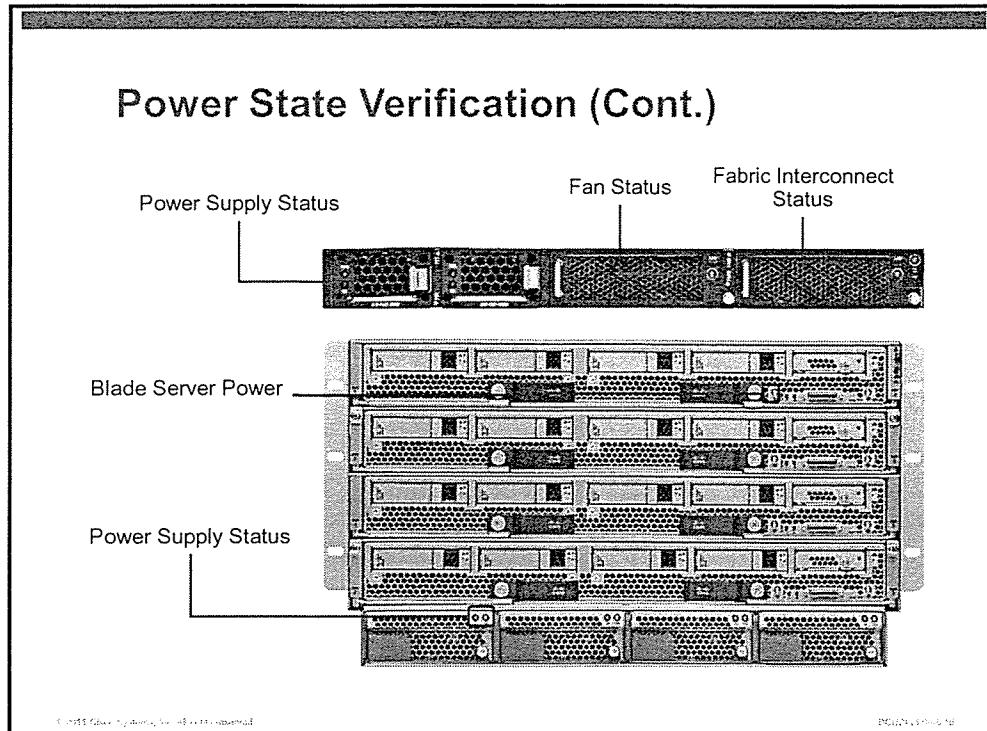
Power State Verification—Chassis Rear



The power status of fabric interconnects and chassis IOMs can be determined by LEDs on the rear of the fabric interconnects and the Cisco UCS 5108 server chassis.

A power state of active or on is indicated by a green LED. A power state of down or off is indicated by an unlit LED.

Power State Verification—Chassis Front



The power status of fabric interconnects and blade servers can also be indicated by LEDs on the rear of the fabric interconnects and blade server faceplates.

A power state of active or on is indicated by a green LED. A power state of down or off is indicated by an unlit LED.

Summary

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

Summary

- Fabric interconnects are powered on by applying power to one or both power supplies and can be rebooted from the CLI.
- The effect of the loss of the fabric interconnect to the cluster and affected hosts depends on whether the active or subordinate node in the cluster fails.
- Host operating systems can be shut down in Cisco UCS Manager through the service profile or by hard reset of the blade front panel.
- The power state of all Cisco Unified Computing System components can be verified physically, through observation of chassis LEDs.

© 2011 Cisco Systems, Inc. All rights reserved.

UCS-400-004-01

Configuring Role-Based Access Control

Overview

Access control is a key requirement for any data-center component. Because an unauthorized user can perpetrate a great scope of damage, securing user interfaces is of paramount importance.

Objectives

Upon completing this lesson, you will be able to configure local users and remote authentication providers and to map users to roles and privileges. This ability includes being able to meet these objectives:

- Articulate the overall framework of RBAC in Cisco UCS B-Series
- Configure local users, roles, and privileges
- Configure organizations and locales
- Demonstrate an understanding of the effective rights of a user, as an intersection of roles and locales that are mapped to that user
- Configure LDAP and Active Directory as an external authentication and authorization service
- Demonstrate how to map Cisco Unified Computing System roles to LDAP and Active Directory attributes

Overall Framework of RBAC in Cisco UCS B-Series

This topic discusses the overall approach to authentication and authorization in the Cisco Unified Computing System.

RBAC and Organizations

RBAC and Organizations

- RBAC and organizations are complimentary constructs.
- They can be used separately or together.

Equipment Servers LAN SAN VM Admin

Filter: User Management

- Users and Groups
 - Authorization
 - LDAP
 - RADIUS
 - TACACS+
 - User Services
 - Locales
 - Locally Authenticated Users
 - Team1-NetworkAdmin
 - Team1-Operator
 - Team3-NetworkAdmin
 - Team3-Oper
 - Team5-NetworkAdmin
 - Team5-Operator
 - admin
 - Remotely Authenticated Users
 - Roles

Equipment Servers LAN SAN VM Admin

Filter: All

- Servers
 - Service Profiles
 - root
 - Sub-Organizations
 - Hypothetical_Inc
 - Sub-Organizations
 - Americas
 - Asia_Pacific
 - EMEA
 - Service Profile Templates
 - root
 - Policies
 - root
 - Pools
 - root

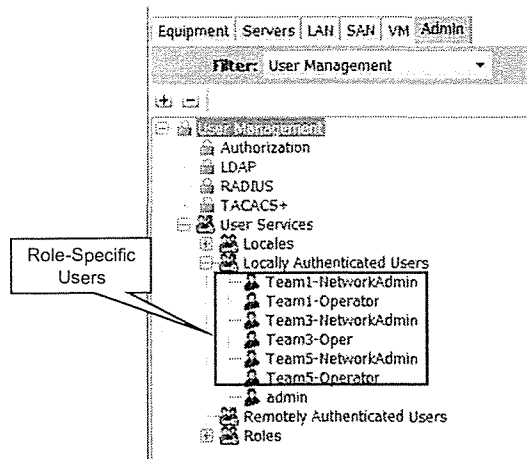
Role-based access control (RBAC) describes authentication and authorization that is tuned to delegate responsibilities within a system. Within the scope of RBAC in Cisco Unified Computing System, two constructs can be used, individually or in combination, for more granular control.

Authentication and authorization services provide granular control of access to Cisco Unified Computing System resources. When these services are used alone, organizations can be thought of as folders for organizing policy.

Role-Based Access Control

RBAC

- RBAC and organizations are complimentary constructs.
- They can be used separately or together.

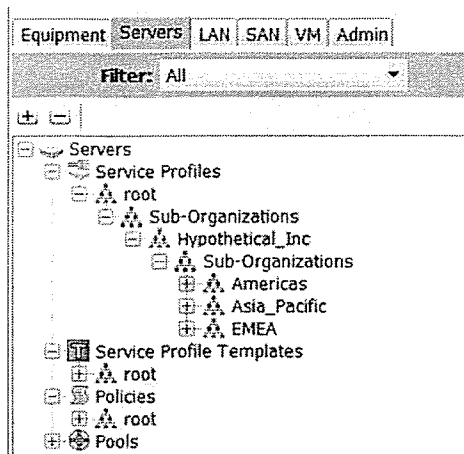


RBAC provides local and remote authentication and authorization services for Cisco Unified Computing System. The user “admin” is the built-in administrator account and cannot be deleted. As many as 40 local user accounts can be configured on the fabric interconnects.

Organization Basics

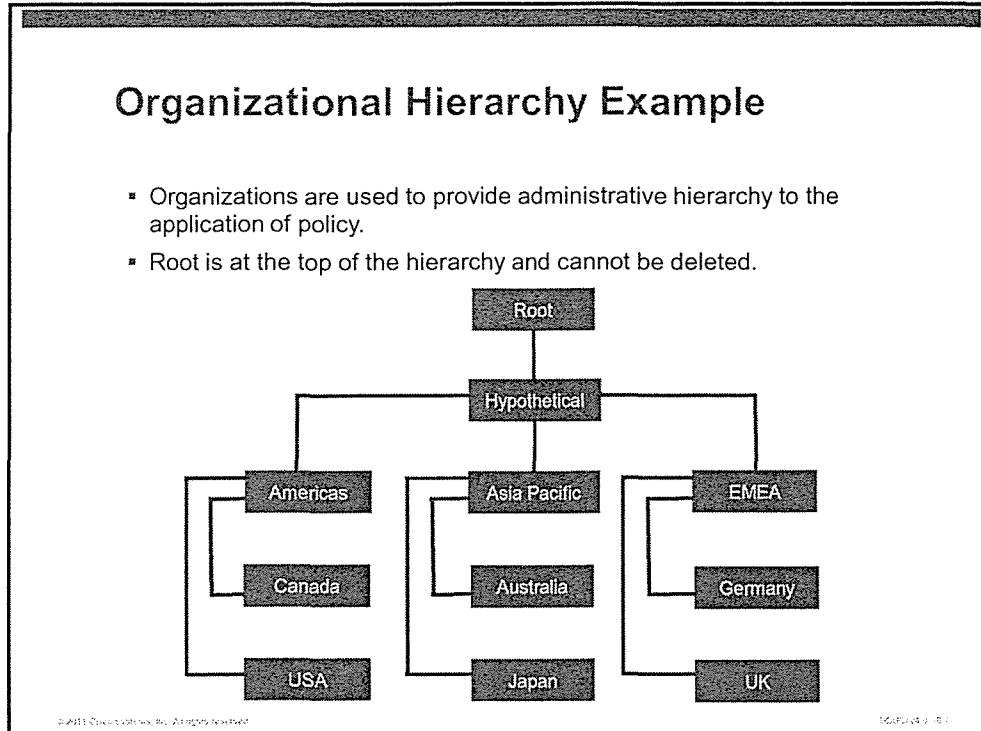
Organizational Basics

- Organizations are used to provide administrative hierarchy to the application of policy.



Organizations are created to organize policy into an administrative hierarchy. Although organizations are not a mandatory component of Cisco Unified Computing System, they can greatly simplify the locating of appropriate policy.

Organizational Hierarchy Example

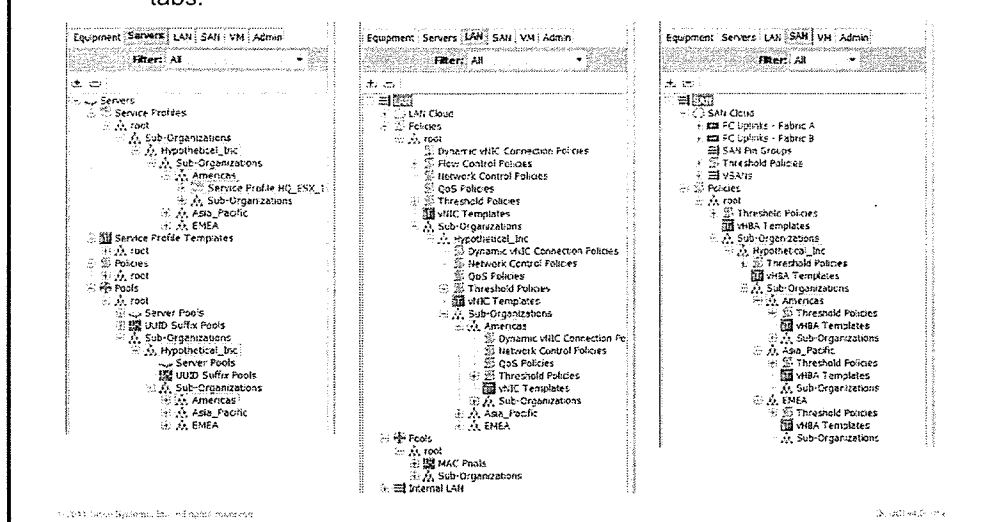


The example in the figure illustrates one approach to organizational hierarchy. Hypothetical Inc. is a fictional multinational company that has decided to use organizations to divide policy by geography. At the top of the hierarchy is an organization called root. Even if organizations are not created in Cisco Unified Computing System, there is always one organization: root.

Scope of Organizations

Scope of Organizations

- Organizations can be created (and exist) on the Server, LAN, and SAN tabs.

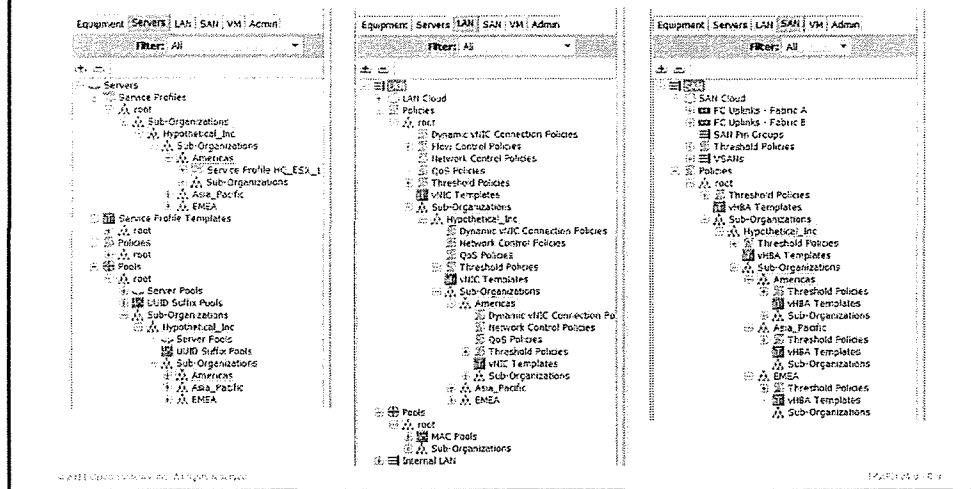


Organizations can be created in the Server, LAN, and SAN tabs of the navigation pane in Cisco Unified Computing System Manager (UCS Manager). Each tab allows the creation of organizations to organize function-specific policy.

What Can Be Configured in an Organization?

What Can Be Configured in an Organization?

- You can create policies, profiles, thresholds, and pools specific to the tab context (Server, LAN, or SAN).

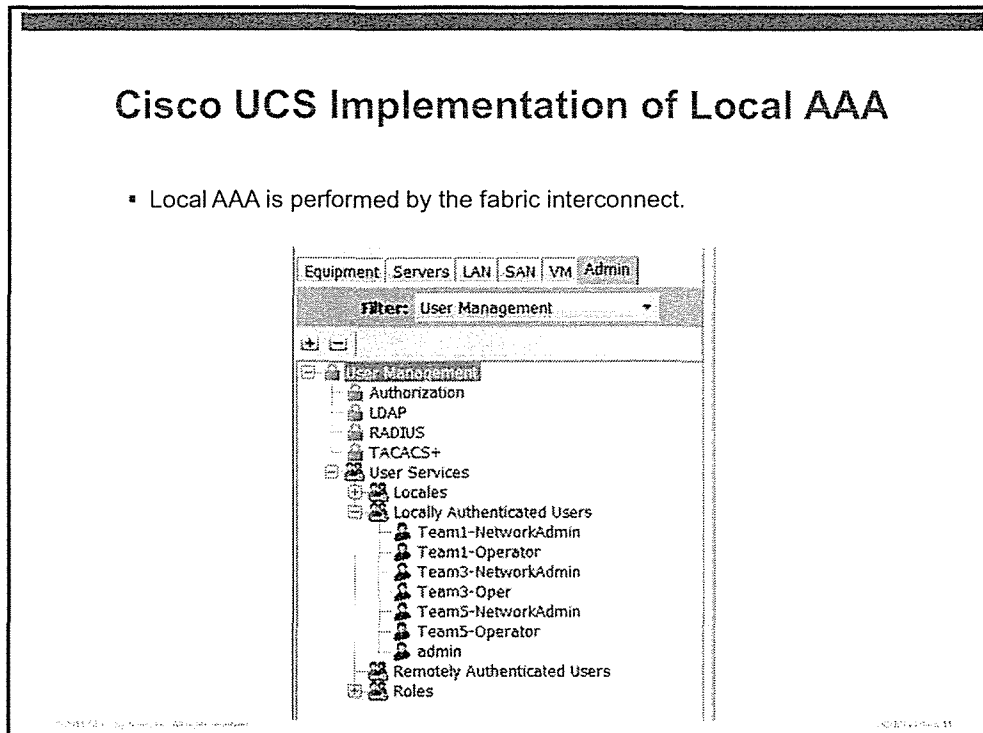


Depending on the tab context in Cisco UCS Manager, organizations can contain service profiles, identity pools, resource pools, policies, and thresholds.

Configuring Local Users, Roles, and Privileges

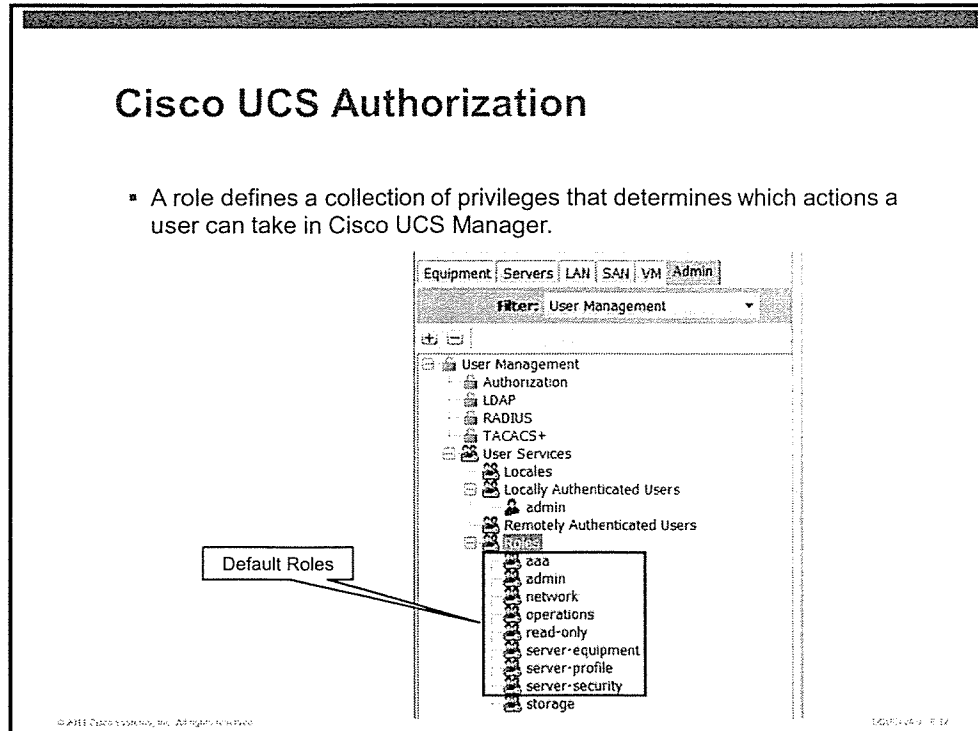
This topic discusses the authentication, authorization, and accounting (AAA) for local users in Cisco UCS Manager.

Cisco UCS Implementation of Local AAA



From the Admin tab in Cisco UCS Manager, choose **User Management** from the drop-down filter list. Expand **User Services > Locally Authenticated Users** to access a list of local users.

Cisco UCS Authorization



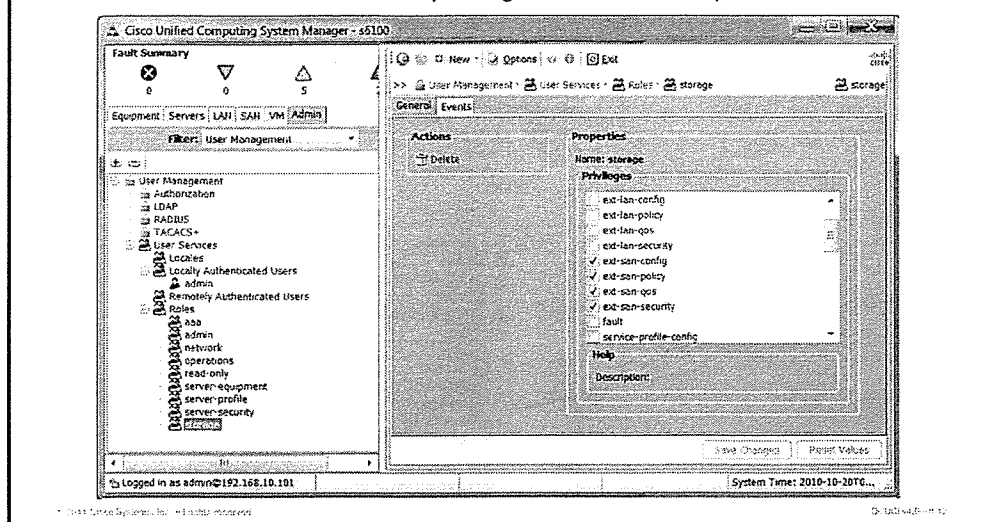
When a user is authenticated with a username and password, the Cisco UCS Manager authorization system is used to enforce the property of least privilege. The doctrine of least privilege provides that any privilege that is not required for users to perform their delegated functions should be administratively prohibited.

Cisco UCS Manager applies authorization policy via a role. There are nine preconfigured roles and the capacity to create custom roles.

Structure of a Role

Structure of a Role

- Select a role to view its privileges in the content pane.



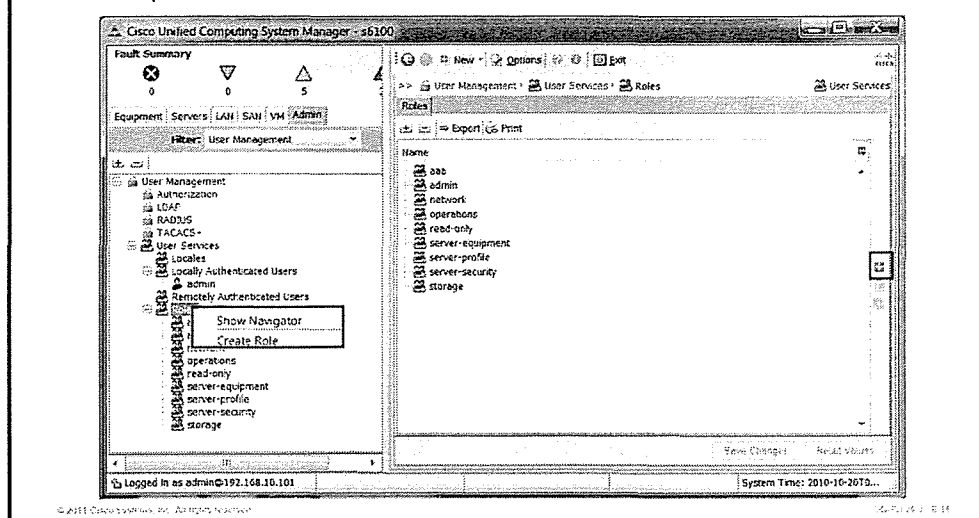
In the example, the storage role is selected. In the content pane, the privileges that define the storage role are indicated by the check boxes that have been checked. There are 34 system-defined privileges. Privileges cannot be deleted and, unlike roles, new privileges cannot be created.

Refer to *Cisco UCS Manager GUI Configuration Guide, Release 1.3(1)* for a detailed description of each privilege and the default role to which each privilege is assigned.

Create a Role—Start the New Role Wizard

Create a Role—Start the New Role Wizard

- Right-click **Roles** or click the plus sign (+) in the content pane.

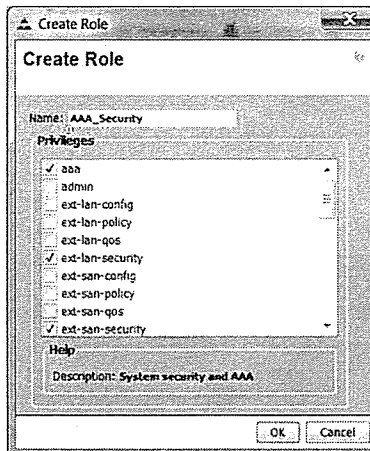


To start the new role wizard, right-click the role in the navigation pane or click the plus sign (+) in the content pane.

Name Role and Define Privileges

Name Role and Define Privileges

- Click on the text of a privilege, and its function will appear in the Help section.

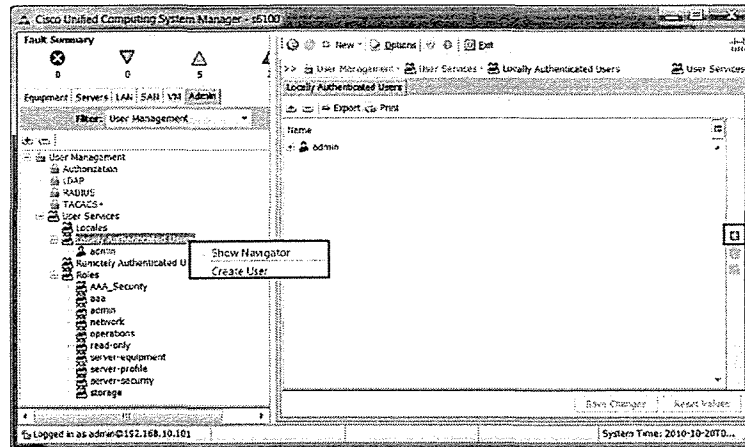


Define a name for the new role and select the appropriate privileges. Click the OK button to finish creating the role.

Create a Local User—Start the New User Wizard

Create a Local User—Start the New User Wizard

- Right-click **Locally Authenticated Users** or click the plus sign (+) in the content pane.



To create a new user, right-click **Locally Authenticated Users** or click the plus sign (+) in the content pane.

Create Local User with Custom Role

Create Local User with Custom Role

- Jeremy will inherit the permissions of the new AAA_Security role.

The screenshot shows the 'Create User' wizard interface. The fields are filled as follows:

- Login ID: jmolton
- First Name: Jeremy
- Last Name: Howlton
- Email: jmolton@cisco.com
- Phone: 415.555.1212
- Password: [masked]
- Confirm Password: [masked]

Under the 'Roles' section, the following roles are listed with checkboxes:

- ☒ AAA_Security
- ☐ admin
- ☐ network
- ☐ operations
- ☐ read-only
- ☐ server-equipment
- ☐ server-profile
- ☐ server-security
- ☐ storage

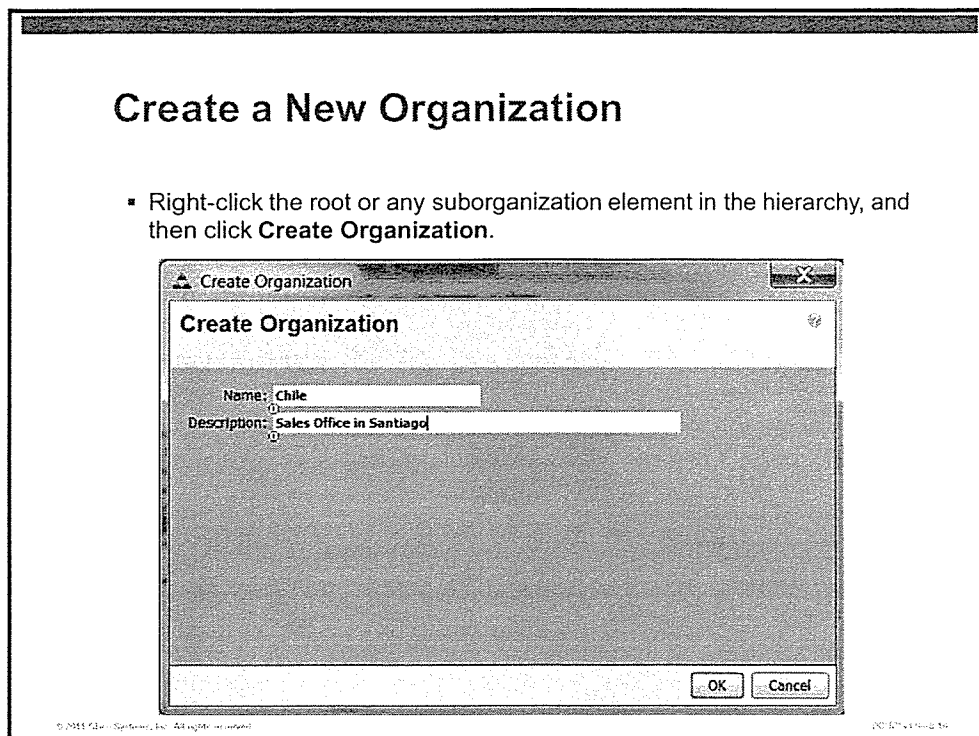
The 'Locales' section is empty. The 'OK' and 'Cancel' buttons are at the bottom right.

The figure shows the settings for the creation of user jmolton. This user will be created with the new AAA_Security role and its inherent privileges. The only two required fields in the Create User wizard are Login ID and Password. If no role is selected, then the user is assigned read-only privileges.

Configuring Organizations and Locales

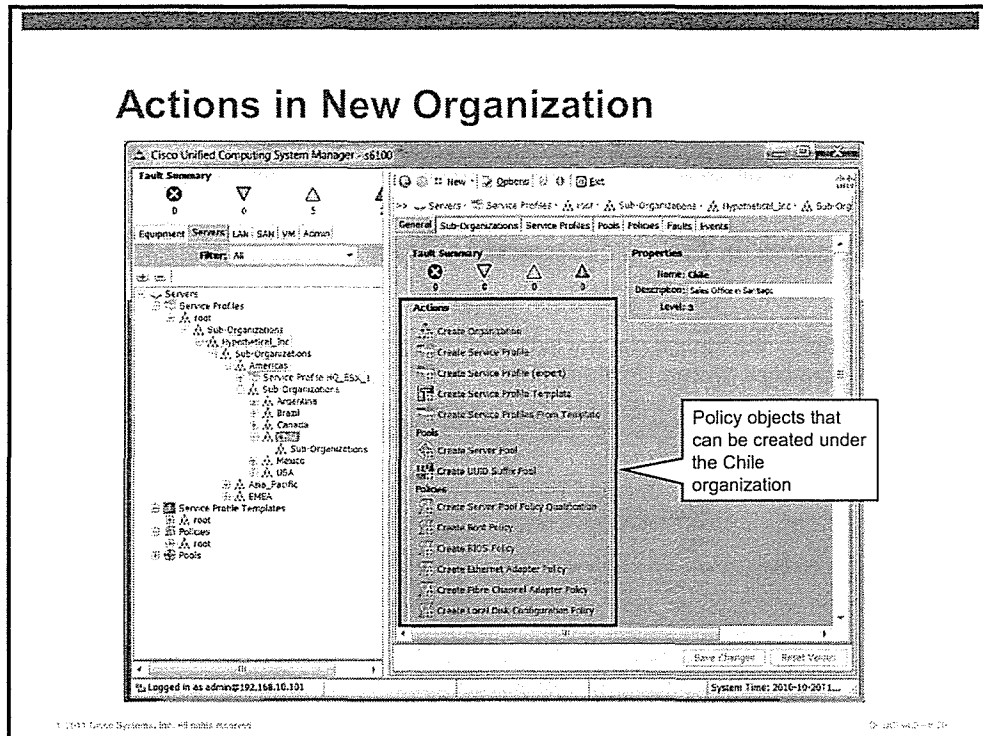
This topic discusses the creation of organizations and locales.

Create a New Organization



To create a new organization, right-click the root organization or any previously created suborganization. New organizations can be created in the Server, LAN, or SAN tab. The new organization is propagated automatically to all three relevant tabs.

Actions in New Organization

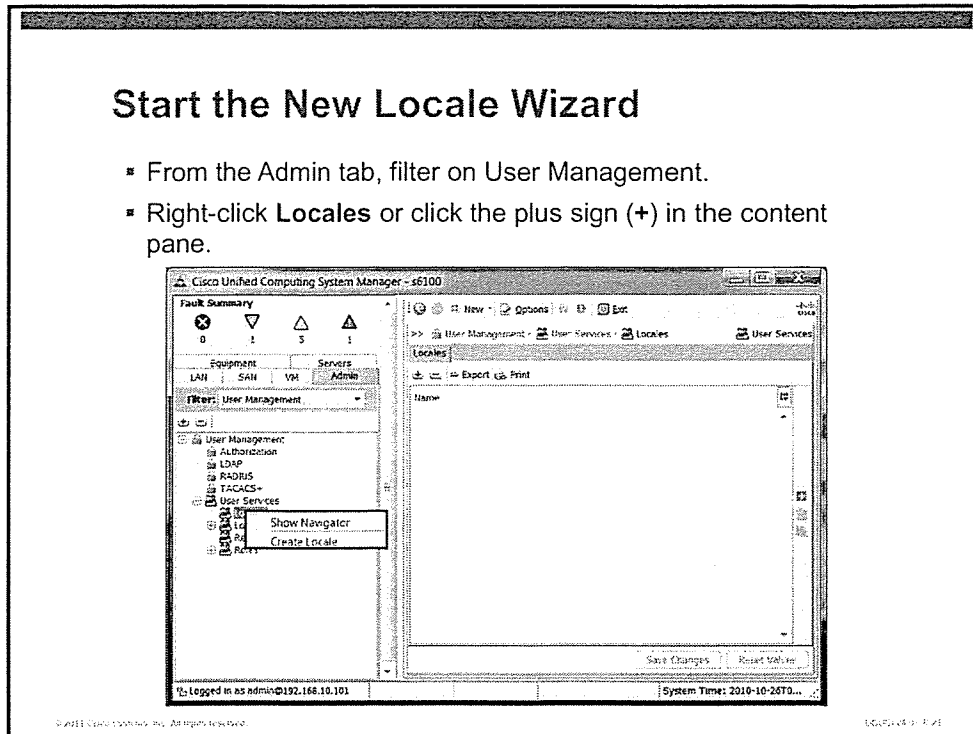


In the example that the figure shows, a new suborganization for Chile is created. Chile is propagated to the LAN and SAN tabs. Because the current context is the Server tab, all of the actions that are available in the Chile organization relate to service profiles, pools, and policies that relate to blade-server definition.

Start the New Locale Wizard

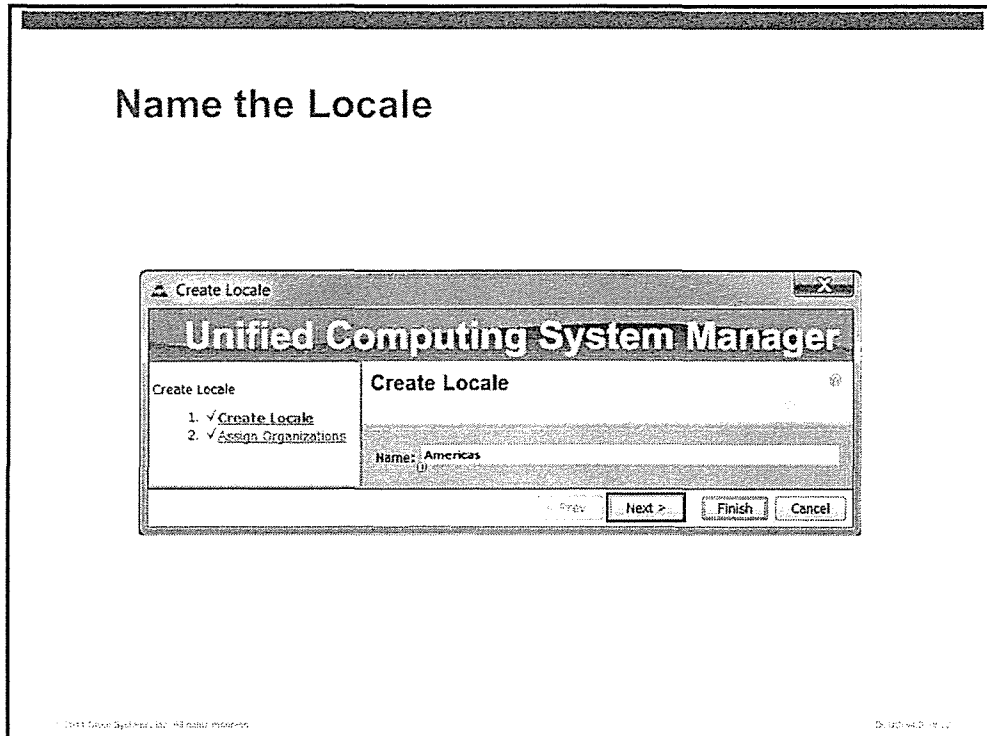
Start the New Locale Wizard

- From the Admin tab, filter on User Management.
- Right-click **Locales** or click the plus sign (+) in the content pane.



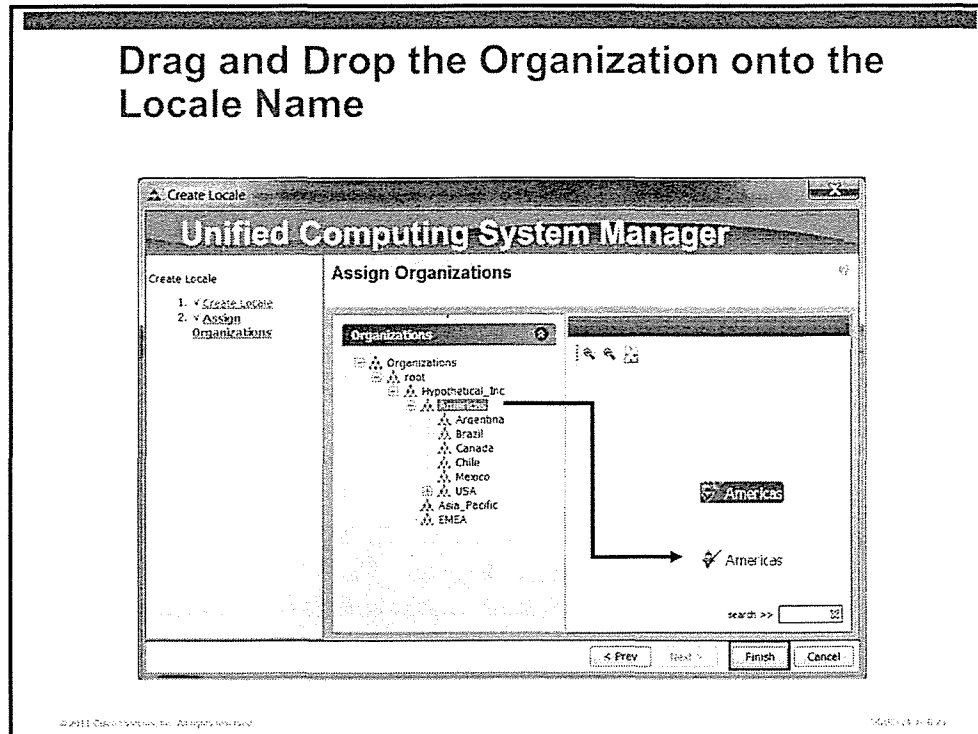
Unlike organizations, locales are created under the Admin tab. Set the filter to User Management from the drop-down list. To create a new locale, either right-click Locale or click the plus sign (+) in the content pane.

Name the Locale



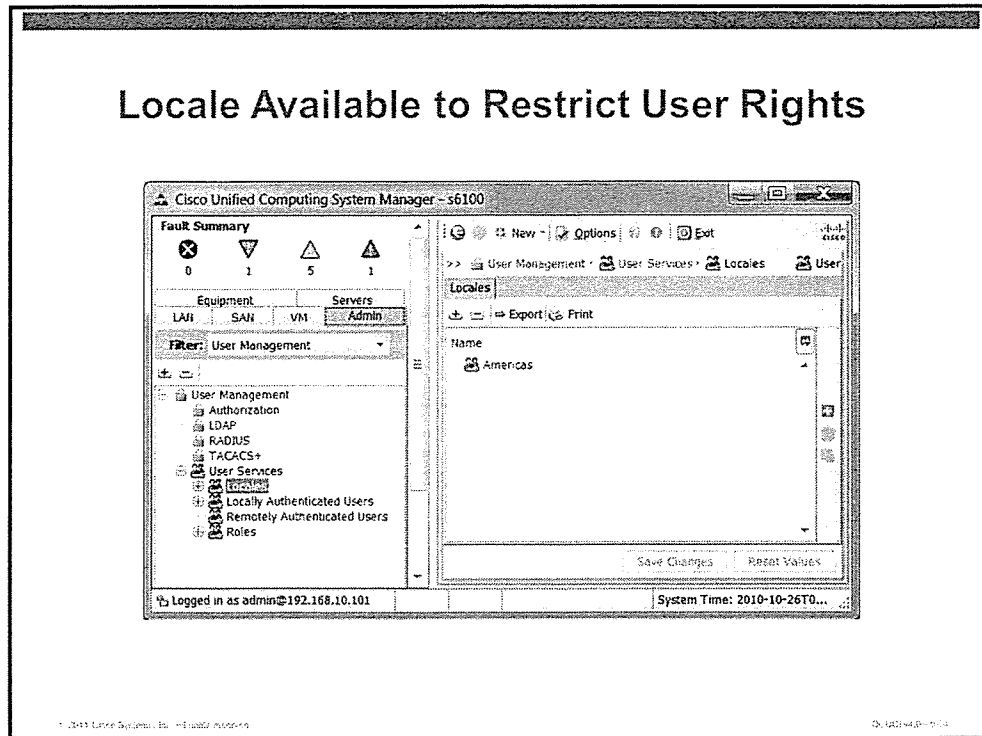
Provide the new locale with a descriptive name.

Drag and Drop the Organization onto the Locale Name



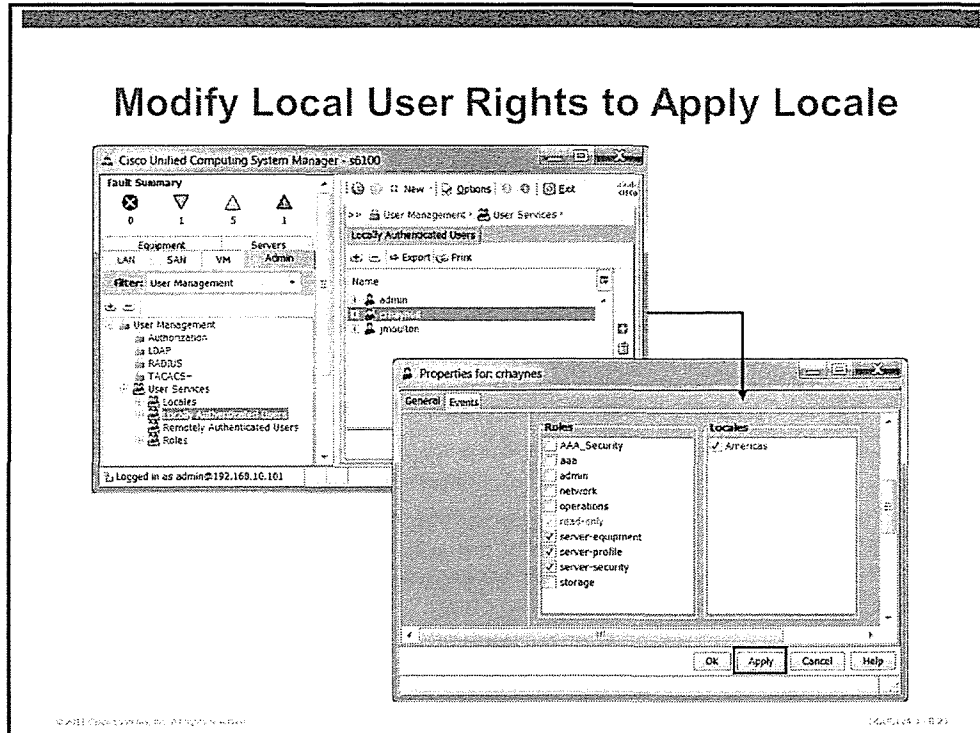
Click the double down-arrow icon and expand the list of organizations. Click the organization that applies to the new locale and drag it into the right-hand window, under the name of the locale. If the operation is successful, the name of the organization appears beneath the name of the locale, with a checkmark to the left of the organization. Click Finish to complete the wizard.

Locale Available to Restrict User Rights



The purpose of creating a locale is to restrict the privileges of the user to a particular organization. Your new locale should appear in the Locales list.

Modify Local User Rights to Apply Locale



In the example, user chrhaynes is assigned the server-equipment, server-profile, and server-security roles. This user is also now bounded by the Americas locale.

Effective Rights of a User, as an Intersection of Mapped Roles and Locales

This topic discusses how the introduction of a locale can change the effective rights of a user.

Determination of Effective Rights

Determination of Effective Rights

- User rights are determined by roles and privileges.
- If no locale is applied, then the user rights begin at the root organization and flow to all suborganizations.
- If a locale is applied to a user profile, then the rights that are assigned to the user begin at the suborganization that is defined by the locale and flow to all organizations beneath that suborganization.

© 2011 Cisco Systems, Inc. All rights reserved. DCUCI v4.0

The effective rights of the user are determined by the privileges that roles membership bestows and those that locale restricts.

Effective User Rights for Admin

Effective User Rights for Admin

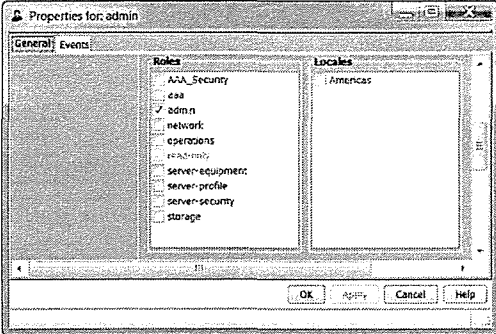
Root

Hypothetical

Americas

USA

- The admin user has unrestricted privileges from the root organization down to every suborganization.
- The admin user cannot be restricted by locale.



© 2011 Cisco Systems, Inc. All rights reserved.13000000-0000

The built-in admin user has complete administrative privileges, from the root organization down to the lowest suborganization. The admin user and any user with the admin role cannot be assigned to a locale.

Effective User Rights for crhaynes

Effective User Rights for crhaynes

- The effective rights for the user crhaynes are the intersection of the server-equipment, server-profile, and server-security roles and the Americas locale.

Properties for crhaynes

Roles	Locales
AAA_Security	
asa	
admin	
network	
operations	
read-only	
☒ server-equipment	☒ Americas
☒ server-profile	
☒ server-security	
storage	

OK Apply Cancel Help

User crhaynes has privileges only in the Americas organization and suborganizations. Although crhaynes has read-only privileges higher up in the organizational hierarchy, this user cannot create any objects that are associated with the assigned roles higher than Americas in the organizational structure.

Configuring LDAP and Active Directory as an External Authentication and Authorization Service

This topic discusses using Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory for remote user authentication and authorization.

Cisco UCS User Security Features

Cisco UCS User Security Features

- AAA
 - Authentication, Authorization, and Accounting
- Cisco Unified Computing System authentication
 - Only one type of authentication (local or remote) can be enabled at a time. All authentication requests are handled by the configured service.
 - Cisco UCS cannot be configured in a mixed mode, in which some users are authenticated locally and some users are authenticated remotely via different AAA services.
 - If remote authentication is enabled, then the only time local authentication is allowed is when the remote service is unreachable and does not respond within a specified time.
- User management and local AAA
 - User management defines the creation, deletion, and maintenance of local users for SAM. AAA services for local user accounts are managed locally.

The local user database is limited to 40 users (39 users plus admin). For additional scalability and security options (such as multifactor authentication), Cisco UCS Manager supports the LDAP and Active Directory, RADIUS, and TACACS protocols.

When a remote authentication method is enabled, the local username database is no longer used. Cisco UCS Manager falls back to the local database only if all remote authentication servers are unresponsive.

User Database

User Database

- Cisco Unified Computing System provides these facilities to support remote AAA:
 - AAA services for these access methods
 - SSH (Telnet is disabled by default)
 - Console
 - HTTP and HTTPS
 - SMASH, CIM-XML, and WS-MAN (DMTF standards)
 - Support for remote AAA (RADIUS, TACACS+, LDAP) requests and responses.
 - Configuration of attributes for RADIUS, TACACS+, and LDAP.

Cisco UCS Manager divides authentication tasks into two categories: console and default. The console category affects authentication access only to the serial consoles of the fabric interconnects. The default category controls the authentication method to these services:

- Secure Shell (SSH)
- Console
- HTTP and HTTPS
- Systems Management Architecture for Server Hardware (SMASH), Common Information Model (CIM)-XML, and Web-Services Management (WS-MAN)

LDAP Statistics

LDAP Statistics

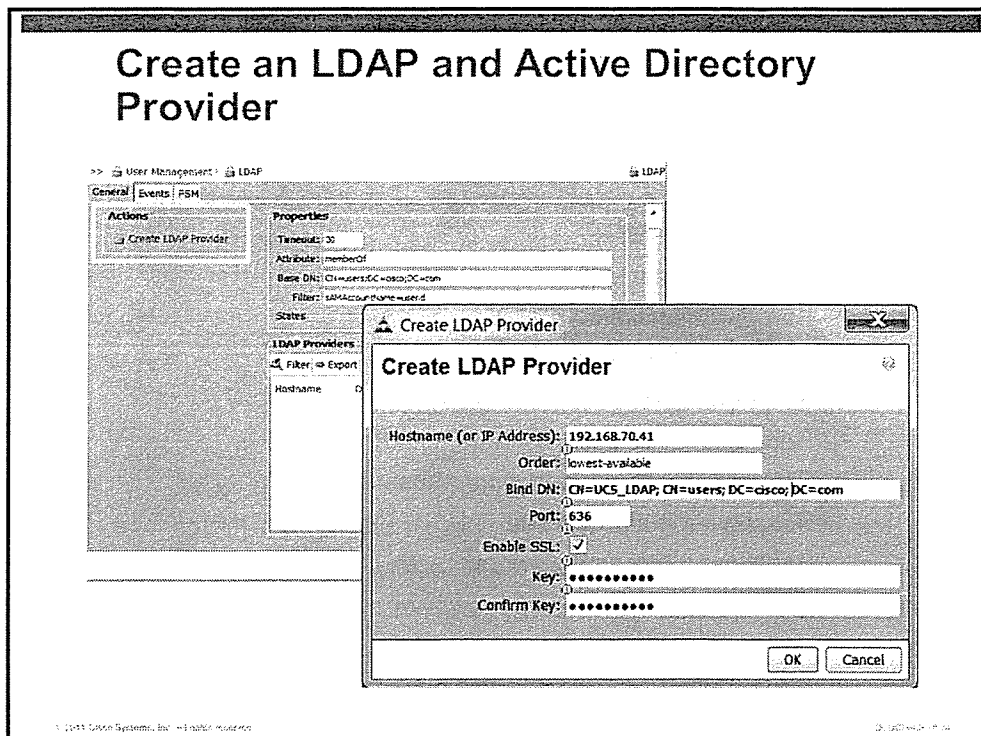
- Users can view the these LDAP server statistics, which are maintained in SAM.
- Authentication statistics
 - Failed transactions
 - Successful transactions
 - Requests sent
 - Requests timed out
 - Responses with no matching requests
 - Responses not processed
 - Responses containing errors

© 2011 Cisco Systems, Inc. All rights reserved.

UCS-UCS-4-10-11

Cisco UCS Manager maintains a running list of statistics that are related to LDAP and Active Directory remote authentication services. Of particular importance is the failed transactions counter. If the failed transactions counter is incrementing quickly, it might indicate that unauthorized access is being attempted.

Create an LDAP and Active Directory Provider



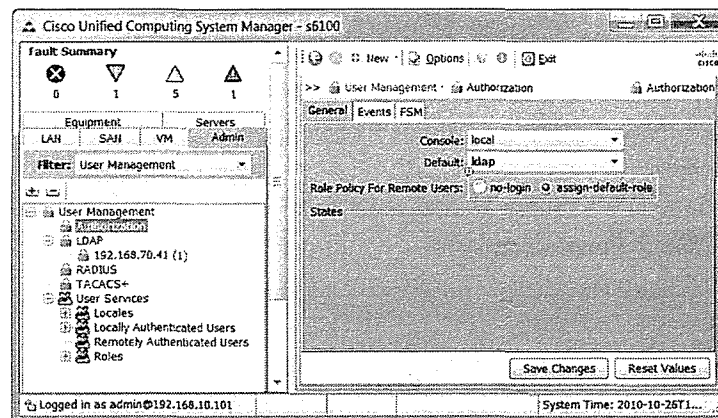
To create an LDAP provider, click the **Admin** tab, set the filter to **User Management**, and click **LDAP**. Click the **Create LDAP Provider** link and fill out the form:

- In the **Hostname (or IP Address)** field, enter the IP address of the LDAP provider or its fully qualified domain name (FQDN).
- In the **Order** field, enter a number or accept the default to have Cisco UCS Manager select the lowest available number. If this is the first LDAP provider, the automatically selected number will be “1”. The number indicates the order in which Cisco UCS Manager selects LDAP servers for authentication. If server 1 is unavailable or unresponsive, then Cisco UCS Manager attempts to authenticate requests with LDAP provider 2, and so on. A total of 16 LDAP servers can be configured for redundancy; at least 2 are recommended.
- In the **Bind DN** field, enter the distinguished name (DN) of the LDAP object that will perform the username and password lookup in the LDAP database. In the example, user UCS_LDAP is configured to perform the lookup. The entry “CN=UCS_LDAP; CN=users; DC=cisco; DC=com” describes the user UCS_LDAP in the users container in the domain Cisco.com. (CN is the abbreviation for common name, and DC is the abbreviation for domain component.) User UCS_LDAP does not require administrative privileges, only the rights that are required to connect to the LDAP database.
- The **Port** field and **Enable SSL** check box are related. The default port for LDAP is TCP port 389. If the default is selected, then authentication requests are processed in cleartext. A best practice is to check the **Enable SSL** check box and change the port to TCP port 636. Microsoft Windows servers listen for LDAP over Secure Sockets Layer (SSL) on TCP port 636.
- In the **Key** and **Confirm Key** fields, enter the password for the LDAP user (in the example, user UCS_LDAP).

Change Authorization to LDAP and Active Directory

Change Authorization to LDAP and Active Directory

- The default is selecting the authentication and authorization provider for all remote logins.
- Keep console set to local until LDAP is tested.



To change the authentication method from local to LDAP, click the **Admin** tab and choose **Authorization** in the navigation pane. In the content pane, choose **LDAP** from the drop-down list to the right of the word “default.” This setting sets the authentication and authorization mode for all remote access authentication requests.

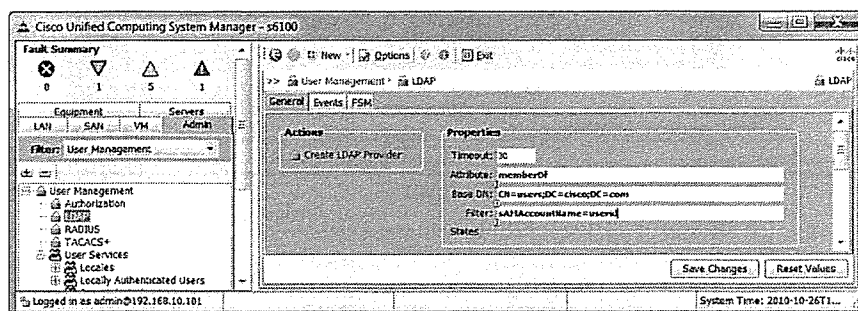
Mapping Cisco Unified Computing System Roles to LDAP and Active Directory Attributes

This topic discusses attribute mapping for role-based authorization.

LDAP Attribute Mapping

LDAP Attribute Mapping

- Timeout = How long to wait for LDAP response
- Attribute = LDAP and Active Directory attribute map to user role
- Base DN = Where to start search for username in LDAP tree
- Filter = Parse username



When you use local authentication, a role is mapped directly to the user. When the authentication is offloaded to a remote server, a method is required to signal to Cisco UCS Manager the role that should be mapped.

The first method is to use the CiscoAVpair attribute. The text value of that attribute can be passed from LDAP to Cisco UCS Manager, to perform the proper role mapping. However, CiscoAVpair is not a default attribute in Active Directory. Adding support for CiscoAVpair requires modifying the Active Directory schema. The policies of a given organization might not support this requirement.

If adding CiscoAVpair to the Active Directory schema is not a viable option, then Cisco UCS Manager can define any unused LDAP attribute, such as Department or Group, to hold and transfer the name of the role to which the user should be mapped.

In the example, the attribute mapping is performed against the value of the Active Directory user group affiliation. To parse the value of a group, the `memberOf` attribute is used. It is important to maintain the capitalization of the attribute exactly, including the capital "O". The base DN instructs Cisco UCS Manager to begin searching the LDAP directory tree, beginning at `CN=users`. The filter field is used to parse the username. In Active Directory, the attribute is named `sAMAccountName`. Again, the capitalization of the attribute must be maintained. If the LDAP server that is used for remote authentication is not Active Directory, then contact your LDAP administrator for the correct attributes.

Summary

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

Summary

- RBAC is a flexible combination of AAA controls and organizational hierarchy.
- Local users are assigned differentiated roles and privileges to delegate configuration functions that are appropriate to their organizational role.
- Organizations can be used for administrative separation of policy or can be linked to a locale to restrict user rights.
- Effective user rights are determined by roles and privileges. Privileges can be further restricted through the use of locales and policy hierarchy.
- LDAP and Active Directory can be configured as an external authentication and authorization provider.
- External authentication providers require attribute mapping to ensure that remotely authenticated users are assigned the correct privileges.

© 2011 Cisco Systems, Inc. All rights reserved.

781-201-1400-0000

Backing up and Restoring the Cisco UCS Manager Database

Overview

Good operational procedure includes maintaining up-to-date backups of Cisco Unified Computing System configuration data. All configuration data in Cisco Unified Computing System is stored in XML format. XML is simply textual data that conforms to the Cisco Unified Computing System XML schema. Even large implementations can be backed up and restored relatively quickly.

There are four main backup operations and two options to restore data to the Cisco Unified Computing System Manager (UCS Manager) database.

Objectives

Upon completing this lesson, you will be able to configure backup and to import and restore jobs. You also will understand the ramifications of selecting the correct backup or restore operation. This ability includes being able to meet these objectives:

- Differentiate between the supported backup types and the functions to which they map in the Cisco UCS Manager database
- Differentiate between an import operation and a disaster-recovery restore operation
- Configure a backup job
- Verify that the backup is created and executed
- Configure an import job to restore the AAA user database
- Verify that the AAA user database is restored
- Configure the backup job to preserve abstracted identities
- Configure the Cisco UCS 6100 Series Fabric Interconnect for disaster-recovery restore

Supported Backup Types and Functions

This topic discusses the procedures to create a disaster-recovery backup.

FULL State Backup

FULL State Backup

- Performs a complete binary dump of database
- Contains all configuration
- Contains all runtime state and status
- Is most useful during Cisco UCS Manager upgrades
 - Out-of-date after associations have changed
 - Cannot be modified selectively
- Can be restored only through a complete configuration wipe and reboot
- Is stored as a .tar.gz file

FULL state backups protect against catastrophic failure of both fabric interconnects in the cluster. This backup type includes all the runtime state information, such as the finite state machine (FSM) state of blades, the associated state of service profiles, and so on. This backup type also includes configuration information, such as users, policies, and so on.

Because the FULL state backup includes runtime state, this type of backup can quickly become outdated. Any changes to blade service profile associations render this backup obsolete.

Configuration Backup

Configuration Backup

- All configuration
 - Union of config-logical and config-system
- Logical configuration
 - Service profiles, templates
 - VLAN and VSAN configuration
 - Organizations, locales
- System configuration
 - AAA configuration, RBAC
 - User database
 - Cisco Unified Computing System configuration
- Stored as XML
- Preserve identities: New option in Cisco UCS Manager 1.2 and higher allows identities derived from pools to be preserved on restore.

Cisco UCS Manager supports three types of XML backups:

- **Logical configuration:** Logical configuration is all configuration that is not associated with authentication, authorization, and accounting (AAA). This configuration includes configured organizations, configured threshold policies, and configured VLANs and virtual storage area networks (VSANs) in your LAN and SAN clouds, respectively.
- **System configuration:** System configuration is all configuration that specifically pertains to the AAA role. Examples include RADIUS, Lightweight Directory Access Protocol (LDAP), TACACS, and users.
- **All configuration:** All configuration is a combination of the logical and system configurations.

Configuration backups are saved as XML representations of the configuration of the Cisco UCS Manager. These backups can be edited by using an XML editor or text editor. This ability makes configuration backups useful for creating templates that can be applied to other Cisco Unified Computing System implementations, or for adjusting the backup files if changes are made to the environment since the backup was last taken. No runtime state data (service profile associations and so on) is stored in these backups.

Use of Configuration Backups

Use of Configuration Backups

XML configuration backups can be edited easily.

- Useful for duplicating configuration in other implementations
- Can be modified before import in disaster-recovery scenarios
- Can be prepopulated for use in consulting engagements

XML configuration-level backups can be useful for more than simple recovery of a failed system. XML is easily edited by various editors and can be easily modified or customized before import.

Import Operations and Disaster-Recovery Restore Operations

This topic compares an import operation and a disaster-recovery restore.

Import vs. Restore

Import vs. Restore

Import from XML backup operation

- Execute from the Cisco UCS Manager GUI or CLI
- Restore service profiles, policies, thresholds, and AAA
- No state information (associated or unassociated)
- Can preserve abstracted (pool provided) identities

Restore operation

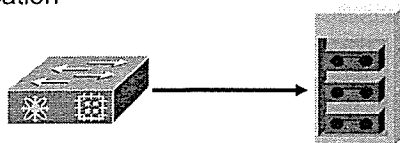
- Execute only from a defaulted fabric interconnect console interface
- Complete moment-in-time snapshot of entire Cisco Unified Computing System
- FULL state for all components

The primary difference between an import operation and a disaster-recovery restore is the scope of the backup. Configuration backups lack the state information that is required to re-establish server profile-to-blade server relationships.

Backup and Import Jobs

Backup and Import Jobs

- Managed as objects within the Cisco Unified Computing System database
- Transfer to remote file system via FTP, TFTP, SCP, and SFTP
- Contains information about backup parameters
 - Backup type
 - Transfer protocol
 - Destination host
 - Destination path
 - Authentication

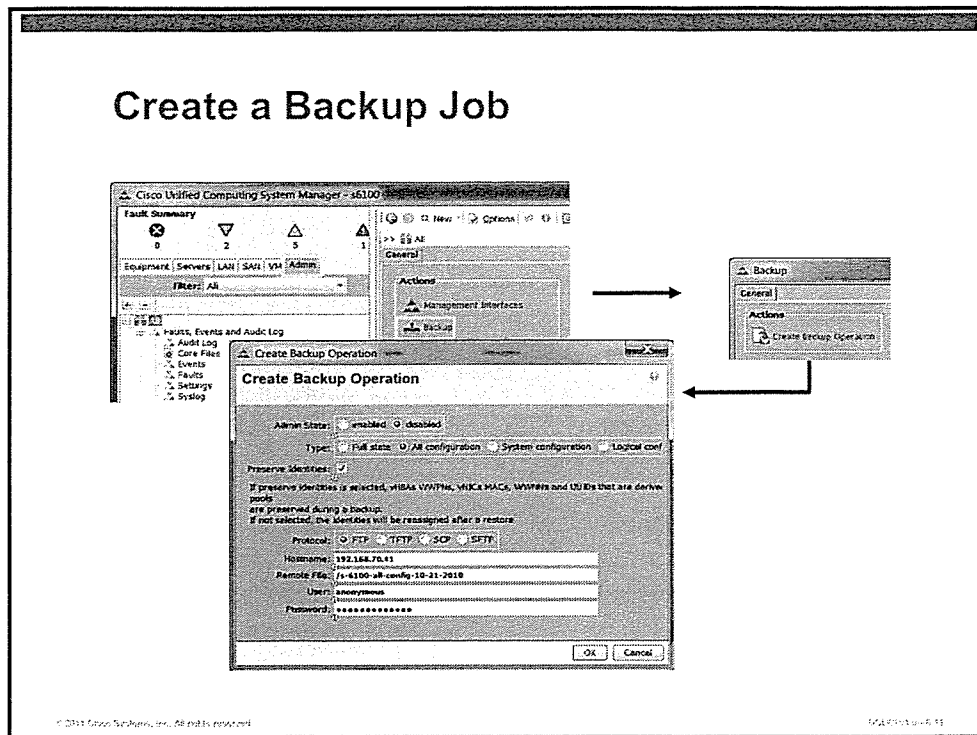


Cisco Unified Computing System processes backup and import operations as managed objects within the Cisco UCS Manager database. No backup data is stored within the database. Only the information that relates to the storage and transfer of the backup is stored in the database.

Configuring a Backup Job

This topic discusses how to configure a backup job.

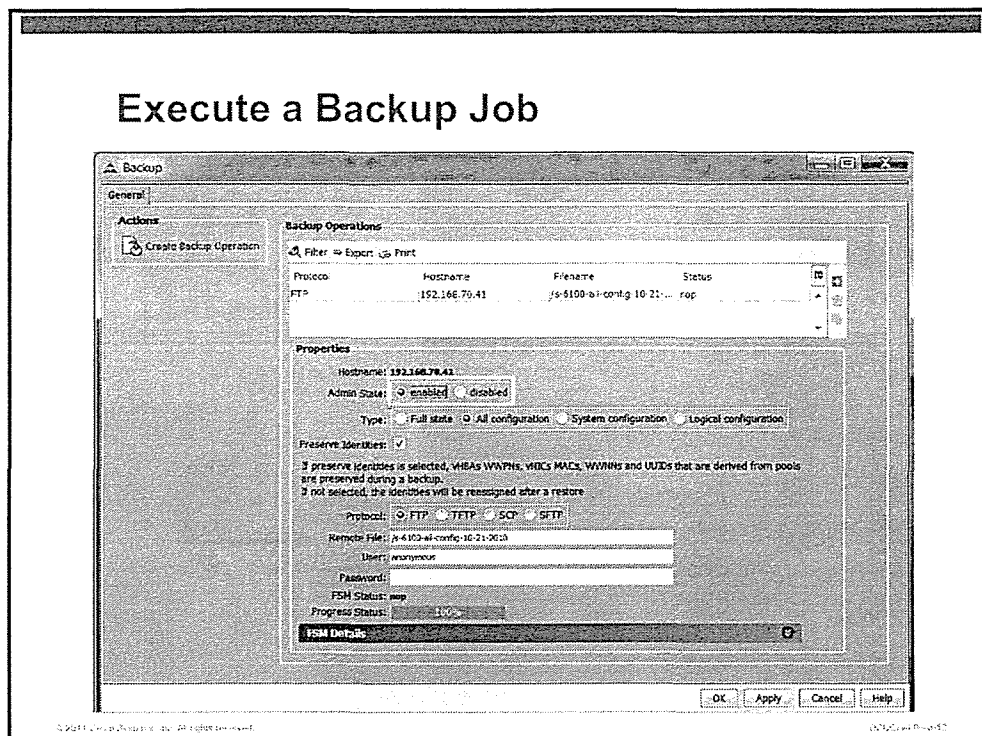
Create a Backup Job



Currently, only one backup configuration can be created per backup server. Backups are identified in Cisco UCS Manager by using the hostname or IP address of the backup server in the configuration.

Click the **Admin** tab in the navigation pane, and choose the **All** object. Click the **Backup** link in the actions pane, and then click **Create Backup Operation** in the window.

Execute a Backup Job



Provide the proper configuration and connectivity values for the backup job. A backup job that is created in the administrative state of “enabled” will run immediately. After the backup job is completed, it changes to a “disabled” state. If the job is created as “disabled”, then it does not run until it is enabled.

After you create the managed object that represents the backup operation, the administrative state of the backup becomes “enabled”. In the background, the state or configuration (or both) are collected and transferred to the backup server, by using the protocol that you choose. You can follow the workflow of the backup by examining the FSM that is associated with the backup. When the backup is complete, its administrative state changes to “disabled”.

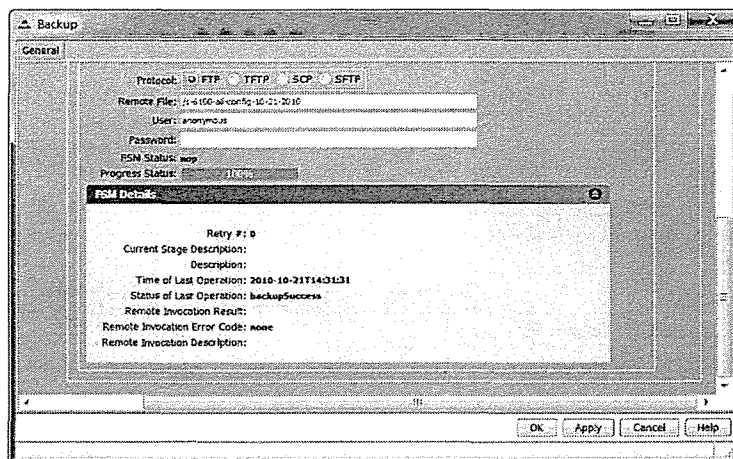
Verifying Backup Creation and Execution

This topic discusses how to verify that the backup has been created and executed.

Verify Backup Job in Cisco UCS Manager

Verify Backup Job in Cisco UCS Manager

- Return code from backup job displayed in the FSM Details window.

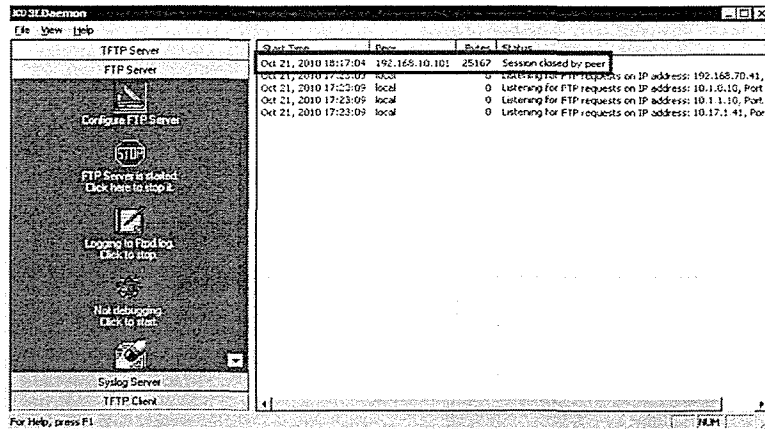


After you enable the backup job, click the double down-arrow icon to the upper-right corner of FSM Details to open the FSM Details window. The return code should read “backupSuccess”. If any other return code appears, edit the backup job. Be certain that the IP address of the remote file system and authentication credentials are correct.

Verify Backup Job on Remote FTP Server

Verify Backup Job on Remote FTP Server

- Verify that the file was received correctly on the remote server.



3CDaemon™ 3Com, Inc.

You can also verify that the backup operation was successful by monitoring the remote file system. Configuration backups are stored in cleartext and can be opened in any text editor.

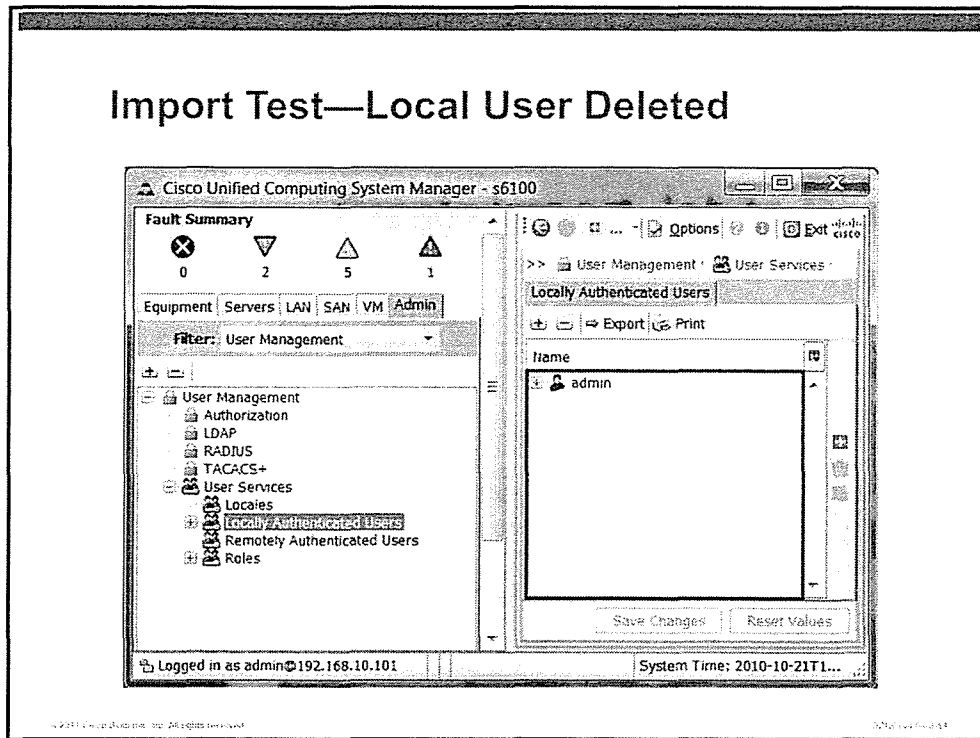
This topic discusses creating and running an import job to restore the AAA database.

Import Test—Delete a Local User

The screenshot displays the Cisco Unified Computing System Manager (s6100) interface. The left sidebar shows a navigation tree with categories like Equipment, Servers, LAN, SAN, VM, and Admin. Under the Admin category, the 'User Management' section is expanded, showing sub-items: Authentication, LDAP, RADIUS, TACACS+, User Services, Locales, **Locally Authenticated Users** (highlighted), and Remotely Authenticated Users. The main pane shows the 'Locally Authenticated Users' list with two entries: 'admin' and 'jmolton'. A 'Delete' dialog box is open, asking 'Are you sure you want to delete jmolton?' with 'Yes' and 'No' buttons. The status bar at the bottom indicates 'Logged in as admin@192.168.10.101' and 'System Time: 2010-10-21T1...'.

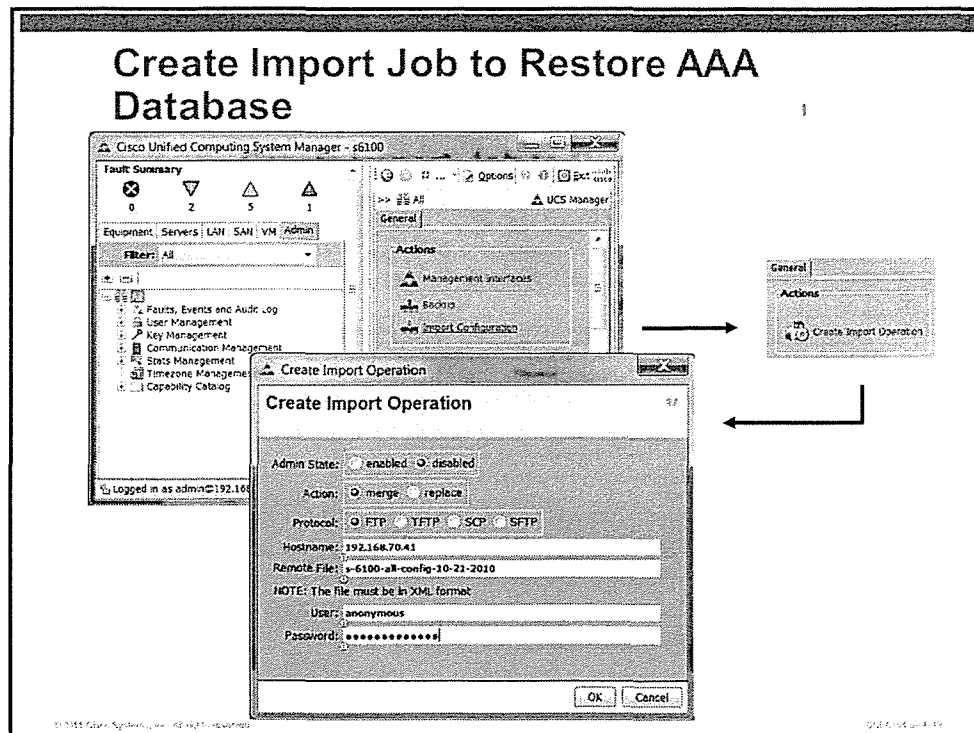
© 2011 Cisco Systems, Inc.

Import Test—Local User Deleted



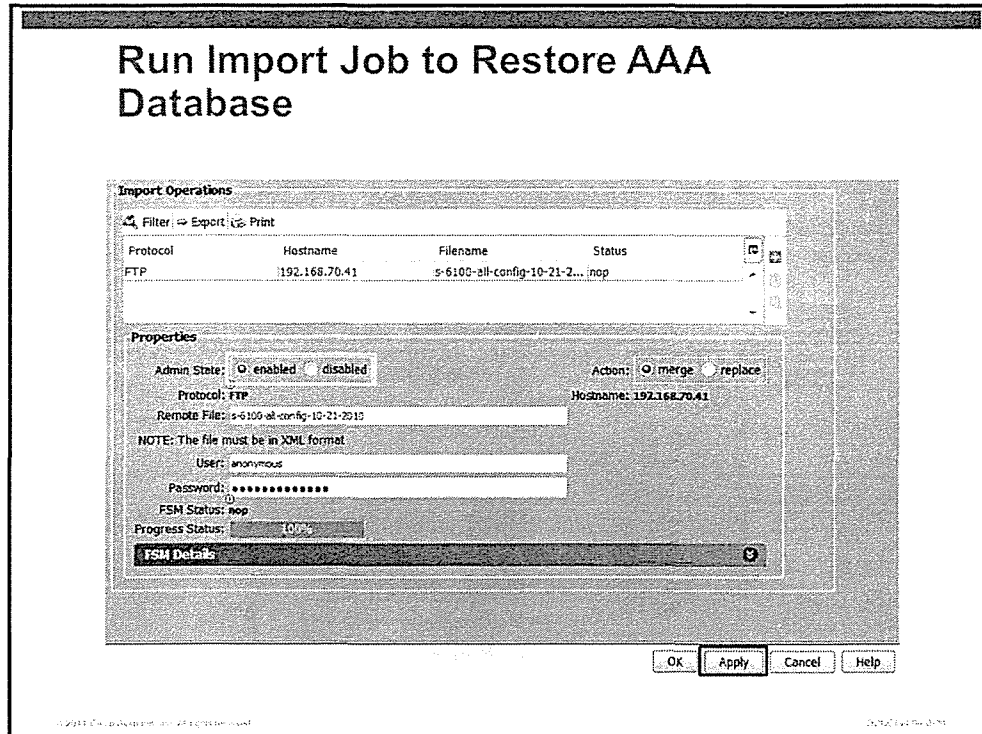
The user jmoulton has been deleted successfully.

Create Import Job to Restore AAA Database



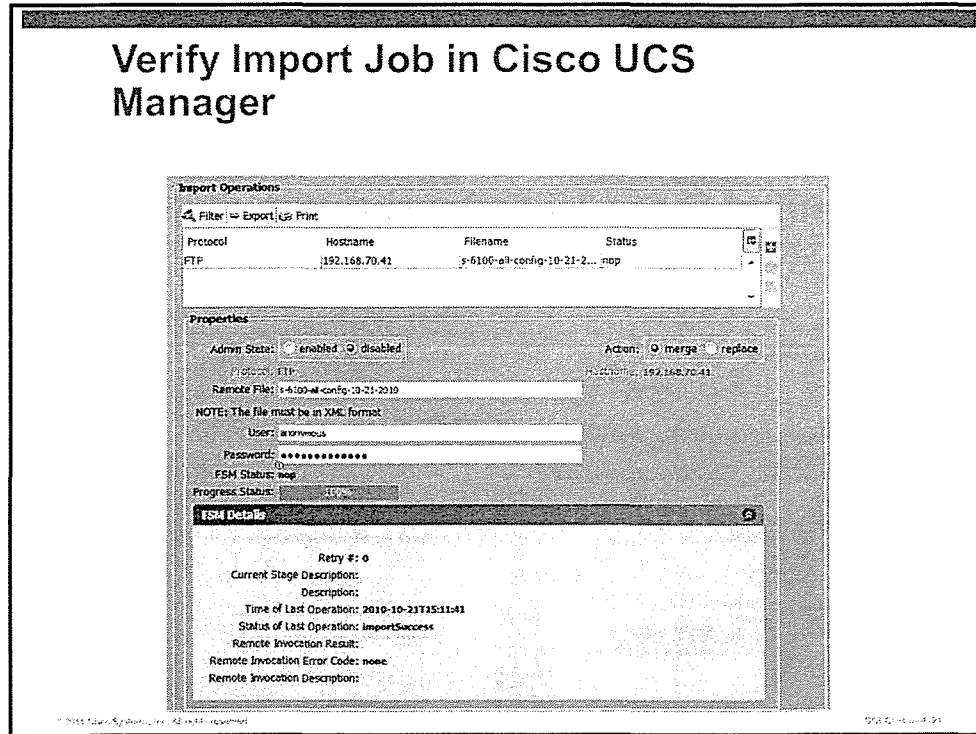
Click the **Admin** tab in the navigation pane and choose the **All** object. Click the **Import Configuration** link in the action pane, and then click **Create Import Operation** in the window. Enter the IP address or name of the remote file system, the name of the backup file, and the authentication credentials to import the file.

Run Import Job to Restore AAA Database



To enable the job, choose the **Enabled** radio button and click **Apply**.

Verify Import Job in Cisco UCS Manager

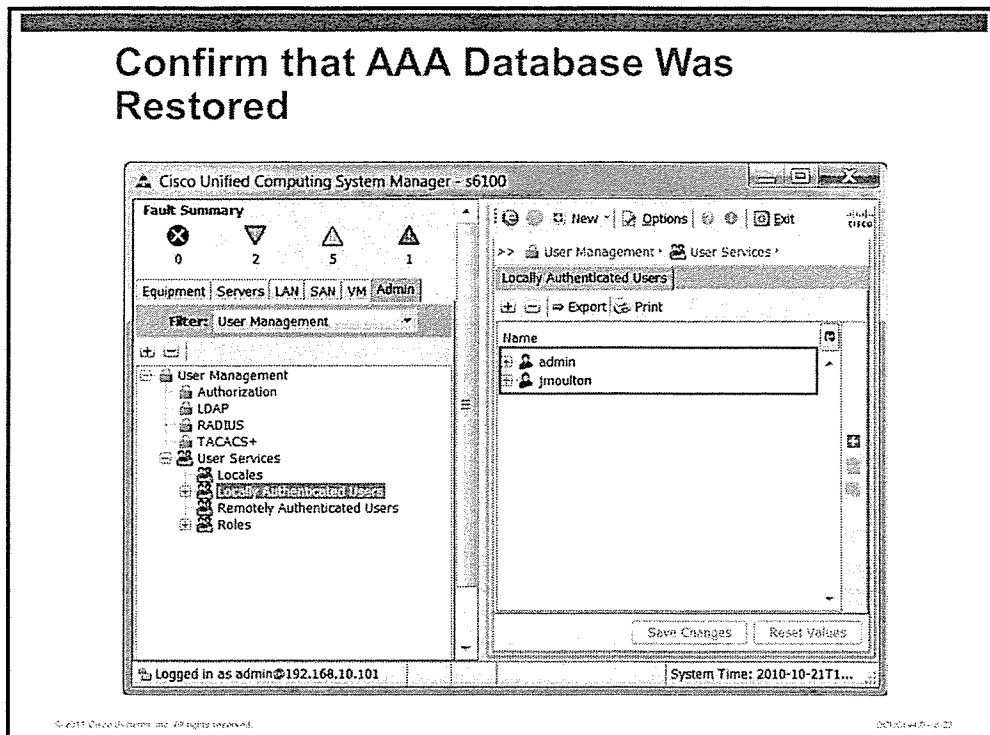


After you enable the import job, click the double down-arrow icon at the upper-right corner of FSM Details to open the FSM Details window. The return code should read “importSuccess”. If any other return code appears, edit the backup job. Be certain that the IP address of the remote file system and authentication credentials are correct.

Verifying Restoration of the AAA User Database

This topic discusses how to verify that the import operation was successful.

Confirm that AAA Database Was Restored



Select the **Admin** tab in the navigation window and select the **User Management** filter from the drop-down list. Expand **User Services** and choose **Locally Authenticated Users**. User jmolton was restored in the import operation.

Configuring the Backup Job to Preserve Abstracted Identities

This topic discusses how to preserve abstracted identities.

Preserve Abstracted Identities

Preserve Abstracted Identities

- The Preserve Identities option maintains MAC addresses, UUIDs, and WWNNs.

The screenshot shows the 'Create Backup Operation' dialog box. The 'Admin State' is set to 'disabled'. The 'Type' is set to 'Full state'. The 'Preserve Identities' checkbox is checked. Below this, a note states: 'If preserve identities is selected, vHBAs WWPNs, vNICs MACs, WWNNs and UUIDs that are derived from pools are preserved during a backup. If not selected, the identities will be reassigned after a restore.' The 'Protocol' is set to 'FTP'. The 'Hostname' is '192.168.70.41'. The 'Remote File' is 'fs-6100-all-config-10-21-2010'. The 'User' is 'anonymous'. The 'Password' is masked with dots. 'OK' and 'Cancel' buttons are at the bottom right.

Beginning with Cisco UCS Manager Version 1.2, a backup job to preserve Universally Unique Identifiers (UUIDs), MAC addresses, and world wide network nodes (WWNN) and world wide port names (WWPNs) is derived from pools in service profiles. Previously, any address that was drawn from an identity pool was discarded when the service profile was imported.

Configuring the Cisco UCS 6100 Series Fabric Interconnect for Disaster-Recovery Restore

This topic discusses how to perform a disaster-recovery restoration operation.

Importing FULL State Backup

Importing FULL State Backup

```
s6100-A# erase configuration
Configuration will be erased. Are you sure? (yes/no): yes
Removing all the configuration. Please wait....
Configurations are cleaned up.
Rebooting....
...
---- Basic System Configuration Dialog ----
...
Enter the setup mode; setup newly or restore from backup. (setup/restore) ?
restore
...
Continue to restore this Fabric interconnect from a backup file (yes/no) ?
yes

Physical Switch Mgmt0 IPv4 address : 192.168.10.101
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 192.168.10.254
```

A fabric interconnect that contains any configuration data must be initialized to factory defaults before a disaster-recovery operation begins. This process can be performed only from a connection to the serial console or to a terminal server that is connected to the serial console.

Connect to the local management shell and issue the **erase configuration** command. The fabric interconnect must be rebooted. This process is similar to issuing the **write erase** and **reload** commands in Cisco IOS Software.

The setup wizard queries the user as to whether this operation is an initial setup or restore. Because a restore operation was indicated, the fabric interconnect needs an IP address to make a connection to the remote file system.

Importing Full-State Backup (Cont.)

- After retrieving and applying the backup, the system is ready for use.

```
Enter the protocol to get backup file (scp/ftp/tftp/sftp) ? ftp
Enter the IP address of backup server: 10.100.100.30
Enter fully qualified backup file name: /backups/ucs-fullbackup.tgz
Enter user ID: adminuser
Enter password: *****
Retrieved backup configuration file.
Configuration file - Ok
```

```
Cisco UCS 6100 Series Fabric Interconnect
s6100-A login:
```

Enter the transfer protocol, IP address of the remote file system, the FULL state backup file, and authentication credentials. When the file transfer and restore operation is complete, a login prompt appears.

Summary

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

Summary

- Four types of backups are available in Cisco UCS Manager.
- Only a FULL state backup has the information needed to restore a cluster of fabric interconnects.
- Backup jobs are created and executed in Cisco UCS Manager.
- Validate backup jobs by using FSM output and verify that the file exists on a remote file system.
- There is only one type of import job, and it can be used to restore the AAA database, service profiles, policies, and thresholds.
- To verify that the AAA database was restored, select the Admin tab in the navigation pane and select local users.
- Selecting the Preserve Identities checkbox in the Backup Creation dialog box maintains identities assigned by a pool in the backup.
- Performing a disaster-recovery restore requires access to the fabric interconnect serial console or terminal server connection.

© 2011 Cisco Systems, Inc. All rights reserved.

2011-10-10 14:25

Managing High Availability

Overview

When two Cisco Unified Computing System (UCS) 6100 Series Fabric Interconnects are configured in a cluster, both data planes forward actively. The management plane forms an active subordinate-to-peer relationship. Both peers are connected by a private network. Understanding the cluster recovery process that occurs during node isolation is important.

Objectives

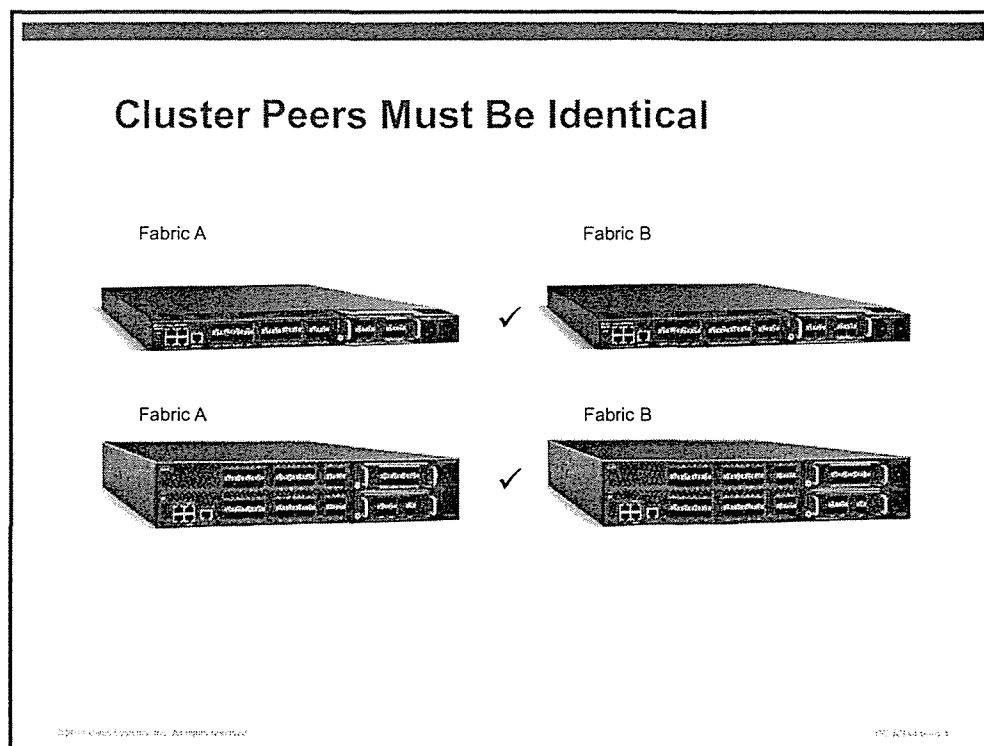
Upon completing this lesson, you will be able to articulate cluster requirements, management, and monitoring. This ability includes being able to meet these objectives:

- Describe high-availability cluster connection requirements for Cisco UCS B-Series Blade Servers
- Describe intercluster communications and Cisco UCS Manager database synchronization
- Describe how the Cisco UCS 5108 chassis serial EEPROM resolves split-brain issues in the high-availability cluster
- Differentiate between cluster partition in space and partition in time conditions
- Modify cluster IP addressing

High-Availability Cluster Connection Requirements for Cisco UCS B-Series Blade Servers

This topic discusses the requirements for high-availability clusters.

Cluster Peers Must Be Identical

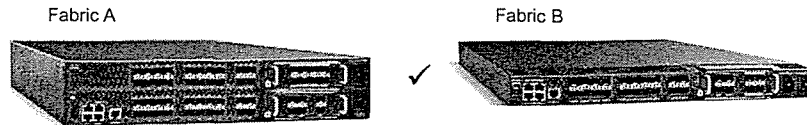


Cisco UCS Fabric Interconnect peers in a cluster must run the same version of Cisco UCS Manager and must peer with the same model. A Cisco UCS 6120 Fabric Interconnect cannot peer a Cisco UCS 6140 Fabric Interconnect.

Cluster Peers Can Be Different to Upgrade Cluster

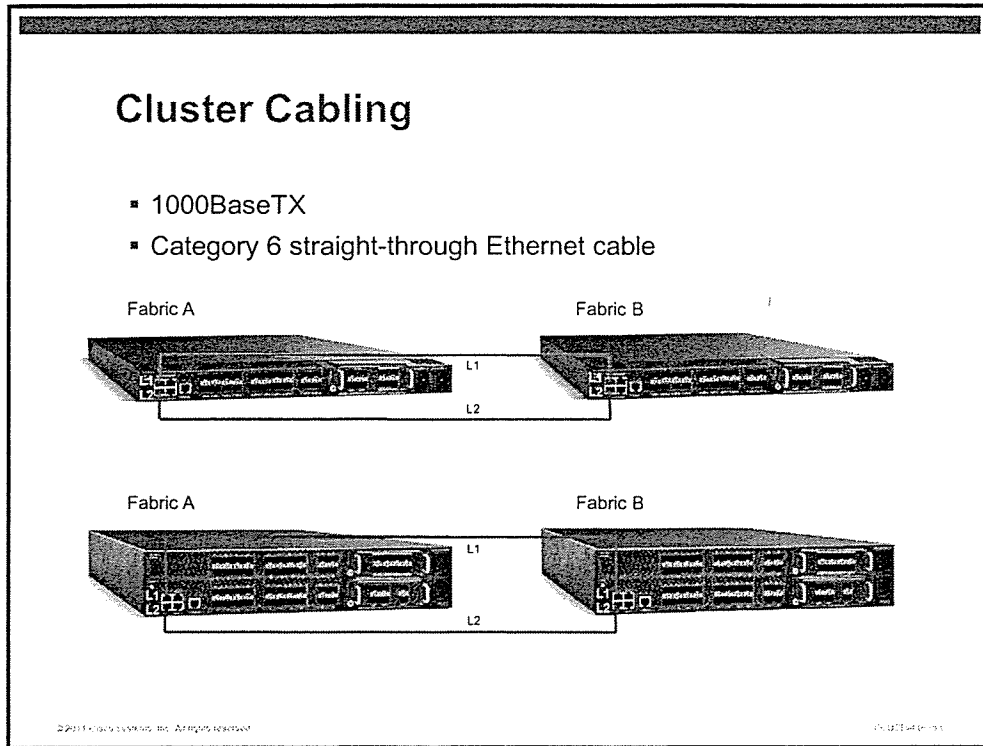
Cluster Peers Can Be Different to Upgrade Cluster

- A Cisco UCS 6120 interconnect can be paired with a Cisco UCS 6140 Fabric Interconnect to facilitate upgrading the cluster from 20 ports to 40 ports.



Cisco offers customers a simple migration path from Cisco UCS clusters, based on the 20-port fabric interconnects to the 40-port Cisco UCS 6140 Fabric Interconnect. An unconfigured Cisco UCS 6140 interconnect is connected to the active member of the Cisco UCS 6120 cluster. When Cisco UCS Manager has synchronized the database with the Cisco UCS 6140 interconnect, the Cisco UCS 6120 interconnect is removed from the cluster. When the Cisco UCS 6140 interconnect becomes the active cluster peer, the secondary Cisco UCS 6140 interconnect is introduced to the cluster and synchronizes with the active peer.

Cluster Cabling



The private cluster interconnect network runs at 1 Gb/s. EIA/TIA Category 6 cabling is required to support reliable communications at complete bandwidth.

The interfaces (L1 and L2) in this figure provide a cluster link between two Cisco UCS 6100 Series Fabric Interconnects. The interfaces carry the cluster heartbeat messages between the two fabric interconnects, as well as carrying high-level messages between Cisco UCS Manager elements. 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). The IP addresses on these links are fixed.

Intercluster Communications and Cisco UCS Manager Database Synchronization

This topic discusses intercluster communications.

Process Management

Process Management

- Cisco UCS Manager controller
 - Distributed application
 - Separate process running on Cisco NX-OS
 - Defines running mode of Cisco UCS Manager processes
- Cisco NX-OS
 - Starts all Cisco UCS Manager processes
 - Monitors and restarts Cisco UCS Manager processes

The Cisco UCS Manager controller is a distributed application that runs on both the primary and subordinate Cisco UCS Manager instance. Each instance is represented by a unique ID (the same as the node ID). The Cisco UCS Manager controller is implemented as a distinct process; the address-space separation guarantees a higher degree of fault isolation. This separation also allows the controller to distinguish between a failure of other system processes and a failure of the controller itself. The Cisco UCS Manager controller decides which Cisco UCS Manager components should run in primary or subordinate mode.

Local and Chassis Data

Local and Chassis Data

- Local storage
 - NVRAM and flash stores static data
 - Read and written by local Cisco UCS Manager instance
 - Replicated when both nodes are up
- Chassis EEPROM
 - Serial EEPROM stores cluster state data
 - Read and written by both chassis management controllers
 - No need to replicate data
 - Used to assist the Cisco UCS Manager in determining state of cluster

© 2011 Cisco Systems, Inc. All rights reserved.

UCS 440-000-000

Local Storage

Each Cisco UCS fabric interconnect maintains its own local storage in NVRAM and flash memory. Local storage contains static data; that is, storage that does not change with cluster membership changes. For example, installable images are stored in the /bootflash partition of internal flash memory. Data such as installable images are replicated at runtime, while both cluster members are present in the cluster. You do not need to (nor can you) download images via the Cisco UCS Manager interface to individual nodes. The download is replicated to both nodes. If a node is not present during an image download, then that image is replicated to that node when the node rejoins the cluster.

Chassis EEPROM

Each chassis management controller maintains its own part of the shared chassis storage in the serial EEPROM. Chassis storage contains a combination of static and dynamic information. For example, the static portion contains the node ID for each node that is configured in the cluster. The dynamic portion contains the version of the configuration as seen by that node. There is no need to replicate the contents of the serial EEPROM. Each node maintains its own portion, whereas both nodes may read from both topics.

Primary Cluster Node Election

Primary Cluster Node Election

- Agreement
- Stability
- Infrequent elections
- Stability under quick restart

© 2011 Cisco Systems, Inc. All rights reserved. EDUCATION-ENR

Agreement

A Cisco UCS Manager instance declares a new leader when these conditions apply:

- The instance has received acknowledgments that its election request has been processed.
- The instance has checked the election counter in the incoming messages, to ensure that the messages all relate to the same election request.
- All processes propose the same new leader.

Stability

The leadership should change only in one of these cases:

- An administrative change in the configuration requires the leader to be moved.
- The leader process fails.

Infrequent Elections

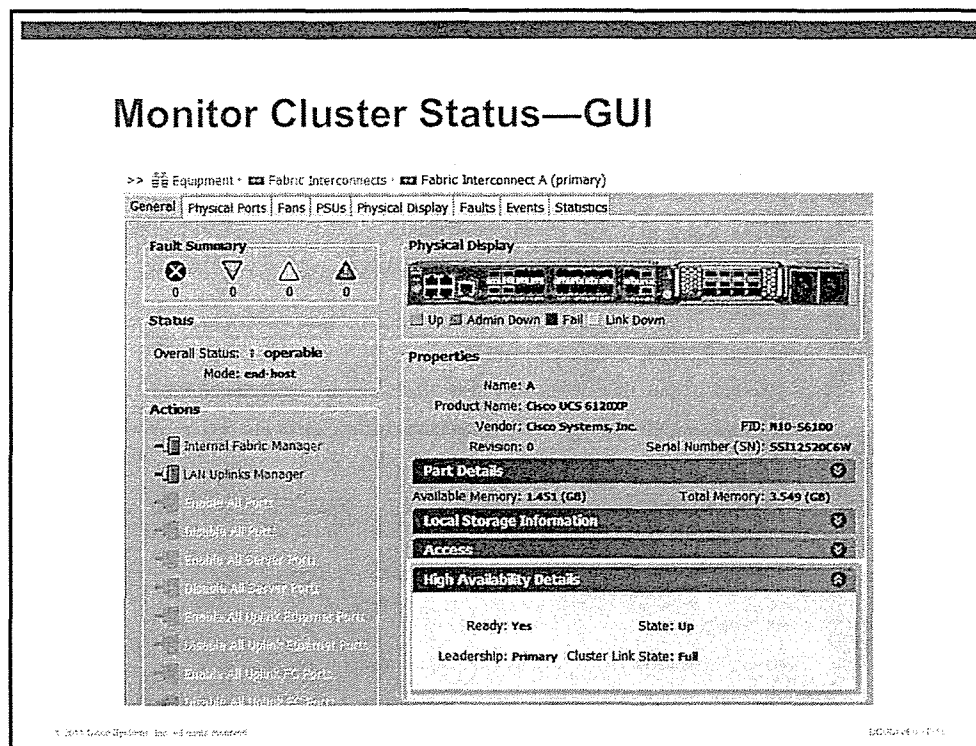
Elections are caused only by these events:

- Administrative configuration change
- New process joining the group
- Process exiting the group
- Process failure

Stability Under Quick Restart

Cisco UCS Manager will allow a leader process to fail, restart, and still join the group as the leader. This allowance prevents a change of leadership when a process (or a node) is the subject of a quick restart. The rationale is that a change of leadership, and therefore a switchover, can be more expensive than waiting for the leader process (or node) to reinitialize.

Monitor Cluster Status—GUI



Choose the fabric interconnect from the Equipment tab of the navigation pane. In the content pane, click the double down-arrow icon to the right of High Availability Details. This figure indicates that fabric interconnect A is the active management node in the cluster and that links L1 and L2 are both operational.

Monitor Cluster Status—CLI

Monitor Cluster Status—CLI

Node Status

```
s6100-A# show cluster extended-state
```

Cisco UCS Manager Status

```
Cluster Id: 0x76cf5fla431711df-0xb1f8000decb21744
```

L1/L2 Status

```
Start time: Fri Oct 1 07:29:04 2010
```

Serial EEPROM Chassis

```
Last election time: Fri Oct 1 07:30:12 2010
```

```
A: UP, PRIMARY
```

```
B: UP, SUBORDINATE
```

```
A: memb state UP, lead state PRIMARY, mgmt services state: UP
```

```
B: memb state UP, lead state SUBORDINATE, mgmt services state: UP
```

```
heartbeat state PRIMARY_OK
```

```
INTERNAL NETWORK INTERFACES:
```

```
eth1, UP
```

```
eth2, UP
```

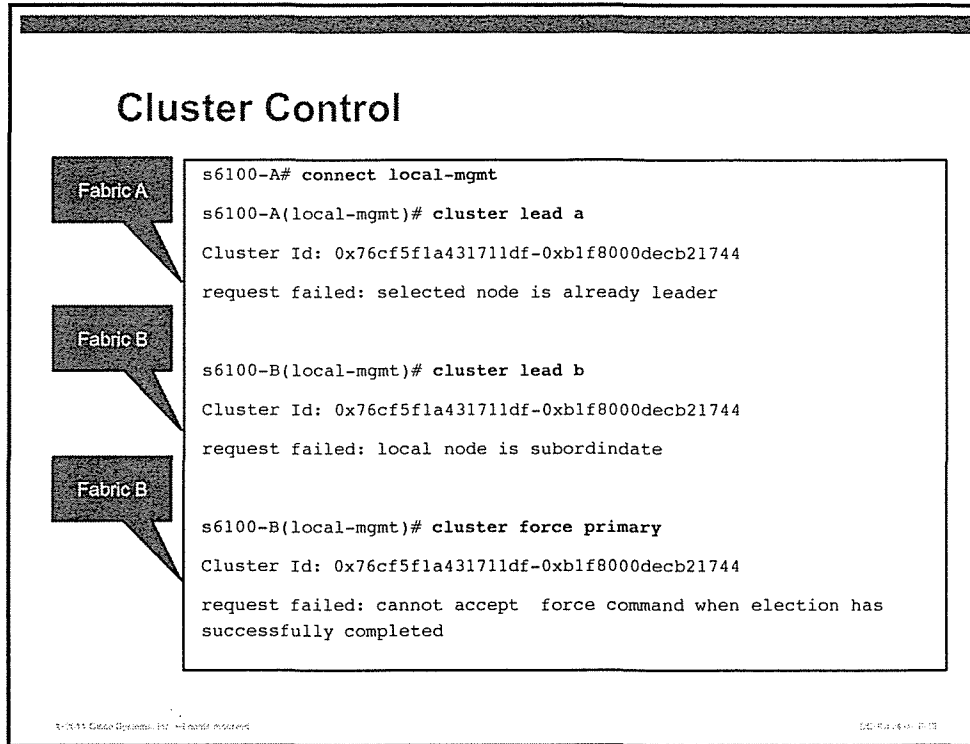
```
HA READY
```

```
Detailed state of the chassis selected for HA storage:
```

```
Chassis, serial: FOX1307H0M8, state: active
```

The **show cluster extended-state** command provides detailed information about cluster operation. The figure indicates the cluster state of both peers, the private network (L1 and L2), and which chassis serial EEPROM is used to resolve split-brain conditions. The ID of the chassis that is used to resolve split-brain conditions can be determined only by using the command-line interface (CLI).

Cluster Control



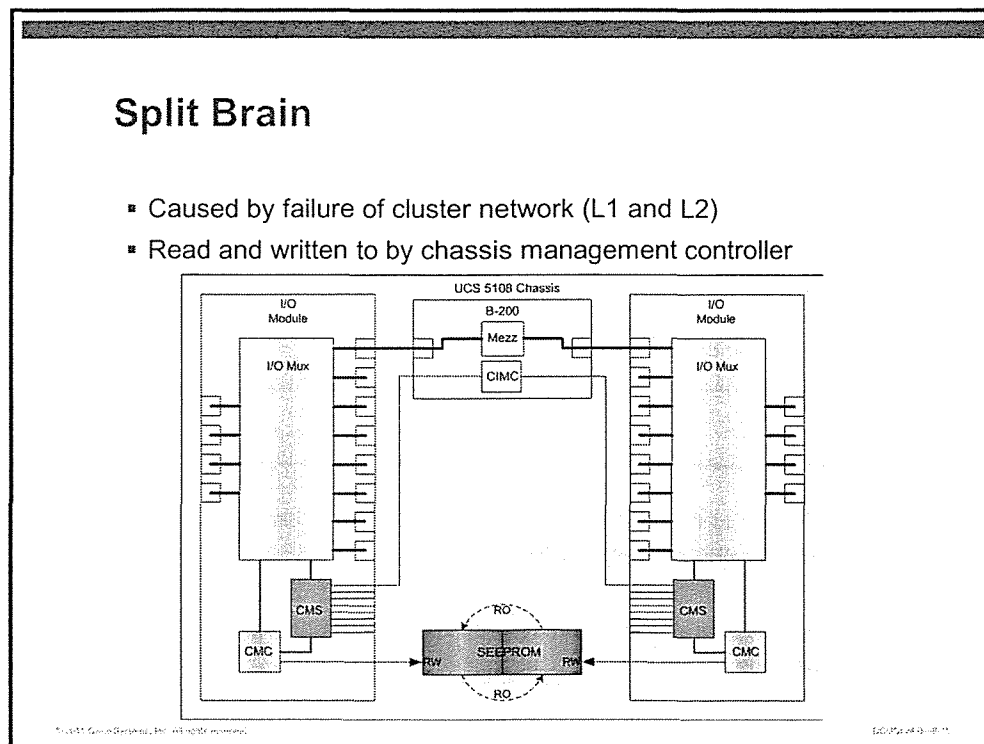
The **cluster lead** and **cluster force primary** commands can be used to change which fabric interconnect is the active management plane.

Note As the figure shows, when the election process has finished, neither command causes a switchover.

How the Cisco UCS 5108 Chassis Serial EEPROM Resolves Split-Brain Issues in the High-Availability Cluster

This topic discusses how the Cisco UCS 5108 chassis serial EEPROM resolves split-brain issues in the high-availability cluster.

Split Brain



A split-brain condition occurs in a cluster when the private network that is responsible for cluster synchronization is unavailable. In Cisco Unified Computing System, a serial EEPROM on the Cisco UCS 5108 server chassis midplane is used to resolve split-brain conditions.

The serial EEPROM is divided into two sections: one for fabric A and one for fabric B. The chassis management controller on fabric A has read/write access to the fabric A portion of the serial EEPROM and read-only access to the section that is under the control of fabric B.

Cluster Partition in Space and Partition in Time Conditions

This topic describes the two split-brain conditions that can occur in the cluster.

Partition in Space

Partition in Space

- A partition in space occurs when the private network fails (no path from L1 to L1 and L2 to L2).
- There is a risk of active-active management node.
- Both nodes are demoted to subordinate and a quorum race begins.
- The node that claims the most resources wins.

A partition in space occurs when nodes fail to communicate with each other over the private network (Layer 1 and Layer 2 links both fail). To resolve this split brain (assuming that both switches are active at the time of the private network failure), each chassis management controller acts on the behalf of the fabric Cisco UCS Manager instance, to reach the serial EEPROM first and write its node ID in the primary field. This process is known as a quorum race. The winner remains in the cluster, and the loser aborts. When the links are restored, the losing node can rejoin the cluster and act as subordinate.

Partition in Time

Partition in Time

- A partition in time occurs when a node boots alone in the cluster.
- The node compares its database version against the serial EEPROM and discovers that its version number is lower than the current database version.
- There is a risk of applying an old configuration to Cisco Unified Computing System components.
- This node will not become the active management node.

© 2011 Cisco Systems, Inc. All rights reserved.

UCS 4.0 User Guide

A partition in time occurs when one of the nodes is down for a time, during which changes to the configuration are made on the active primary node. These changes do not replicate to the down node.

If the primary node shuts down after having made configuration changes to the database, but before being able to replicate them to the other (downed) node, and that downed node tries to join the cluster alone, then that condition is referred to as a partition in time.

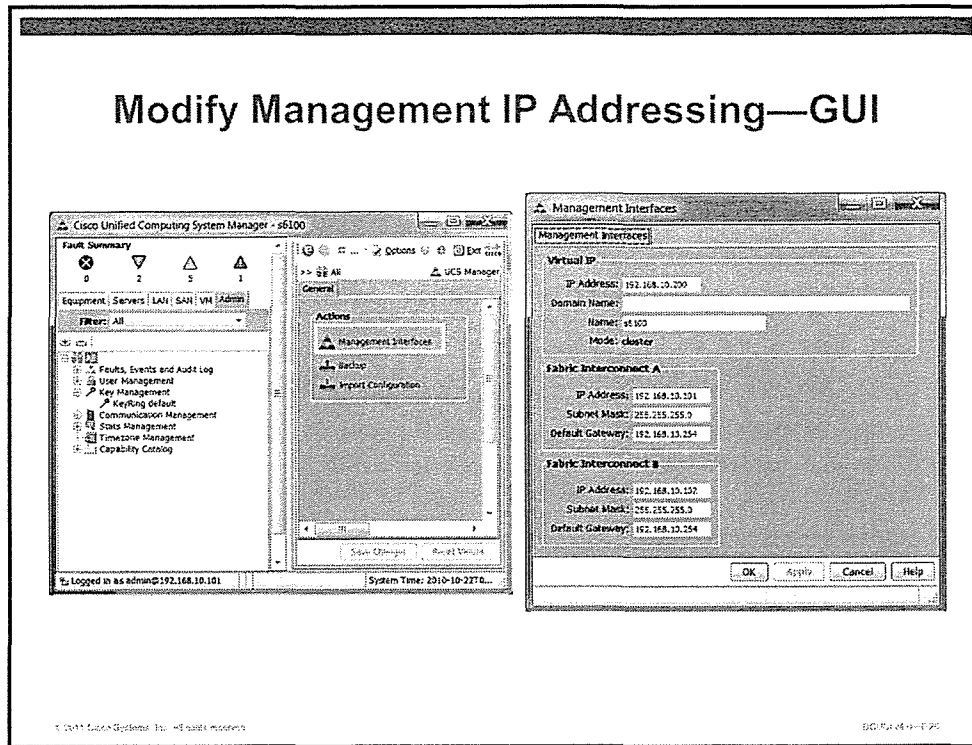
To resolve this split brain, a version number that represents the configuration is written to the EEPROM. On solo startup, a node compares its version number to that of the other node. (Both nodes can read both parts of the EEPROM.) If the version number of the first node is the same or higher than that of the other node, then the first node can start the cluster. If the version number is lower than that of the other node, then the first node does not become the active management node. This process protects against using an old version of the Cisco UCS Manager database.

Note	To force the fabric interconnect to become the active management node, use the cluster force primary command.
-------------	--

Modifying Cluster IP Addressing

This topic discusses how to modify cluster IP addressing from the GUI and CLI.

Modify Management IP Addressing—GUI



To change the IP address of either fabric interconnect, or to change the virtual IP address that is used to access the active management node, select the Admin tab in the navigation pane. In the content pane, click the Management Interfaces link.

Modify Management IP Addressing—CLI

Modify Management IP Addressing—CLI

```
s-6100-A# scope system
s-6100-A /system # set virtual-ip ?
    A.B.C.D   System IP Address

s-6100-A # scope fabric-interconnect a
s-6100-A /fabric-interconnect # set out-of-band ?
    gw        Gw
    ip         Ip
    netmask    Netmask
```

The management IP addresses can also be changed from the CLI.

Summary

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

Summary

- The high-availability cluster requires an active gigabit link between L1 and L1 or to L2 and L2.
- The active management node synchronizes configuration and firmware images to the subordinate node.
- Data stored in the Cisco UCS 5108 chassis serial EEPROM resolves split-brain issues in the fabric interconnect cluster.
- Partition in space and partition in time conditions are two types of split-brain issues.
- Cluster IP addressing can be modified in the Cisco UCS Manager GUI or CLI.

© 2011 Cisco Systems, Inc. All rights reserved.

UCSR1143-0.22

Monitoring System Events

Overview

When a Cisco Unified Computing System implementation is underway and in production operation, detailed knowledge of the logging and monitoring facilities of Cisco Unified Computing System Manager (UCS Manager) can greatly speed configuration and troubleshooting. The Cisco Smart Call Home feature can send predictive failure messages to the Cisco Technical Assistance Center (TAC) so that replacement parts can be shipped before they actually fail.

Objectives

Upon completing this lesson, you will be able to configure console, monitor, and file logging as well as syslog and Smart Call Home. This ability includes being able to meet these objectives:

- Describe the fault management system and evaluate fault severity levels
- Use the audit log to track administrative changes to the Cisco UCS Manager database
- Differentiate areas of operation that are subject to FSM validation and learn how to interpret the FSM output
- Differentiate the configuration and validation of logging options, including local buffer, console, and external syslog servers
- Configure the Smart Call Home feature
- Validate the Smart Call Home feature
- Configure settings for logs, events, and faults

Fault Management System and Fault Severity Levels

This topic discusses the fault management system and fault severity.

Global Fault Summary

Global Fault Summary

- The global fault summary is displayed above the configuration tabs in the navigation pane of Cisco UCS Manager.
- From left to right, the color images represent:
 - Critical
 - Major
 - Minor
 - Warning

Fault Summary

0 2 4 1

Equipment Servers LAN SAN VM Admin

Filter: All

Equipment

- Chassis 1
 - Fans
 - IO Modules
 - IO Module 1
 - IO Module 2
 - PSUs
 - Servers
 - Fabric Interconnects
 - Fabric Interconnect A (primary)
 - Fabric Interconnect B (subordinate)

The global fault summary lists faults, according to severity, across all elements of the Cisco Unified Computing System. 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.

Fault Severity

Fault Severity	
Severity Level	Description
Critical	A service-affecting condition that requires immediate corrective action. This severity might indicate that the managed object is out of service and its capability must be restored.
Major	A service-affecting condition that requires urgent corrective action. This severity might indicate a severe degradation in the capability of the managed object and that its full capability must be restored.
Minor	A non-service-affecting fault condition that requires corrective action to prevent a more serious fault from occurring. This severity might indicate that the detected alarm condition is not currently degrading the capacity of the managed object.
Warning	A potential or impending service-affecting fault that currently has no significant effects in the system. Action should be taken to further diagnose, if necessary, and correct the problem to prevent it from becoming a more serious service-affecting fault.
Condition	An informational message about a condition, possibly independently insignificant.
Info	A basic notification or informational message, possibly independently insignificant.

In addition to the four severity levels that are listed in the global Fault Summary window, there are two additional severity levels: info and condition. Although these levels are not displayed in the global Fault Summary window, they do appear in the global fault log. To find the levels, on the Admin tab expand **Faults, Events and Audit Log** and then choose **Faults**.

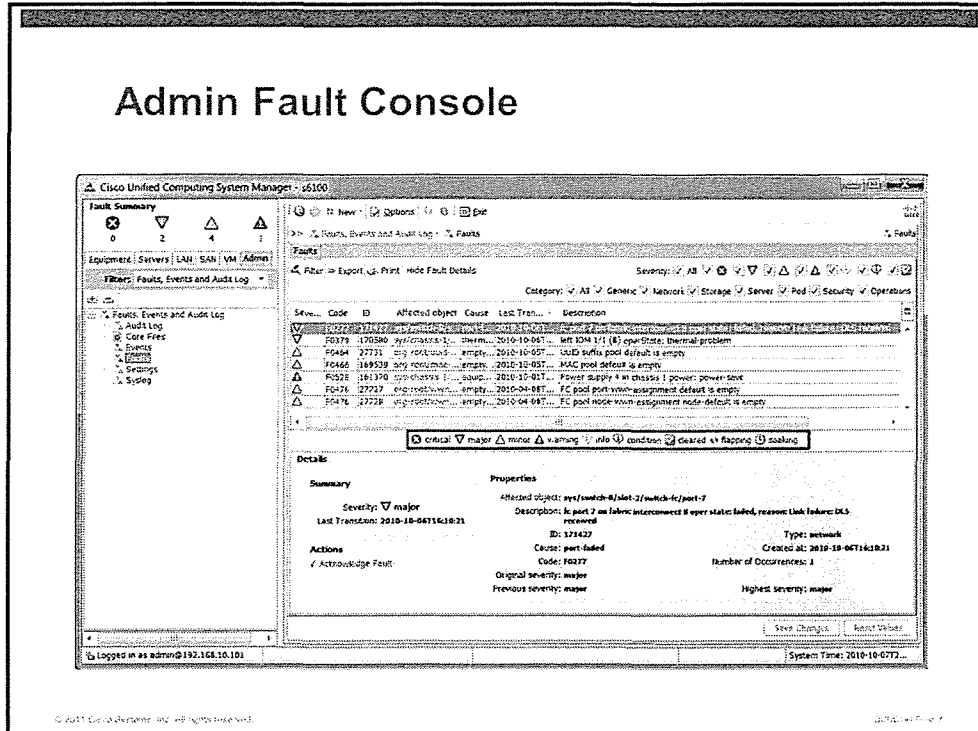
Fault States

Fault States	
Severity Level	Description
Active	A fault was raised and is currently active.
Cleared	A fault was raised but did not reoccur during the flapping interval. The condition that caused the fault has been resolved, and the fault has been cleared.
Flapping	A fault was raised, cleared, and then raised again within a short time interval, known as the flap interval.
Soaking	A fault was raised and then cleared within a short time interval, known as the flap interval. Because this might be a flapping condition, the fault severity remains at its original active value, but this state indicates that the condition that raised the fault has cleared. If the fault does not reoccur, the fault moves into the cleared state. Otherwise, the fault moves into the flapping state.

There are four possible fault states in Cisco Unified Computing System.

- **Active:** Active faults in the Faults window are displayed along with one of the six severity icons in the Severity column of the fault.
- **Cleared:** Cleared faults display a green checkmark (Cleared icon) in the Severity column.
- **Flapping:** Faults in the flapping state display a circular arrow (Flapping icon) in the Severity column.
- **Soaking:** Faults in the soaking state display with a stopwatch (Soaking icon) in the Severity column.

Admin Fault Console



The example highlights the nine possible icons that can appear in the Severity column of the Faults console.

Fault in Soaking State

Fault in Soaking State

- An interface has transitioned between operational and non-operational within the 10-second flapping interval.

The screenshot displays the Cisco Faults, Events and Audit Log interface. The top navigation bar includes tabs for Faults, Events, Audit Logs, Syslog, Core Files, and Settings. Below the navigation bar, there are filters for Severity (All, Critical, Major, Minor, Warning, Info, Condition, Cleared, Flapping, Soaking) and Category (All, Generic, Network, Storage, Server, Pod, Security, Operations). The main table lists faults with columns for Severity, Code, Affected object, Cause, Last Tran..., and Description. A fault with Code F0277 is highlighted, showing a description: "fc port 1 on fabric interconnect A oper state: failed, reason: Link failure: OLS received". A callout box labeled "Soaking" points to the fault entry. The bottom of the interface shows a legend for fault states: critical, major, minor, warning, info, condition, cleared, flapping, and soaking.

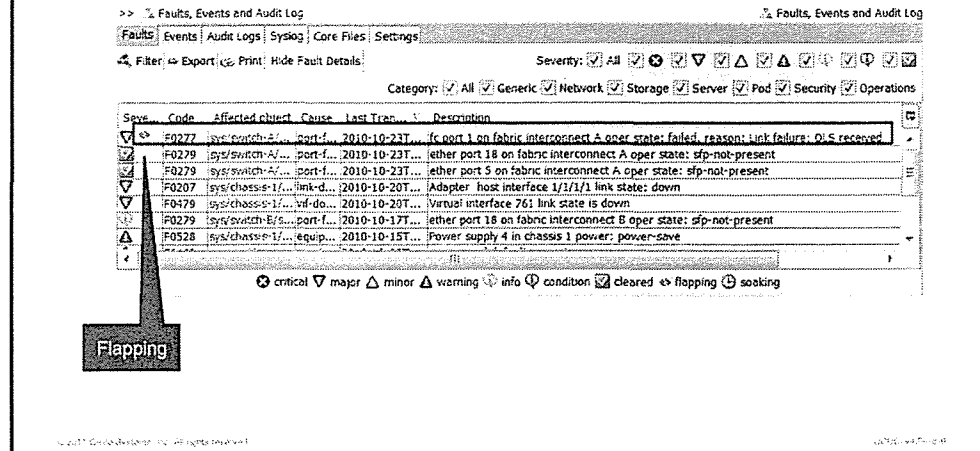
Sev...	Code	Affected object	Cause	Last Tran...	Description
Info	F0277	sys/switch-A/...	port-f...	2010-10-23T...	fc port 1 on fabric interconnect A oper state: failed, reason: Link failure: OLS received
Warning	F0279	sys/switch-A/...	port-f...	2010-10-23T...	ether port 18 on fabric interconnect A oper state: sfp-not-present
Warning	F0279	sys/switch-A/...	port-f...	2010-10-23T...	ether port 5 on fabric interconnect A oper state: sfp-not-present
Warning	F0207	sys/chassis-1/...	link-d...	2010-10-20T...	Adapter host interface 1/1/1 link state: down
Warning	F0479	sys/chassis-1/...	vf-do...	2010-10-20T...	Virtual interface 761 link state is down
Warning	F0279	sys/switch-B/s...	port-f...	2010-10-17T...	ether port 18 on fabric interconnect B oper state: sfp-not-present
Warning	F0528	sys/chassis-1/...	equip...	2010-10-15T...	Power supply 4 in chassis 1 power: power-save

A fault in the soaking state has transitioned from active to inactive at least once within the flapping window. A fault in the soaking state indicates that the flapping window is still open.

Fault in Flapping State

Fault in Flapping State

- An interface has transitioned between operational and non-operational for longer than the 10-second flapping interval.



A fault in the flapping state indicates that the fault was still raised after the flapping interval expired.

Admin Fault Console Detail

The screenshot displays the 'Admin Fault Console Detail' interface. At the top, there's a navigation bar with tabs for 'Faults', 'Events', 'Audit Logs', 'Syslog', 'Core Files', and 'Settings'. Below this is a filter section with 'Filter', 'Export', 'Print', and 'Hide Fault Details' options. A 'Severity' dropdown is set to 'All', and a 'Category' section includes checkboxes for 'All', 'Generic', 'Network', 'Storage', 'Server', 'Pod', 'Security', and 'Operations'. The main area contains a table of faults with columns for 'Sev...', 'Code', 'Affected object', 'Cause', 'Last Tran...', and 'Description'. The table lists several faults, including F0277, F0279, F0278, F0267, F0479, and F0528. Below the table, there's a legend for severity levels: critical (red square), major (orange triangle), minor (yellow triangle), warning (green triangle), info (blue circle), condition (purple circle), cleared (green circle), flapping (red circle), and soaking (blue circle). The 'Details' section on the left shows 'Summary' with 'Severity: cleared' and 'Last Transition: 2010-10-23T08:33:30', and 'Actions' with 'Acknowledge Fault'. The 'Properties' section on the right provides detailed information about the selected fault: 'Affected object: sys/switch-A/slot-1/switch-ether/port-18', 'Description: ether port 18 on fabric interconnect A oper state: sfp-not-present', 'ID: 184309', 'Type: network', 'Cause: port-failed', 'Created at: 2010-10-17T12:36:45', 'Code: F0279', 'Number of Occurrences: 1', 'Original severity: info', 'Previous severity: info', and 'Highest severity: info'.

Sev...	Code	Affected object	Cause	Last Tran...	Description
	F0277	sys/switch-A/...	port-f...	2010-10-23T...	fc port 1 on fabric interconnect A oper state: failed, reason: link failure: OLS received
	F0279	sys/switch-A/...	port-f...	2010-10-23T...	ether port 18 on fabric interconnect A oper state: sfp-not-present
	F0278	sys/switch-A/...	port-f...	2010-10-23T...	ether port 5 on fabric interconnect A oper state: sfp-not-present
	F0267	sys/chassis-1/...	link-d...	2010-10-20T...	Adapter host interface 1/1/1 link state: down
	F0479	sys/chassis-1/...	int-do...	2010-10-20T...	Virtual interface 761 link state is down
	F0279	sys/switch-B/s...	port-f...	2010-10-17T...	ether port 18 on fabric interconnect B oper state: sfp-not-present
	F0528	sys/chassis-1/...	equip...	2010-10-15T...	Power supply 4 in chassis 1 power: power-save

Details

Summary

Severity: ☒ cleared
Last Transition: 2010-10-23T08:33:30

Actions

☒ Acknowledge Fault

Properties

Affected object: sys/switch-A/slot-1/switch-ether/port-18
Description: ether port 18 on fabric interconnect A oper state: sfp-not-present
ID: 184309
Type: network
Cause: port-failed
Created at: 2010-10-17T12:36:45
Code: F0279
Number of Occurrences: 1
Original severity: info
Previous severity: info
Highest severity: info

The figure shows an example of the Properties window that appears when you click a fault. Depending on your screen resolution, you might not be able to see the complete text of the fault description. The Properties window always displays the complete text of the fault.

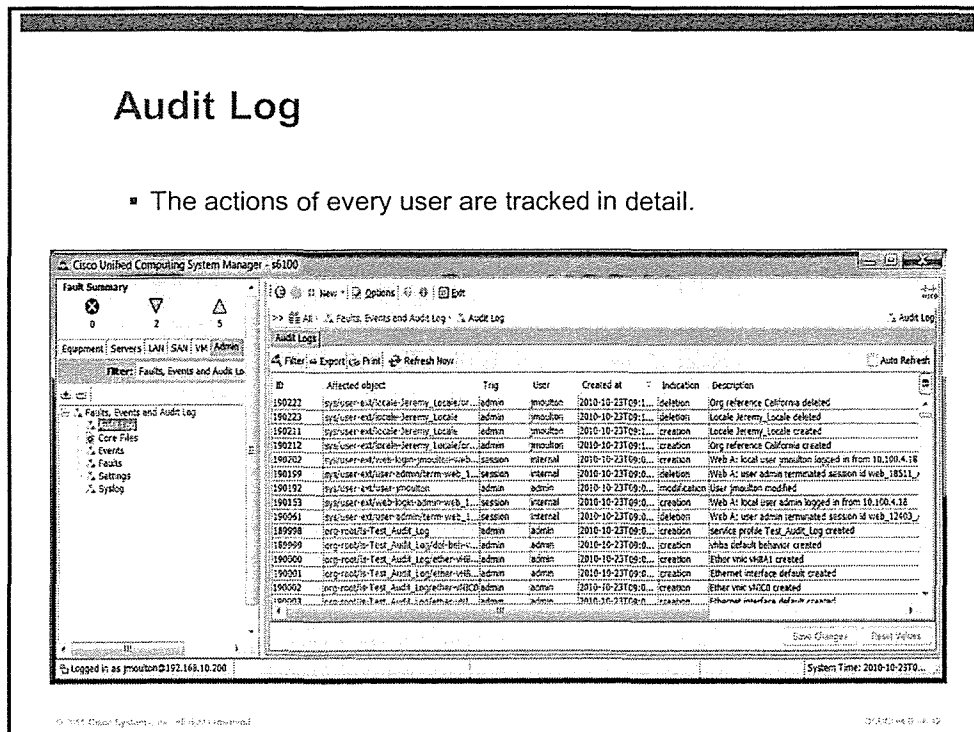
Using the Audit Log to Track Administrative Changes to the Cisco UCS Manager Database

This topic discusses the configuration and use of the audit log.

Audit Log

Audit Log

- The actions of every user are tracked in detail.

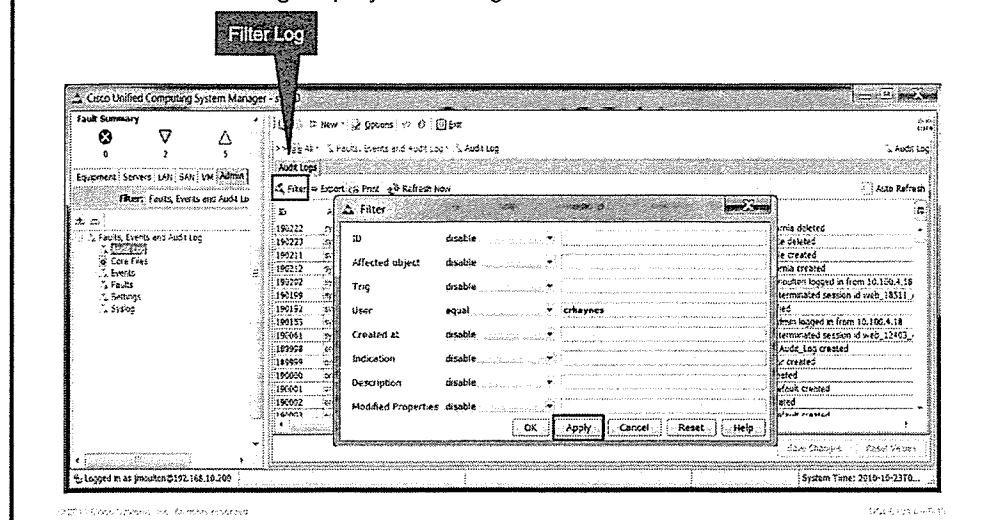


The audit log can be accessed under the Admin tab. Expand **Faults, Events and Audit Log**, and then choose **Audit Log**. The audit log records login events for all users and the actions they performed in the Cisco UCS Manager interface. This information is useful if an unapproved change has been made.

Filter Audit Log Output

Filter Audit Log Output

- Limit the log display according to user-selected criteria.

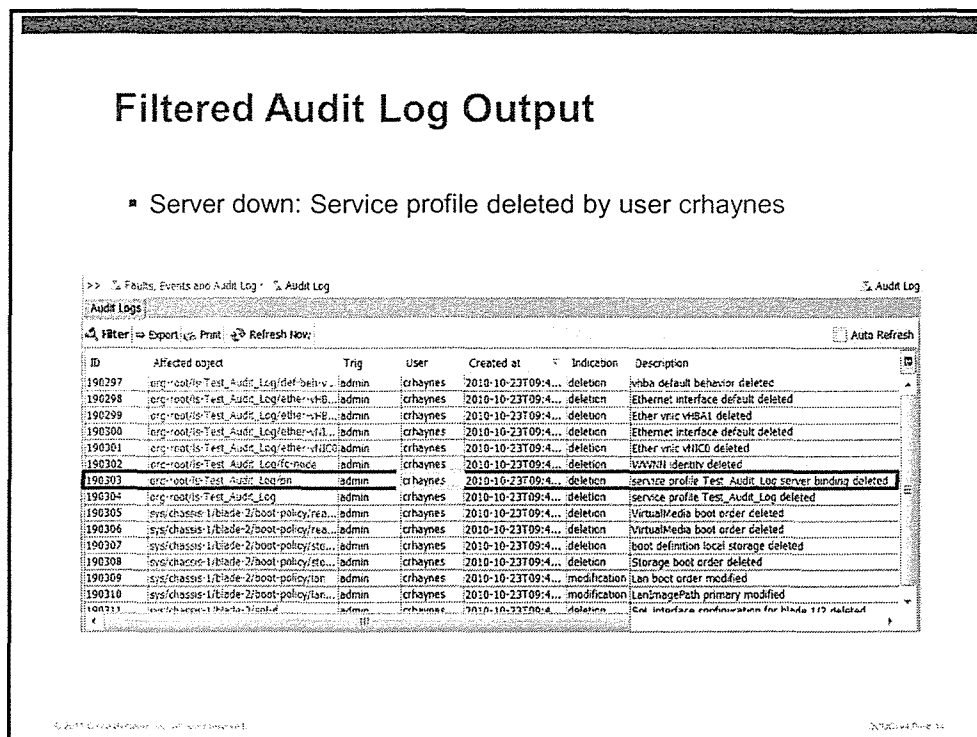


The audit log can be intimidating to work with because of the large number of entries. As the example in the figure shows, click the Filter button and then select the criteria on which to filter. In this example, the administrator has decided to determine which actions have been taken by user crhaynes.

Filtered Audit Log Output

Filtered Audit Log Output

- Server down: Service profile deleted by user crhaynes



The screenshot displays a web-based interface for viewing audit logs. At the top, there's a title bar and a search/filter bar. Below that, a table lists audit log entries. The entry with ID 190303 is highlighted in red, showing a deletion event for a service profile named 'Test_Audit_Log_server_banding' by user 'crhaynes' on 2010-10-23T09:41:00. The description for this entry is 'service profile Test_Audit_Log_server_banding deleted'.

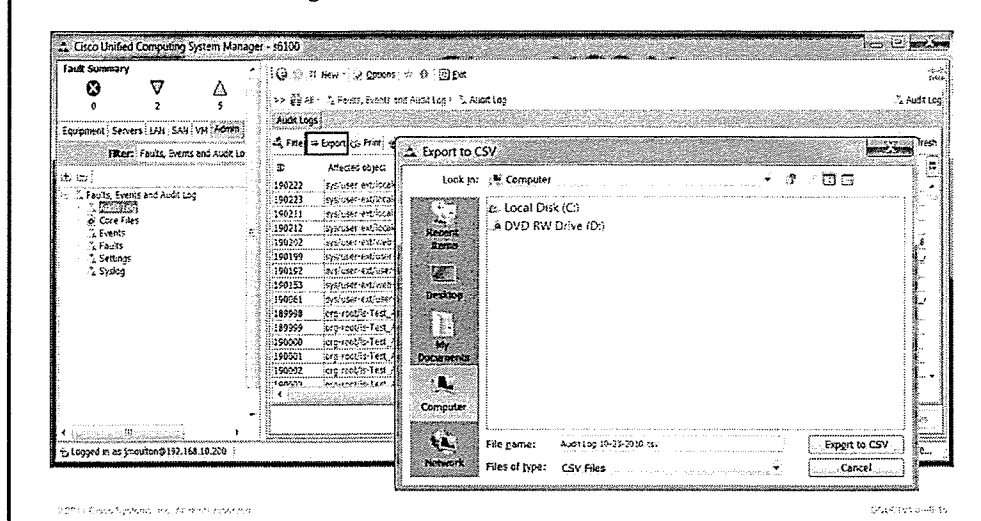
ID	Affected object	Trig	User	Created at	Index	Description
190297	erg-rootfs-Test_Audit_Log/def-beh-v...	admin	crhaynes	2010-10-23T09:41:00	deletion	nvra default behavior deleted
190298	erg-rootfs-Test_Audit_Log/ether-vhB...	admin	crhaynes	2010-10-23T09:41:00	deletion	Ethernet interface default deleted
190299	erg-rootfs-Test_Audit_Log/ether-vhB...	admin	crhaynes	2010-10-23T09:41:00	deletion	Ether vnic vHBAT deleted
190300	erg-rootfs-Test_Audit_Log/ether-vhB...	admin	crhaynes	2010-10-23T09:41:00	deletion	Ethernet interface default deleted
190301	erg-rootfs-Test_Audit_Log/ether-vhB...	admin	crhaynes	2010-10-23T09:41:00	deletion	Ether vnic vHIC0 deleted
190302	erg-rootfs-Test_Audit_Log/ether-vhB...	admin	crhaynes	2010-10-23T09:41:00	deletion	VLAN11 identity deleted
190303	erg-rootfs-Test_Audit_Log/def-beh-v...	admin	crhaynes	2010-10-23T09:41:00	deletion	service profile Test_Audit_Log_server_banding deleted
190304	erg-rootfs-Test_Audit_Log/def-beh-v...	admin	crhaynes	2010-10-23T09:41:00	deletion	service profile Test_Audit_Log deleted
190305	sys-chassis-1/blade-2/boot-policy/rea...	admin	crhaynes	2010-10-23T09:41:00	deletion	VirtualMedia boot order deleted
190306	sys-chassis-1/blade-2/boot-policy/rea...	admin	crhaynes	2010-10-23T09:41:00	deletion	VirtualMedia boot order deleted
190307	sys-chassis-1/blade-2/boot-policy/rea...	admin	crhaynes	2010-10-23T09:41:00	deletion	boot definition local storage deleted
190308	sys-chassis-1/blade-2/boot-policy/rea...	admin	crhaynes	2010-10-23T09:41:00	deletion	Storage boot order deleted
190309	sys-chassis-1/blade-2/boot-policy/rea...	admin	crhaynes	2010-10-23T09:41:00	modification	Lan boot order modified
190310	sys-chassis-1/blade-2/boot-policy/rea...	admin	crhaynes	2010-10-23T09:41:00	modification	Lan boot order modified
190311	sys-chassis-1/blade-2/boot-policy/rea...	admin	crhaynes	2010-10-23T09:41:00	deletion	Get interface modification for blade 112 deleted

A production server went out of service unexpectedly. This example shows that the administrator deleted the wrong service profile.

Export Audit Log

Export Audit Log

- Save audit log to a .csv file.



Audit-log data can be exported manually to a comma-separated values (.csv) file. The file can be read in a text editor or spreadsheet application.

Areas of Operation that Are Subject to FSM Validation and FSM Output Interpretation

This topic discusses the Cisco Unified Computing System components whose state transitions are validated by a finite state machine (FSM).

Operations Subject to FSM Validation

Operations Subject to FSM Validation

- Physical components
 - Chassis
 - IOM
 - Servers
- Logical components
 - LAN cloud
 - Policies
- Workflow
 - Server discovery
 - Service profile association and disassociation
 - Firmware downloads
 - Component upgrades
 - Backup and import jobs

Many components and processes within Cisco Unified Computing System are characterized by highly complex state transitions. FSMs are assigned to audit the state transitions and to validate correct operation.

Reset IOM—Discovery Process in FSM

Reset IOM—Discovery Process in FSM

- FSM tracking the transition states of IOM discovery

FSM Status: FeConnDiscoverChassis
Retry #1: 1

Current Stage Description: Triggering chassis discovery via IOM 1/1 (left) (FSM-STAGE:asmcdmcfabricIOMCard/eConnDiscoverChassis)
Description: configuration of IOM 1/1 (left) connectivity to fabric interconnect R(FSM:asmcdmcfabricIOMCard/eConn)

Time of Last Operation: 2010-10-23T16:50:00
Status of Last Operation: FeConnDiscoverChassis
Remote Invocation Result: end-point-unavailable
Remote Invocation Error Code: 1002
Remote Invocation Description: no connection to PK endpoint

Progress Status: 25%

Completion	FSM Flags	Item	ID
------------	-----------	------	----

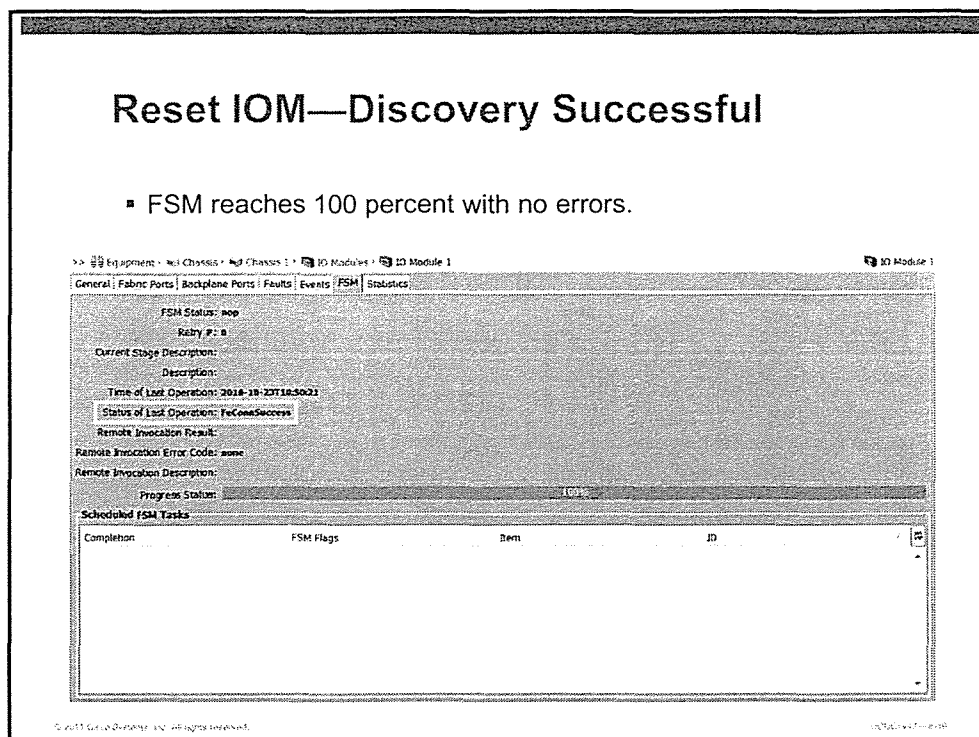
In the example, the I/O module (IOM) for fabric A was manually reset. The Current Stage Description field clearly indicates that chassis discovery is underway. The Description field indicates that IOM connectivity is being restored.

The Progress Status indicator provides a graphical representation of how far the FSM processed tree has proceeded. In many cases, there might be a long pause at a particular percentage point. This pause is process-specific and usually nothing to worry about. If the FSM stops responding for more than a certain amount of time, a timeout occurs and the operation fails.

Reset IOM—Discovery Successful

Reset IOM—Discovery Successful

- FSM reaches 100 percent with no errors.



The example illustrates a successful reset of the IOM and the resulting discovery process. The result code of `feConnSuccess` might seem cryptic, but it means that the fabric extender (FEX) connection was a success. FEX is a term that is sometimes applied to the IOM.

FSM Discovery Details

FSM Discovery Details

- Click the Event tab to review the log of FSM state transitions.

>> Equipment > N7 Class 1 > N7 Chassis 1 > IO Modules > IO Module 1

General | Fabric Ports | Backplane Ports | Faults | **Events** | FSM | Statistics

Filter | Export | Print

affected object	Cause	Created at	Description
sys/chassis-1/slot-1	transition	2010-10-23T10:50:21	[FSM:STAGE-RETRY]: triggering chassis discovery via IOM 1/1(left)/FSM-STAGE:sam:dme:EquipmentIOCardFe...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:21	[FSM:STAGE-STALE-SUCCESS]: triggering chassis discovery via IOM 1/1(left)/FSM-STAGE:sam:dme:EquipmentIOCardFe...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:21	[FSM:STAGE-END]: triggering chassis discovery via IOM 1/1(left)/FSM-STAGE:sam:dme:EquipmentIOCardFe...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:21	[FSM:STAGE-ASYNC]: enabling chassis 1 on left side(FSM-STAGE:sam:dme:EquipmentIOCardFeConn...EnableChas...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:21	[FSM:STAGE-STALE-SUCCESS]: enabling chassis 1 on left side(FSM-STAGE:sam:dme:EquipmentIOCardFeConn...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:21	[FSM:STAGE-END]: enabling chassis 1 on left side(FSM-STAGE:sam:dme:EquipmentIOCardFeConn...EnableChasps)
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:END]: configuration of IOM 1/1(left) connectivity to fabric interconnect B(FSM:sam:dme:EquipmentIOCardFe...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-STALE-SUCCESS]: configuring fabric interconnect B mgmt connectivity to IOM 1/1(left)/FSM-STAGE:s...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-END]: configuring fabric interconnect B mgmt connectivity to IOM 1/1(left)/FSM-STAGE:sam:dme:Eoa...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-ASYNC]: configuring IOM 1/1(left) virtual name space(FSM-STAGE:sam:dme:EquipmentIOCardFeCon...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-STALE-SUCCESS]: configuring IOM 1/1(left) virtual name space(FSM-STAGE:sam:dme:EquipmentIO...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-END]: configuring IOM 1/1(left) virtual name space(FSM-STAGE:sam:dme:EquipmentIOCardFeConn...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-ASYNC]: configuring management identity to IOM 1/1(left)/FSM-STAGE:sam:dme:EquipmentIOCardFe...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-STALE-SUCCESS]: configuring management identity to IOM 1/1(left)/FSM-STAGE:sam:dme:Equipme...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-END]: configuring management identity to IOM 1/1(left)/FSM-STAGE:sam:dme:EquipmentIOCardFeC...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-ASYNC]: triggering chassis discovery via IOM 1/1(left)/FSM-STAGE:sam:dme:EquipmentIOCardFeC...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-STALE-FAIL]: triggering chassis discovery via IOM 1/1(left)/FSM-STAGE:sam:dme:EquipmentIOCard...
sys/chassis-1/slot-1	transition	2010-10-23T10:50:00	[FSM:STAGE-REMOTE-ERROR]: Result: end-point-unavailable Code: unspecified Message: no connection to MC en...
sys/chassis-1/slot-1	transition	2010-10-23T10:49:59	[FSM:STAGE-END]: identifying IOM 1/1(FSM-STAGE:sam:dme:EquipmentIOCardFePresenceIdentify)
sys/chassis-1/slot-1	transition	2010-10-23T10:49:59	[FSM:END]: detection of IOM 1/1(left) connection to fabric interconnect B(FSM:sam:dme:EquipmentIOCardFePre...
sys/chassis-1/slot-1	transition	2010-10-23T10:49:59	[FSM-BEGIN]: configuration of IOM 1/1(left) connectivity to fabric interconnect B(FSM:sam:dme:EquipmentIOCard...
sys/chassis-1/slot-1	transition	2010-10-23T10:49:59	[FSM:STAGE-END]: FSM-STAGE:sam:dme:EquipmentIOCardFeConn:begin
sys/chassis-1/slot-1	transition	2010-10-23T10:49:59	[FSM:STAGE-ASYNC]: configuring fabric interconnect B mgmt connectivity to IOM 1/1(left)/FSM-STAGE:sam:dme...
sys/chassis-1/slot-1	transition	2010-10-23T10:49:59	[FSM:STAGE-REMOTE-ERROR]: WRONG STATE-Result: not-applicable Code: unspecified Message: (sam:dme:Ea...
sys/chassis-1/slot-1	transition	2010-10-23T10:49:58	[FSM-BEGIN]: detection of IOM 1/1(left) connection to fabric interconnect B(FSM:sam:dme:EquipmentIOCardFePre...

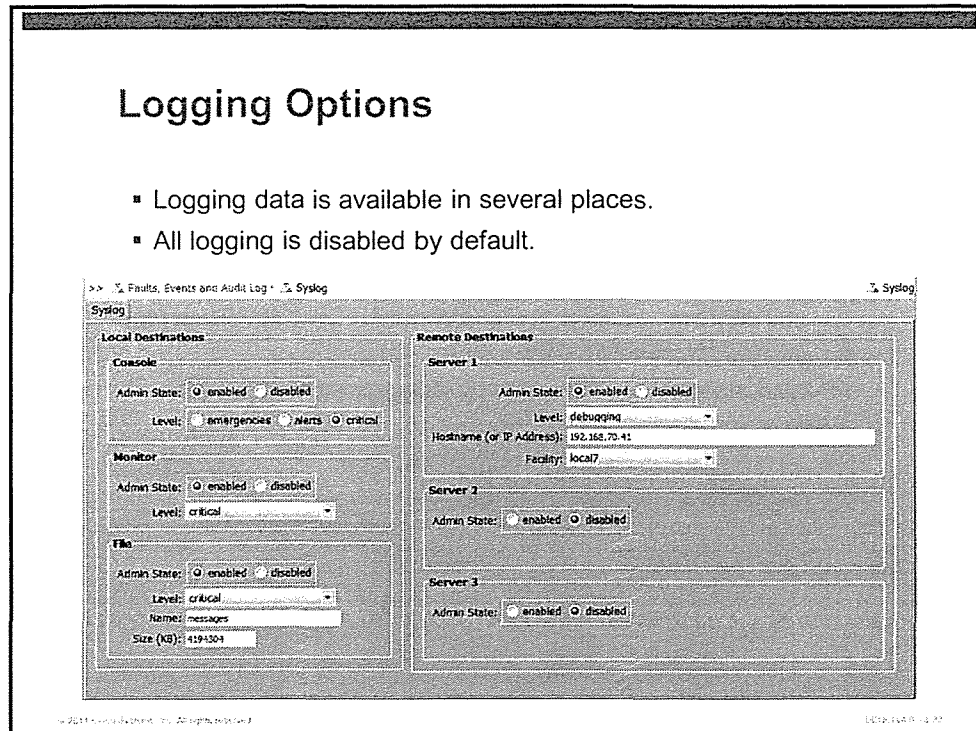
© 2011 Cisco Systems, Inc. All rights reserved. Page 1 of 1

In many cases, the FSM state transitions occur too quickly for a human operator to read. Click the Events tab to display a detailed list of all the transitions.

Configuration and Validation of Logging Options

This topic discusses internal and external logging options that are available within Cisco UCS Manager.

Logging Options



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.

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.

Configuring the Smart Call Home Feature

This topic discusses the configuration of the Cisco Smart Call Home feature.

Call Home

Call Home

- Call Home generates an email to notify administrators or support organization of failures or events.
- Call Home can generate multiple email formats:
 - shortTxt is suitable for a pager or mobile device.
 - xml contains detailed event information in XML format for parsing by an automated tool.
- Profiles determine which severity levels are sent to which recipients and in which format.
- Recipients can be listed in multiple policies.
 - Duplicate entries are consolidated.

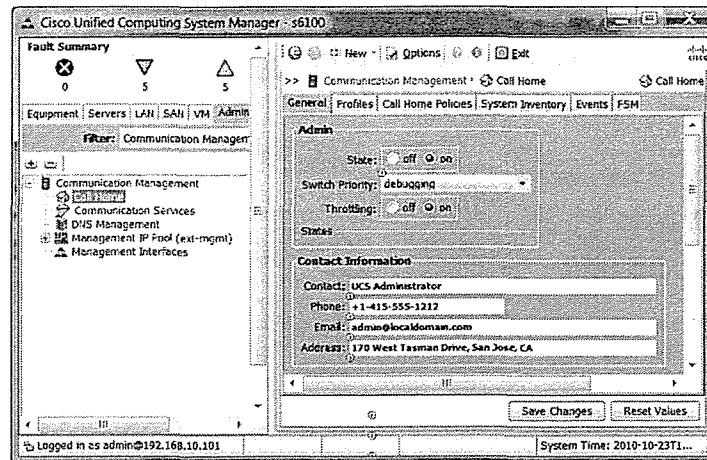
© 2011 Cisco Systems, Inc. All rights reserved. EODUCI v4.0

Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a network operations center, or use Cisco Smart Call Home services to generate a case with Cisco TAC.

Contact Configuration

Contact Configuration

- Begin by configuring the contact information that will be included in the Call Home messages.



Before Call Home can be enabled, contact information, including the SMARTnet contract ID, site ID, and customer ID, must be entered.

Email Notification

Email Notification

- Provide any necessary identification information.
- Supply the From and Reply To values for the email envelope.
- Specify the SMTP server to be used for outbound emails.

The screenshot displays the Cisco Unified Computing System Manager (v6100) web interface. The left sidebar shows a navigation tree with 'Communication Management' selected. The main content area is titled 'Email Notification' and contains several input fields for configuration. The 'General' tab is active, showing fields for 'Customer ID', 'Contract ID', and 'Site ID'. Below these are 'Email Addresses' with 'From' and 'Reply To' fields, and an 'SMTP Server' section with 'Host (IP Address or Hostname)' and 'Port' fields. 'Save Changes' and 'Reset Values' buttons are at the bottom right. The status bar at the bottom indicates the user is logged in as 'admin@192.168.10.101' and the system time is '2010-10-23T11:00:00'.

Email notification relies on the configuration of email addresses and a Simple Mail Transfer Protocol (SMTP) server address.

Call Home Profiles

Call Home Profiles

- Three default profiles exist.
 - CiscoTAC-1, which is useful for sending XML data to Cisco TAC
 - Uses special ciscoTac alert group to collect information needed by Cisco TAC
 - full_txt, for sending full XML data
 - By default, includes all alert groups at warning severity
 - short_txt, for sending short, plain text data
 - By default, includes all alert groups at warning severity
- Alert groups allow profiles to send only data related to specific functional areas.
- Additional profiles can be created as needed.
 - Default profiles can be modified but not removed.

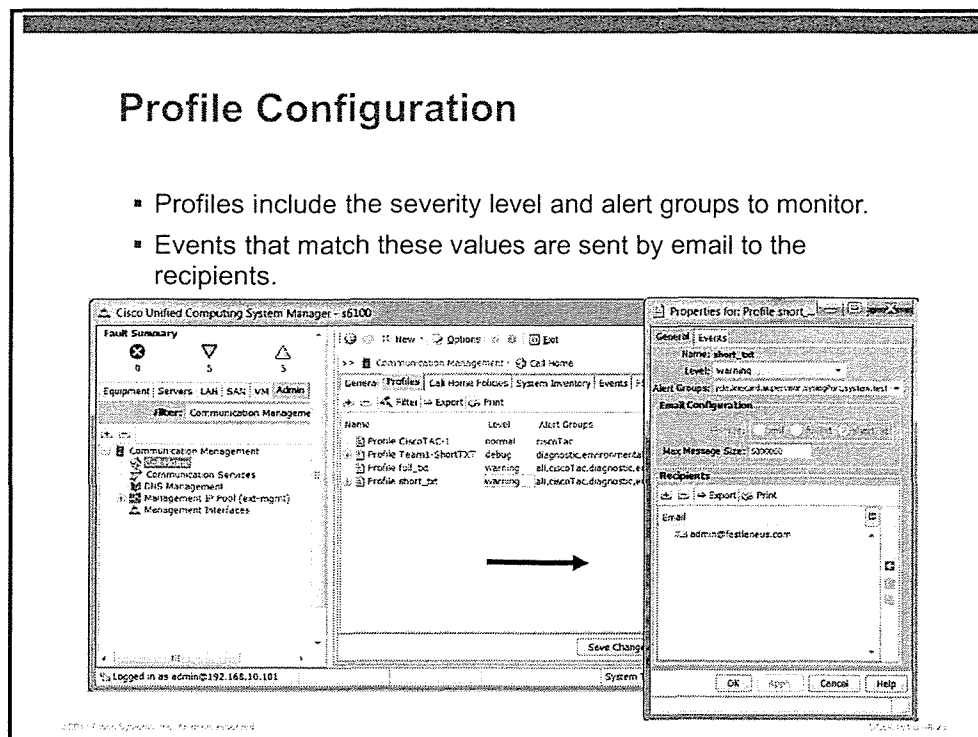
Call Home profiles determine which alert groups and recipients receive email alerts for events that occur at a specific severity. You can also use these profiles to specify the format of the alert for a specific set of recipients and alert groups.

By default, you must configure the Cisco TAC-1 profile. You can also create profiles to send email alerts to one or more groups when events occur at a level that you specify.

Profile Configuration

Profile Configuration

- Profiles include the severity level and alert groups to monitor.
- Events that match these values are sent by email to the recipients.

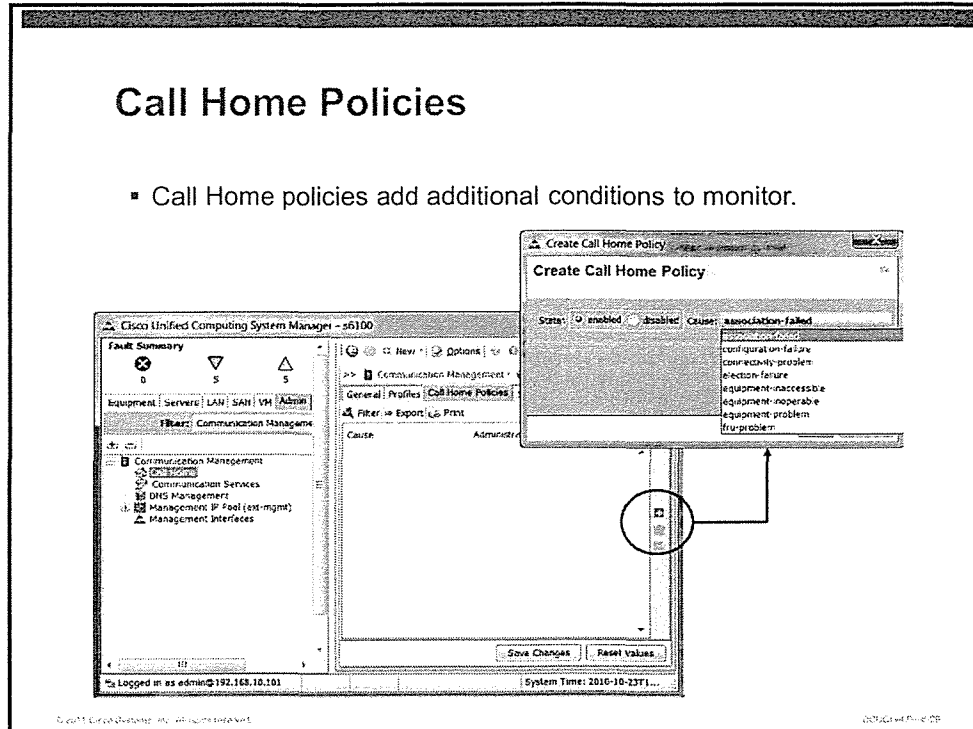


Call Home profiles define the alert groups, notification levels, and users to receive the emails. The example shows the called profile `short_txt`, which is configured to send emails in nonverbose text format to one recipient.

Call Home Policies

Call Home Policies

- Call Home policies add additional conditions to monitor.

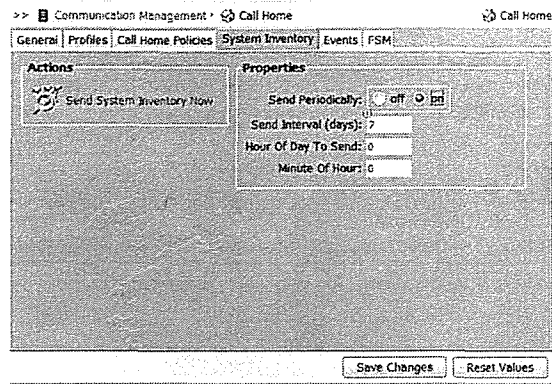


Call Home policies can also be created to restrict the conditions that will trigger an alert.

System Inventory

System Inventory

- System inventory information can be sent manually or scheduled periodically.
- This information aids support organizations in tracking changes to installed equipment.

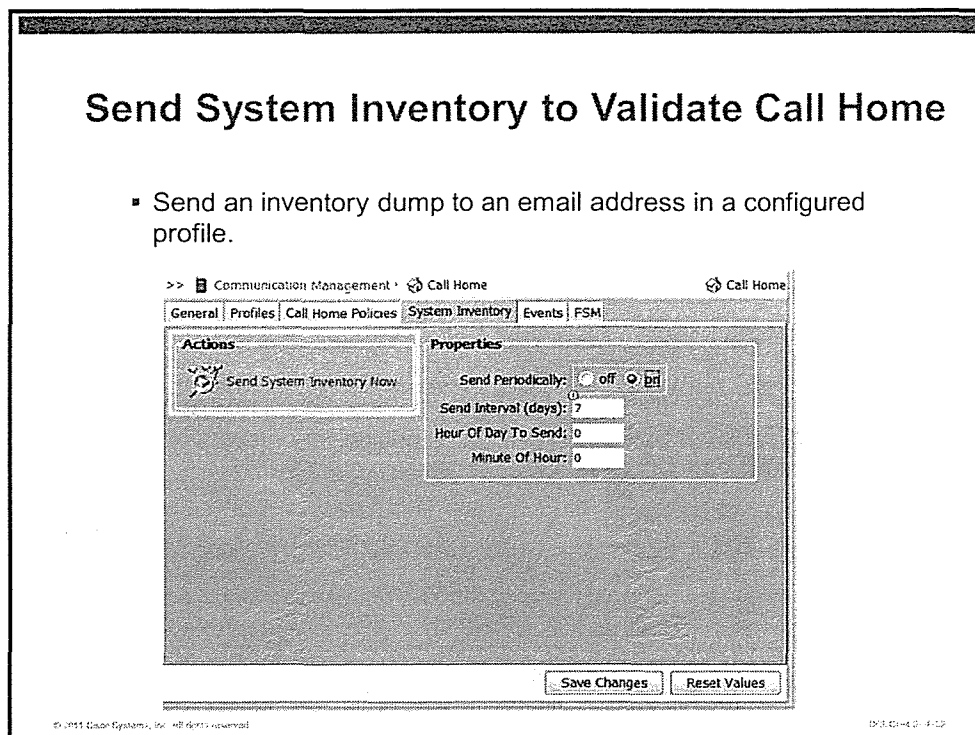


The system inventory can be configured to periodically send information about field-replaceable units (FRUs) to the Cisco TAC. For Cisco TAC to provide the best possible service, you must keep their database up-to-date with the components in your system.

Validating the Smart Call Home Feature

This topic discusses how to validate Smart Call Home.

Send System Inventory to Validate Call Home



An easy way to validate the configuration of your Smart Call Home setup is to enable a Call Home profile that is set to an email destination. When you click the button to send system inventory, an email should be generated to the destination email address that you configured in the profile.

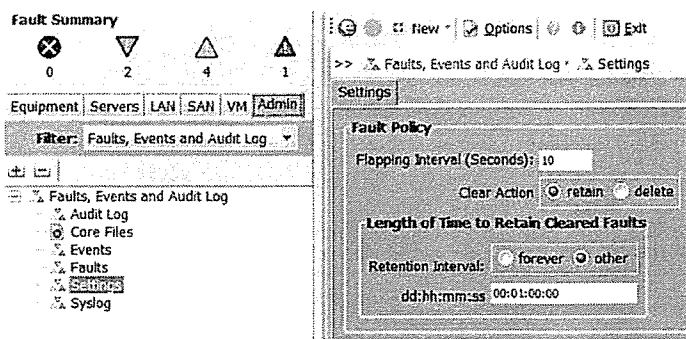
Settings for Logs, Events, and Faults

This topic discusses how to configure settings for logs, events, and faults.

Fault Settings and Retention Policy

Fault Settings and Retention Policy

- The configuration of the retention policy is governed by organizational policy and regulatory compliance requirements.



The screenshot displays the 'Fault Settings and Retention Policy' configuration window. On the left, a 'Fault Summary' section shows four icons representing different fault types with counts: 0, 2, 4, and 1. Below this is a 'Filter' dropdown menu set to 'Faults, Events and Audit Log'. The main area is titled 'Fault Policy' and contains the following settings:

- Flapping Interval (Seconds):** 10
- Clear Action:** ☐ retain ☐ delete
- Length of Time to Retain Cleared Faults:**
 - Retention Interval:** ☒ forever ☐ other
 - dd:hh:mm:ss:** 00:01:00:00

The default settings and retention policy allows the Cisco Unified Computing System administrator to tune the flapping interval and faults retention policy. These values should be set according to organizational or regulatory compliance requirements.

Summary

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

Summary

- Cisco UCS Manager maintains faults and errors as managed objects.
- The audit log can be used to track changes made by any user to the Cisco UCS Manager database.
- Several processes in Cisco UCS Manager are subject to FSM validation.
- Logging options include local buffer, console, and external syslog servers.
- The Smart Call Home feature allows Cisco UCS Manager to send inventory and predictive failure messages to Cisco TAC.
- You can validate the Smart Call Home feature by generating an email.
- Logs, events, and faults have user definable traits.

© 2011 Cisco Systems, Inc. All rights reserved.

UCS Manager 5.2

Managing and Upgrading Cisco UCS B-Series Firmware

Overview

Before the introduction of the Cisco Unified Computing System, firmware management in blade-server environments was challenging. A cornerstone design goal of Cisco Unified Computing System is to simplify firmware management. To allow for administrative consistency and stateless computing, firmware images in Cisco Unified Computing System can be attached as a policy to a service profile. If the service profile is moved to a new blade, then there is no need for manual firmware intervention.

Objectives

Upon completing this lesson, you will be able to locate firmware images on Cisco.com, perform software updates to the fabric interconnects, and update individual components both manually and automatically, through a service profile. This ability includes being able to meet these objectives:

- Describe where to find Cisco UCS B-Series firmware packages on Cisco.com
- Update the Cisco UCS B-Series firmware
- Perform a direct upgrade of Cisco IMC, IOM, and mezzanine adapter firmware
- Describe software updates on the fabric interconnect
- Perform firmware updates via service profile
- List the differences between the firmware processes of Cisco UCS 61x0 Fabric Interconnects and Cisco IMC, IOM, and adapter

Where to Find Cisco UCS B-Series Firmware Packages on Cisco.com

This topic discusses how to locate Cisco Unified Computing System firmware bundles and individual images on Cisco.com.

Locate Firmware on Cisco.com



To download individual images or bundles for Cisco Unified Computing System, you need a Cisco.com login that is attached to a SMARTnet contract that covers the Cisco Unified Computing System components that are to be upgraded.

Open a browser to <http://www.cisco.com>. Move your mouse to hover over the **Support** tab, as indicated in the example. Click the **Download Software** link.

Locate Cisco Unified Computing System Firmware on Cisco.com

Locate Cisco Unified Computing System Firmware on Cisco.com

- Choose Unified Computing.

Download Software

Select a Software Product Category

- [Application Networking Services](#)
- [Cisco IOS and NX-OS](#)
- [Network Management](#)
- [Optical Networking](#)
- [Physical Security and Building Systems](#)
- [Routers](#)
- [Security](#)
- [Service Exchange](#)
- [Storage Networking](#)
- [Switches](#)
- [TelePresence](#)
- [Unified Computing](#)
- [Unified Catalysts and Access Servers](#)
- [Video, Cable and Content Delivery](#)
- [Voice and Unified Communications](#)

Software Download Search

Software Downloads Related Search

Get the [Software Download search plugin](#) for your browser

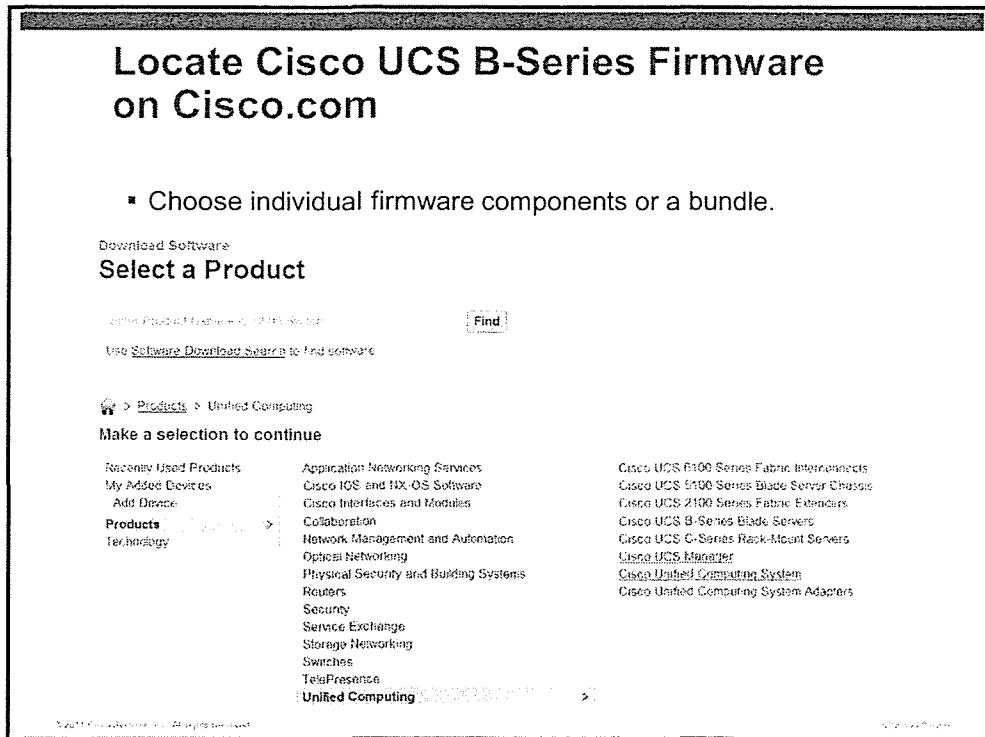
Software Tools

- [Cisco Notification Service](#) NEW!
- Subscribe to get email or RSS notifications for software
- [Cisco MIBs](#)
- Locate MIBs supported by Cisco products
- [Software Adviser](#)
- Research Hardware-Software-Feature compatibility and related MIBs and bugs
- [Special File Access](#)
- [Bug Toolkit](#)

© 2011 Cisco Systems, Inc. All rights reserved.1042810101-0000

Scroll down the list of software categories until you reach Unified Computing, and then click the link.

Locate Cisco UCS B-Series Firmware on Cisco.com



The third dialog pane lists all of the Cisco Unified Computing System (UCS) B-Series and C-Series firmware categories.

Choose Cisco Unified Computing System Bundle Image

Choose Cisco Unified Computing System Bundle Image

- Choose bundle image to upgrade all Cisco Unified Computing System components.

Cisco UCS 6120XP 20-Port Fabric Interconnect

Download Software

 [Download Cart \(0 items\)](#)  [Help](#)

Select a Software Type 

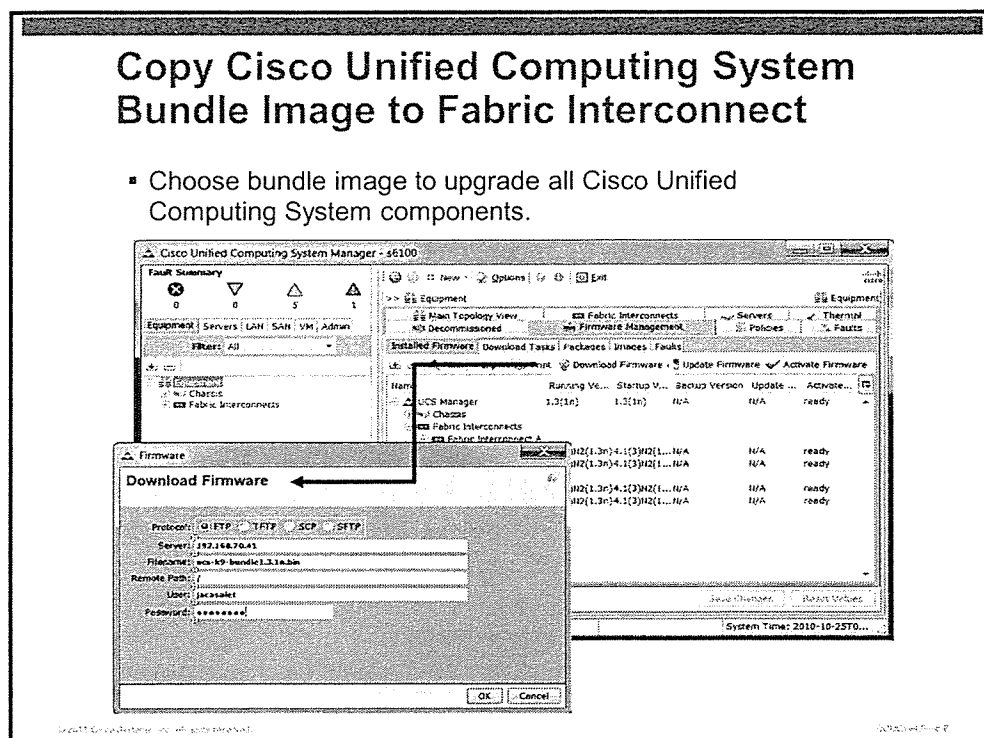
 > [Products](#) > [Unified Computing](#) > [Cisco UCS 6100 Series Fabric Interconnects](#) > [Cisco UCS 6120XP 20-Port Fabric Interconnect](#) > [Software on Chassis](#)

[Unified Computing System \(UCS\) Complete Software Bundle](#)
[Unified Computing System \(UCS\) Fabric Interconnect Kickstart Software](#)
[Unified Computing System \(UCS\) Fabric Interconnect System Software](#)
[Unified Computing System \(UCS\) Manager Software](#)

© 2011 Cisco Systems, Inc. All rights reserved. [Cisco Confidential](#)

In most cases, a bundle image is the best way to download Cisco Unified Computing System firmware. A bundle image is guaranteed to be compatible with all individual constituent images. If only one component needs to be upgraded to a new version, then selecting firmware for that element results in a much faster download.

Copy Cisco Unified Computing System Bundle Image to Fabric Interconnect



When the bundle image is downloaded, it must be transferred to the flash file system of the active management node. As long as you browse to the virtual IP address of the cluster, the image is updated only to the active management node.

Navigate to **Equipment > Firmware Management > Installed Firmware**, and then click the **Download Firmware** button.

Enter the IP address or fully qualified domain name (FQDN) of the host on which the downloaded bundle image resides. Select the appropriate transfer protocol, enter the filename and authentication credentials, and click the **OK** button.

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.

Updating Cisco UCS B-Series Firmware

This topic discusses general issues surrounding component firmware upgrades.

Suggested General Upgrade Practices

Suggested General Upgrade Practices

- Upgrade all components to the latest level available at initial installation, before deploying operating systems.
- Carefully study the release notes of the new firmware to determine whether version dependencies or open caveats could lead to issues with current production systems.
- Consult with operating system and application vendors for adapter firmware dependencies.
- Test new code, if available, on a Cisco Unified Computer System development system for testing.
- Upgrade from outside-in: Upgrade adapter, then Cisco IMC, then IOM, then Cisco UCS Manager, and then the fabric interconnects.
- Do not select all and attempt to activate all components at once.

When the Cisco Unified Computing System is in production use, gaining authorization to update firmware components requires an approval process and a change control window. Therefore, you should update all components of the Cisco Unified Computing System to the latest version before installing operating system applications and user access.

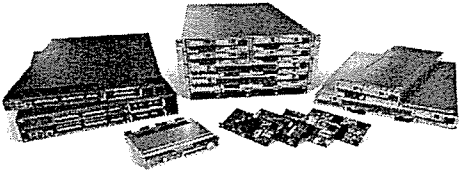
A step that many administrators neglect is the careful review of the release notes of any new firmware that is to be applied to the Cisco Unified Computing System. The release notes provide an alert to any version dependencies or open caveats that might relate specifically to the operating system versions or application versions in your production network. Failure to abide by the recommendations in the release notes can result in system instability and loss of availability.

It might seem counterintuitive, but an outside-in approach is recommended when updating the firmware of an entire Cisco Unified Computing System. This approach means updating the server adapters first, followed by the Cisco Integrated Management Controller (IMC), I/O modules (IOMs), Cisco UCS Manager, and fabric interconnects.

Upgrade Overview

Upgrade Overview

- Components to upgrade
 - Cisco UCS 61x0 Fabric Interconnect
 - IOM
 - Cisco IMC
 - CNAs
 - Option ROMs
 - BIOS
 - LSI (RAID firmware)
- Methods of upgrade
 - CLI
 - GUI
- Downloading images
 - TFTP, FTP, SFTP, and SCP
 - Bundles



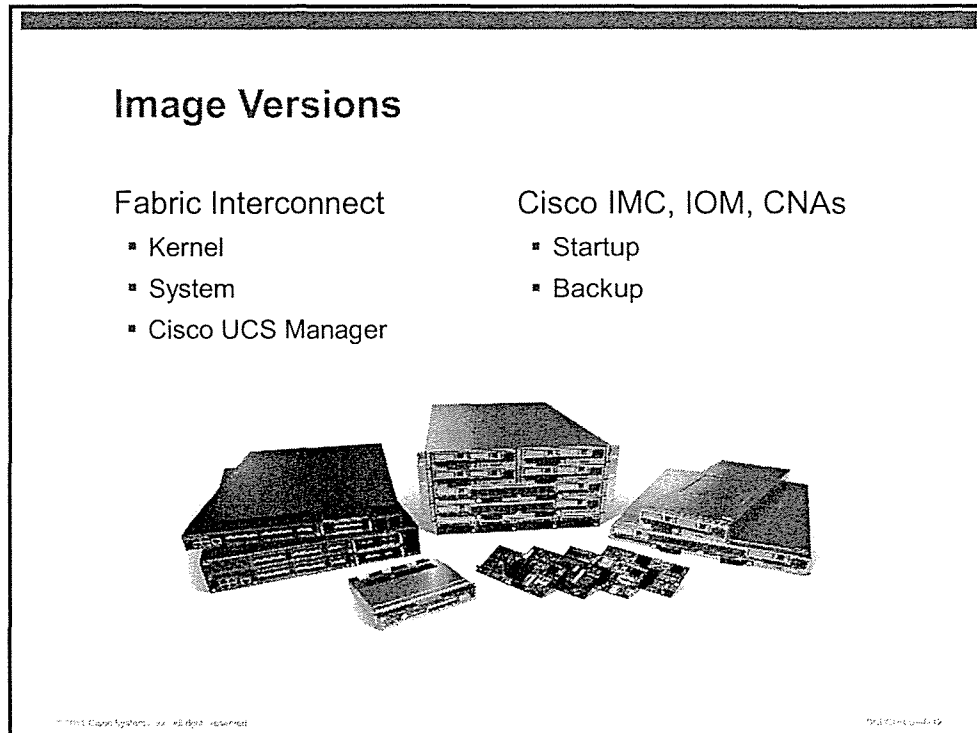
© 2011 Cisco Systems, Inc. All rights reserved.

DCUCI v4.0-1.55

The following Cisco UCS components are firmware upgradable:

- Cisco UCS 6100 Series Fabric Interconnects
- Cisco UCS Manager
- Cisco 2104 IOMs
- Cisco UCS Converged Network Adapters (CNAs)
- Cisco IMC instances
- Cisco Host Bus Adapters (HBAs)
- Cisco HBA Option ROMs
- Cisco UCS BIOS

Image Versions



The fabric interconnects require three distinct firmware updates:

- **Cisco Nexus Operating System (NX-OS) Kernel:** This update contains the boot loader and low-level operating system and loads Cisco NX-OS.
- **Cisco NX-OS System:** This image is the binary image of Cisco NX-OS. This image loads Cisco UCS Manager.
- **Cisco UCS Manager:** Cisco UCS Manager runs as a process on dedicated management processors in the fabric interconnects.

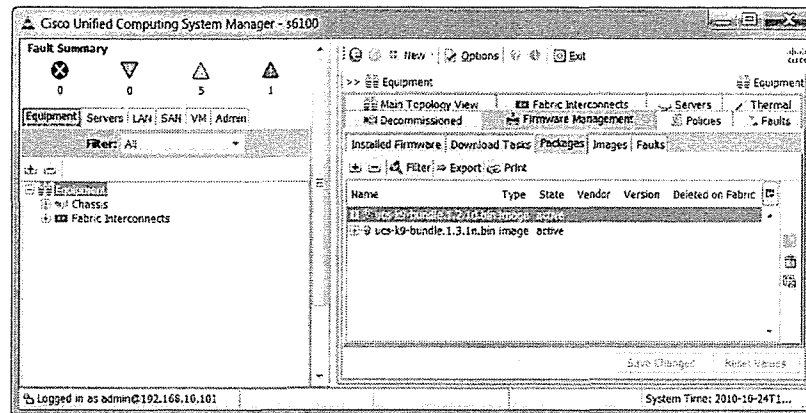
IOMs, Cisco IMC, and CNAs store firmware in two repositories:

- **Startup:** This image is the boot image.
- **Backup:** This image is loaded if the startup image is unavailable or unloadable.

Displaying Installable Images

Displaying Installable Images

- Installable images and packages can be viewed in the Firmware Management tab of the Equipment content pane.



In the example, the Packages tab indicates that two version bundles are loaded on the fabric interconnects. To list the individual component firmware elements, click the Images tab.

Direct Upgrade of Cisco IMC, IOM, and Mezzanine Adapter Firmware

This topic discusses the direct firmware update of Cisco IMC instances, IOMs, and adapters.

Update Dual-Flash Components

Update Dual-Flash Components

- Before activating firmware updates, you must perform an update operation to load an image to the device.
- Cisco IMC, IOM, and Ethernet adapters have two flash partitions for firmware:
 - **Startup partition:** The endpoint loads this image when powered on or reset.
 - **Backup partition:** The endpoint loads this firmware if the startup image fails to load.

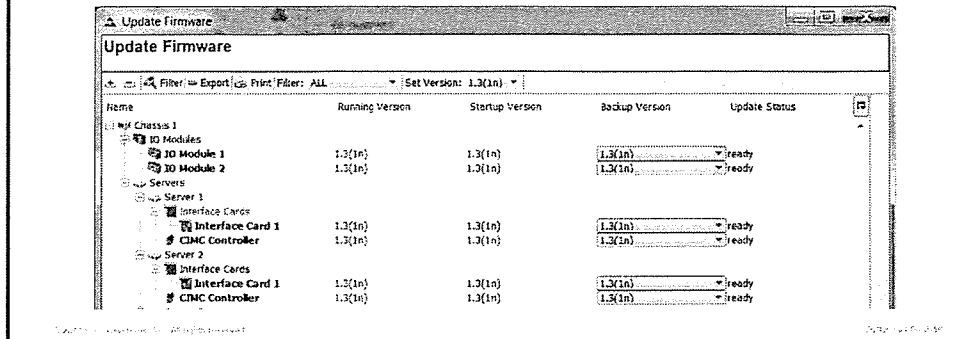
As was discussed earlier in the lesson, IOM, Cisco IMC, and mezzanine components have two flash partitions for firmware images. Before the startup image can be activated on a new version, the backup image must be updated with the desired version.

You can update a single component, a single category of components, or all components on a common version of firmware. It is strongly recommended that you do not activate all components in all chassis at one time.

Update Components

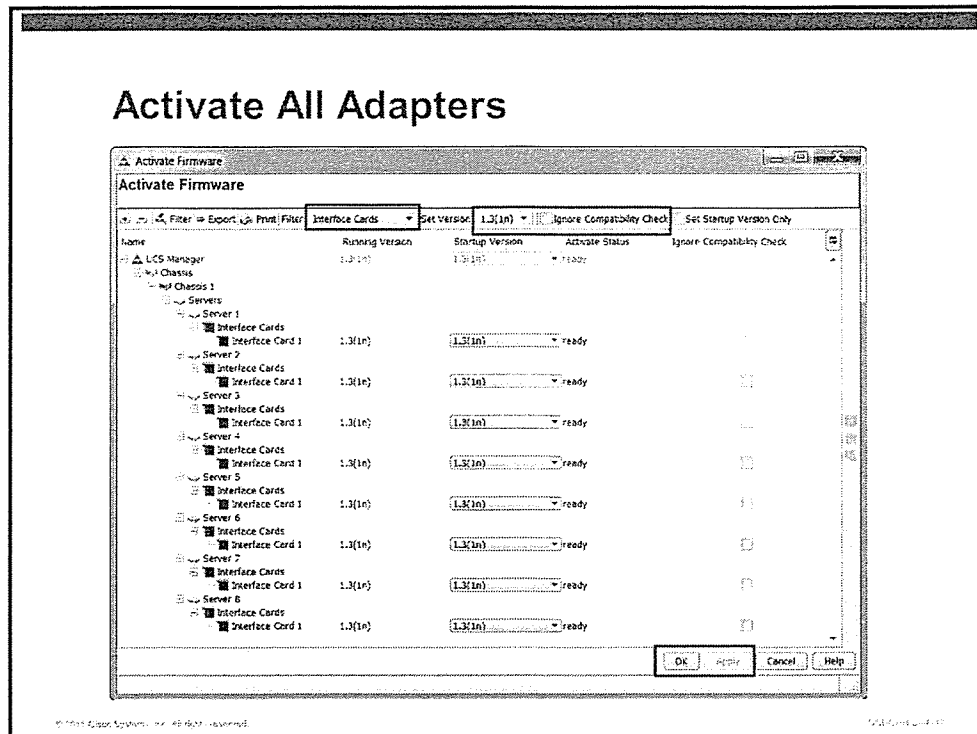
Update Components

- 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.



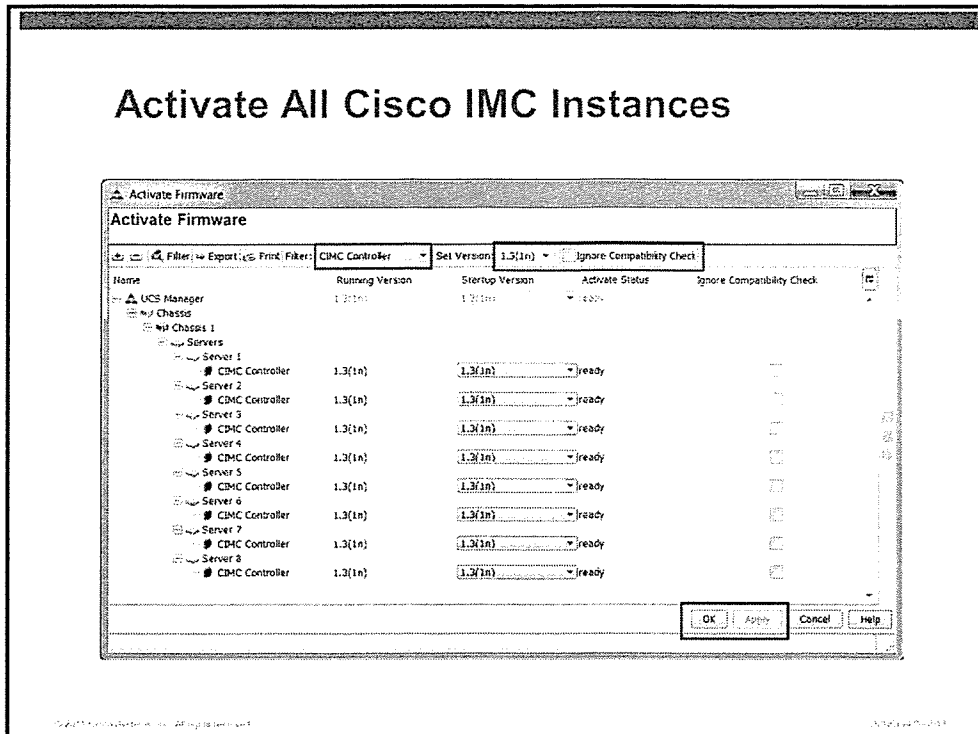
The update process operates strictly on the backup partition of flash for a given component. You can safely update the backup partition of any component during regular business hours. Performing this step now will save much time during the maintenance window for activating the new firmware.

Activate All Adapters



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.

Activate All Cisco IMC Instances



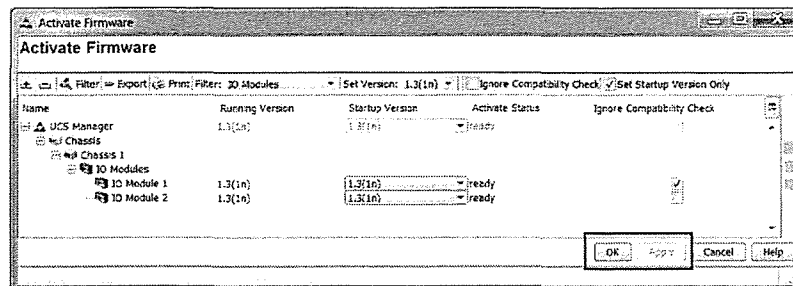
The safest firmware upgrade that an administrator can perform on the Cisco Unified Computing System is that of updating and activating Cisco IMC instances. As discussed earlier, updating the backup partition of a Cisco IMC has no impact on communications. Activating the new startup version to the eight servers in the example does not affect any in-band Ethernet or Fibre Channel communications to the blade servers.

Note Three out-of-band (OOB) management services are unavailable during activation: keyboard, video, mouse (KVM) over IP, serial over LAN (SoL), and Intelligent Platform Management Interface (IPMI).

Activate Both IOMs

Activate Both IOMs

- Set the filter to select the IOMs and select a common version from the drop-down menu.
- Set Startup Version Only updates the startup flash partition but does not take effect until the IOM is reset.
- Check the Ignore Compatibility Check check box, based on release notes or Cisco TAC recommendation.



From Equipment > Firmware Management > Installed Firmware, click the **Activate Firmware** button. In the Activate Firmware pop-up window, select **IO Modules** from the Filter drop-down menu. Select the common version that the I/O modules should share from the Set Version drop-down menu. Click the **Apply** button to start activation. The activation process does not actually copy an image from the backup to the startup partition. Activation simply moves the startup pointer and promotes the backup partition to startup. When the activation is complete, the old startup version becomes the backup version.

Best practice is to select the Set Startup Version Only checkbox when activating new firmware on IOMs. This setting causes the IOM to wait until its associated fabric interconnect reboot.

Note If an IOM is upgraded to a version that is incompatible with its associated fabric interconnect, then the fabric interconnect automatically reactivates the IOM with a compatible version. Therefore, the Set Startup Version Only checkbox is important.

Software Updates on the Fabric Interconnect

This topic discusses firmware updates to the fabric interconnect.

Fabric Interconnect Firmware Update

Fabric Interconnect Firmware Update

- Upgrade firmware of Cisco UCS Manager first, then subordinate fabric interconnect.
- Upgrade firmware of active fabric interconnect.
- Monitor the upgrade process on the serial console directly or through a terminal server.

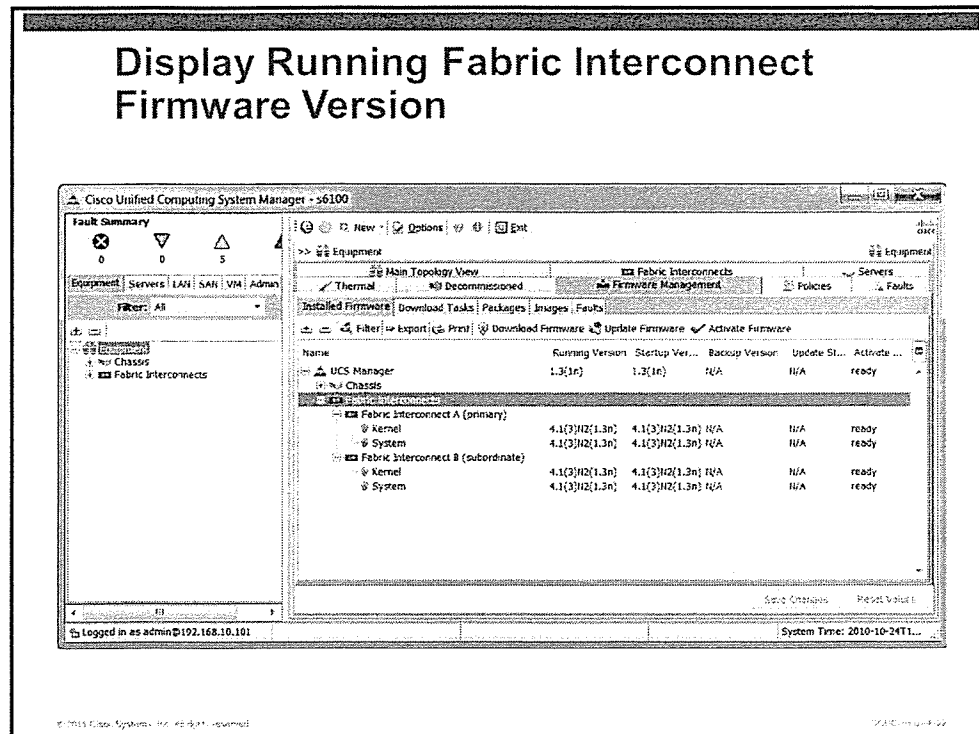
© 2011 Cisco Systems, Inc. All rights reserved. DCUCI-140-03.01

Because the fabric interconnects operate in a cluster, it is possible to update fabric interconnects during production operation. However, the administrator is strongly encouraged to schedule a change control window to perform this maintenance. This process can be time consuming to complete and can result in unplanned downtime.

To avoid the worst-case scenario of both fabric interconnects being in a nonuseable state, update them one at a time. Begin by updating the subordinate fabric interconnect. When the new firmware begins activating on the subordinate fabric interconnect, the subordinate fabric interconnect will reboot. A connection to the fabric interconnect serial interfaces or Remote Terminal (RT) server interface that connects to them is useful. This connection will allow you to watch for errors during the update process.

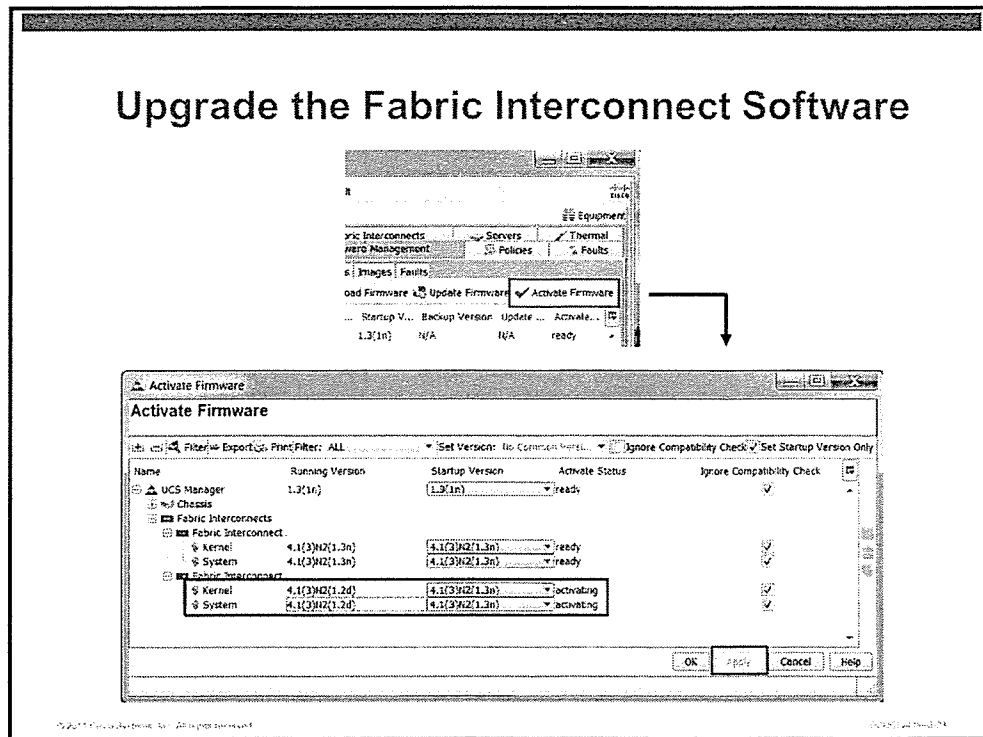
When the subordinate fabric interconnect is back online, updating and activating the primary fabric interconnect should be safe. Depending on the version of firmware, plan on 45 minutes to 1 hour per fabric interconnect. For estimating a change control window, 4 hours should be adequate to allow for either success or rollback.

Display Running Fabric Interconnect Firmware Version



Navigate to **Equipment > Firmware Management > Installed Firmware** to view the running version of firmware on both fabric interconnects.

Upgrade the Fabric Interconnect Software



From **Equipment > Firmware Management > Installed Firmware**, click the **Activate Firmware** button. A new dialog box appears, allowing the selection of the desired firmware version from drop-down lists. When the correct version appears next to the fabric interconnect for kernel and system images, click the **Apply** button to begin the upgrade.

Note The kernel and system must be on the same major version; for example, a kernel version of 1.2(1d) and a system version of 1.3(1n) are incompatible.

Firmware Updates via Service Profile

This topic discusses the creation of host firmware packages that travel from blade server to blade server on an associated service profile.

Host Firmware Package Mandatory

Host Firmware Package Mandatory

- Some firmware packages can be updated only in a firmware package that is attached to a service profile.
- These devices cannot be directly updated in the Cisco UCS Manager GUI or CLI interface:
 - BIOS
 - RAID controller
 - HBA
 - HBA option ROM

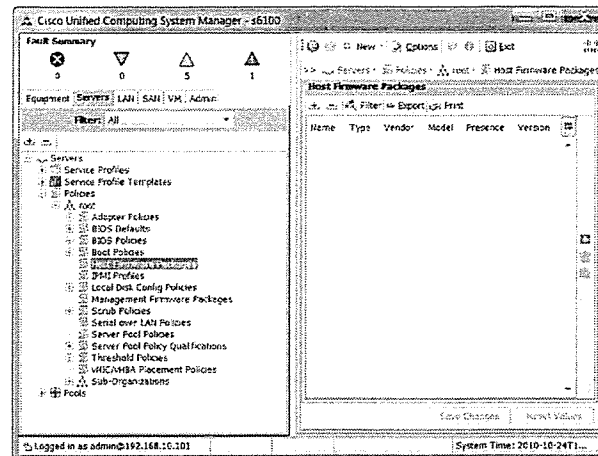
Note: BIOS images can be updated in Cisco UCS Manager via Recover Corrupted BIOS, but this facility should not be used if the BIOS is bootable. This is not a valid BIOS upgrade option.

A few upgradable components cannot be updated through direct firmware updates. The server BIOS, HBA, HBA option ROM, and Redundant Array of Independent Disks (RAID) controller firmware must be updated within an operating system that runs on the blade server, or via a host firmware package that is associated with the service profile.

Host Firmware Package Creation

Host Firmware Package Creation

- Host and management firmware packages are created, modified and deleted on the Servers, tab under Policies.

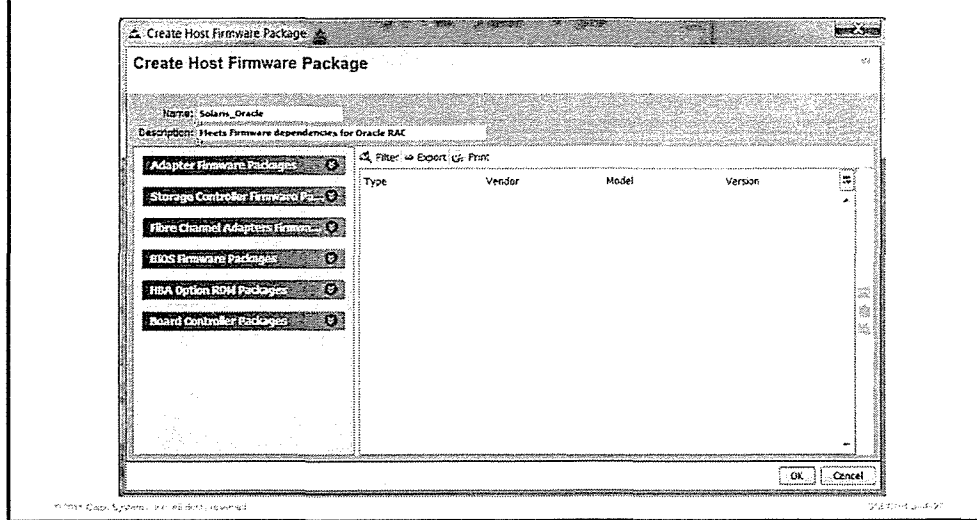


Under the Policy category of the navigation pane Server tab, choose the **Host Firmware Packages** item. The Host Firmware Package creation wizard is started by right-clicking the policy or by clicking the small plus sign (+) in the content pane.

Host Firmware Categories

Host Firmware Categories

- This wizard allows you to select the firmware categories.



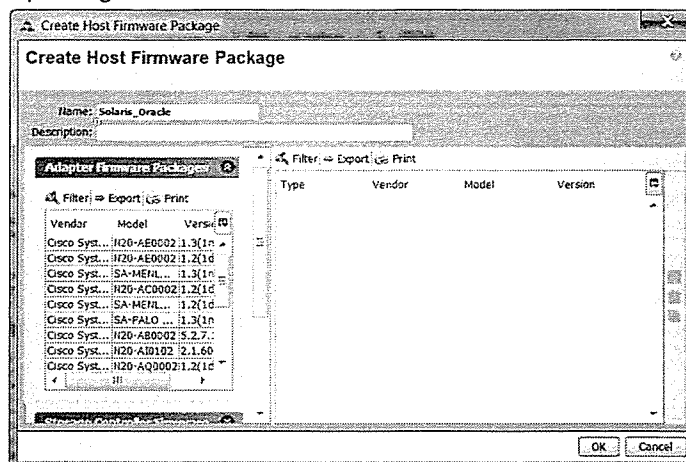
There are six host firmware categories in which an administrator can choose update images to apply to blade servers, through the associated service profile.

Category	Description
Adapter Firmware Packages	Ethernet firmware
Storage Controller Firmware Packages	LSI RAID controller
Fibre Channel Adapters Firmware Packages	HBA firmware
BIOS Firmware Packages	Server BIOS
HBA Option ROM Packages	HBA boot logic BIOS
Board Controller Packages	Cisco IMC firmware

Host Firmware Selection

Host Firmware Selection

- Expand categories to select individual component firmware packages.

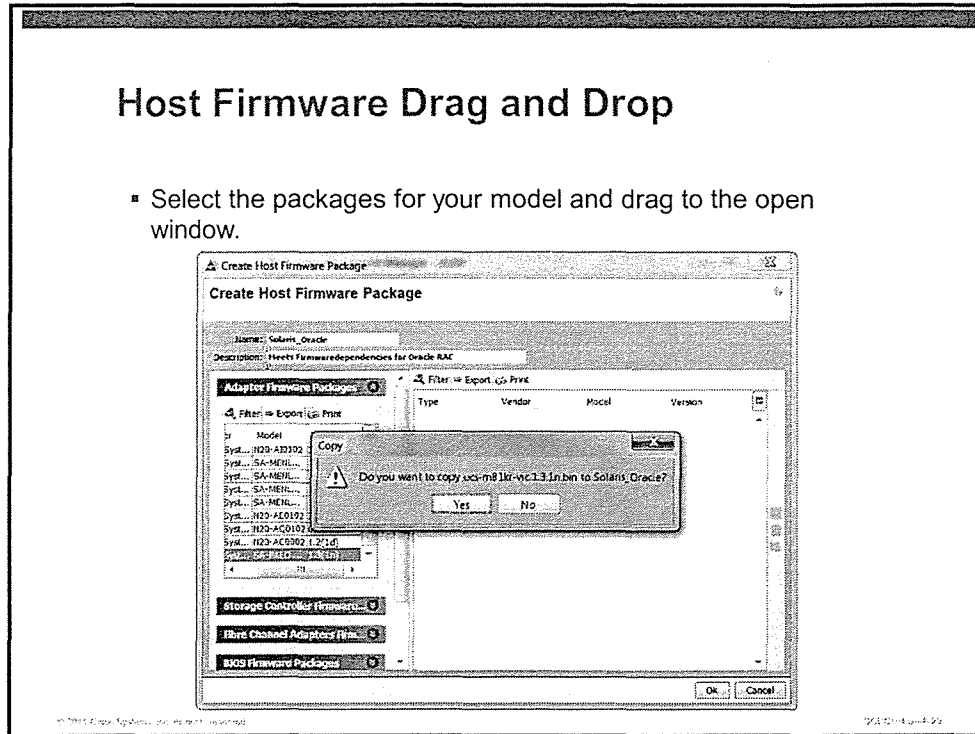


Click the double down-arrow icon and expand the first firmware category.

Host Firmware Drag and Drop

Host Firmware Drag and Drop

- Select the packages for your model and drag to the open window.



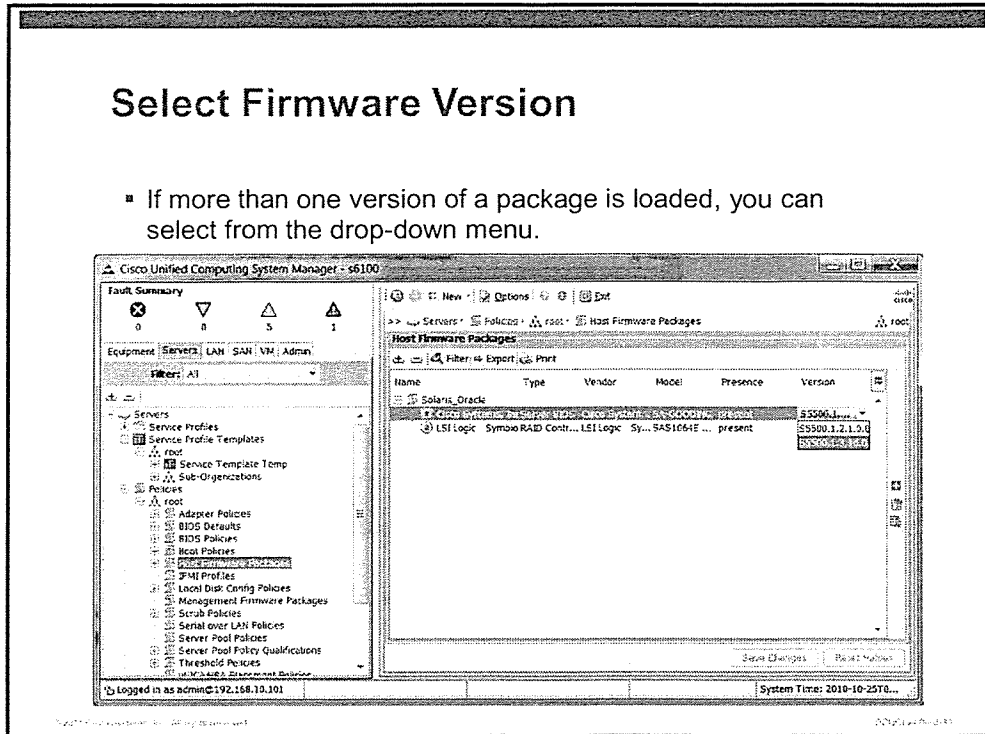
Click and drag firmware components from the category pane into the right-hand pane. The pop-up Copy dialog box in this example shows that you are copying the firmware image for the Cisco UCS M81KR Virtual Interface Card (VIC).

Continue expanding categories and copying firmware images until the package for your application is complete.

Select Firmware Version

Select Firmware Version

- If more than one version of a package is loaded, you can select from the drop-down menu.

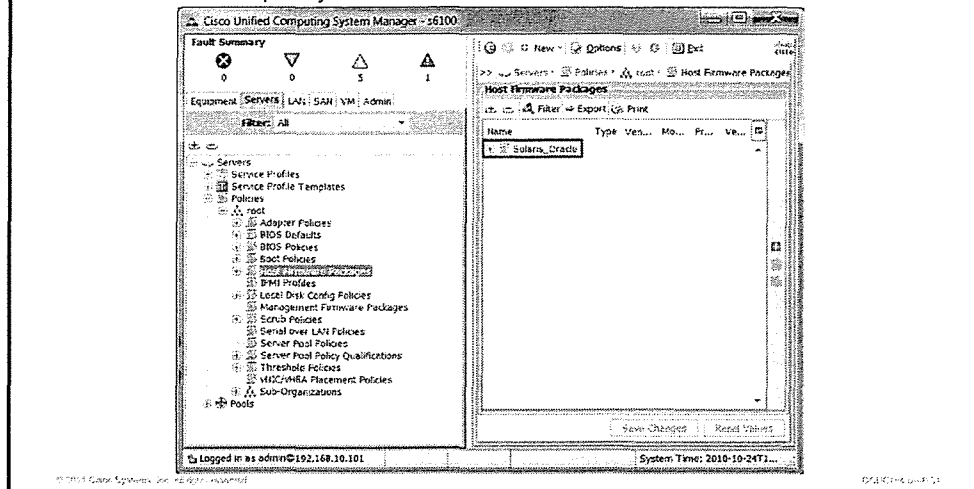


In some cases, you might need to choose from multiple versions of the firmware element that is populated in the new policy. Click the drop-down box to the right of the firmware name to determine which versions are available. Click the Save Changes button to complete the firmware package.

Host Firmware Package Ready to Apply

Host Firmware Package Ready to Apply

- The Solaris_Oracle firmware package can now be applied to a service policy.



The example shows the completed policy Solaris_Oracle. You will learn how to associate this former policy with the service profile in the module “Server Resources Implementation.”

Note When a service profile with a firmware package is associated with a blade server, direct firmware updates for those components are no longer possible.

Differences Between Firmware Processes of Cisco UCS 61x0 Fabric Interconnects and Cisco IMC, IOM, and Adapter

This topic summarizes the differences between firmware update capabilities.

Component Firmware Update Differences

Component Firmware Update Differences	
Component	Update Requirements
Fabric Interconnect	Activate the subordinate cluster member and allow it to resume normal operation. Then activate the primary fabric interconnect.
Cisco USC Manager	No backup image. Activate on active management node. Automatically synchronized to subordinate node.
Cisco IMC, IOM, Ethernet	These components have two flash partitions for firmware: startup and backup. You can update and activate the backup partition without disrupting the operation of the component.
BIOS, HBA, HBA option ROM, RAID controller	Must be updated with the service profile bound to a host firmware update policy.

The table summarizes the primary differences between update types. Cisco UCS Manager in the fabric interconnects automatically restarts at activation. IOMs, adapters, and Cisco IMC instances have two flash partitions for firmware updates. Updating and activating the backup partition during production operations are safe. Some components can be updated only from a firmware package that is associated with the service profile or from within the operating system that runs on the blade server.

Summary

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

Summary

- Cisco UCS B-Series firmware packages can be downloaded from Cisco.com.
- Most Cisco UCS B-Series firmware can be updated manually, on a component-by-component basis.
- The backup image of the Cisco IMC, IOM, and mezzanine adapter firmware can be updated safely any time and activated in a maintenance window.
- Upgrade of the fabric interconnect cluster and Cisco UCS Manager is the last step in a major update.
- Firmware updates to adapter HBA option ROM, BIOS, and RAID controllers must be implemented via the service profile.
- The Cisco IMC, IOM, and mezzanine adapters have a primary and standby flash partition for the firmware images.

© 2011 Cisco Systems, Inc. All rights reserved.

UCS-1000-08-01

Module Summary

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

Module Summary

- Cisco UCS RBAC allows administrators to select from a range of local and remote AAA tools and organizations to administratively divide policy and provide for granular control.
- The startup and shutdown procedure for elements of Cisco Unified Computing System depend on the individual component.
- Cisco UCS Manager offers the ability to easily perform configuration backups and import operations, as well as disaster-recovery backups used to restore an entire system.
- Cisco UCS Fabric Interconnects can form a high-availability cluster and can leverage the chassis serial EEPROM to resolve split-brain issues in the cluster and ensure continuous operation.
- System events and faults are valuable monitoring and troubleshooting tools that can be viewed within Cisco UCS Manager and exported to external files and file systems.
- Cisco Unified Computing System breaks tradition with previous blade server systems and provides a robust set of tools for managing device firmware.

This module examined a broad range of functional areas that are associated with system management and maintenance.

Role-based access control (RBAC) consists of local and remote authentication, authorization, and accounting (AAA) controls. RBAC can combine the organizational hierarchy to provide granular access control to identity pools, service profiles, and policies. RBAC and organization elements can be used in isolation or in combination.

The startup procedure for Cisco Unified Computing System (UCS) 6100 Series Fabric Interconnects in a Cisco UCS 5108 server chassis is a matter of applying power. Blade servers can be booted from the power button on the front panel or, as is more common, through a service profile. Blade servers can be powered off via the front panel reset button, service profile, or operating system. Cisco UCS 6100 Series Fabric Interconnects in the Cisco UCS 5108 server chassis were designed for continuous operation and do not include power switches.

Cisco UCS Manager includes two facilities for backing up system data. A FULL state backup includes the Cisco UCS Manager database as well as FULL state data for all managed objects in the system. A FULL state backup can be used to restore an entire Cisco Unified Computing System. Configuration backups are also available to quickly and easily back out of a misconfiguration or accidental deletion of Cisco Unified Computing System configuration elements.

Cisco UCS 6100 Series Fabric Interconnects are designed to operate in a high-availability cluster. A private network port channel is provided by two dedicated Gigabit Ethernet interfaces that are labeled L1 and L2 on each fabric interconnect. If there is a private network failure, then a split-brain condition exists and there is a risk of both management nodes asserting themselves as the active management node. The fabric interconnects use the server chassis serial EEPROM to resolve this split-brain condition.

The fault console provides real-time fault event reporting for all elements of Cisco Unified Computing System. This reporting provides valuable information that is needed to effectively troubleshoot hardware and connectivity issues as they arise. Fault data can be exported either in a comma-separated values (.csv) format or to a remote syslog server. The audit log records every configuration action that Cisco UCS Manager users take, whether from a command-line interface (CLI) or GUI.

A key design criterion of Cisco Unified Computing System is to simplify firmware updates for system components. Cisco introduced the groundbreaking concept of allowing firmware versions to be bound to a policy that is associated with the given server. If the service profile is moved to a different blade server in the future, no firmware remediation is required for normal operation. This greatly reduces the time to recover from blade failure.

References

For additional information, refer to these resources:

- Gai, S., T. Salli, et al. *Project California: a Data Center Virtualization Server*. Raleigh, NC: Lulu.com; 2009.
- Cisco Systems, Inc. *Cisco UCS Manager GUI Configuration Guide, Release 1.3(1)—Chassis Discovery Policy*.
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCS_M_GUI_Configuration_Guide_1_3_1_chapter1.html#concept_40AFE09861FA4D02A9879856A1411FAC.
- Cisco Systems, Inc. *Cisco UCS SMASH Reference Guide*.
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/utilities/smash/reference/guide/ucs_smash_reference.html.
- Cisco Systems, Inc. *Cisco UCS Manager CLI Configuration Guide, Release 1.3(1)—Uplink Ethernet Port Channels*.
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/1.3.1/CLI_Config_Guide_1_3_1_chapter5.html#concept_15B479F615A44205BB3851188C06F328.
- Cisco Systems, Inc. *Cisco UCS Manager CLI Configuration Guide, Release 1.3(1)—Service Profiles that Override Server Identity*.
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/1.3.1/CLI_Config_Guide_1_3_1_chapter25.html#concept_472B3819CBB04CC9AC60044602D2C7CA.
- Cisco Systems, Inc. *Cisco Fabric Manager Interfaces Configuration Guide—Configuring N Port Virtualization*.
http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/5_0/configuration/guides/int/fm/npv.html.
- Cisco Systems, Inc. *Cisco UCS Manager GUI Configuration Guide, Release 1.3(1)—Configuring Named VSANs*.
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCS_M_GUI_Configuration_Guide_1_3_1_chapter20.html.

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) On which three tabs can organizations be created? (Choose three.) (Source: “Configuring Role-Based Access Control”)
- A) Equipment
 - B) Server
 - C) LAN
 - D) SAN
 - E) VM
 - F) Admin
- Q2) How many built-in user roles are in Cisco UCS Manager? (Source: “Configuring Role-Based Access Control”)
- A) 1
 - B) 5
 - C) 9
 - D) 10
 - E) 15
 - F) 20
- Q3) Which three protocols can be configured for remote authentication in Cisco UCS Manager? (Choose three.) (Source: “Configuring Role-Based Access Control”)
- A) RADIUS
 - B) TACACS
 - C) TACACS+
 - D) local
 - E) LDAP and Active Directory
 - F) Kerberos
- Q4) What is the maximum number of local users? (Choose three.) (Source: “Configuring Role-Based Access Control”)
- A) 5
 - B) 10
 - C) 15
 - D) 20
 - E) 25
 - F) 30
 - G) 35
 - H) 40
- Q5) What is required to authorize a remotely authenticated user in Cisco UCS Manager? (Source: “Configuring Role-Based Access Control”)
- A) role-attribute mapping
 - B) user mapping object
 - C) role mapping object
 - D) user mapping policy
 - E) role mapping policy

- Q6) Which two conditions occur when the active fabric interconnect is shut down? (Choose two.) (Source: “Implementing Cisco Unified Computing System Startup and Shutdown Procedures”)
- A) The fabric A data plane stops forwarding.
 - B) The redundant data plane stops forwarding.
 - C) Hosts with hardware failover enabled recover with fabric failover.
 - D) The management plane shuts down in both fabrics.
 - E) Hosts that are configured with only NIC teaming lose connectivity.
- Q7) Which statement describes the best practice for shutting down a blade server? (Source: “Implementing Cisco Unified Computing System Startup and Shutdown Procedures”)
- A) Right-click the server on the Equipment tab and choose Shutdown.
 - B) Right-click the server on the Server tab and choose Shutdown.
 - C) Choose the service profile on the Server tab and then choose Shutdown.
 - D) Follow the shutdown procedure in the operating system or hypervisor.
- Q8) What is the result of momentarily pressing the hardware reset button on the faceplate of a blade server? (Source: “Implementing Cisco Unified Computing System Startup and Shutdown Procedures”)
- A) The result is the same as when you remove the blade from its slot and then reinstall it.
 - B) The result is the same as when you push the reset button on a standalone server.
 - C) This action immediately powers down the server.
 - D) By default, this button has no effect unless it is enabled in the BIOS.
 - E) This action sends an ACPI call to gracefully shut down the operating system.
- Q9) What is the result of pressing the hardware reset button on the faceplate of a blade server for at least 4 seconds? (Source: “Implementing Cisco Unified Computing System Startup and Shutdown Procedures”)
- A) The result is the same as when you remove the blade from its slot and then reinstall it.
 - B) The result is the same as when you push the reset button on a standalone server.
 - C) This action immediately powers down the server.
 - D) By default, this button has no effect unless it is enabled in the BIOS.
 - E) This action sends an ACPI call to gracefully shut down the operating system.
- Q10) Which process powers up a Cisco UCS 5108 server chassis? (Source: “Implementing Cisco Unified Computing System Startup and Shutdown Procedures”)
- A) Apply power to one or more power supplies.
 - B) Apply power to one or more power supplies, and then set the master switch to the ON position.
 - C) Apply power to one or more power supplies, and then make a connection from the IOMs to the fabric interconnects.
 - D) Apply power to one or more power supplies, and then set the power supply switches on each enabled power supply to the ON position.

- Q11) Which three backup types are valid for Cisco Unified Computing System? (Choose three.) (Source: "Backing up and Restoring the Cisco UCS Manager Database")
- A) scheduled
 - B) FULL state
 - C) disaster recovery
 - D) incremental
 - E) logical
 - F) system
- Q12) Which process applies a FULL state backup? (Source: "Backing up and Restoring the Cisco UCS Manager Database")
- A) From the All item in the Admin tab, choose Import and then enter the filename.
 - B) From the All item in the Equipment tab, choose Import and then enter the filename.
 - C) From the Equipment tab, choose Import and then enter the filename.
 - D) From the Equipment tab, choose Import and then enter the filename.
 - E) From the serial console, set the setup type to restore.
- Q13) Which three items are backed up in a logical backup? (Choose three.) (Source: "Backing up and Restoring the Cisco UCS Manager Database")
- A) service profiles and templates
 - B) VLAN and VSAN configuration
 - C) organizations and locales
 - D) AAA configuration and RBAC
 - E) user database
 - F) Cisco Unified Computing System configuration
- Q14) Which three items are backed up in an all-configuration backup? (Choose three.) (Source: "Backing up and Restoring the Cisco UCS Manager Database")
- A) LDAP database
 - B) AAA configuration and RBAC
 - C) RADIUS user database
 - D) TACACS+ database
 - E) TACACS database
 - F) local user database
 - G) VLAN and VSAN configuration
- Q15) In which format are Cisco UCS Manager backup files eligible for import operation? (Source: "Backing up and Restoring the Cisco UCS Manager Database")
- A) .txt
 - B) .csv
 - C) .xml
 - D) .tar.gz
- Q16) Which two types of cable are certified for complete bandwidth gigabit cluster communications? (Choose two.) (Source: "Managing High Availability")
- A) EIA/TIA Category 5
 - B) EIA/TIA Category 5e
 - C) EIA/TIA Category 6
 - D) EIA/TIA Category 6a
 - E) EIA/TIA Category 6e

- Q17) Which command displays the serial number of the Cisco UCS 5108 server chassis that is used to reconcile a split-brain condition in the cluster? (Source: "Managing High Availability")
- A) **show cluster seeprom chassis**
 - B) **show cluster lead**
 - C) **show cluster**
 - D) **show cluster state-extended**
 - E) **show cluster chassis seeprom**
 - F) **show cluster extended-state**
 - G) The chassis can be determined only in the Cisco UCS Manager GUI.
- Q18) Which two CLI shells can access cluster information? (Choose two.) (Source: "Managing High Availability")
- A) adapter shell
 - B) Cisco UCS Manager CLI shell
 - C) local management shell
 - D) Cisco NX-OS shell
 - E) I/O manager shell
- Q19) What is the primary risk of the split-brain partition in space condition? (Source: "Managing High Availability")
- A) Cisco UCS Manager database transactions are duplicated on both fabric interconnects.
 - B) When each fabric interconnect detects the loss of a peer, the management plane switches off until its peer returns.
 - C) Both fabric interconnects believe that they are the active management node.
 - D) STP introduces a delay before the redundant data plane can become active.
 - E) Both data planes become active forwarders and introduce a loop in the Layer 2 topology.
- Q20) Which method does a fabric interconnect use to resolve the split-brain partition in time condition? (Source: "Managing High Availability")
- A) The IOM of both peers reads the serial EEPROM on the fabric interconnects to determine whether the database version is out of date.
 - B) The IOM of both peers reads the serial EEPROM version from flash to determine whether the database version is out of date.
 - C) The chassis management controller reads the database version from its partition of the serial EEPROM and becomes active if its database version is greater than or equal to that value.
 - D) The chassis management controller reads the database version from the peer partition of the serial EEPROM and becomes active only if its database version is greater than or equal to that value.
- Q21) Which two fault severities are not listed on a global fault summary? (Choose two.) (Source: "Monitoring System Events")
- A) Info
 - B) Warning
 - C) Condition
 - D) Major
 - E) Critical
 - F) Minor

- Q22) Which fault state indicates that a fault stops flapping before the end of the flapping timer? (Source: "Monitoring System Events")
- A) Cleared
 - B) Soaking
 - C) Open
 - D) Flapping
 - E) Resolved
 - F) Closed
- Q23) Which log can you check to determine who deleted the service profile? (Source: "Monitoring System Events")
- A) SEL
 - B) syslog
 - C) fault log
 - D) OBFL
 - E) audit Log
 - F) AAA accounting log
- Q24) Which three entities have transition states that are managed by FSM? (Choose three.) (Source: "Managing High Availability")
- A) audit log
 - B) VLAN creation
 - C) VSAN creation
 - D) service profile association
 - E) policies
 - F) firmware downloads
 - G) IOM
- Q25) Which Smart Call Home element allows the administrator to be selective about which events generate a Call Home message? (Source: "Managing High Availability")
- A) policy
 - B) profile
 - C) threshold
 - D) ACL
 - E) wizard
- Q26) Which firmware-upgradeable Cisco Unified Computing System element benefits from the activation option? (Source: "Managing and Upgrading Cisco UCS B-Series Firmware")
- A) Cisco UCS Manager
 - B) fabric interconnect
 - C) mezzanine adapter
 - D) Cisco IMC
 - E) IOM
 - F) BIOS

- Q27) In which order should you update and activate new firmware components? (Source: "Managing and Upgrading Cisco UCS B-Series Firmware")
- A) Cisco UCS Manager, fabric interconnects, IOM, adapter, Cisco IMC, BIOS
 - B) fabric interconnects, Cisco UCS Manager, IOM, adapter, Cisco IMC, BIOS
 - C) BIOS, adapter, Cisco IMC, IOM, Cisco UCS Manager, fabric interconnects
 - D) adapter, Cisco IMC, IOM, Cisco UCS Manager, fabric interconnects
 - E) Cisco UCS Manager, fabric interconnects, IOM, adapter, Cisco IMC
 - F) adapter, Cisco IMC, IOM, fabric interconnects, Cisco UCS Manager
 - G) Cisco IMC, adapter, IOM, Cisco UCS Manager, fabric interconnects
- Q28) Which three firmware-updatable Cisco Unified Computing System components have backup and startup flash partitions? (Choose three.) (Source: "Managing and Upgrading Cisco UCS B-Series Firmware")
- A) fabric interconnect
 - B) IOM
 - C) Cisco UCS Manager
 - D) BIOS
 - E) adapter
 - F) Cisco IMC
 - G) HBA
 - H) HBA option ROM
- Q29) Which three components can update firmware only through a firmware policy that is attached to a service profile? (Choose three.) (Source: "Managing and Upgrading Cisco UCS B-Series Firmware")
- A) fabric interconnect
 - B) IOM
 - C) Cisco UCS Manager
 - D) BIOS
 - E) adapter
 - F) Cisco IMC
 - G) HBA
 - H) HBA option ROM
- Q30) Which three selections are available in host firmware policy? (Choose three.) (Source: "Managing and Upgrading Cisco UCS B-Series Firmware")
- A) BIOS firmware packages
 - B) adapter firmware packages
 - C) IOM firmware packages
 - D) Cisco IMC firmware packages
 - E) board controller firmware packages
 - F) Cisco UCS Manager firmware packages

Module Self-Check Answer Key

- Q1) B, C, D
- Q2) C
- Q3) A, C, E
- Q4) H
- Q5) A
- Q6) A, C
- Q7) D
- Q8) E
- Q9) C
- Q10) A
- Q11) B, E, F
- Q12) E
- Q13) A, B, C
- Q14) B, F, G
- Q15) C
- Q16) C, D
- Q17) F
- Q18) B, C
- Q19) C
- Q20) D
- Q21) A, C
- Q22) B
- Q23) E
- Q24) D, E, G
- Q25) B
- Q26) E
- Q27) D
- Q28) B, E, F
- Q29) D, G, H
- Q30) A, B, E

Survey of Cisco Data Center Unified Computing Implementation E-Learning

Overview

The Cisco Data Center Unified Computing Implementation (DCUCI) course is designed to satisfy the needs of a diverse range of skill-sets and experience. Approximately 10 hours of Cisco Unified Computing System (UCS) and virtualization foundational topics are included in an e-learning format. It is recommended that all students watch the e-learning component before attending the instructor-led training (ILT). Exam topics for the DCUCI certification exam include material from the ILT and e-learning materials.

Objectives

Upon completing this lesson, you will demonstrate your mastery of Cisco UCS and virtualization fundamentals. The review will encompass the following subject areas:

- Challenges of data center server management
- Cisco Unified Computing System
- Cisco UCS C-Series hardware components
- Cisco UCS C-Series hardware installation
- Cisco UCS B-Series hardware components
- Cisco UCS B-Series architecture and features
- Cisco UCS use cases
- Server virtualization
- Cisco Nexus 1000V Series Switches
- VMware Ethernet networking
- Cisco Nexus 1000V architecture

Review the Benefits of Cisco UCS

This topic reviews the benefits of the Cisco UCS.

Differentiate Between Stages of Data Center Evolution

This subtopic reviews data center evolution.

Answer: Differentiate Between Stages of Data Center Evolution		
Scale Up	Scale Out	Scale In
Large monolithic system	Commoditized servers	Blade servers
Many CPUs	Few CPUs	Multicore CPUs
Proprietary hardware and operating system	Commoditized operating system	Commoditized operating system
Many applications run on one system	One application per server	One application per virtual machine

Over the last 20 years, the data center has undergone dramatic changes. Some of the underlying reasons for these changes are based on server evolution.

Server evolution could be categorized by the hardware and methodology that are used to accommodate the growing demands of applications and users.

To illustrate the server evolution, the process is divided into three distinct approaches:

- Scale Up
- Scale Out
- Scale In

In the 1990s, data centers used computer systems that were large, monolithic enclosures. These were referred to as supercomputers. Some of the more popular manufacturers of these large devices were companies including Sun, DEC, HP, and IBM. These systems traditionally used proprietary hardware and operating systems.

The architectural design of these large systems could scale up to 64 CPUs. This high processing capability allowed many applications to run simultaneously while supporting numerous users. Although these monolithic servers could service many applications and users, components for these systems were expensive, which made the total expense of ownership very costly. Furthermore, because of the large number of dependent applications and users, these systems created a significant failure domain.

In the early 2000s, the data center experienced a significant shift in the type of computing system used for processing applications. The next change in computing resources came in the form of commoditized servers, also referred to as tower and rack-mounted servers. These smaller servers cost significantly less than the monolithic systems. The major difference was that these servers had fewer processing resources, perhaps only a single CPU. Because these servers had limited processing capabilities, they were traditionally dedicated to support single applications per server.

Because of the way applications are distributed across many small servers, this is referred to as the Scale Out approach. The increase in server hardware added to overall operational costs. More servers meant higher costs for space, cabling, power, and cooling. Additionally, servers running only single applications were underutilized. This, of course, was an inefficient use of hardware, which can have a negative impact on the return on investment (ROI) for a company.

Since the mid 2000s, IT has begun to move away from traditional tower or rack-mounted servers in favor of blade servers. Tower and rack-mounted servers require more space and need their own power supply, networking, and SAN cables. For smaller data centers, these infrastructure requirements are not problematic, but in a large data center, these requirements result in increasing complexity and cost of ownership.

By putting the computing resources of a server in a blade server form factor within a chassis enclosure, administrators gain these advantages:

- Maximum use of physical space
- Shared power distribution
- Shared networking and storage access
- More efficient power and cooling

This form of hardware consolidation is the primary concept of the Scale In approach.

Select Four Management Challenges in a Blade Server Environment

Answer: Select Four Management Challenges in a Blade Server

- ✓ Additional cabling requirements
- ✓ Additional power requirements
- Limited operating system choices
- ✓ Additional cooling requirements
- ✓ Management complexity
- Limited scalability

As the physical density of a blade environment increases relative to rack-mounted servers, there may be more power and cooling required in the same physical space. This can cause challenges in powering and cooling the data center.

The relatively high density of compute resources in a blade environment often requires significantly more bandwidth and cabling.

Each chassis in a blade environment typically will have a management IP address used for monitoring system and blade health. Additionally, each local LAN or SAN switch, if installed, also adds management overhead and overall network design challenges.

As computing capacity increases within the data center, so does complexity. Blade servers solve many issues, but they also bring an additional point of management per chassis into the data center. Several independent systems must be managed, including LAN, SAN, servers, and storage. These separate resources must be managed at each network layer—access, aggregation, and core. Typically, these resources are managed by individual teams and can be monitored by using proprietary system monitoring tools. Often, customers must use multiple monitoring applications to cover all aspects of the data center.

Review of Cisco UCS

This section provides a review of UCS general topics.

List Two Benefits Made Possible by Unified I/O

Answer: List Two Benefits Made Possible by Unified I/O

- Cabling consolidated on Fibre Channel transport
- ✓ Cabling consolidated on Ethernet transport
- Cabling consolidated on InfiniBand transport
- ✓ 10-Gb/s Ethernet
- 8-Gb/s Fibre Channel
- 40-Gb/s InfiniBand

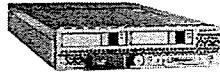
By consolidating the I/O infrastructure for storage, TCP/IP, and interprocess communication (IPC) traffic, data centers can reduce the number and type of devices that require power, cooling, and management.

Consolidated I/O solutions should maintain the same management processes as are available to each network type. Having to replace software, skill sets, and procedures would be too disruptive for the technology to adopt.

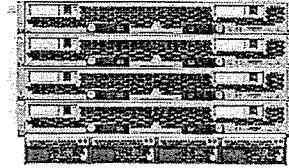
However, most importantly, the consolidated I/O solution must satisfy the physical and logical (bandwidth, throughput, delay, congestion, and management) requirements that the individual protocols support. For example, Ethernet is considered a “lossy” protocol because it relies on higher-level protocols, such as IP and TCP, to respond to dropped or lost packets. Fibre Channel, on the other hand, is a “lossless” protocol because none of the layers of the Fibre Channel stack can tolerate or respond to dropped or lost frames. Fibre Channel has a link-level buffer-to-buffer signaling mechanism that allows transmitters to know whether receivers can receive frames. Fibre Channel transports Small Computer Systems Interface (SCSI) in SAN environments and SCSI does not tolerate lost data in a timely or efficient manner. A consolidated I/O solution, therefore, must account for and support both lossy and lossless protocols.

Name the Components of Cisco UCS

Answer: Name the Components of Cisco UCS



UCS B200



UCS 5108



UCS B250



UCS 2104



UCS B440

The purpose of this question is to gauge general knowledge of Cisco UCS B-Series hardware.

Differentiate Between IEEE Standards of Data Center Bridging

Answer: Differentiate Between IEEE Standards of Data Center Bridging

IEEE Standard	Protocol	Purpose
802.1Qbb	Priority Flow Control	Enable multiple traffic types to share the same link (using CoS values)
802.1Qaz	Enhanced Transmission Selection	Manage bandwidth between different types of traffic on same link
802.1Qau	Congestion Management	Manage end-to-end congestion
802.1Qab	DCBX	Discover and negotiate DCB capabilities

Priority flow control (PFC) provides a link-level flow-control mechanism that can be controlled independently for each priority. The goal of this mechanism is to ensure zero loss due to congestion in data center bridging (DCB) networks.

Bandwidth management, also referred to as enhanced transmission selection (ETS), provides a common management framework for assignment of bandwidth to traffic classes.

Congestion notification provides end-to-end congestion management for protocols that do not already have built-in congestion control mechanisms (for example, Fibre Channel over Ethernet [FCoE]). Congestion notification is also expected to benefit protocols such as TCP, which have native congestion management, because it reacts to congestion more efficiently. Using congestion notification is an alternative to using PFC on a hop-by-hop basis.

Data Center Bridging Capacity Exchange Protocol (DCBCXP) is a discovery and capability exchange protocol. It is used for conveying capabilities and configuration of features between neighbors to ensure consistent configuration across the network. This protocol is expected to leverage functionality that is provided by 802.1ab (Link Layer Discover Protocol [LLDP]).

Select Four Features of FCoE

Answer: Select Four Features of FCoE

- ✓ Unified fabric
- Limited performance
- ✓ High performance
- ✓ Reduced cabling
- Increased cabling
- Proprietary
- ✓ Standards-based

The protocol behind the unified fabric is Fibre Channel over Ethernet (FCoE). FCoE technology coexists with Fibre Channel fabric, allowing IT organizations to implement incrementally, while reaping business benefits, including the following:

- FCoE reduces the number of network interface cards (NICs) and cables that customers need to purchase, reducing costs and simplifying cable management.
- Because FCoE follows the same model as Fibre Channel, storage administrators can manage their fabrics in the same manner that they always have.
- FCoE does not have a stateful gateway, but simply maps Fibre Channel traffic onto lossless Ethernet, resulting in performance benefits over technologies that require a gateway.
- Significant savings in the amount of power that is expended per rack results when FCoE is employed. By consolidating I/O, less power is expended on NICs and cables. Companies also save power on the cooling expended to compensate for the heat produced.

Review of Cisco UCS C-Series Hardware Components

This topic focuses on Cisco UCS C-Series hardware specifications and capabilities.

Select Two Chassis That Can Support at Least 256-Mb RAM and RAID 50

Answer: Select Two Chassis That Can Support at Least 256 Mb RAM and RAID 50

- C200
- C210
- ✓ C250
- ✓ C460

The Cisco UCS C-Series offers four models: C200, C210, C250, and C460.

The C200 was the first model introduced. It is a 1-rack unit (RU), rack-mount server that is designed to balance simplicity, performance, and density for production-level virtualization, web infrastructure, and other mainstream data center workloads.

The C200 supports up to two Intel Xeon 5500 Series multicore processors. With two processors, the C200 can support up to 96 GB of double data rate 3 (DDR3) memory. Also, when it comes to local storage, the C200 supports up to four internal serial attached SCSI (SAS) or Serial Advanced Technology Attachment (SATA) disk drives, for up to 2 terabytes (TB) total.

The C210 is a large internal storage model. It is designed to balance performance, density, and efficiency for workloads requiring economical, high-capacity, reliable, internal storage.

The C210 M1 supports up to two Intel Xeon 5500 Series multicore processors. With the two processors, the C210 can support up to 96 GB of DDR3 memory. When it comes to local storage, the C210 M1 can support up to 16 internal small form-factor (SFF), SAS, or SATA disk drives—up to 8 TB total.

The C250 is a large memory server that is designed to increase performance and capacity for demanding virtualization and large-data-set workloads.

The C250 M1 supports up to two Intel Xeon 5500 Series multicore processors. With the two processors, the C250 M1 can support up to 384 GB of DDR3 memory. Cisco Extend Memory Technology provides access to up to 384 GB of memory with two processors.

The C460 is a high-performance rack-mount server that is designed with the performance and reliability to power compute-intensive, enterprise-critical, standalone applications and virtualized workloads.

C460 M1 supports two or four Intel Xeon 7500 Series multicore processors, for up to 32 processing cores. Also with 64 DIMM slots of DDR3 memory, the C460 M1 can support up to 512 GB of memory. This combination allows for fast processing and a large memory footprint. This is ideal for virtualization applications. Regarding local storage, the C460 M1 supports up to 12 front-accessible, hot-swappable, 2.5-in. (6.35-cm) SAS or SATA drives.

Select Five Configurable Options for C-Series BIOS

Answer: Select Five Configurable Options for C-Series BIOS

- ✓ Time and date
- MAC addresses
- Fiber Channel WWN
- ✓ Boot order
- Cisco Integrated Management Controller IP address
- ✓ LOM PXE Boot
- Receive-side scaling
- ✓ Intel VT-d
- ✓ Hyperthreading
- Multipath I/O

The BIOS is responsible for hardware initialization. It starts with the CPU and continues on to the other chips on the motherboard. The BIOS also discovers all of the I/O devices in the system and initializes them, such as Peripheral Component Interconnect Express (PCIe) devices. It boots the operating system and configures hardware for the operating system to use.

BIOS provides these main features:

- Optional ROM to provide PCI-connected device boot
- Management of boot devices (SCSI, Fibre Channel, Network, USB)
- Processor settings
- Memory settings
- Power management

Select Two C-Series Chassis That Allow for RAID 10

Answer: Select Two C-Series Chassis That Allow for RAID 10

- C200
- C210
- ✓ C250
- ✓ C460

The Cisco UCS C200 and C210 models come with an integrated onboard SATA controller. The built-in SATA controller is the Intel ICH10R. The controller takes advantage of proven Intel RAID controller technology. It is capable of providing RAID 0 and 1. In addition, it can support up to four SATA drives. However, SAS drives are not supported on the onboard SATA controller. The onboard SATA controller is integrated on the motherboard of the C200 and C210 models.

The LSI 1064-based controller is from LSI, one of the leading manufacturers of RAID controller technology. It only takes up one PCIe slot. This adapter provides support for both RAID 0 and 1 as well as 1E, a variation of RAID 1. This adapter can support up to four SAS or SATA drives. The LSI 1064-based controller is supported on the C200 and C210 models.

The LSI 3081-based controller card can provide high throughput to internal storage arrays. The LSI 3081 can support up to eight SAS or SATA drives with eight internal 3-Gb/s ports. In addition, this RAID controller card supports both RAID 0 and 1. This is an ideal controller for servers requiring medium- to high-capacity internal storage.

The LSI 6G MegaRAID 9260-4i controller has features that can provide fault tolerance for critical data. This controller can support up to four SAS or SATA drives. It supports RAID 0, 1, 5, 6, 10, and 50. It requires only one PCIe slot and includes 512 MB of write cache. In addition, an optional battery backup can be installed. The card is supported on the C200 model.

The LSI 6G MegaRAID 9261-8i controller has features that can provide fault tolerance for critical data. This controller can support up to 16 SAS or SATA drives. It supports RAID 0, 1, 5, 6, 10, 50, and 60. This card requires only one PCIe slot and includes 512 MB of write cache. In addition, an optional battery backup can be installed. The card is supported on the C210 and C250 servers.

The LSI MegaRAID 9240-8i RAID controller can support up to 12 SAS or SATA drives. It only supports RAID 0 and 1. This card must be installed in a dedicated SAS riser PCIe slot and is supported on the C460 server.

The LSI MegaRAID 9260-8i RAID Controller is one of the higher performance adapters that can be installed in the C-Series servers. The features of this controller can provide high performance as well as fault tolerance for critical data. This controller can support up to 12 SAS or SATA drives, and can provide this with 6-Gb/s throughput per board. It currently supports RAID 0, 1, 5, 6, 10, and 50. This adapter also has the ability to perform auto resume or rebuild. These feature options can minimize the delay in reconstructing or recovering from hardware failure.

Select C-Series LAN, SAN, and Management Connectivity Options

Answer: Select C-Series LAN, SAN, and Management Connectivity Options			
Model	# Ethernet	# Fibre Channel	NIC Teaming
Cisco P81E	12	2	No – Uses Hardware Failover
Emulex OneConnect	4	2	Yes
Qlogic QLE8152	4	2	Yes
Broadcom 5709	4	0	Yes
Broadcom 57711	2	0	Yes
Emulex LPe11002	0	2	N/A
Qlogic QLE2462	0	2	N/A

The Broadcom NetXtreme II 5709 quad-port Ethernet PCIe adapter card is a converged network interface controller. It provides simultaneous connection to LAN and SAN over standard Ethernet. This adapter can improve network application performance and server redundancy with NIC teaming and failover feature. Also, the Host Bus Adapter (HBA) functionality supports iSCSI for IPv4 and IPv6, which can be used to transmit data over LANs. In addition, this device provides TCP/IP Offload Engine (TOE) for Windows, which can significantly reduce CPU utilization.

The Cisco UCS P81E Virtual Interface Card (VIC) is a virtualization-optimized Fibre Channel over Ethernet (FCoE) PCIe 2.0 x8 10-Gb/s adapter. It is designed for use with Cisco UCS C-Series rack-mount servers. The VIC is a dual-port 10-Gb Ethernet PCIe adapter that can support up to 128 PCIe standards-compliant virtual interfaces. This can be dynamically configured so that both their interface type (NIC or HBA) and identity (MAC address and world wide name [WWN]) are established using just-in-time provisioning. In addition, the Cisco UCS P81E can support network interface virtualization and Cisco VN-Link technology.

The QLogic QLE8152 is a dual port 10-Gb/s Ethernet-to-PCIe converged network adapter (CNA). Each port provides 10 Gb/s maximum throughput for high-bandwidth storage (SAN) and networking (LAN) traffic. The adapter offers complete hardware offload for FCoE protocol processing and works seamlessly with existing Fibre Channel storage. In addition, it offers complete support for TCP/IP and Ethernet performance enhancements such as priority-based flow control (802.1Qbb), jumbo frames, checksum offloads, and segmentation offloads.

QLogic SANblade QLE2462 is a dual port 4-Gb/s Fibre Channel-to-PCIe HBA. It offers 4/2/1 Gb/s autonegotiation and 150,000 IOPS per port. This adapter comes Multi-ID and N_Port virtualization ready. Also, the universal boot support manages multiple hardware platforms and boot options. In addition, this adapter is Cisco VSAN ready, which allows physical ports to be part of multiple logical networks.

The Emulex OCe10102-FX-C is a high performance 10-Gb/s FCoE adapter that consolidates traffic for networking. This adapter supports a common 10-Gb Ethernet infrastructure for unified networking and storage and extends the Cisco standards-based unified network fabric. It provides boot from LAN/SAN Fibre Channel SAN and Preboot Execution Environment (PXE).

Which C-Series Chassis Support More Than Two Power Supplies?

Answer: Which C-Series Chassis Supports More Than Two Power Supplies?

- C200
- C210
- C250
- ✓ C460

The C200 and C210 use a 650 W power supply unit with an added 5 A standby. One power supply always comes standard with the base chassis.

The Cisco UCS C250 model uses an 850 W power supply unit. Similar to the other models, one power supply unit comes standard with the base chassis. The C250 server supports two power supply units for redundancy, but the redundant unit must be ordered.

The Cisco UCS C460 uses an 850 W power supply unit. In addition, it can support up to four power supplies. If the unit is initially ordered with two processors, then two power supplies come standard with the base chassis. Up to two redundant power supplies can be ordered. However, in a four-processor configuration, four power supplies come standard with the base chassis and no extra power supplies are needed.

Review of Installing Cisco UCS C-Series Hardware

This topic reviews installation of Cisco UCS C-Series hardware.

Select Two C-Series Rack-Mounting Requirements for Physical Enclosure

Answer: Select Two C-Series Rack Mounting Requirements for Physical Enclosure

- 19" (48.3cm) Relay Rack
- ✓ 19" (48.3cm) Four-Post Rack
- Round hole only
- Square hole only
- ✓ Round or square hole

Like Cisco UCS B-series components, C-series hardware requires mounting in a 19-inch (48.3-cm) four-post rack or cabinet. Unlike the B-series, however, C-series mounting brackets can be installed in a rack or cabinet with square or round holes.

Select Four Steps in the Process of Opening the Server Enclosure

Answer: Select Four Steps in the Process of Opening a C-Server Enclosure

- ✓ Remove all power cords
 - Remove from rack
- ✓ Remove Philips screws ***
 - Press release button and slide the cover forward
- ✓ Press release button and slide the cover rearward
- ✓ Lift off cover

There are up to four steps that are required to open a C-series server enclosure:

- To reduce the risk of electrical shock, remove all power cords.
- On C200 M1 and C210 M1, remove the Philips screws that hold the cover in place.
- Press the release button or buttons and slide the cover to the rear.
- Lift off the cover of the chassis.

Note	Though it is not necessary to remove the chassis from the rack, a ladder may be required to reach the top of the enclosure.
-------------	---

Select Two ESD Precautions

Answer: Select Two ESD Precautions

- Cisco UCS C-Series components are not subject to ESD damage.
- Touch something metal before handling any C-Series internal component.
- Leave power cords plugged in for proper ground.
- ✓ Ground ESD wrist strap to rack.
- Surfaces like plastic and cloth provide good protection against ESD damage.
- ✓ Store components in ESD-shielded bags.

Nearly every component inside of a C-series chassis can be damaged or degraded by ESD. Always wear an ESD wrist strap that is grounded to the server chassis. Always store components that are not installed in the chassis in an ESD-shielded bag or box.

Select Minimum Cabling Required to Access Cisco IMC Console

Answer: Select Two of the Minimum Cabling Requirements for Accessing Cisco IMC Console

- ✓ USB keyboard
- PS/2 keyboard
- USB mouse
- PS/2 mouse
- ✓ VGA monitor
- LOM Ethernet

A USB keyboard and VGA monitor are required for initial access to any C-series server. This connection is required to access the Cisco Integrated Management Controller BIOS console to program IP addressing information required for remote access. When the Cisco Integrated Management Controller is available on the network, remote keyboard, video, mouse (KVM) access is available.

Review of Cisco UCS B-Series Hardware Components

This topic reviews Cisco UCS B-Series hardware components.

Select Six Components of the Cisco UCS 6100 Series Fabric Interconnect

Answer: Select Six Components of the Cisco UCS 6100 Series Fabric Interconnect

- ✓ SFP module
- ✓ SFP+ module
- ✓ 6-port 10-GE module
 - 8-port 10-GE module
- ✓ 4-port 10-GE Fibre Channel combo module (1, 2, 4, 8 Gb/s)
 - 4-port 10-GE Fibre Channel combo module (1, 2, 4, 8 Gb/s)
- ✓ 6-port Fibre Channel module (1, 2, 4, 8 Gb/s)
 - 6-port Fibre Channel module (1, 2, 4 Gb/s)
- ✓ 8-port Fibre Channel module (1, 2, 4 Gb/s)

Small form-factor pluggable plus (SFP+) modules are required for external 10-Gb Ethernet connectivity to the aggregation layer of the network. SFP modules are required for Fibre Channel connectivity to Cisco Multilayer Director Switch (MDS) switches.

The Cisco UCS 6100 Series is equipped to support several expansion module options. The expansion modules provide connectivity into your enterprise Ethernet LAN and Fibre Channel SAN networks. There are currently three expansion modules from which to choose: Fibre Channel-only, combination Fibre Channel and Ethernet, and Ethernet-only.

- **Fibre Channel-only:** The Fibre Channel-only expansion module contains eight SFP ports that support 1-, 2-, and 4-Gb/s Fibre Channel. The Fibre Channel module provides six ports of 1-, 2-, 4-, and 8-Gb/s native Fibre Channel using the SFP or SFP+2.
- **Combination Fibre Channel and Ethernet:** The combination expansion module contains four SFP+ ports that support 10-Gb Ethernet and four SFP ports that support 1-, 2-, and 4-Gb/s Fibre Channel.
- **Ethernet-only:** The Ethernet-only expansion module contains six SFP+ ports that support 10-Gb Ethernet.

Define the Purpose of Internal Components of the Cisco UCS 2104 IOM

Answer: Define the Purpose of Internal Components of the Cisco UCS 2104 IOM

Component	Purpose
I/O MUX	Multiplex 10GbaseKR connection from server blades to fabric interconnect
Chassis management controller (CMC)	Responsible for chassis discovery, sensor and threshold monitoring, and fan speed control
Chassis management switch (CMS)	Connects I/O MUX and CMC to Cisco Integrated Management Controller chip on servers

The Cisco UCS 2104XP I/O module (IOM) also manages the chassis environment—the power supply and fans as well as the blades—with the fabric interconnect, which eliminates the need for separate chassis management modules.

This management is performed by a chassis management controller (CMC). The CMC collects status data from the IOM using the Intelligent Platform Management Interface (IPMI) protocol over the inter-integrated circuit (I2C) serial bus. This information is then communicated to the management node using the Ethernet server link. The CMC also serves as a proxy for the Cisco UCS Manager to the blade servers for certain functionality. It has a role in the high-availability protocols. Also, if two IOM are present in a chassis, they will cluster in an active-passive configuration.

Moreover, the CMC performs the following functions:

- Controls the chassis fan
- Monitors and logs fan speed
- Monitors and logs ingress and egress temperatures
- Powers up and down power supplies
- Monitors and logs voltages, currents, and temperatures inside the chassis
- Detects presence, insertion, and removal of Cisco UCS blades
- Reads the IDs of the chassis, Cisco UCS blades, and IOM

Another important component of the Cisco 2104 IOM is the chassis management switch (CMS). The CMS provides connectivity to the Cisco Integrated Management Controller (IMC) on each server blade. The CMS has eight 100-Mb/s dedicated connections to the Cisco IMC. In addition, the CMS has a 1-GE connection to the I/O MUX. The CMS provides the vital connection to facilitate the monitoring and configuring of each blade server.

The I/O MUX provides a bridge between server blades and fabric interconnect. The I/O MUX is the ASIC that implements the data plane of the IOM.

The I/O MUX provides the following:

- Eight 10-GE external downlink ports to server blades
- Four 10-GE external uplink ports to the fabric interconnect
- One 1-GE internal port to connect to the CMS
- One 100-Mb/s internal port towards the CMC

Describe Implementation Rationale for the Cisco UCS B-Series Mezzanine Cards

Answer: Describe Implementation Rationale for the Cisco UCS B-Series Mezzanine Cards

Adapter	Rationale for Choice
82598KR-CI	iSCSI SAN, NFS NAS, and high-speed transport in non-virtualized, non-Fibre Channel installations
M71KR-E M71KR-Q	Support for existing certified Fibre Channel drivers over FCoE
M81KR	Virtualized interface card for high Fibre Channel I/O performance and up to 128 virtual interfaces

The choice of network adapter is based on operating system, application requirements, and whether adapter virtualization is required.

Select Five Field-Installable Component Options of the Cisco UCS B-Series Blade Servers

Answer: Select Five Field Installable Component Options of the Cisco UCS B-Series Blade Servers

- Cisco Integrated Management Controller
- ✓ CPU
- ✓ RAM
- ✓ Hard drive
- ✓ Network adapter
- ✓ Battery Backup Unit (BBU)
- RAID adapter

CPU, RAM, hard drives, network adapters, and battery backup units (for the B440 RAID adapter) are currently the only field-installable components for Cisco UCS B-Series blade servers.

Review of B-Series Architecture and Features

This topic reviews Cisco UCS B-Series features and architecture.

Select Three Primary Methods to Access Cisco UCS B-Series Blade Server Management Interface

Answer: Select Three Primary Methods to Access Cisco UCS B-Series Blade Server Management Interface

- SMASH CLP
- ✓ Cisco UCS Manager CLI
- CIM XML
- SNMP
- ✓ Cisco UCS Manager GUI
- ✓ XML API

Although each element listed is technically correct, the three primary methods to access the management interface on a Cisco UCS B-Series blade server are the Cisco UCS Manager GUI, Cisco UCS Manager CLI, or the XML API.

Select Three B-Series Hardware Redundancy Components for Data and Management Planes

Answer: Select Three B-Series Hardware Redundancy Components for Data and Management Planes

- ✓ Redundant fabric interconnects
 - Redundant server chassis
 - Redundant 10-Gb/s cluster connections
- ✓ Redundant 1-Gb/s cluster connections
- ✓ Redundant I/O modules

Redundant fabric interconnects provide data plane and management plane fault tolerance for all blade chassis.

Redundant cluster connections between the fabric interconnects allow for the failure of one link without disrupting management plane operations.

Redundant I/O modules in the blade chassis provide data and management plane fault tolerance for all blade servers within the chassis.

Review of Cisco UCS Use Cases

This topic reviews Cisco UCS case studies.

Select Four Challenges of Deploying Microsoft Exchange 2010

Answer: Select Four Challenges of Deploying Microsoft Exchange 2010

- ✓ Performance
- ✓ Availability
 - Macintosh integration
- ✓ Scalability
- ✓ Decrease TCO
 - Larger mailboxes

When deploying an application like Microsoft Exchange 2010 in the data center, there is always pressure to increase the productivity of end users by using high-performance hardware and software. Also, there is the challenge of decreasing downtime and maintaining business continuity. In addition, designs must increase capacity without implementing a new architecture or management tools. Another challenge is to simplify application and infrastructure management to reduce support efforts. Most importantly, there is the goal of decreasing total cost of ownership (TCO).

Select Four Microsoft Exchange 2010 Server Roles

Answer: Select Four Microsoft Exchange 2010 Server Roles

- ✓ Hub transport server
- Spoke transport server
- ✓ Edge transport server
- ✓ Client access server
- Hub access server
- ✓ Mailbox server

With this solution, all Microsoft Exchange 2010 server roles are virtualized. There are different roles with different responsibilities. First, there is the hub transport server. It is responsible for intelligently routing messages within an Exchange Server 2010 environment. Next is the client access server, which provides the connection point for client systems. Also, there is the mailbox server that holds user mailbox information. The final server is the edge transport server. This is a dedicated server responsible for providing unsolicited email message and virus filtering.

Review of Server Virtualization

This topic reviews server virtualization concepts.

Select Four Benefits of Server Virtualization

Answer: Select Four Benefits of Server Virtualization

- ✓ Server consolidation
- ✓ Increased utilization
- Avoidance of server sprawl
- ✓ Lower costs for power and cooling
- ✓ Fewer racks needed

When server virtualization is used, operating systems and applications become independent of the underlying hardware. This allows a virtual machine to be provisioned to any physical server. Because the operating system and application are encapsulated in a virtual machine, multiple virtual machines can be run on the same physical server. Thus, server virtualization offers significant benefits when compared to physical server deployment, including the following:

- Physical hardware can be consolidated.
- Resources of a physical machine can be shared among virtual machines.
- Resource utilization is improved so that fewer resources are wasted.

A physical server configuration uses three servers that have a low average load ranging from 10 percent to a maximum of 40 percent. A virtualized solution uses just one server with three virtual machines deployed significantly better than with the former configuration. This means that the physical server average load is the sum of virtual machine average loads, which is approximately 70 percent.

Select Four Benefits of Storage Virtualization

Answer: Select Four Benefits of Storage Virtualization

- ✓ Nondisruptive data migration
- ✓ Improved utilization
 - Reduced complexity
- ✓ Fewer points of management
- ✓ Vendor interoperability

Using NetApp MultiStore has many benefits, such as the following:

- **Storage virtualization:** MultiStore partitions a single storage controller into multiple virtual controllers.
- **Delegation of management:** vFiler unit administrators can have different levels of access compared to the storage system administrator. The storage administrator is able to delegate vFiler-level permissions to vFiler departmental or tenant administrators without risk to other vFiler units or the host storage system.
- **Secure isolation:** Security is a primary concern that is associated with combining data storage onto a single hardware platform. With MultiStore, each vFiler unit can be configured to meet individual security requirements, independent of other vFiler units.
- **Data consolidation:** By utilizing Common Internet File System (CIFS) and Network File System (NFS) within vFiler units, administrators can consolidate and still maintain data separation. This produces a more efficient use of resources and reduces expenses because there are fewer resources to manage.

Select Three Benefits of Network Virtualization

Answer: Select Three Benefits of Network Virtualization

- ✓ Secure traffic isolation
- ✓ Administrative separation
- ✓ Access control
- Reduced complexity

The use of virtual device contexts (VDCs) provides a number of benefits, including the following:

- Offers a secure network partition between different user department traffic.
- Provides departments with the ability to administer and maintain their own configuration.
- Provides a device context for testing new configuration or connectivity options without impacting production systems.
- Consolidates multiple department switch platforms to a single physical platform while still maintaining independence from the operating system, administration, and traffic perspective.
- Uses a device context for network administrator and operator training purposes.

Introduction to the Data Center Access Layer

This topic describes the data center access layer.

Select Two Basic Designs for Data Center Access Layer

Answer: Select Two Basic Designs for Data Center Access Layer

- ✓ Top-of-rack (ToR)
- Middle-of-rack (MoR)
- End-of-rack (EoR)
- ✓ End-of-row (EoR)

Typical data center access layers are built in one of two ways:

- **Top-of-rack (ToR) architectures:** Switches are placed at the top of each rack for server access.
- **End-of-row (EoR) architectures:** Switches are placed at the end of server rack rows for server connections.

In a ToR network design, redundant switches are placed at the top of each server rack. This allows top-down cabling with fewer uplinks to aggregation switches. This design minimizes cabling complexity, but adds management complexity and power and cooling costs.

In an EoR design, servers are cabled to access switches placed at the end of each server row. This design increases the complexity of cabling while reducing the management complexity.

Review of VMware Ethernet Networking

This topic reviews VMware Ethernet networking.

Select Three Characteristics of the VMware vSwitch

Answer: Select Three Characteristics of the VMware vSwitch

- ✓ Forwards frames based on Layer 2 MAC address
- Forwards frames based on Layer 3 IP address
- ✓ Maintains a MAC address table
- Maintains an IP routing table
- ✓ Supports 802.1Q trunking

A VMware vSwitch is a software program that provides both internal virtual machine (VM) communication and outbound uplinks for VMs. vSwitches operate like physical switches. The VMware vSwitch provides some of these features:

- Forwards frames that are based on Layer 2 information using MAC addresses
- Maintains a MAC address table
- Supports internal switching for virtual machines
- Tags frames with a VLAN ID using 802.1Q tagging
- Supports port channels for active-active NIC teaming only

Select Three Limitations of the VMware vSwitch

Answer: Select Three Limitations of the VMware vSwitch

- ✓ Lack of access control
- Complex configuration
- ✓ Difficulty monitoring VM-to-VM communication
- ✓ vSwitch configuration does not move during vMotion

The vSwitch provides basic connectivity between virtual machines and physical switches, but this is not a perfect solution. The vSwitch does not provide the capability of creating access control lists (ACLs) to filter virtual machine communications. The vSwitch also does not provide a flexible facility for monitoring virtual machine-to-virtual machine traffic within the same vSwitch. vSwitch configurations have to be manually synchronized on a host-by-host basis because network configuration does not move with the virtual machine during vMotion.

Select Two VMware DVS Features That Are *Not* Available in vSwitch

Answer: Select Two VMware DVS Features That Are *Not* Available in vSwitch

- ACLs
- ✓ PVLANS
- ✓ Network vMotion
- SSH
- Telnet

Use of the VMware distributed virtual switch provides two features that are *not* available in the vSwitch:

- Private VLANs
- Network vMotion

Select Three Features of VMware Port Groups

Answer: Select Three Features of VMware Port Groups

- ✓ Segment traffic based on VLAN
- ✓ Segment traffic based on traffic type (Vmkernel, service console)
- Only available in vSwitch
- Only available in distributed virtual switch
- ✓ Available in vSwitch, DVS, and Cisco Nexus 1000V

Port groups are configured on vSwitches to segregate traffic that is based on type or VLAN.

Review of Cisco Nexus 1000V Series Architecture

This topic reviews Cisco Nexus 1000V Series architecture.

Select Three Features of VN-Link in Software

Answer: Select Three Features of VN-Link in Software

- ✓ Policy-based VM connectivity
- ✓ Mobility of network and security policy
 - Only available in vSwitch
 - Only available in distributed virtual switch
- ✓ Only available in Cisco Nexus 1000V
 - Available in vSwitch, DVS, and Cisco Nexus 1000V

The Cisco Nexus 1000V Series Switch is a software-based solution providing VM-level network configurability and management. The Cisco Nexus 1000V works with any upstream switching system to provide standard networking controls to the virtual environment.

Cisco Virtual Network Link (VN-Link) technology was jointly developed by Cisco and VMware. It has been proposed to the IEEE for standardization. The technology is designed to move the network access layer into the virtual environment in order to provide enhanced network functionality at the VM level. Cisco VN-Link is deployed as a hardware-based solution offering VM visibility, policy-based VM connectivity, policy mobility, and a nondisruptive operational model.

Select Three Examples Where VNTag Is Implemented

Answer: Select Three Examples Where VNTag Is Implemented

- Between Cisco Nexus 1000V and Cisco UCS 6100 Fabric Interconnect
- Between VMware vSwitch and Cisco UCS 6100 Fabric Interconnect
- ✓ Between Cisco UCS 2104 IOM and Cisco UCS 6100 Fabric Interconnect
- ✓ Between MK81KR VIC and Cisco UCS 6100 Fabric Interconnect
- ✓ Between Cisco Nexus 2000 Series FEX and Cisco Nexus 5000 Series

Cisco VNTag is required wherever network interface virtualization is present. Examples of network interface virtualizers include the Cisco UCS 2104 IOM, UCS MK81KR VIC, and Cisco Nexus 2000 Series Fabric Extender.

Summary

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

Summary

- Cisco UCS Manager relieves many challenges to data center server management by providing a single point of management for server provisioning.
- The Cisco UCS is a family of integrated components that include compute and switching resources.
- Cisco UCS C-Series hardware components include rack-mount chassis, CPU, RAM, RAID controller, hard drives, and network adapters.
- Cisco UCS C-Series hardware installation requires knowledge of proper ESD precautions and rack-mounting procedures.
- Cisco UCS B-Series hardware components include blade servers, fabric extenders, and fabric interconnects.

© 2011 Cisco Systems, Inc. All rights reserved.

DCUCI v4.0 35

Summary (Cont.)

- Cisco UCS B-Series architecture includes integrated management, FCoE, and N-Port Virtualization.
- Cisco UCS use cases highlight the attributes of successful implementations of operating systems and applications on the Cisco UCS platform.
- Server virtualization allows for better utilization and return on investment for compute resources.
- Cisco Nexus 1000V implements granular and mobile policies for virtual machines in VMware distributed virtual switching system available in vSphere 4.0 and later.
- VMware standard Ethernet networking architecture implements the concept of virtual switches that interconnect virtual machines and physical switches.
- Cisco Nexus 1000V architecture includes a Virtual Supervisor Module to control policy for Virtual Ethernet Modules that provide switching and access control to virtual machines.

© 2011 Cisco Systems, Inc. All rights reserved.

DCUCI v4.0 36

Troubleshooting Cisco UCS B-Series Hardware

Overview

The primary learning objective for this module is to enable you to collect management information from all the various sources in a Cisco Unified Computing System (UCS) environment. Some of this information can be gathered from protocols running outside Cisco UCS (for example, Simple Network Management Protocol [SNMP]), some information from the GUI or command-line interface (CLI) (for example, faults and events), and some from the operating system (for example, sosreport).

Objectives

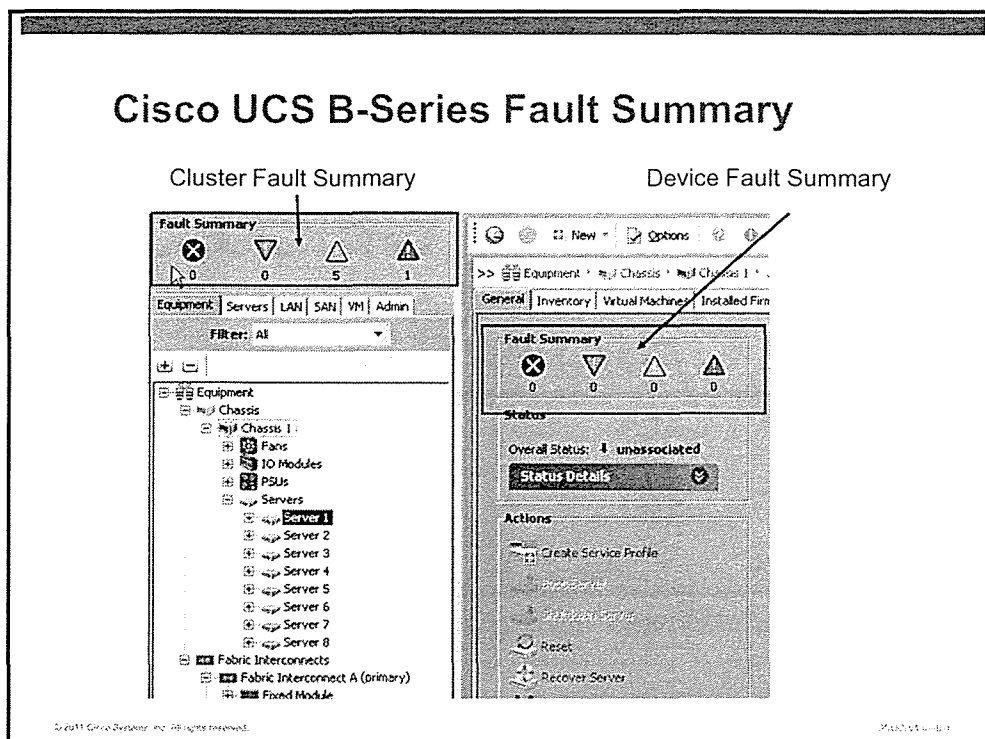
Upon completing this lesson, you will be able to meet these objectives:

- Describe the device fault color coding scheme to determine relative fault level on a given component
- Differentiate between common errors that are observed during hardware discovery
- Describe LED error codes on every component of the Cisco UCS B-Series
- Describe how to harvest and view core files
- Differentiate between common forms of the **show tech** command within the local management shell

Cisco UCS B-Series Fault Color Coding Scheme

This topic discusses the Cisco UCS B-Series fault color coding scheme.

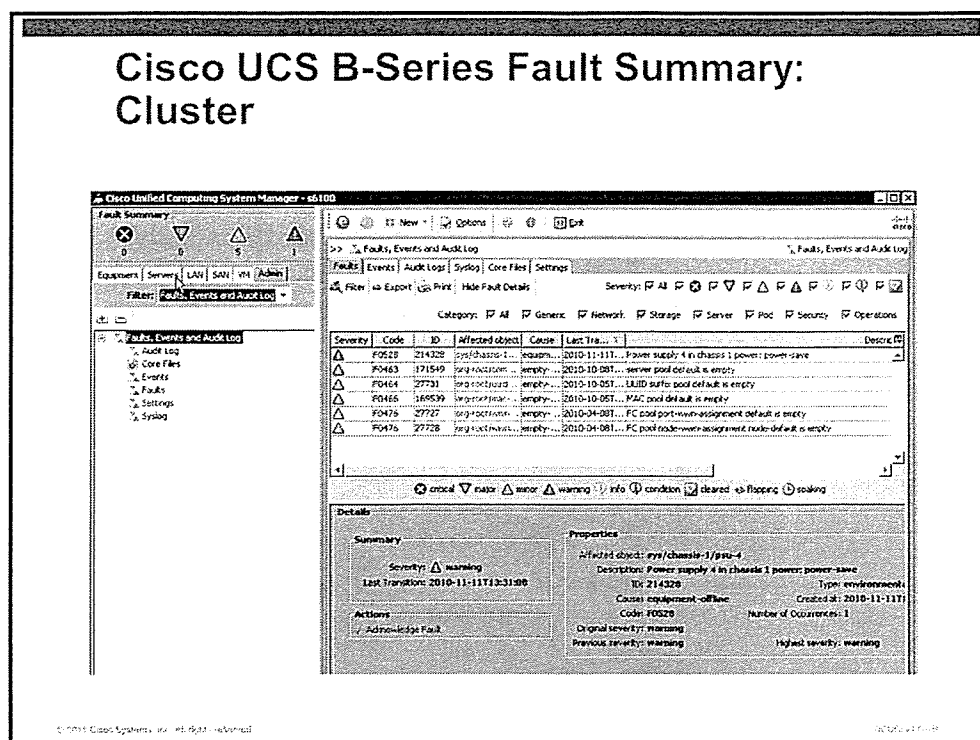
Cisco UCS B-Series Fault Summary



Cisco UCS Manager provides a summary view of faults and events from directly within the GUI. The color-coded symbols (red, orange, yellow, and green) represent the severity of various faults and events within the cluster, shown at the top of the navigation pane, and device-specific, shown at the top of the content pane.

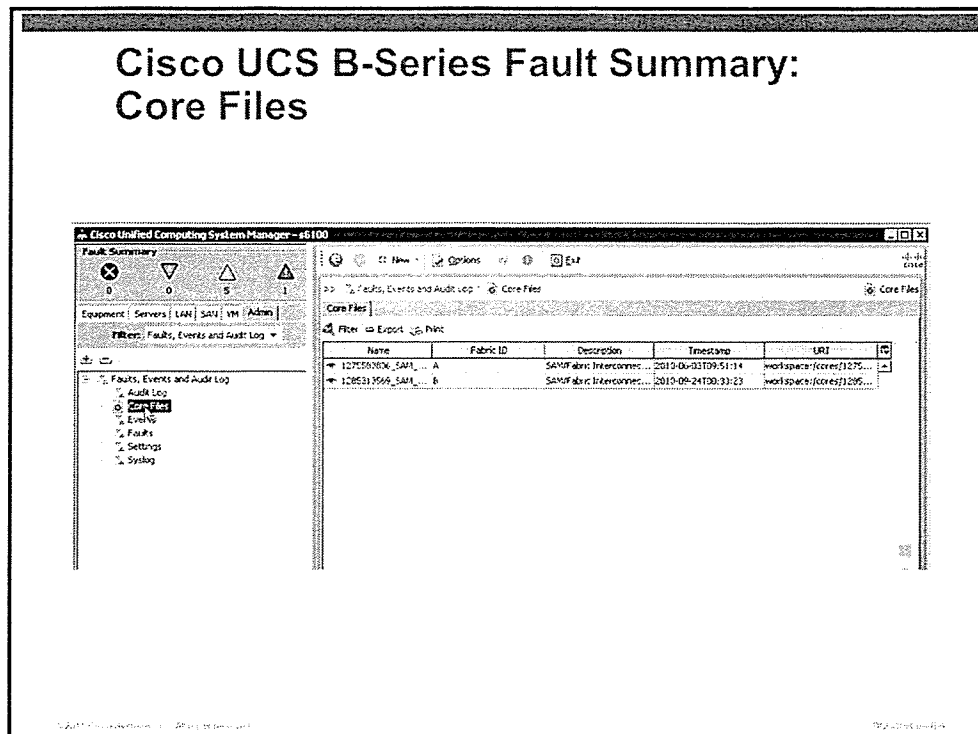
The red circle represents a major fault, orange represents a minor fault, yellow represents an alert, and green indicates an informational message, such as an interface state change.

Cisco UCS B-Series Fault Summary: Cluster



The Cisco UCS cluster fault summary may be viewed by selecting the Admin tab that is located at the right side of the navigation pane. By choosing the filter settings of Faults, Events, and Audit Logs, you can view the cluster Fault Summary organized by event type in the content pane.

Cisco UCS B-Series Fault Summary: Core Files



You can view the Cisco UCS cluster fault summary by selecting the Admin tab that is located at the right side of the navigation pane. By choosing the filter settings of Faults, Events, and Audit Logs, you can view the cluster Core Files setting. The directory of available core files appears in the right content pane.

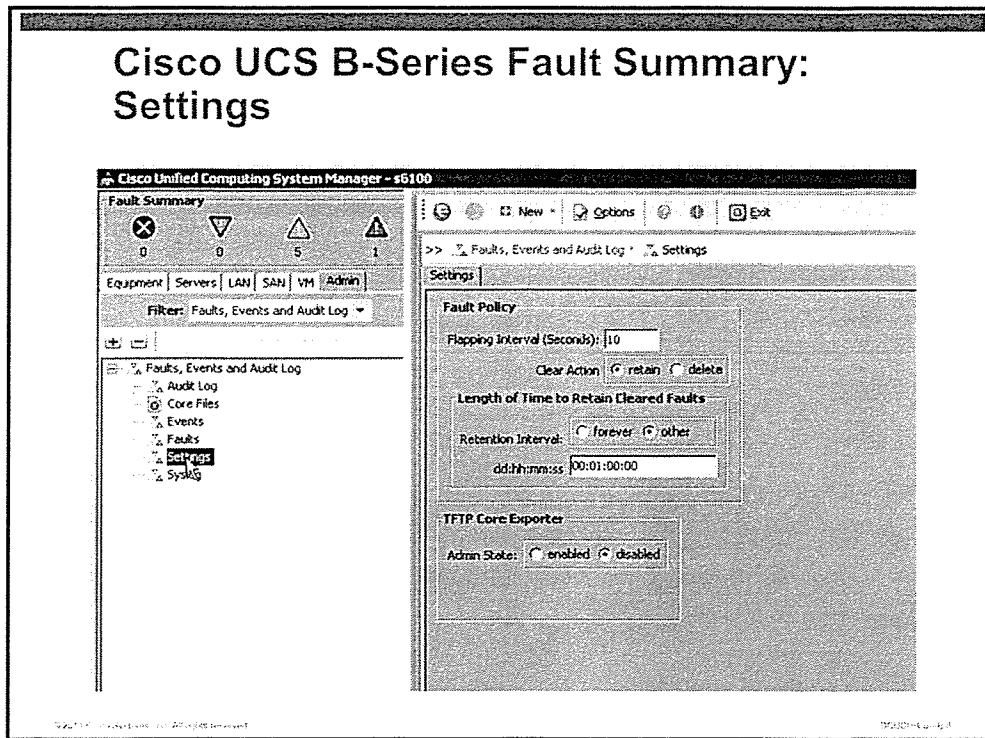
Cisco UCS B-Series Fault Summary: Events

Cisco UCS B-Series Fault Summary: Events

Affected object	Code	ID	Cause	Created at	User
Fabric/Storage...	E4195...	222867	Transition 2010-11-171...	Internal	[FSM:STAGE:STALE-SUCCESS]: QoS Classification Definition cla...
Fabric/Storage...	E4195...	222868	Transition 2010-11-171...	Internal	[FSM:STAGE:END]: QoS Classification Definition classification to...
Fabric/Storage...	E4195...	222869	Transition 2010-11-171...	Internal	[FSM:END]: QoS Classification Definition classification configura...
Fabric/Storage...	E4195...	222864	Transition 2010-11-171...	Internal	[FSM:STAGE:STALE-SUCCESS]: QoS Classification Definition cla...
Fabric/Storage...	E4195...	222865	Transition 2010-11-171...	Internal	[FSM:STAGE:END]: QoS Classification Definition classification co...
Fabric/Storage...	E4195...	222866	Transition 2010-11-171...	Internal	[FSM:STAGE:ASYNC]: QoS Classification Definition classification co...
Fabric/Storage...	E4195...	222860	Transition 2010-11-171...	BOSS-Admin	[FSM:BEGIN]: QoS Classification Definition classification configura...
Fabric/Storage...	E4195...	222861	Transition 2010-11-171...	BOSS-Admin	[FSM:STAGE:END]: [FSM:STAGE:success]: QoS Classification Defi...
Fabric/Storage...	E4195...	222862	Transition 2010-11-171...	BOSS-Admin	[FSM:STAGE:ASYNC]: QoS Classification Definition classification...
SystemEvent	E4195...	222840	Transition 2010-11-171...	Internal	[FSM:STAGE:STALE-SUCCESS]: user configuration to secondary...
SystemEvent	E4195...	222841	Transition 2010-11-171...	Internal	[FSM:STAGE:END]: user configuration to secondary[FSM:STAGE...
SystemEvent	E4195...	222842	Transition 2010-11-171...	Internal	[FSM:END]: user configuration[FSM:success]: user configuration...
SystemEvent	E4195...	222839	Transition 2010-11-171...	Admin	[FSM:BEGIN]: user configuration[FSM:success]: user configuration...
SystemEvent	E4195...	222831	Transition 2010-11-171...	Admin	[FSM:STAGE:END]: [FSM:STAGE:success]: user configuration to primary...
SystemEvent	E4195...	222832	Transition 2010-11-171...	Admin	[FSM:STAGE:ASYNC]: user configuration to primary[FSM:STAGE...
SystemEvent	E4195...	222837	Transition 2010-11-171...	Internal	[FSM:STAGE:STALE-SUCCESS]: user configuration to primary[FSM:STAGE...
SystemEvent	E4195...	222838	Transition 2010-11-171...	Internal	[FSM:STAGE:END]: user configuration to primary[FSM:STAGE...
SystemEvent	E4195...	222839	Transition 2010-11-171...	Internal	[FSM:STAGE:ASYNC]: user configuration to secondary[FSM:STAGE...

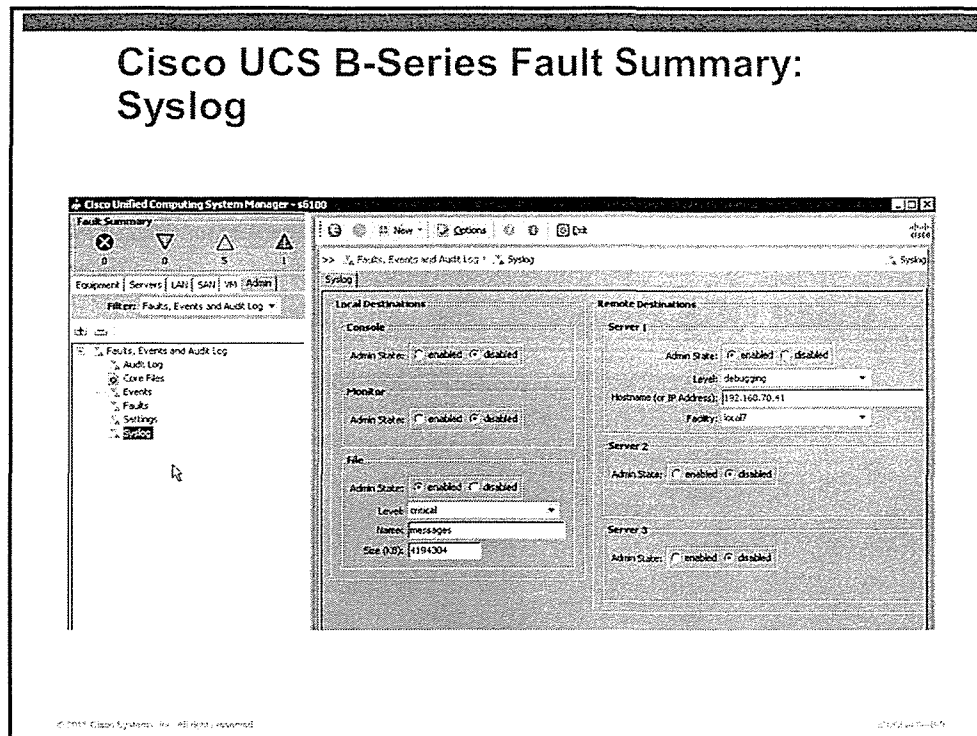
You can view the Cisco UCS cluster fault summary by selecting the Admin tab that is located at the right side of the navigation pane. By choosing the Filter settings of Faults, Events, and Audit Logs, you can view the cluster Events that are shown and organized by event type in the content pane.

Cisco UCS B-Series Fault Summary: Settings



You can view the UCS cluster fault summary by selecting the Admin tab that is located at the right side of the navigation pane. By choosing the Filter settings of Faults, Events, and Audit Logs, you can configure the cluster fault policy. By selecting the Settings tab under the main Admin tab, the configuration wizard appears in the content pane.

Cisco UCS B-Series Fault Summary: Syslog

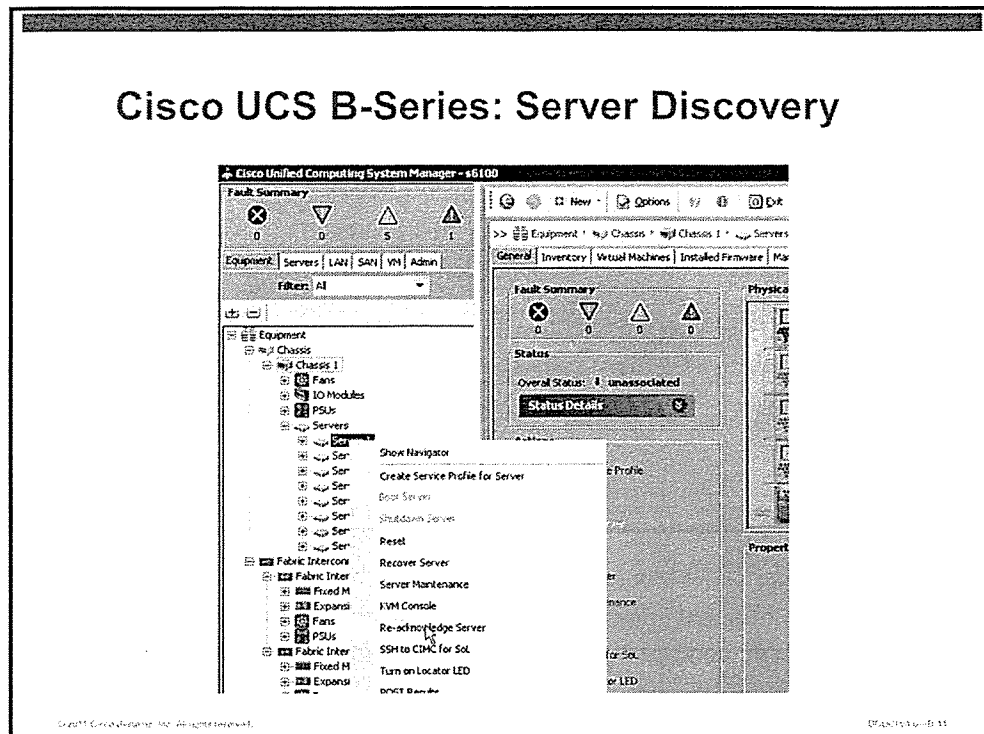


You can view the Cisco UCS cluster fault summary by selecting the Admin tab that is located at the right side of the navigation pane. By choosing the Filter settings of Faults, Events, and Audit Logs, you can configure the cluster syslog setting. By choosing Syslog (under the main Admin tab), the configuration wizard appears in the content pane.

Cisco UCS B-Series Hardware Discovery Common Errors

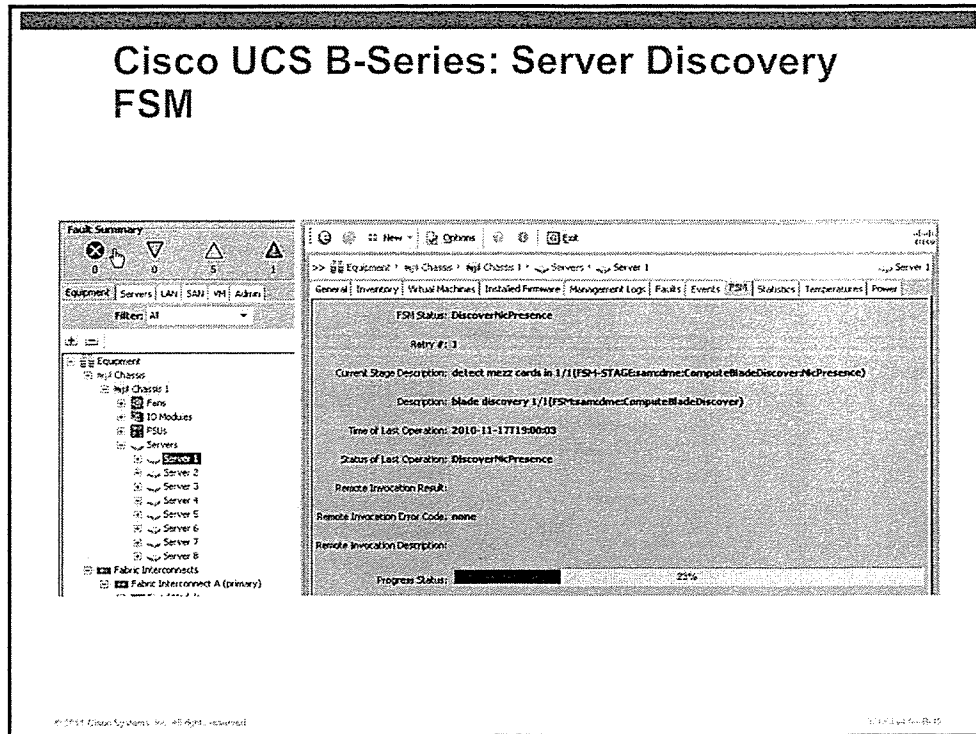
This topic discusses common errors during hardware discovery of the Cisco UCS B-Series.

Cisco UCS B-Series: Server Discovery



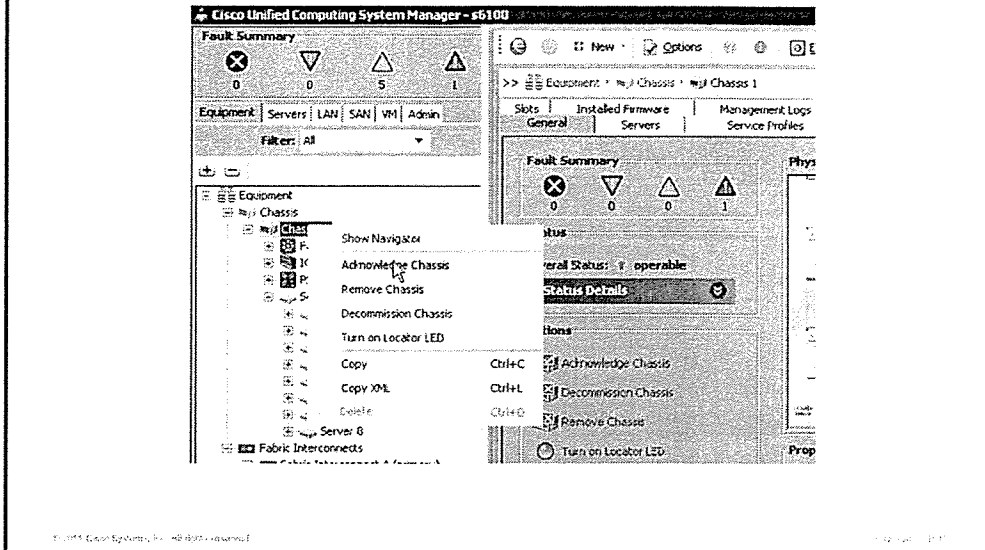
You can initiate the server discovery process from the main Equipment tab. Select the desired chassis, right-click, and select **Re-acknowledge Server**. The status of the process may be viewed from the FSM tab in the right content pane.

Cisco UCS B-Series: Server Discovery FSM



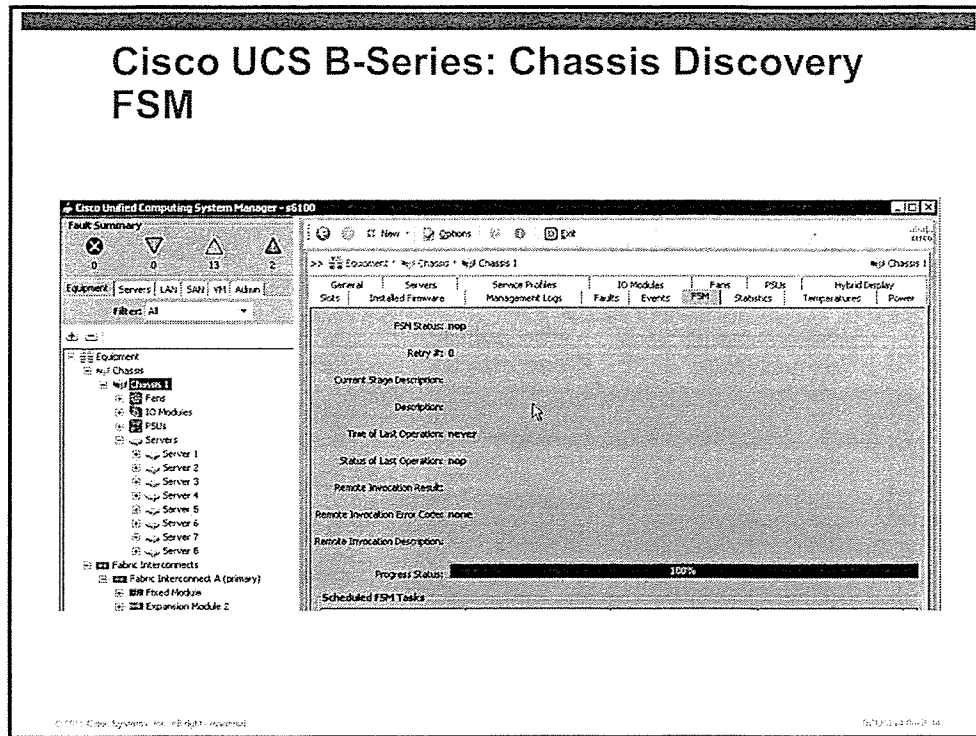
You can access the finite state machine (FSM) option from the main Equipment navigation tab. The FSM option provides real-time status of many Cisco UCS processes and includes diagnostic messages for any failed processes. In this example in the figure, the server discovery process has partially completed.

Cisco UCS B-Series: Chassis Discovery



You can initiate the chassis discovery process from the main Equipment tab. Select the desired chassis, right-click, and select **Acknowledge Chassis**. You can view the status of the process from the FSM tab in the right content pane.

Cisco UCS B-Series: Chassis Discovery FSM

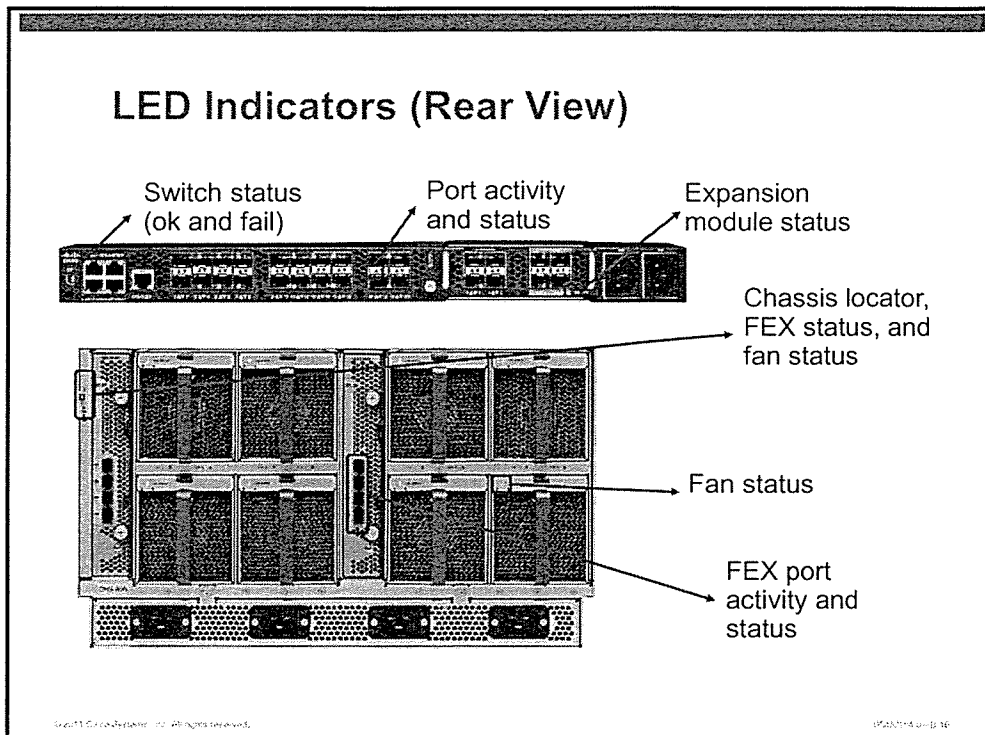


You can access the FSM option from the main Equipment navigation tab. The FSM option provides real-time status of many Cisco UCS processes and includes diagnostic messages for any failed processes. In this example, the chassis acknowledgment process has completed successfully.

Cisco UCS B-Series Hardware LED Error Codes

This topic discusses Cisco UCS B-Series hardware LED error codes.

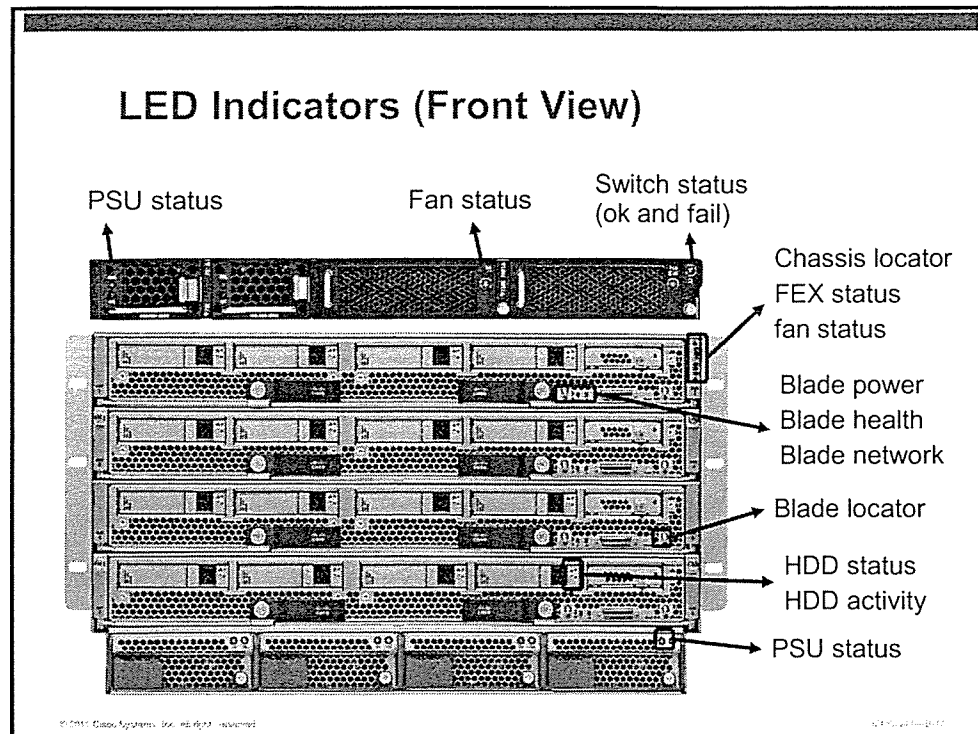
LED Indicators (Rear View)



The illustration in the figure of the rear view of a Cisco UCS shows the various LED indicators that you can use to identify components and their states. Different LEDs have different colors and flashing patterns to indicate their status. Some of the components support beaconing (for example, fabric extender [FEX] cards) to help test pattern monitors (TPMs) and fabric extenders locate them.

L1, L2, MGMT0, and MGMT1 ports also have status and activity lights in the rear.

LED Indicators (Front View)



The front view of the Cisco UCS also has diagnostic lights that show status and locators for certain components. Some of these diagnostic LED indicators are duplicated on front and back (for example, chassis locator, FX status, fan status, and switch status).

Interpret LED Indicators

Interpret LED Indicators		
LEDs	States	Description
Bi-color LEDs	Off	Not connected, no power
	Green	Normal operation
	Amber	Booting up, running diagnostics, or minor temperature alarm
	Blinking amber	Failed, including major temperature alarm
	Blinking green	Used as traffic activity on ports
Locator	Off	Locator feature not enabled
	Blinking blue	Locator feature enabled

The logic expressions shown in the figure describe how to interpret the LED indicators on each of the Cisco UCS components, including the following:

- Chassis
- Chassis fan module
- Chassis power supply
- FEX card
- FEX port
- Disk drive
- Server
- Server processor
- Switch
- Switch port
- Switch power supply
- Switch fan
- Switch generic expansion module (GEM)
- Switch GEM port

Chassis

ok = off, fail = off	no power
ok = green, fail = amber	no I/O module (IOM) installed
ok = green, fail = off	normal operation
ok = off, fail = amber	minor temperature alarm in some component
ok = off, fail = blinking amber	some component failed or major temperature alarm in some component

Chassis fan tray

light = off	no power
light = green	normal operation
light = amber	booting
light = blinking amber	some fan in tray failed

Chassis power supply

ok = off, fail = off	no power
ok = green, fail = off	normal operation
ok = off, fail = amber	failure due to overvoltage or temperature
ok = off, fail = blinking	high temperature, high power, and slow fan
ok = blinking, ok = off	AC is present and power supply unit (PSU) is off

FEX

light = off	no power
light = green	normal operation
light = amber	booting or minor temperature alarm
light = blinking amber	stopped in uBoot due to user intervention or unable to come online or major temperature alarm

FEX port

light = off	link enabled but not connected
light = green	link connected
light = amber	operator disabled
light = blinking amber	disabled due to error

Server

power = off	power off
power = green	normal operation
power = amber	standby
link LED = off	none of network link (mezzanine to IOM) is up
link LED = green	at least one network link is up
health LED = off	power off
health LED = green	normal operation
health LED = amber	minor error
health LED = blinking amber	critical error

Disk drive

activity = off	inactive
activity = green	outstanding I/O to drive
fault = off	no fault
fault = amber	some fault

Server processor

power = off	power off
power = amber	standby
power = green	power on
activity = off	???
activity = green	???
health = green	normal operation
health = amber	health degraded
health = blinking amber	health degraded critically

Switch

stat = off	no power
stat = green	ok
stat = amber	booting, running diagnostics, or minor temperature alarm
stat = blinking amber	failed to boot or major temperature alarm

Switch port

mgmt port left = off	link enabled but not connected
mgmt port left = green	link connected
mgmt port left = amber	operator disabled
mgmt port left = blinking amber	disabled due to error
mgmt port right = off or blinking green	link activity

Switch power supply

ok = off, fail = off	no power
ok = green, fail = off	normal operation
ok = off, fail = amber	failed due to over-current, voltage, or temperature
ok = off, fail = blinking	warning (temperature, power, or slow fan) but continues to operate
ok = blinking, fail = off	AC present but PSU is off

Switch fan

status = off	no power
status = green	normal operation
status = amber	booting
status = blinking amber	failed

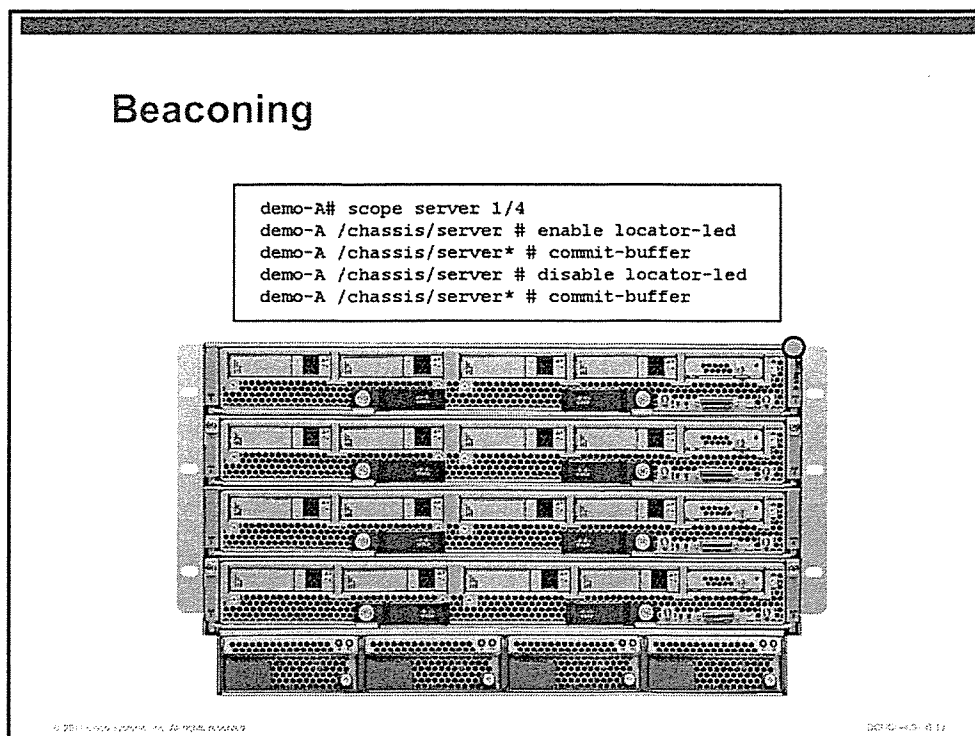
Switch GEM

module = off	no power
module = green	normal operation
module = amber	booting, running diagnostics, or minor temperature alarm
module = blinking amber	failed to boot or major temperature alarm

Switch GEM port

light = off	link enabled but not connected
light = green	link connected
light = amber	operator disabled
light = blinking amber	disabled due to error

Beaconing



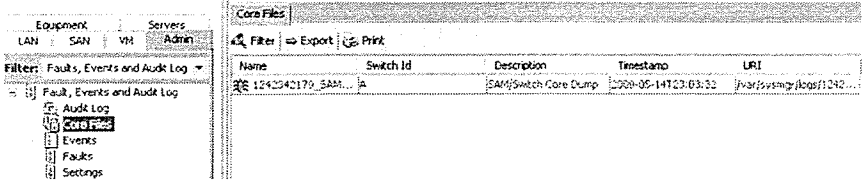
The Beacon feature enables a remote administrator to provide on-site service personnel with a visual indication of the major chassis components. It is possible to beacon the chassis and FEX cards, though this is not shown in the figure. The beacon may be turned off by setting the locator LED to **Off** or by depressing the locator button on the blade itself. The same functionality is available from the GUI.

Cisco UCS B-Series Core Files

This topic discusses Cisco UCS B-Series core files.

Displaying Core Dumps

Displaying Core Dumps



Name	Switch Id	Description	Timestamp	URI
1242342179_SAM_demo-A_svc_sam_bladeAG_log.3088.tar.gz	A	SAM/Switch Core Dump	2009-05-14T23:03:32	/var/sysmgr/logs/1242...

```
demo-A# scope monitoring
demo-A /monitoring # scope sysdebug
demo-A /monitoring/sysdebug # show cores detail

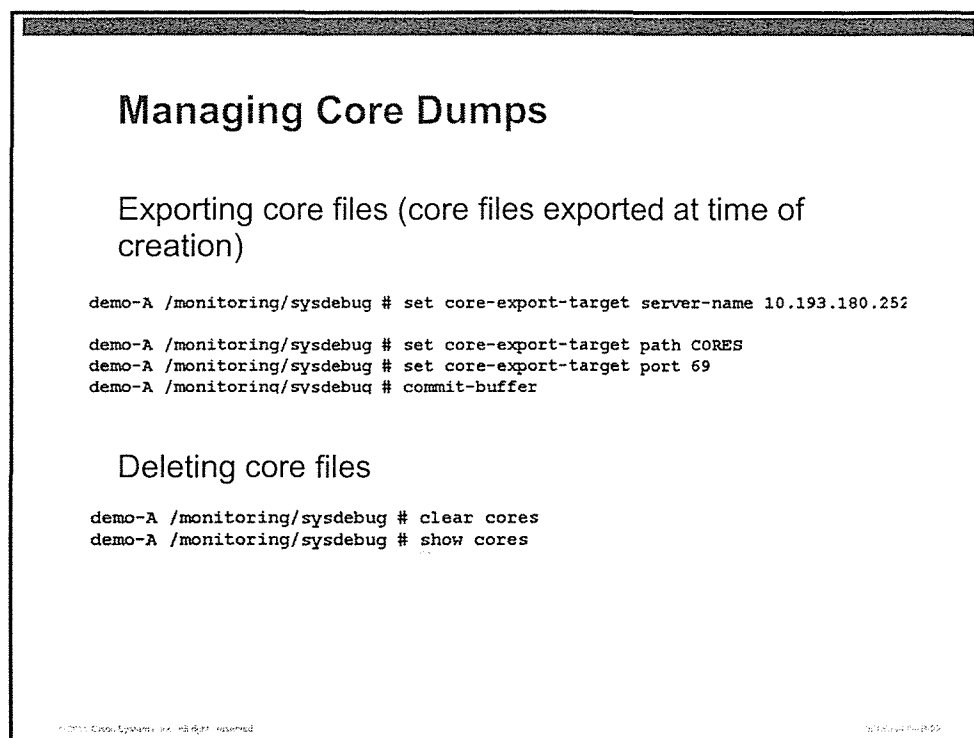
Core Files:
  Name: 1242342179_SAM_demo-A_svc_sam_bladeAG_log.3088.tar.gz
  Switch Id: A
  Description: SAM/Switch Core Dump
  Size: 8407484
  Timestamp: 2009-05-14T23:03:32
  URI: /var/sysmgr/logs/1242342179_SAM_demo-A_svc_sam_bladeAG_log.3088.tar.gz
```

You can display core dumps in either the GUI or the CLI. “Displaying” a core dump is simply listing its existence in a directory structure on the switch. Later, there will be discussion of how to export this dump off the switch to another host on the network. Note that the name of the core dump reflects the source of the file. For example, 1242342179_SAM_demo-A_svc_sam_bladeAG_log.3088.tar.gz is a core dump with the following characteristics:

- It was dumped 1,242,342,179 seconds after January 1, 1970.
- It was dumped by a storage area management (Cisco UCS Manager) process.
- The name of the interconnect on which that process was running is switch A.
- The name of the process that dumped this core file is svc_sam_bladeAG.
- The process ID of that process when it dumped core was 3088.

Of course, the core dump itself will contain much more useful information about the running state of that process when it abnormally exited.

Managing Core Dumps



When you have identified a core dump that you wish to analyze, you will have to export it off the switch onto another host or file server. The illustration in the figure shows configuring a target server (in this example, 10.193.180.252), port (in this example, 69, which is TFTP), and a path (in this example, /CORES under /tftpboot). The illustration also shows how to delete core files from your switch to make room for more files.

Cisco UCS B-Series Local Management

This topic describes Cisco UCS B-Series local management.

show tech-support **Commands**

show tech-support **Commands**

- These commands are accessed through the primary fabric interconnect CLI.
- Use SSH to access the primary fabric interconnect.
- Issue the **connect local-mgmt** command.
- The **show tech-support** command has very detailed output enabling advanced troubleshooting on the Cisco UCS cluster.

In order to access the CLI of the primary fabric interconnect, the administrator may initiate a Telnet or SSH session to the management IP of the device. After providing the username and password login credentials, a CLI prompt will appear. By typing the **connect local-mgmt** command, the local management shell prompt will appear, which supports the variety of **show tech-support** commands.

show tech-support **Commands (Cont.)**

Overview of **show tech-support** commands:

- Similar to “explorer” utilities from other vendors
- Gathers operating system information from:
 - NX-OS
 - CMC
 - BMC
 - Adapters
- Gathers configuration and state from Cisco UCS Manager

The **show tech-support** command is similar to explorer utilities that other vendors provide. It is intended to be run on the production switch and collect as much static (configuration) and dynamic (runtime) information as possible, so that a technical support engineer (front-line or back-line) can debug or reproduce a problem. All of this static and dynamic information is collated into a .tar file of compressed .tar files.

show tech-support **Commands (Cont.)**

show tech-support chassis 1 cimc 1

- The command output includes the following information:
 - Cisco IMC build
 - Cisco IMC FRU data
 - Cisco IMC process table and pidstat output
 - Cisco IMC /var/log/messages
 - Cisco IMC core dump directory listing
 - BIOS, mezzanine, and blade power status

```
demo-A(local-mgmt)# show tech-support chassis 1 bmc 1 brief
```

```
Brief Technical Support Information for IBMC 1 on Chassis 1
```

```
*****
```

```
Thu Jan 8 21:14:10 UTC 1970
```

```
BMC Version Info
```

```
ver: 1.0(0.45n)
```

```
info: Branch: trunk, SVN rev: 26402
```

```
Linux NUOVA-IBMC 2.6.16.12 #1 Tue Apr 21 21:59:25 PDT 2009 exported armv5tej l u  
nknown
```

```
RAMFS Build Time [ Tue Apr 21 22:10:25 PDT 2009 ]
```

```
Blade Identity File Contents:
```

```
virtual_hostname="demo"
```

```
CSN="BC01_IBMC01"
```

```
tftp_core_dir="sysdebug/tftp_cores"
```

```
Slot ID Info:
```

```
1
```

```
BMC FRU Info:
```

```
FRU_Max_Img_Size = 0x0200
```

```
Fetching FRU-0 via IPMI
```

```
(Raw FRU Data)
```

000: 01 01 26 0C 1A 00 00 B2 01 03 00 05 00 01 00 0C

010: 01 02 06 00 02 06 00 23 33 A9 13 94 00 00 00 33

020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

(output skipped)

show tech-support **Commands (Cont.)**

show tech-support chassis 1 iom 1

- The chassis ID identifies this chassis among all other chassis.
- The fabric ID is 1 (for the "left" switch) or 2 (for the "right" switch).
- The cluster ID is stored in the SEEPROM and consumed when running in HA mode.
- The slot ID identifies the IOM (0 for the "left" IOM and 1 for the "right" IOM).
- Status indicators for several of the chassis components are listed in the command output.

Brief Technical Support Information for Fabric Extender 1 from A

Output of 'dmclient_test':--

Last scan time : 1228180

Chassis-id : 1

Fabric-id : 1

Cluster-id : 40881dc0-39ef-11de-a44e-000decbl4504

Slot id : 0

Amber LED status : ON

Green LED status : OFF

Chassis ok LED status : ON

Chassis fault LED status : ON

Locate LED status : OFF

Locate button status : 0

Backplane status : 1

Blades present : 0 1 2 3

Blades powered on : 0 1 2 3 4 5 6 7

Blades alerted : 0 1 2 3

Fans present : 0 1 2 3 4 5 6 7

Fans alerted : 0 1 2 3 4 5 6 7

PSs present : 1 2 3

PSs RMT on : 0 1 2 3
PS DC ok : 1 2
PS AC ok : 1 2
SFPs present :
Redwood pll status : 0 1 2
Redwood status : 0
IBMC Link status : 0 1 2 3
uBoot post status : 0x00000000
Peer uBoot post status : 0x00000000
CMC post status : 0x01000000
Peer CMC post status : 0x01000000
Health status : 0x04000000
Peer Health status : 0x04000000
Number of ethernet addresses : 10
Start IOM ethernet address : 00:23:33:a9:18:e2
Eth0 MAC: : 00:23:33:a9:18:e2
Eth1 MAC : 00:23:33:a9:18:e3
HIF state : 0 2

Version information:--

CMC Version:

1.0.0.26402.45n

Tue Apr 21 21:49:28 PDT 2009

CMC kernel version:

(output skipped)

show tech-support **Commands (Cont.)**

show tech-support ucsm

- System version and platform information
- Switch tech-support information
 - VSANs
 - Interfaces
 - VLANs
 - FE
- SAM configuration and Cisco UCS inventory
 - sam.config
 - Cluster
 - Chassis
 - Server status
 - Service profile status

Brief Technical Support Information for Fabric A

System Version and Platform Information

`show system uptime`

System start time: Thu May 7 21:38:22 2009

System uptime: 7 days, 3 hours, 23 minutes, 17 seconds

Kernel uptime: 7 days, 3 hours, 26 minutes, 58 seconds

Active supervisor uptime: 7 days, 3 hours, 23 minutes, 17 seconds

`show system resources`

Load average: 1 minute: 0.00 5 minutes: 0.10 15 minutes: 0.18

Processes : 399 total, 2 running

CPU states : 0.0% user, 2.0% kernel, 98.0% idle

Memory usage: 3634788K total, 1874288K used, 1760500K free

83336K buffers, 1237668K cache

`show version`

Cisco UCS 6100 Series Fabric Interconnect

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

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

The copyrights to certain works contained herein are owned by other third parties and are used and distributed under license.

Some parts of this software may be covered under the GNU Public License or the GNU Lesser General Public License. A copy of each such license is available at

<http://www.gnu.org/licenses/gpl.html> and

<http://www.gnu.org/licenses/lgpl.html>

Software

BIOS: version 1.2.0

loader: version N/A

kickstart: version 4.0(1a)N2(1.1) [build 4.0(1a)N2(1.0.45n)] [gdb]

(output skipped)

show tech-support **Commands (Cont.)**

show tech-support chassis 1 all detail

- Collects all diagnostic information available on the following:
 - Chassis
 - BMC
 - Adapters
- Creates a .tar file of gzipped .tar files, one for each BMC

demo-A(local-mgmt)# **show tech-support chassis 1 all detail**

Initiating tech-support information task on Chassis 1 FabricExtender 1 ...

Initiating tech-support information task on Chassis 1 FabricExtender 2 ...

Initiating tech-support information task on IBMC 1 on Chassis 1 ...

Initiating tech-support information task on Adaptor 1 on Chassis/Blade 1/1 ...

Initiating tech-support information task on IBMC 2 on Chassis 1 ...

Adapter on Chassis/Blade 1/2 is either not network-managed or is not currently active.

Initiating tech-support information task on IBMC 3 on Chassis 1 ...

Initiating tech-support information task on Adaptor 1 on Chassis/Blade 1/3 ...

Initiating tech-support information task on IBMC 4 on Chassis 1 ...

Adapter on Chassis/Blade 1/4 is either not network-managed or is not currently active.

Completed initiating tech-support subsystem tasks (Total: 8)

Waiting (Timeout: 600 Elapsed: 25) for completion of subsystem tasks (2/8).

Waiting (Timeout: 600 Elapsed: 45) for completion of subsystem tasks (3/8).

Waiting (Timeout: 600 Elapsed: 65) for completion of subsystem tasks (3/8).

Waiting (Timeout: 600 Elapsed: 85) for completion of subsystem tasks (3/8).

Waiting (Timeout: 600 Elapsed: 106) for completion of subsystem tasks (6/8).

All tech-support subsystem tasks are completed (Total: 8)

show tech-support **Commands (Cont.)**

show tech-support ucsd detail

- DHCP
- df
- ifconfig
- dmesg
- iptables
- /var/sysmgr
- /var/log/messages
- /opt/db

demo-A(local-mgmt)# **show tech-support sam detail**

Initiating tech-support information task on FABRIC A ...

Initiating tech-support information task on FABRIC B ...

Completed initiating tech-support subsystem tasks (Total: 2)

All tech-support subsystem tasks are completed (Total: 2)

Summary

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

Summary

- The Cisco UCS B-Series GUI provides both cluster and device-specific fault summaries.
- Detailed fault information can be obtained from the Admin tab within the Cisco UCS Manager GUI navigation pane.
- The Cisco UCS B-Series hardware provides detailed LED status indication on all major components.
- The Cisco UCS Manager Core files may be accessed from the GUI and CLI.
- The primary fabric interconnect local management shell may be used to derive detailed information for troubleshooting purposes.

© 2011 Cisco Systems, Inc. All rights reserved.

UCS-B-4000-01-01

Troubleshooting Cisco UCS B-Series Service Profiles

Overview

This lesson describes common configuration errors that affect successful service profile association. After the configuration errors are identified from within the Cisco UCS Manager GUI, appropriate corrective action is presented.

Objectives

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

- Describe troubleshooting of resource assignment errors in the FSM status
- Describe troubleshooting of server profile issues after assignment

Troubleshooting Resource Assignment Issues

This topic discusses troubleshooting resource assignment issues.

Overview of FSM

Overview of FSM

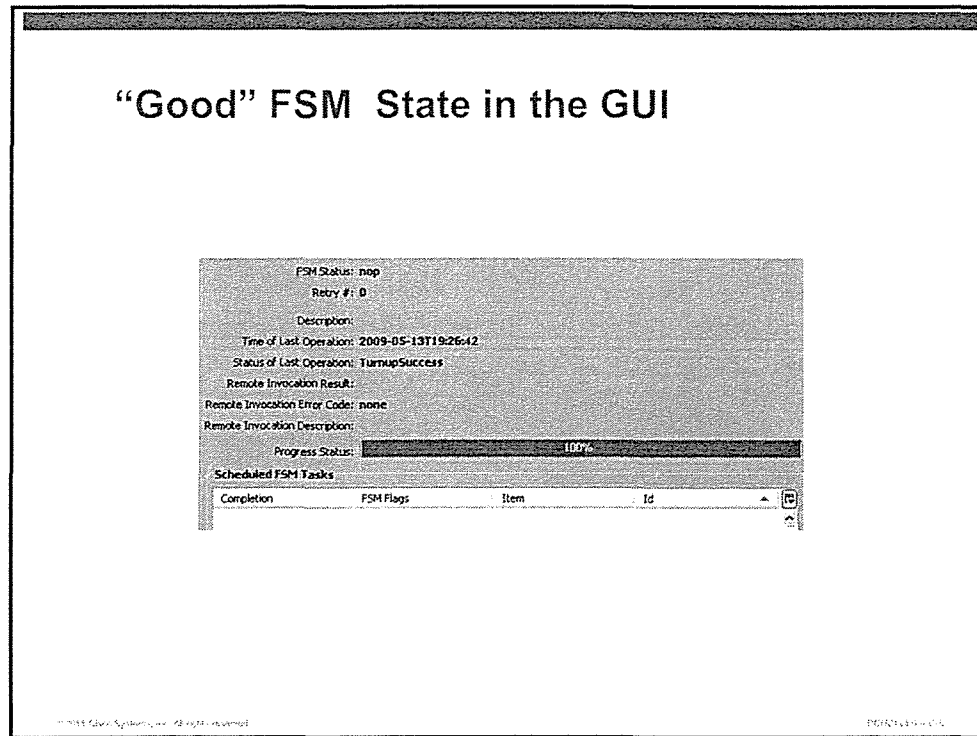
- Finite state machine (FSM) is reflection of object model
- FSMs are associated with the following objects
 - Physical components (chassis, FEXs, servers)
 - Logical components (LAN cloud, policies)
 - Workflows (downloads, upgrades, backups)
- Useful for diagnosing problems

The finite state machine (FSM) is a reflection of the state of an object in the object model. There are only a finite number of states in which an object can be at any time. Transitions from one state to another state are defined in the logic of the object model. The state of the object in the model is a reflection of the actual state that is represented by the object. For example, there is an object for a server that is a logical representation of an actual physical server. The FSM applies to the object directly and therefore to the actual thing indirectly.

FSMs are associated with several—but not all—objects in the object model. Some physical components, such as fabric extender (FEX) cards, have an associated FSM. Other physical components, such as a mezzanine adapter, do not have an associated FSM.

FSMs are useful when debugging problems. If the FSM is in the equivalent of a success state, then at least as far as Cisco UCS Manager is concerned, that object is okay. On the other hand, if the object cannot transition through the state machine successfully, then Cisco UCS Manager considers this object (and the thing it represents) to be in some faulty state. The verbosity of the FSM in the GUI and command-line interface (CLI) is terse, but can be a good starting point for diagnosing problems with your Cisco UCS Manager components.

“Good” FSM State in the GUI

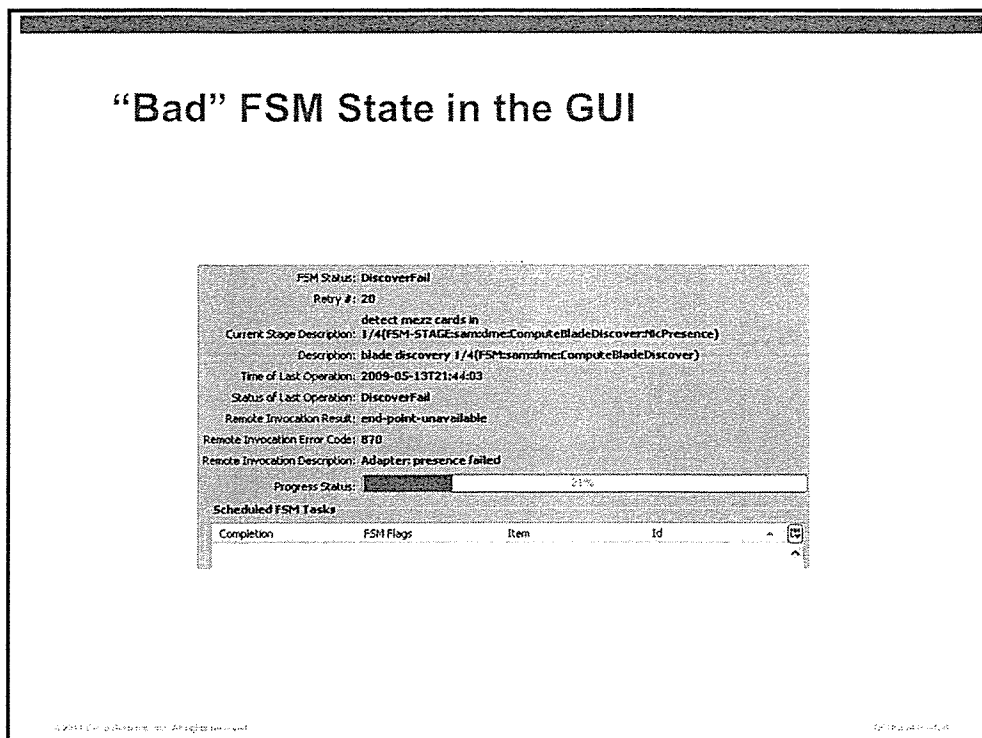


How would you know that this represents a “good” FSM state? There are a few indicators:

- The FSM status is “nop” (short for no operation). In other words, there is no more that this FSM needs to do.
- The status of the last operation is “TurnupSuccess.” In other words, whatever “Turnup” means, it was apparently successful.
- The remote invocation error code is “none.” In other words, there are no errors.
- The program status is “100%.” In other words, this FSM is complete.

Also note that there are no other FSM tasks that are scheduled for this component at this time.

“Bad” FSM State in the GUI



How would you know that this represents a “bad” FSM state? There are a few indicators:

- The FSM status is not “nop.” (In this case, it is DiscoverFail.) In other words, the FSM has more to do. Which is not bad by itself (perhaps you need to be more patient and wait for the FSM to complete), except given other information as described here.
- The remote invocation result is “end-point unavailable.” In the context of the discovery process, this cannot be good.
- The remote invocation error code is 870. This implies some sort of error condition (usually “none” or 0 is a “good” error code).
- The remote invocation description is “Adapter: presence failed.” Again, in the context of network interface card (NIC) discovery, this cannot be good.
- The program status is not complete (in this case, 21%), so the FSM is still working on it.
- The retry number is 20. An FSM will attempt to complete successfully in 20 retries at which point it will reset the retry counter and start at 0. FSMs do not stop trying until the user does something that conflicts with the FSM.

There is no direct way to cancel an FSM. In some restricted instances, however, you can request that Cisco UCS Manager perform the opposite action. For example, if you associate a service profile with a server and the FSM state for that association appears unsuccessful, you could disassociate the service profile from that server. In effect, this will cancel the association FSM. You could also decommission a server, which will cancel the current FSM running for that blade and remove any pending management requests.

Examining FSM State at the CLI

Examining FSM State at the CLI

```
demo-A# scope server 1/4
demo-A /chassis/server # show fsm status

Slot: 4
Server: sys/chassis-1/blade-4

FSM 1:
  Remote Result: End Point Protocol Error
  Remote Error Code: 1002
  Remote Error Description: Error communicating with Management Controller
  Status: Discover Blade Power On
  Previous Status: Discover Blade Power On
  Timestamp: 2009-05-13T21:49:40
  Try: 1
  Flags: 0
  Progress (%): 9
  Current Task: power on server 1/4 for discovery (FSM-STAGE:sam:dme:ComputeBladeDiscover:BladePowerOn)

FSM 2:
  Status: Nop
  Previous Status: Identify Success
  Timestamp: 2009-05-12T19:24:23
  Try: 0
  Progress (%): 100
  Current Task:
```

You can view the FSM of a managed object using the CLI. You may wish to set terminal settings (such as length and width) in addition to CLI settings (such as the delimiter) when displaying the FSM for enhanced readability.

Common Service Profile Configuration Issues Preventing Association

Common Service Profile Configuration Issues Preventing Association

- Insufficient Identities
 - UUID, MAC, WWNN, and WWPN pools
 - Service profile will not associate without sufficient pool resources
- Local disk configuration policy
 - Local disk policy must match local storage capability
- vNICs and vHBAs assigned to the same fabric
 - If two or more vNICs or vHBAs are created in service profile, assign to different fabrics

There are a number of parameters that must be correctly configured in order for the service profile to associate successfully. Some of the more common parameters include providing sufficient identities including universally unique identifiers (UUIDs), MAC addresses, world wide node names (WWNNs), and world wide port names (WWPNs). This is especially true when specifying and referencing identity pools within the service profile or service profile template.

In addition, the local disk policy of the specified server disk must match the policy that is configured on the local disk.

Providing the proper LAN and SAN connectivity assignments for both virtual NICS (vNICs) and virtual host bus adapters (vHBAs) is also critical for successful service profile association.

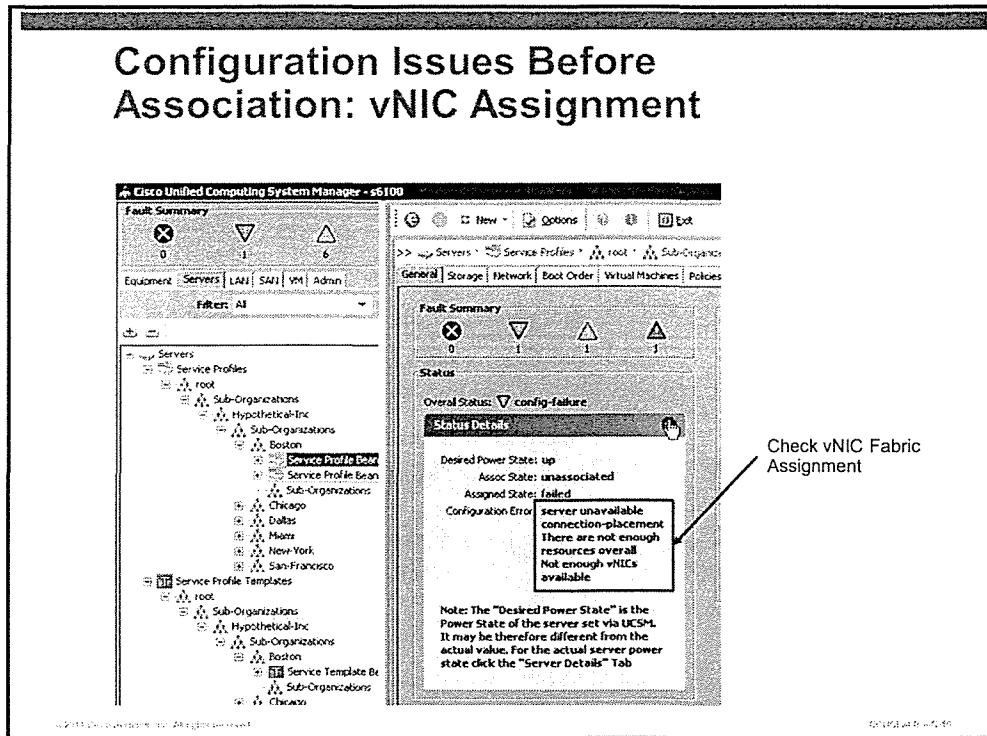
Configuration Example

Configuration Example	
Parameter	Description
Suborganization	Boston
Service profile template	Beantown
Server pool	Beantown-Chassis 1, Servers 7 and 8
UUID pool	Beantown-UUID (2 entries)
MAC pool	Beantown-MAC (2 entries)
WWNN pool	Beantown-WWNN (1 entry)
WWPN pool	Beantown-WWPN (2 entries)
Service profiles	Beantown-ESX1, Beantown-ESX2
Boot order	Default

In the configuration example shown in the figure, a suborganization named Boston has been created to house the service profile template, Beantown. The purpose of this example is to illustrate some of the common misconfiguration issues that preclude successful service profile association.

A server pool has been manually created and contains the servers that are contained in chassis 1 of the cluster, slots 7 and 8. UUID, MAC, WWNN, and WWPN pools have also been created with the listed number of entries. The default boot order has been specified and two service profiles—Beantown-ESX1 and ESX2—have been distilled from the Beantown service profile template.

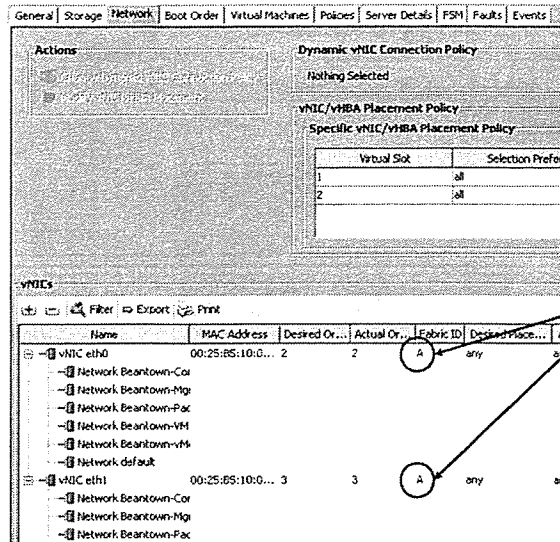
Configuration Issues Before Association: vNIC Assignment



The service profile Beantown-ESX1 has been selected to be associated with the server pool Beantown. The status message that is shown in the content pane indicates there are not enough vNICs available.

This problem is usually caused by improper assignment of one of the vNICs during the creation of the service profile or service profile template. If two vNICs are created in the profile, one must be assigned to Fabric A and the other to Fabric B. If the administrator inadvertently assigned both vNICs to a single fabric, it would preclude successful service profile association.

Configuration Issues Before Association: vNIC Assignment (Cont.)

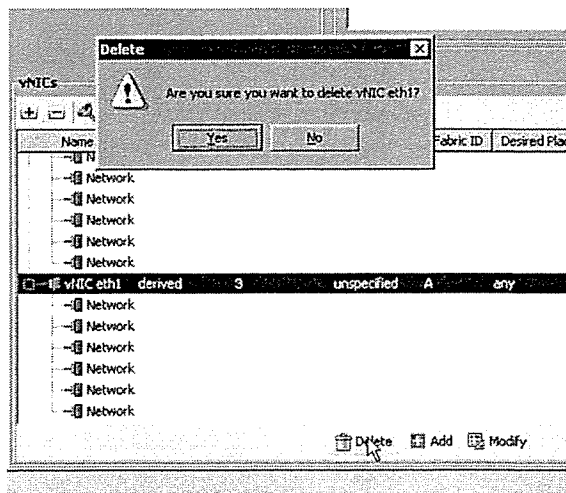


Name	MAC Address	Desired Or...	Actual Or...	Fabric ID	Desired Place...	Ac
vNIC eth0	00:25:85:10:0...	2	2	A	any	any
vNIC eth1	00:25:85:10:0...	3	3	A	any	any

Both vNICs assigned to the same fabric

The vNIC assignments may be reviewed by first selecting the Beantown Service Profile Template subtab (under the main Server tab) in the main navigation pane and then selecting the Network tab in the content pane. As shown, both vNICs have been assigned to Fabric A, which will preclude successful service profile association.

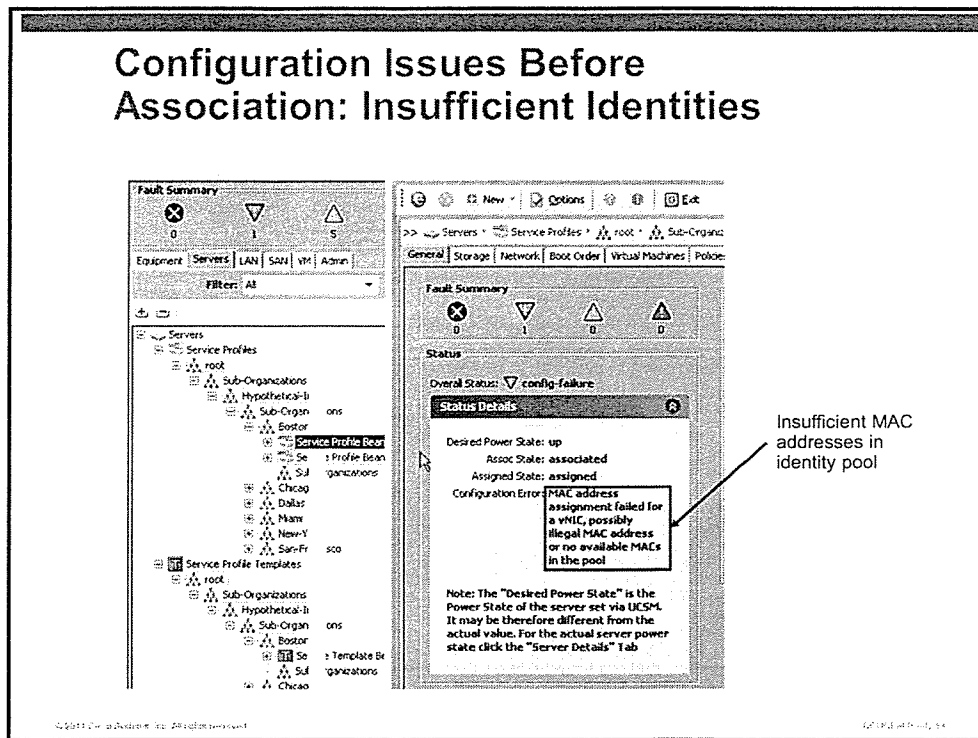
Configuration Issues Before Association: vNIC Assignment (Cont.)



Delete vNIC eth1, re-create it, and assign it to fabric B

The solution is to delete either vNIC. Then select **Save Changes** at the bottom of the Network window and re-create the vNIC with the proper fabric connectivity assignment. This will solve this issue as soon as the changes are saved.

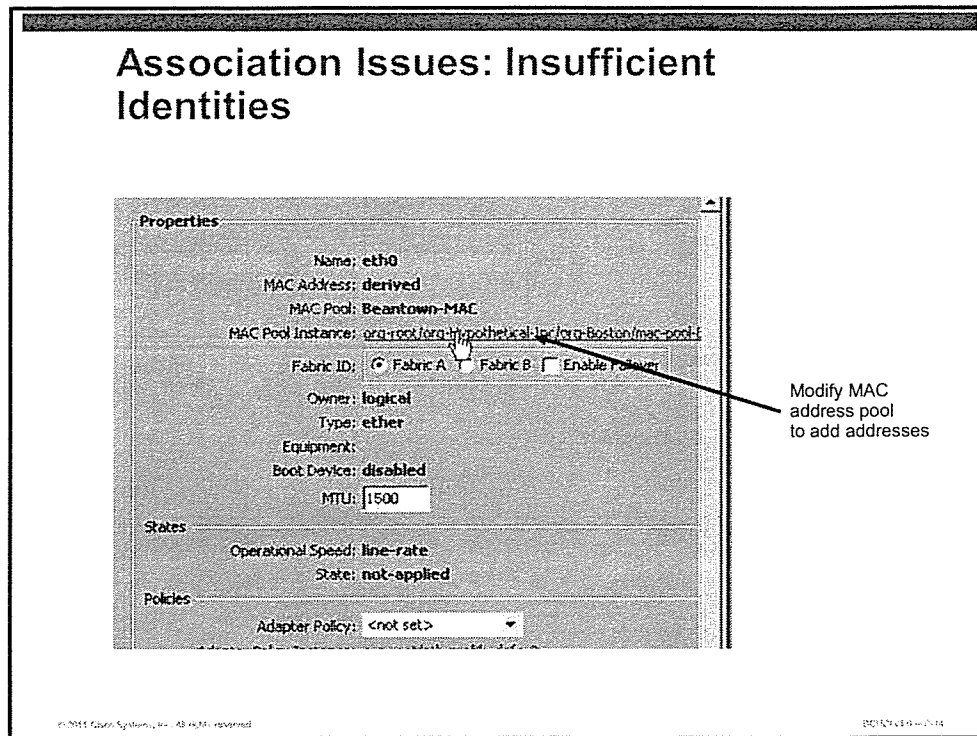
Configuration Issues Before Association: Insufficient Identities



The vNIC connectivity issue has been corrected and the Beantown-ESX1 service profile has again been assigned to the Beantown server pool. The content pane Status tab now indicates another service profile association problem.

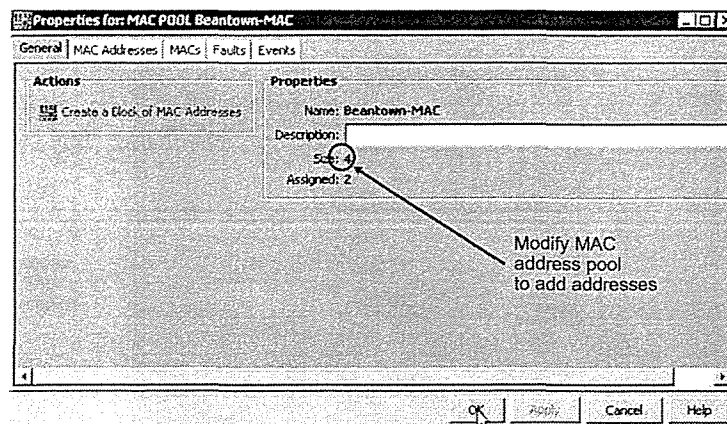
In this case, there are insufficient MAC addresses that are contained within the Beantown MAC pool. This condition would apply to all identity types and the service profile will not begin the association process until there are sufficient identity resources available.

Association Issues: Insufficient Identities



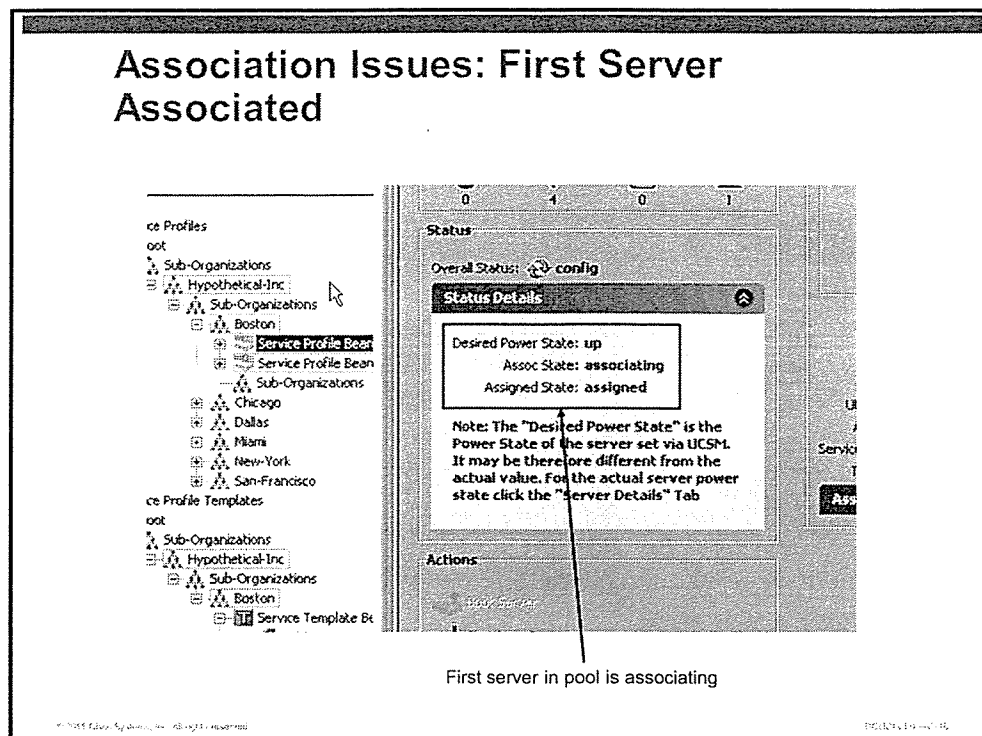
The solution to this issue is to access the Beantown MAC pool and provide additional addresses. You can access the Beantown MAC pool by selecting the Beantown Service Profile Template (under the Servers main navigation tab) and then choosing the Network content pane tab. The MAC pool instance is shown under the Properties window.

Association Issues: Insufficient Identities (Cont.)



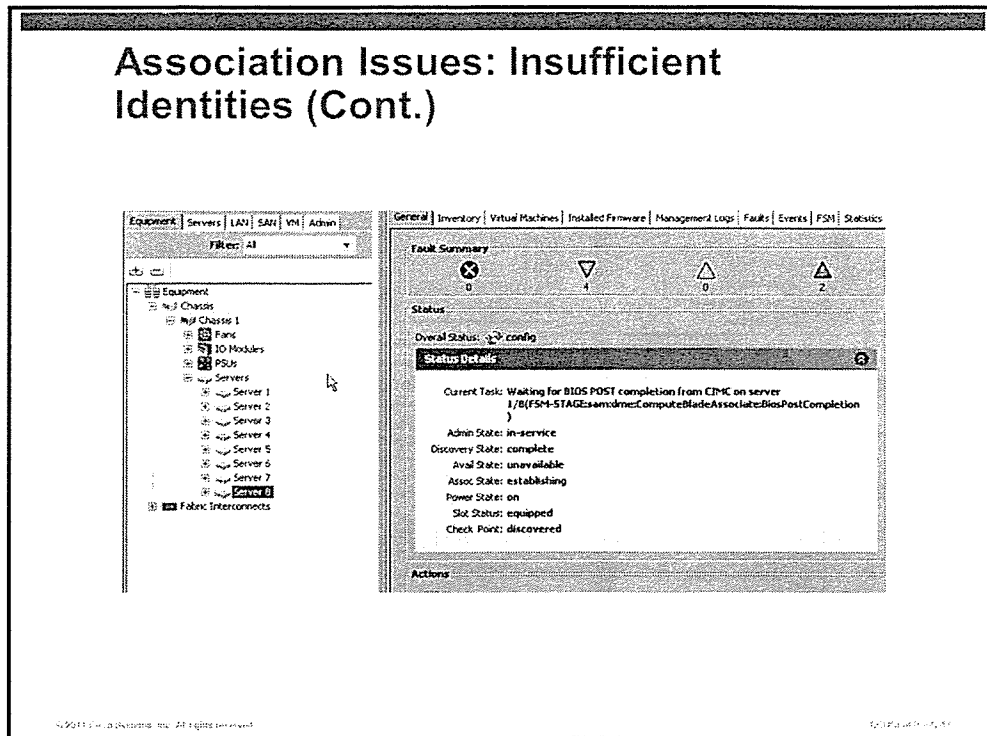
The Beantown MAC address pool has been modified to include two additional addresses. This would provide the sufficient number of MAC identities for the configuration example. This includes two servers in the Beantown server pool, each having two vNICs assigned to separate fabrics.

Association Issues: First Server Associated

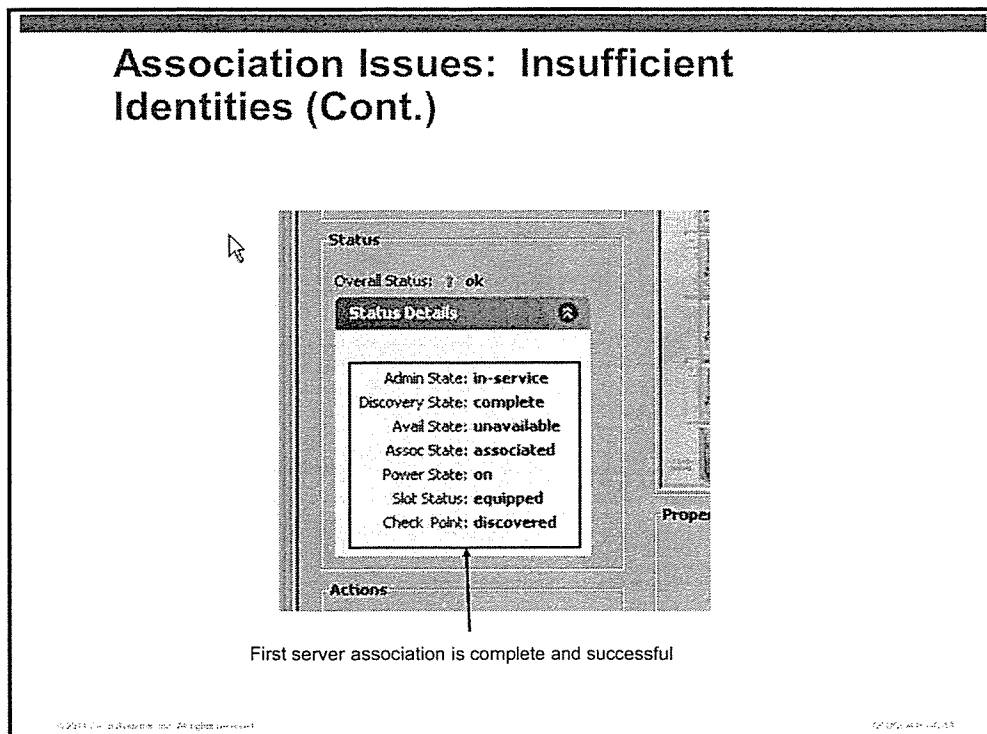


Now that the vNIC connectivity and MAC address pool issues have been corrected, the first server in the Beantown server pool (Chassis 1, Server 8) is now successfully associating to the service profile Beantown-ESX1.

Association Issues: Insufficient Identities (Cont.)



This status window appears by selecting the main Equipment tab in the Cisco UCS Manager navigation pane, followed by the Chassis 1, Server 8 subtab. Then choose the General tab within the content pane and view the Status window.



The Status tab now indicates that the first server in the Beantown server pool has successfully associated to the Beantown-ESX1 service profile.

Association Issues: Insufficient WWNN Identities

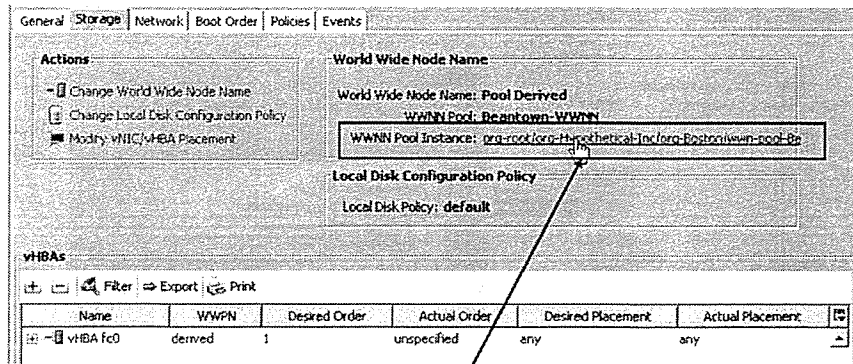
Association Issues: Insufficient WWNN Identities

Insufficient WWNN identities within pool;
second server association is unsuccessful

When the second service profile Beantown-ESX2 is assigned to the Beantown Server Pool, a config-failure message appears within the Status window. The message indicates a problem with the WWNN identity assignment.

This may be due to either a duplicate WWNN or there are insufficient WWNN identities that are contained within the Beantown WWNN pool.

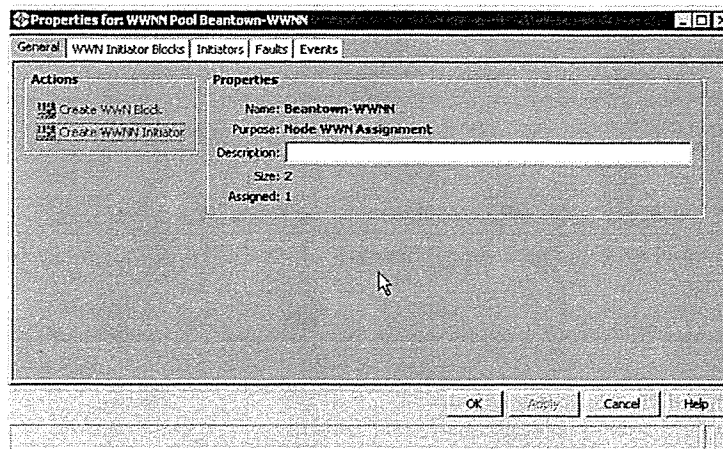
Association Issues: Insufficient WWNN Identities (Cont.)



Modify the WWNN pool to add more identities

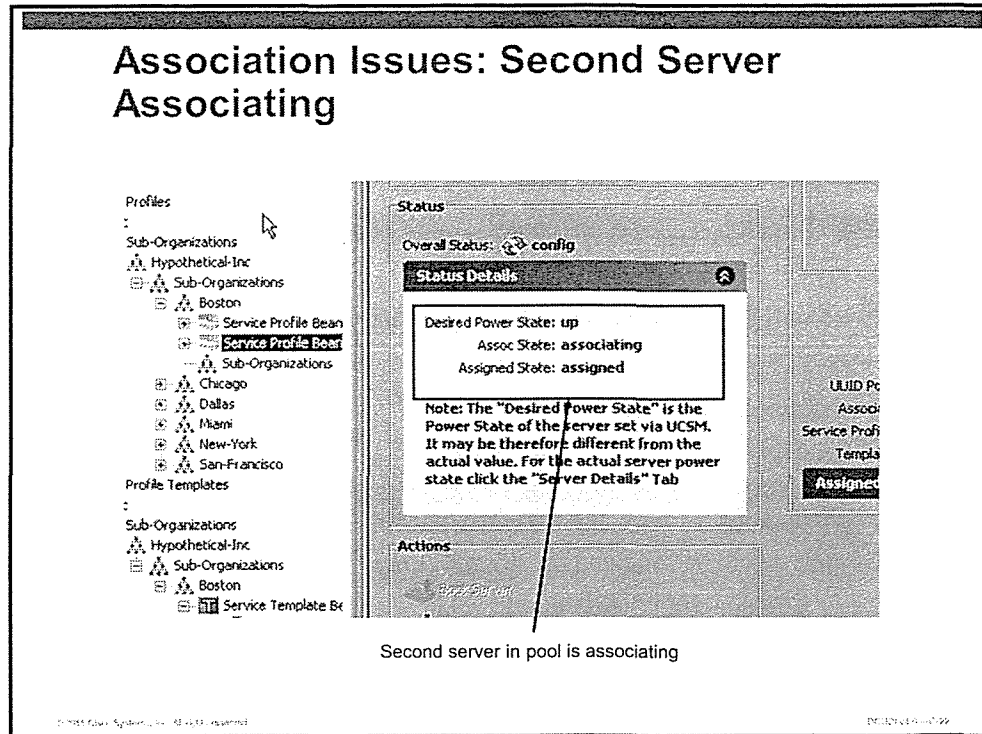
The solution to this issue is to access the Beantown WWNN pool and provide additional addresses. You can access the Beantown WWNN pool by selecting the Beantown Service Profile Template subtab (under the Servers main navigation tab) and then choosing the Storage tab. The WWNN pool instance is shown under the World Wide Node Name window.

Association Issues: Insufficient WWNN Identities (Cont.)



The Beantown WWNN address pool has been modified to include one additional address. This would provide the sufficient number of WWNN identities for the configuration example, which includes two servers in the Beantown server pool, each having a single mezzanine adapter.

Association Issues: Second Server Associating



The configuration issue that is associated with insufficient WWNN identities has been corrected and the Status window indicates that the second server in the Beantown server pool is now successfully completing the association process.

Three separate and unique configuration issues have been identified and corrected: vNIC connectivity assignment and insufficient MAC and WWNN identities. By correcting these issues, the service profiles Beantown-ESX1 and ESX2 have successfully associated, enabling the Cisco UCS Utility Operating System to complete the boot cycle.

However, there are additional configuration issues that can preclude the server from successfully booting either a guest operating system or hypervisor.

Troubleshooting Service Profile Issues After Association

This topic discusses troubleshooting service profile issues after association.

Service Profile Issues After Association

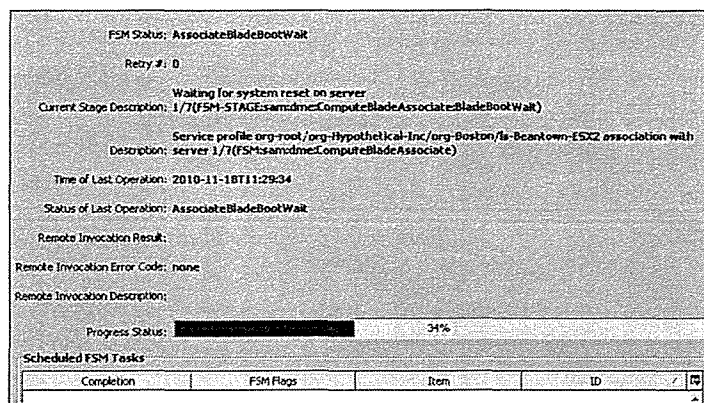
Service Profile Issues After Association

- Incorrect boot order
 - If LAN boot, connectivity issues
 - If SAN boot, incorrect boot target WWPN and LUN number
- Incorrect LUN masking on storage array
 - Check VSAN assignment
- Incorrect server BIOS settings
 - BIOS settings may be accessed from the KVM
- Incorrect virtual media mapping

© 2011 Cisco Systems, Inc. All rights reserved. | DCUCI v4.0 - 15/21

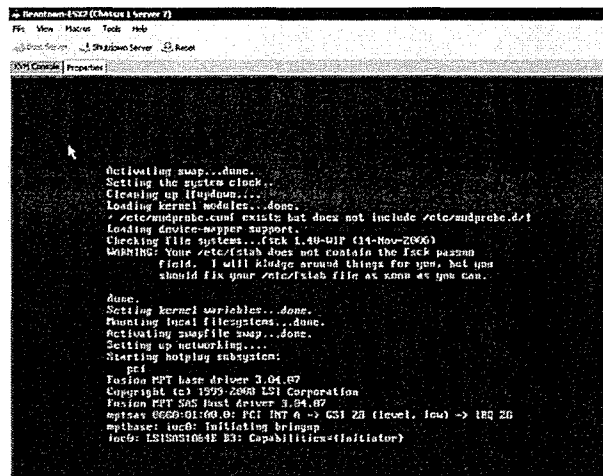
There are configuration issues that can affect the successful booting of either a guest operating system or hypervisor image on the server. These may include specifying an incorrect boot order, configuring incorrect logical unit number (LUN) masking on the SAN storage array, incorrect server BIOS setting, and an incorrect mapping of the virtual media.

Service Profile Issues After Association (Cont.)



The illustration in the figure of the Chassis 1, Server 7 FSM window provides status of the server association process. The successful association time is approximately 3 minutes after assigning the service profile to either an individual server or to a server pool.

Service Profile Issues After Association (Cont.)



The illustration in the figure shows the server keyboard, video, mouse (KVM) window and shows the Cisco UCS Utility Operating System successfully completing the boot cycle.

Service Profile Issues After Association (Cont.)

```
CLIENT MAC ADDR: 00 25 B5 10 00 0F GUID: 76CF5F1A 4317 11DF 0F0F 0F0F0F0F0F01
PXE-ES1: No DHCP or proxyDHCP offers were received.

PXE-M0F: Exiting Intel Boot Agent.

Intel(R) Boot Agent XG v2.1.11
Copyright (C) 1997-2008, Intel Corporation

CLIENT MAC ADDR: 00 25 B5 10 00 0C GUID: 76CF5F1A 4317 11DF 0F0F 0F0F0F0F0F01
PXE-ES1: No DHCP or proxyDHCP offers were received.

PXE-M0F: Exiting Intel Boot Agent.

Reboot and Select proper Boot device
or Insert Boot Media in selected Boot device and press a key

Intel(R) Boot Agent XG v2.1.11
Copyright (C) 1997-2008, Intel Corporation

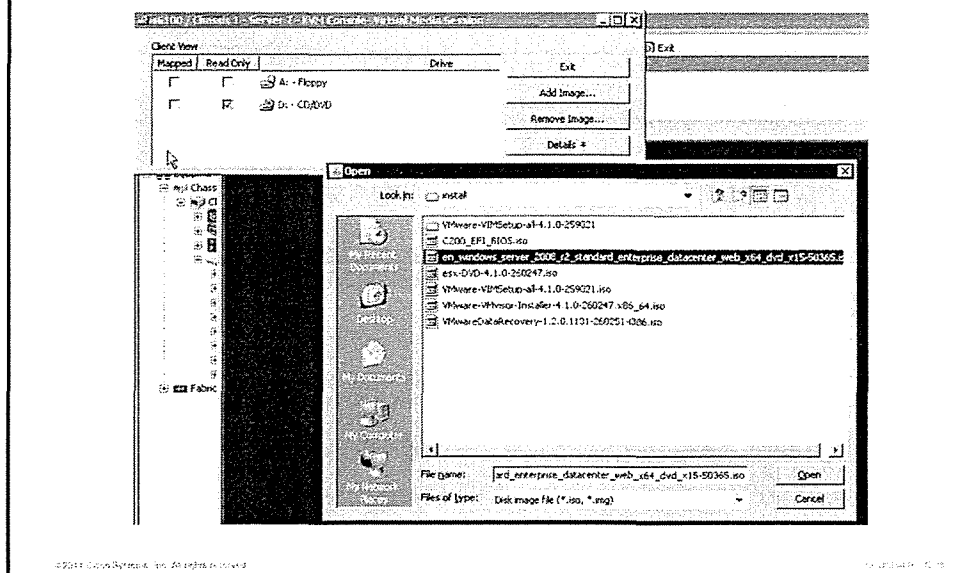
CLIENT MAC ADDR: 00 25 B5 10 00 0F GUID: 76CF5F1A 4317 11DF 0F0F 0F0F0F0F0F01
DHCP...1
```

The Cisco UCS Utility Operating System has completed, but the server cannot find the Guest operating system .iso image to boot from.

The Cisco UCS Utility Operating System has successfully completed the boot cycle, but, unfortunately, the server is unable to locate a suitable .iso image to continue booting either a guest operating system or hypervisor.

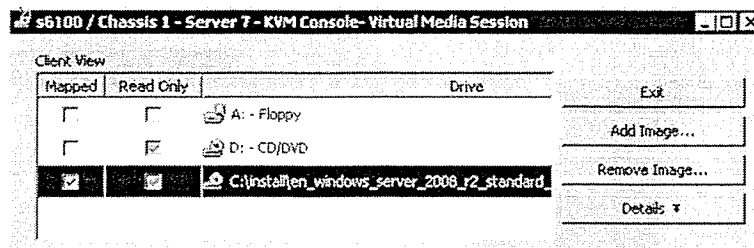
The problem could be either an incorrect boot order configuration within the service profile template, or mapping of the virtual media, or both.

Service Profile Issues After Association (Cont.)



The correct virtual media mapping is being configured. The Launch Virtual Media window is accessed by selecting the Tools menu directly from the server KVM. Then, choose **Launch Virtual Media**. When the window appears, select the Add Image tab and browse to the location on the local desktop that contains the guest operating system or hypervisor image.

Service Profile Issues After Association (Cont.)

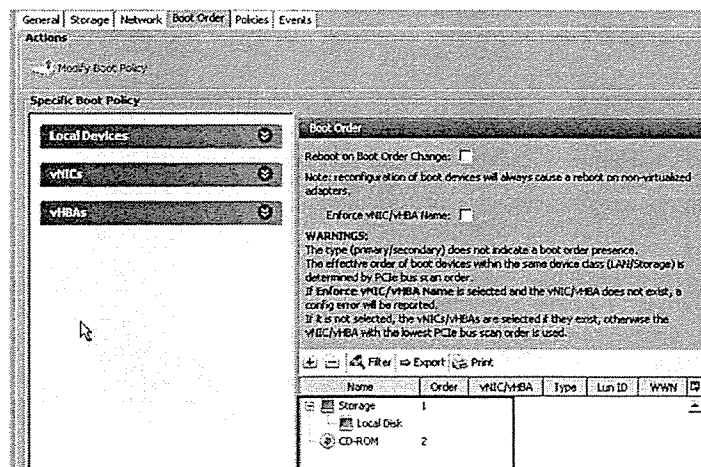


Setting the proper virtual media mapping is critical for the server to identify the path and location of the Guest operating system .iso image.

The illustration in the figure shows the Windows Server 2008 .iso image being mapped from the C: drive located on the local desktop that is running the Cisco UCS Manager application.

It is important to keep the Launch Virtual Media window open during the guest operating system boot process. The window can be minimized, but if it is closed, the mapping and path to the .iso image will be lost.

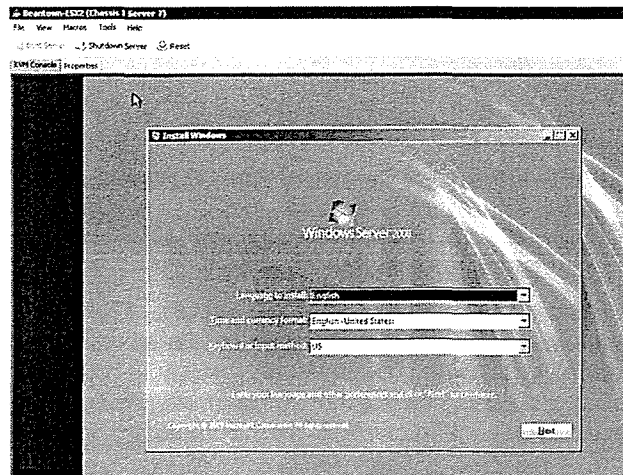
Service Profile Issues After Association (Cont.)



The proper boot order is critical for the server to boot an operating system.

The boot order configuration issue has been corrected. The server will now attempt to find the .iso image, first from the local disk and, if it is unsuccessful, will check the virtual CD-ROM.

Service Profile Issues After Association (Cont.)



The server has located the .iso image and is ready for configuration.

The image from the server KVM now indicates that the guest operating system .iso image has been found and the server is ready for configuration of the operating system.

Summary

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

Summary

- Successful service profile association can be compromised for a variety of reasons. These issues include incompatible local disk policy, insufficient identity pool resources, and improper vNIC or vHBA assignment.
- After successful service profile association, other parameters can preclude successful booting of the Guest operating system or hypervisor. These issues include improper boot order, improper or nonexistent virtual media mapping, and incorrect LAN or SAN boot target parameters.

Troubleshooting Cisco UCS B-Series Communications Failures

Overview

This lesson describes Cisco UCS Manager GUI and command-line interface (CLI) features that assist with the successful troubleshooting of LAN and SAN connectivity issues. The methodology that is presented will enable you to quickly and effectively determine problems and provide corrective action.

Objectives

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

- Describe the troubleshooting methodology for tracking communications from the blade server to the northbound Ethernet or SAN switch
- Describe the process to troubleshoot Ethernet connectivity within the Cisco UCS cluster
- Describe the process to troubleshoot Fibre Channel connectivity within the Cisco UCS cluster
- Describe the process to troubleshoot FCoE within a Cisco UCS cluster

Troubleshoot Communications from Server to Ethernet or SAN Switch

This topic discusses troubleshooting communications from the server to Ethernet or SAN switch.

Server Adapter View of Internal Backplane Ports

Server Adapter View of Internal Backplane Ports

Name	Overall Status	Fabric ID	Peer
Backplane Port 1/1	link-down	0	sys/chassis-1/blade-1/adapter...
Backplane Port 1/2	link-down	0	sys/chassis-1/blade-2/adapter...
Backplane Port 1/3	link-down	0	sys/chassis-1/blade-3/adapter...
Backplane Port 1/4	link-down	0	sys/chassis-1/blade-4/adapter...
Backplane Port 1/5	link-down	0	sys/chassis-1/blade-5/adapter...
Backplane Port 1/6	link-down	0	sys/chassis-1/blade-6/adapter...
Backplane Port 1/7	link-down	0	sys/chassis-1/blade-7/adapter...
Backplane Port 1/8	link-down	0	sys/chassis-1/blade-8/adapter...

Backplane ports should have a link-down status when the server is unassociated.

The first step in validating system connectivity from the mezzanine adapter to the northbound LAN or SAN switch is to view the backplane ports. The backplane ports are statically mapped to the I/O module (IOM) fabric uplink ports in a way that is determined by the number of active fabric uplinks.

To view the backplane ports that are mapped to the IOM fabric ports, select the Equipment tab within the main navigation page. Then choose the specific chassis under consideration and choose the particular IOM of interest. The summary of the backplane ports is shown on the content pane in the figure.

Notice that all of the backplane ports show an overall status of link-down. This is because none of the listed servers within Chassis 1 have service profiles that are associated with them. When a server has successfully associated with a service profile, the overall backplane port link-status should show as “up.”

View of Fabric Uplink Ports (I/O Module)

View of Fabric Uplink Ports (I/O Module)

The screenshot displays the Cisco UCS Manager interface. On the left, a navigation tree shows the hierarchy: Equipment > Chassis 1 > I/O Modules > I/O Module 1 > Fabric Ports. The main panel shows a table of four fabric uplink ports, all with an 'Overall Status' of 'Up'. A table at the bottom provides details for each port.

Name	Overall Status	Peer Slot ID	Peer Port ID	Fabric ID	Acknowledged	Peer
Fabric Port ... 10	Up	1	1	0	OK	SystemSwitch-B10...
Fabric Port ... 10	Up	2	2	0	OK	SystemSwitch-B10...
Fabric Port ... 10	Up	3	3	0	OK	SystemSwitch-B10...
Fabric Port ... 10	Up	4	4	0	OK	SystemSwitch-B10...

This figure shows the status of the IOM 1 fabric uplink ports. The illustration shows the overall status of all four fabric uplinks as up. This condition is correct after the chassis has successfully completed the acknowledgment process.

View of Server Ports from Fabric Interconnect

View of Server Ports from Fabric Interconnect						
Server Ports						
Filter Export Print						
Slot	Port ID	MAC	If Role	If Type	Overall Status	Administrative State
1	1	00:0D:EC:B2:1...	server	physical	up	enabled
1	2	00:0D:EC:B2:1...	server	physical	up	enabled
1	3	00:0D:EC:B2:1...	server	physical	up	enabled
1	4	00:0D:EC:B2:1...	server	physical	up	enabled

This view from the fabric interconnect perspective shows the overall status of the other end of the four fabric uplinks. They show an overall status of up.

To view this window, select the Equipment tab from the main navigation pane. Then select either the fabric interconnect A or B subtab. Choose the **Server Ports** option from the Actions window within the content pane.

Validate Northbound LAN Connectivity

Validate Northbound LAN Connectivity					
s6100-A(nxos)# show cdp neighbors					
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge					
S - Switch, H - Host, I - IGMP, r - Repeater,					
V - VoIP-Phone, D - Remotely-Managed-Device,					
s - Supports-STP-Dispute					
Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
N7010-C1(TBM12234289)	Eth1/19	170	R S I s	N7K-C7010	Eth2/9
N7010-C2(TBM12234230)	Eth1/20	178	R S I s	N7K-C7010	Eth2/9

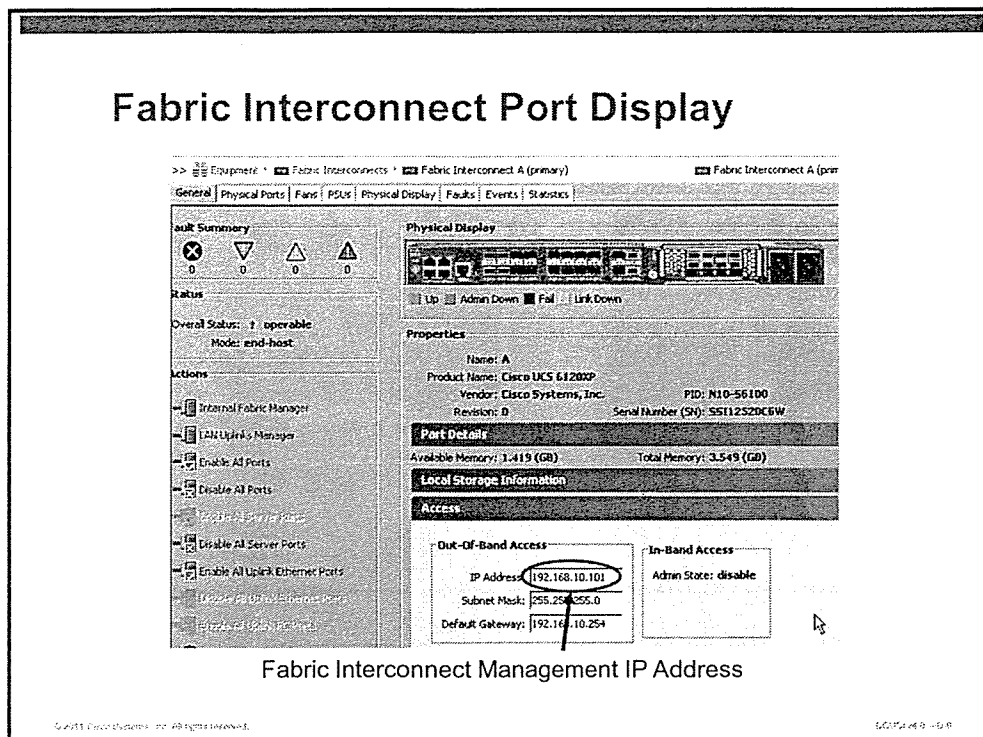
The **show cdp neighbors** command, issued from the primary fabric interconnect NX-OS shell, shows connectivity to the northbound Nexus 7010 switch. The local fabric interconnect interfaces are Eth1/19 and 20. The interface on the Nexus 7010 switch is Eth2/9.

The backplane ports should show an overall status of link-down when they are unassociated, and up when they are associated to a service profile. The fabric uplinks should show an overall status of up when chassis acknowledgment is completed. The northbound LAN uplinks status may be viewed from the primary fabric interconnect CLI.

Troubleshooting Ethernet Connectivity

This topic discusses troubleshooting Ethernet connectivity.

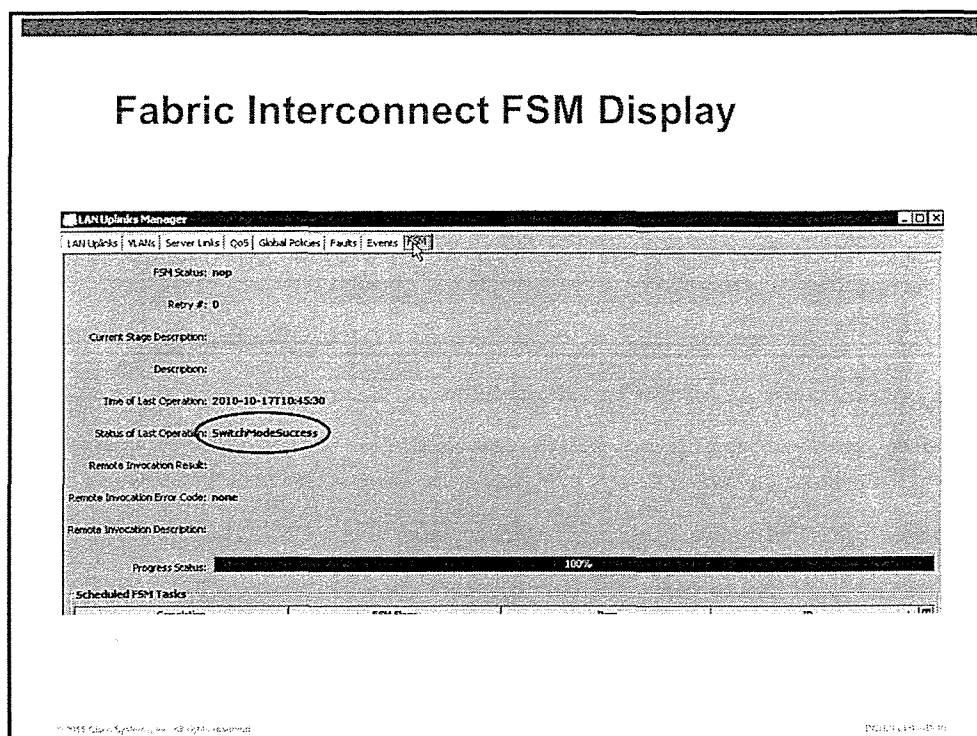
Fabric Interconnect Port Display



This is a view of the fabric interconnect General content pane window. The overall device status is operable and the mode of operation is end-host. This means that there is no local LAN switching being performed by the fabric interconnect. In addition, a visual representation of the fabric interconnect is shown with the operational status (green indicates up and operational) of the server, uplink, and Fibre Channel ports.

Also shown is the management IP address of the fabric interconnect, which in this example is 192.168.10.101. This may be used to set up a Telnet or SSH connection for remote management of the fabric interconnect.

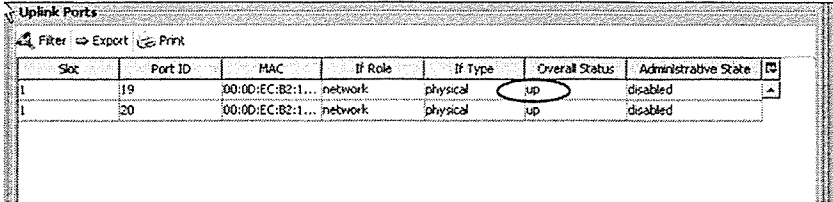
Fabric Interconnect FSM Display



This image displays the fabric interconnect FSM view and displays the Status of Last Operation as **SwitchModeSuccess**. This indicates that the fabric interconnect has booted successfully and is fully operational.

View of Northbound LAN Uplink Ports from Fabric Interconnect

View of Northbound LAN Uplink Ports from Fabric Interconnect



Slot	Port ID	MAC	If Role	If Type	Overall Status	Administrative State
1	19	00:00:EC:B2:1...	network	physical	up	disabled
1	20	00:00:EC:B2:1...	network	physical	up	disabled

This window displays the status of the northbound LAN uplinks that are connected to the upstream Nexus 7010 switch. The overall status is up, indicating a fully functioning LAN uplink. Notice that the illustration indicates that two out of the 20 fixed ports are being used as northbound LAN uplinks, which is fully recognized by Cisco UCS Manager.

To view this window from within Cisco UCS Manager, select the Equipment tab from the main navigation pane. Then choose the desired fabric interconnect subtab. From the Actions content pane options, choose **LAN Uplinks Manager**.

Validating VLAN Assignments

Validating VLAN Assignments

Name	ID	Fabric ID	Type	Transport	Native
VLAN ESXControl-g1 (173)	173	dual	lan	ether	no
VLAN ESXControl-g2 (172)	172	dual	lan	ether	no
VLAN ESXControl-g1 (171)	171	dual	lan	ether	no
VLAN ESXControl-g2 (170)	170	dual	lan	ether	no
VLAN ESXControl-g1 (175)	175	dual	lan	ether	no
VLAN ESXControl-g2 (174)	174	dual	lan	ether	no
VLAN ESXControl-g1 (177)	177	dual	lan	ether	no
VLAN ESXControl-g2 (176)	176	dual	lan	ether	no
VLAN POD1-10 (10)	10	dual	lan	ether	no
VLAN POD2-20 (20)	20	dual	lan	ether	no
VLAN POD3-30 (30)	30	dual	lan	ether	no
VLAN POD4-40 (40)	40	dual	lan	ether	no
VLAN POD5-50 (50)	50	dual	lan	ether	no
VLAN POD6-60 (60)	60	dual	lan	ether	no
VLAN default (1)	1	dual	lan	ether	yes

Fabric ID = Dual indicates that the VLAN is enabled on both fabrics.

By choosing the VLANs subtab to the right of the LAN Uplinks tab within the LAN Uplinks Manager, all configured and active VLANs that have been created on both fabric interconnects are listed.

The VLAN name, ID (number), and Fabric ID are listed. A Fabric ID listed as dual means that the VLAN has been enabled on both Fabric A and B.

Troubleshooting Fibre Channel Connectivity

This topic discusses troubleshooting Fibre Channel connectivity.

Fabric Interconnect Fibre Channel Interface Validation

Fabric Interconnect Fibre Channel Interface Validation

```
s6100-A(nxos)# show interface brief
```

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc2/1	11	NP	off	up	sw1	NP	4	--
fc2/2	11	NP	off	up	sw1	NP	4	--
fc2/3	11	NP	off	up	sw1	NP	4	--
fc2/4	11	NP	off	up	sw1	NP	4	--
fc2/5	11	NP	off	up	sw1	NP	4	--
fc2/6	11	NP	off	up	sw1	NP	4	--
fc2/7	11	NP	off	up	sw1	NP	4	--
fc2/8	11	NP	off	up	sw1	NP	4	--

Indicates that the fabric interconnect is operating in NPV mode.

Copyright © 2011 Cisco Systems, Inc. All rights reserved. SDCN14087-01-01

The **show interface brief** command that is issued from the primary fabric interconnect NX-OS shell first lists the Fibre Channel interfaces contained within the single fabric interconnect expansion module. The output lists all eight Fibre Channel interfaces, the VSAN assigned to fabric A (11), the status, and the operating speed of 4 Gb/s.

This is a valuable command to validate VSAN assignment and northbound SAN connectivity.

Fibre Channel Connectivity from SAN Switch View

Fibre Channel Connectivity from SAN Switch View

```
MDS9124-1# sh flogi database
```

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
fc1/3	11	0xdb0100	20:41:00:0d:ec:b2:17:40	20:0b:00:0d:ec:b2:17:41
fc1/3	11	0xdb010f	20:00:00:25:b5:01:0a:01	20:99:00:25:b5:01:00:01
		[dcucd-bl-a]		
fc1/4	11	0xdb0000	20:42:00:0d:ec:b2:17:40	20:0b:00:0d:ec:b2:17:41
fc1/5	11	0xdb0400	20:43:00:0d:ec:b2:17:40	20:0b:00:0d:ec:b2:17:41
fc1/6	11	0xdb0300	20:44:00:0d:ec:b2:17:40	20:0b:00:0d:ec:b2:17:41
fc1/7	11	0xdb0200	20:45:00:0d:ec:b2:17:40	20:0b:00:0d:ec:b2:17:41
fc1/8	11	0xdb0500	20:46:00:0d:ec:b2:17:40	20:0b:00:0d:ec:b2:17:41
fc1/9	11	0xdb0600	20:47:00:0d:ec:b2:17:40	20:0b:00:0d:ec:b2:17:41
fc1/10	11	0xdb0700	20:48:00:0d:ec:b2:17:40	20:0b:00:0d:ec:b2:17:41
fc1/12	11	0xdb0800	50:06:01:60:3b:a0:07:c9	50:06:01:60:bb:a0:07:c9
		[emc1-spa]		
fc1/13	11	0xdb0900	50:06:01:60:3b:a0:08:ed	50:06:01:60:bb:a0:08:ed
		[emc2-spa]		
fc1/15	11	0xdb0b00	50:06:01:60:3b:a0:08:9f	50:06:01:60:bb:a0:08:9f
		[emc3-spa]		

```
Total number of flogi = 12.
```

The **show flogi database** command that is issued from the upstream Fibre Channel switch has a valuable output that can determine which Fibre Channel ports have successfully completed the fabric login (FLOGI) process and been assigned an active Fibre Channel ID (which is analogous to a dynamically assigned IP address within the LAN environment).

The command output indicates that all eight of the Fibre Channel uplinks have successfully completed the fabric login process. Also shown is the nondefault VSAN 11 that has been assigned to Fabric A, as well as the world wide port names (WWPNs) and world wide node names (WWNNs).

Lastly, interface fc1/12 shows the Fibre Channel connection to the EMC storage array with a WWPN and WWNN prefix of 50 (indicates the vendor code for EMC).

Fibre Channel Switch Device Aliases

Fibre Channel Switch Device Aliases

```
MDS9124-1# show device-alias database
device-alias name p1-b-a-esx pwwn 20:00:00:25:b5:20:20:00
device-alias name p1-b-b-esx pwwn 20:00:00:25:b5:20:20:01
device-alias name p1-c-a-esx pwwn 20:00:00:25:b5:40:40:00
device-alias name p1-c-b-esx pwwn 20:00:00:25:b5:40:40:01
device-alias name p2-b-a-esx pwwn 20:00:00:25:b5:20:20:02
device-alias name p2-b-b-esx pwwn 20:00:00:25:b5:20:20:03
device-alias name p2-c-a-esx pwwn 20:00:00:25:b5:40:40:02
device-alias name p2-c-b-esx pwwn 20:00:00:25:b5:40:40:03
device-alias name p3-b-a-esx pwwn 20:00:00:25:b5:20:20:04
device-alias name p3-b-b-esx pwwn 20:00:00:25:b5:20:20:05
device-alias name p3-c-a-esx pwwn 20:00:00:25:b5:40:40:04
device-alias name p3-c-b-esx pwwn 20:00:00:25:b5:40:40:05
device-alias name p4-b-a-esx pwwn 20:00:00:25:b5:20:20:06
device-alias name p4-b-b-esx pwwn 20:00:00:25:b5:20:20:07
device-alias name p4-c-a-esx pwwn 20:00:00:25:b5:40:40:06
device-alias name p4-c-b-esx pwwn 20:00:00:25:b5:40:40:07
device-alias name p5-b-a-esx pwwn 20:00:00:25:b5:20:20:08
device-alias name p5-b-b-esx pwwn 20:00:00:25:b5:20:20:09
device-alias name p5-c-a-esx pwwn 20:00:00:25:b5:40:40:08
device-alias name p5-c-b-esx pwwn 20:00:00:25:b5:40:40:09
device-alias name p6-b-a-esx pwwn 20:00:00:25:b5:20:20:0a
device-alias name p6-b-b-esx pwwn 20:00:00:25:b5:20:20:0b
device-alias name p6-c-a-esx pwwn 20:00:00:25:b5:40:40:0a
```

The Cisco MDS Fibre Channel switch allows you to create aliases for WWNNs and WWPNS to make them easy to spot in various **show** commands. The **show device-alias database** command outputs a filterable list of WWNN and WWPNS aliases.

Fibre Channel Connectivity from SAN Switch View (Cont.)

- Output shows the eight Fibre Channel uplinks from the fabric interconnect to the SAN switch.
- Output shows the Fibre Channel connection to the storage array.

```
MDS9124-1# show fcns database
```

```
VSAN 11:
```

FCID	TYPE	PWWN	(VENDOR)	FC4-TYPE:FEATURE
0xdb0000	N	20:42:00:0d:ec:b2:17:40	(Cisco)	npv
0xdb0100	N	20:41:00:0d:ec:b2:17:40	(Cisco)	npv
0xdb0200	N	20:45:00:0d:ec:b2:17:40	(Cisco)	npv
0xdb0300	N	20:44:00:0d:ec:b2:17:40	(Cisco)	npv
0xdb0400	N	20:43:00:0d:ec:b2:17:40	(Cisco)	npv
0xdb0500	N	20:46:00:0d:ec:b2:17:40	(Cisco)	npv
0xdb0600	N	20:47:00:0d:ec:b2:17:40	(Cisco)	npv
0xdb0700	N	20:48:00:0d:ec:b2:17:40	(Cisco)	npv
0xdb0800	N	50:06:01:60:3b:a0:07:c9	(Clariion)	scsi-fcp[emcl-spa]

```
Total number of entries = 9
```

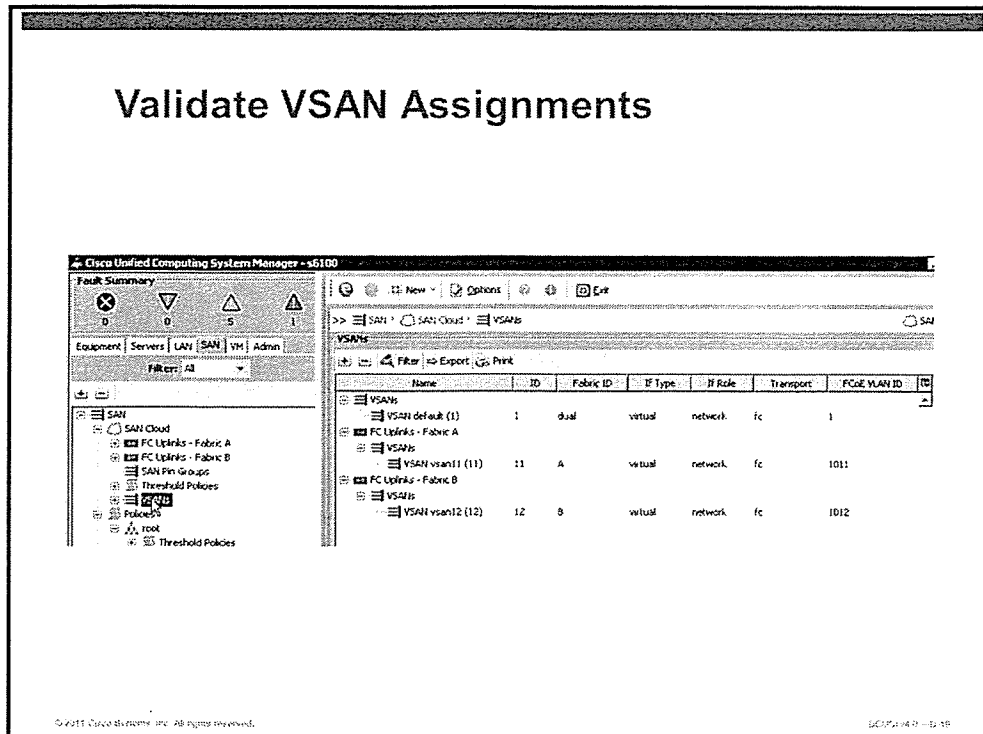
The **show fcns database** command that is issued from the northbound SAN switch (MDS9124) has a similar output to the **show flogi database** command, but it also provides the vendor name of the device that has connected to the name server object within the SAN switch.

Also notice that the FC-4 Type: Feature column shows npv, which stands for N-Port Virtualization. This is the only active mode currently available within Cisco UCS Manager. This means that there is no local SAN switching being performed on the fabric interconnect. The last entry in the command output lists the EMC Clariion storage array with a Small Computer Systems Interface (SCSI) (upper-layer storage protocol)-Fibre Channel Protocol (FCP) mapping.

Troubleshooting FCoE Connectivity

This topic discusses troubleshooting Fibre Channel over Ethernet (FCoE) connectivity.

Validate VSAN Assignments



This figure shows the VSAN assignment and may be used to troubleshoot VSAN configuration and connectivity. The output shows the default VSAN 1 assigned to both fabrics, with VSAN 11 assigned to Fabric A and VSAN 12 assigned to Fabric B.

To reach this window within Cisco UCS Manager, select the SAN main tab from the navigation pane. Then select the VSAN subtab from the SAN inventory pane.

Summary

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

Summary

- The Cisco UCS Manager GUI may be used to validate server connectivity to the northbound LAN or SAN switch.
- VLANs should be assigned to both fabrics in the Cisco UCS cluster.
- The **show cdp neighbors** command may be issued from the fabric interconnect NX-OS shell to validate northbound Ethernet connectivity.
- The **show flogi database** and **show fcns database** commands may be used from the SAN switch to validate proper Fibre Channel performance.

© 2011 Cisco Systems, Inc. All rights reserved.

DG-B4-M-0-000

