Cisco UCS Manager Troubleshooting Reference Guide

First Published: 2016-01-20

Last Modified: 2019-07-29

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

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2016–2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Audience

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

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

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

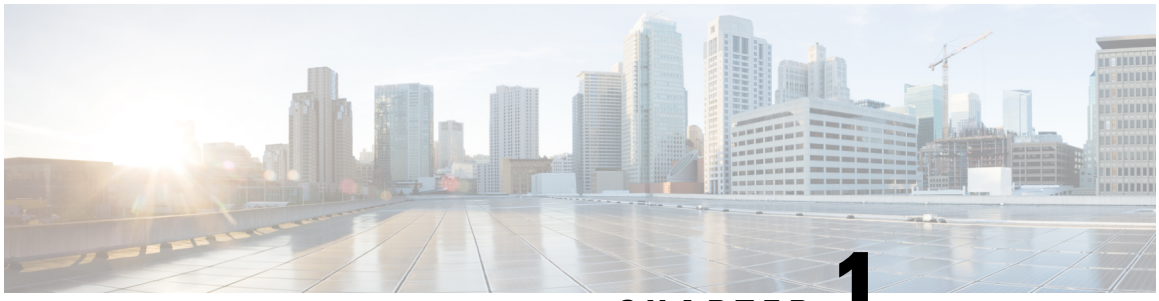
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@external.cisco.com. We appreciate your feedback.



CHAPTER 1

Overview

This chapter includes the following sections:

Overview

Troubleshooting in Cisco Unified Computing System Functional Planes

Cisco Unified Computing System (Cisco UCS) is designed with a distinct separation of management, control, and data planes. This section provides a brief background on how the distribution of processes across the three planes can arise troubleshooting scenarios that must be uniquely identified and resolved.

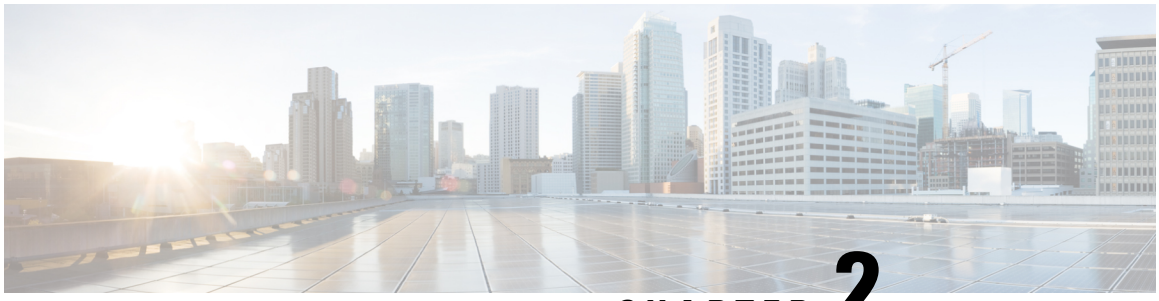
After Cisco UCS Manager configures a system, it runs without interaction with the management plane. The system accomplishes tasks, such as moving network profiles along with virtual machines, completely through control plane interactions. In a high availability configuration with synchronized state and failover between the two fabric interconnects, Cisco UCS Manager can fail or be taken out of service while its software is upgraded. It can be shut down and upgraded to a new version without affecting the data and control planes. The OS and application can still send or receive LAN and SAN traffic even while Cisco Manager is disabled.

Troubleshooting Reference Guide Overview

This guide provides information to help you troubleshoot common problems in the three functional planes of Cisco UCS. The following table describes the overall organization of the guide:

Chapter	Description
Overview	Overview of troubleshooting in Cisco Unified Computing System based on the three functional planes of operation — management, control, and data planes.
General Troubleshooting Solutions	Information about tools available in Cisco UCS Manager for troubleshooting.
Management Plane	

Chapter	Description
Troubleshooting issues with Cisco UCS B-Series Operation	Troubleshooting information for issues related to Cisco UCS B-Series operation such as server boot, KVM and fabric interconnect issues. It also includes troubleshooting information for Cisco UCS Manager initial configuration.
Control and Data Planes	
Troubleshooting Cisco UCS SAN Connectivity	Troubleshooting information for issues related to SAN boot and SAN Connectivity.
Troubleshooting and Upgrading Cisco UCS Manager	Troubleshooting information for issues related to Firmware upgrade process.
Troubleshoot Server Hardware issues	Troubleshooting information for issues related to server hardware including DIMM memory, CPU, RAID and adapter issues.
Troubleshooting IOM Issues	Troubleshooting information for IOM–related issues.
Additional Troubleshooting Information	Links to additional troubleshooting documents.



CHAPTER 2

General Troubleshooting Solutions

This chapter includes the following sections:

Guidelines for Troubleshooting

When you troubleshoot issues with Cisco UCS Manager or a component that it manages, you should follow the guidelines listed in the following table.

Table 1: Troubleshooting Guidelines

Guideline	Description
Check the release notes to see if the issue is a known problem.	The release notes are accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.
Take screenshots of the fault or error message dialog box, the FSM for the component, and other relevant areas.	These screenshots provide visual cues about the state of Cisco UCS Manager when the problem occurred. If your computer does not have software to take screenshots, check the documentation for your operating system, as it might include this functionality.

Guideline	Description
Record the steps that you took directly before the issue occurred.	If you have access to screen or keystroke recording software, repeat the steps you took and record what occurs in Cisco UCS Manager. If you do not have access to that type of software, repeat the steps you took and make detailed notes of the steps and what happens in Cisco UCS Manager after each step.
Create a technical support file.	The information about the current state of the Cisco UCS domain is very helpful to Cisco support and frequently provides the information needed to identify the source of the problem.

Faults

In Cisco UCS, a fault is a mutable object that is managed by Cisco UCS Manager. Each fault represents a failure in the Cisco UCS domain or an alarm threshold that has been raised. During the lifecycle of a fault, it can change from one state or severity to another.

Each fault includes information about the operational state of the affected object at the time the fault was raised. If the fault is transitional and the failure is resolved, the object transitions to a functional state.

A fault remains in Cisco UCS Manager until the fault is cleared and deleted according to the settings in the fault collection policy.

You can view all faults in a Cisco UCS domain from either the Cisco UCS Manager CLI or the Cisco UCS Manager GUI. You can also configure the fault collection policy to determine how a Cisco UCS domain collects and retains faults.

Note All Cisco UCS faults are included in MIBs and can be trapped by SNMP.

Fault Severities

A fault raised in a Cisco UCS domain can transition through more than one severity during its lifecycle. The following table describes the fault severities that you may encounter.

Severity	Description
Critical	Service-affecting condition that requires immediate corrective action. For example, this severity could indicate that the managed object is out of service and its capability must be restored.
Major	Service-affecting condition that requires urgent corrective action. For example, this severity could indicate a severe degradation in the capability of the managed object and that its full capability must be restored.

Severity	Description
Minor	Nonservice-affecting fault condition that requires corrective action to prevent a more serious fault from occurring. For example, this severity could indicate that the detected alarm condition is not degrading the capacity of the managed object.
Warning	Potential or impending service-affecting fault that has no significant effects in the system. You should take action to further diagnose, if necessary, and correct the problem to prevent it from becoming a more serious service-affecting fault.
Condition	Informational message about a condition, possibly independently insignificant.
Info	Basic notification or informational message, possibly independently insignificant.

Fault States

A fault raised in a Cisco UCS domain transitions through more than one state during its lifecycle. The following table describes the possible fault states in alphabetical order.

State	Description
Cleared	Condition that has been resolved and cleared.
Flapping	Fault that was raised, cleared, and raised again within a short time interval, known as the flap interval.
Soaking	Fault that was raised and cleared within a short time interval, known as the flap interval. Because this state may be a flapping condition, the fault severity remains at its original active value, but this state indicates the condition that raised the fault has cleared.

Fault Types

A fault raised in a Cisco UCS domain can be one of the types described in the following table.

Type	Description
fsm	FSM task has failed to complete successfully, or Cisco UCS Manager is retrying one of the stages of the FSM.
equipment	Cisco UCS Manager has detected that a physical component is inoperable or has another functional issue.
server	Cisco UCS Manager cannot complete a server task, such as associating a service profile with a server.
configuration	Cisco UCS Manager cannot successfully configure a component.

Type	Description
environment	Cisco UCS Manager has detected a power problem, thermal problem, voltage problem, or loss of CMOS settings.
management	Cisco UCS Manager has detected a serious management issue, such as one of the following: • Critical services could not be started • The primary fabric interconnect could not be identified • Components in the Cisco UCS domain include incompatible firmware versions
connectivity	Cisco UCS Manager has detected a connectivity problem, such as an unreachable adapter.
network	Cisco UCS Manager has detected a network issue, such as a link down.
operational	Cisco UCS Manager has detected an operational problem, such as a log capacity issue or a failed server discovery.
generic	Cisco UCS Manager has detected a generic issue, such as Board Controller upgrade requires a manual power cycle of the server.
sysdebug	Cisco UCS Manager has detected a system debug issue, such as auto core transfer failure at remote server since the remote server is not accessible or because the remote server details for transfer are incorrect.
security	Cisco UCS Manager has detected a security issue, such as invalid certificate.
chassis profile	This fault is raised when Cisco UCS Manager cannot complete a chassis task, such as associating a chassis profile with a chassis.

Fault Properties

Cisco UCS Manager provides detailed information about each fault raised in a Cisco UCS domain. The following table describes the fault properties that you can view in Cisco UCS Manager CLI or Cisco UCS Manager GUI.

Property Name	Description
Severity	Current severity level of the fault, which can be any of the severities described in Fault Severities, on page 4 .
Last Transition	Day and time on which the severity for the fault last changed. If the severity has not changed since the fault was raised, this property displays the original creation date.
Affected Object	Component that is affected by the condition that raised the fault.
Description	Description of the fault.

Property Name	Description
ID	The unique identifier associated with the message.
Type	Type of fault that has been raised, which can be any of the types described in Fault Types, on page 5 .
Cause	Unique identifier associated with the condition that caused the fault.
Created at	Day and time when the fault occurred.
Code	The unique identifier assigned to the fault.
Number of Occurrences	Number of times the event that raised the fault occurred.
Original Severity	Severity assigned to the fault the first time it occurred.
Previous Severity	Previous severity level. This property is only used if the severity of a fault changes during its lifecycle.
Highest Severity	Highest severity encountered for this issue.

Lifecycle of Faults

Faults in Cisco UCS are stateful. Only one instance of a given fault can exist on each object. If the same fault occurs a second time, Cisco UCS increases the number of occurrences by one.

A fault has the following lifecycle:

1. A condition occurs in the system and Cisco UCS Manager raises a fault. This is the active state.
2. When the fault is alleviated, it enters a flapping or soaking interval that is designed to prevent flapping. Flapping occurs when a fault is raised and cleared several times in rapid succession. During the flapping interval, the fault retains its severity for the length of time specified in the fault collection policy.
3. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared.
4. The cleared fault enters the retention interval. This interval ensures that the fault reaches the attention of an administrator even if the condition that caused the fault has been alleviated and the fault has not been deleted prematurely. The retention interval retains the cleared fault for the length of time specified in the fault collection policy.
5. If the condition reoccurs during the retention interval, the fault returns to the active state. If the condition does not reoccur, the fault is deleted.

Faults in Cisco UCS Manager GUI

If you want to view faults for a single object in the system, navigate to that object in the Cisco UCS Manager GUI and click the **Faults** tab in the **Work** pane. If you want to view faults for all objects in the system, navigate to the **Faults** node on the **Admin** tab under **Faults, Events and Audit Log**.

In addition, you can also view a summary of all faults in a Cisco UCS domain in the **Fault Summary** area in the upper left of the Cisco UCS Manager GUI. This area provides a summary of all faults that have occurred in the Cisco UCS domain.

Each fault severity is represented by a different icon. The number below each icon indicates how many faults of that severity have occurred in the system. If you click an icon, the Cisco UCS Manager GUI opens the **Faults** tab in the **Work** pane and displays the details of all faults with that severity.

Faults in Cisco UCS Manager CLI

If you want to view the faults for all objects in the system, enter the **show fault** command from the top-level scope. If you want to view the faults for a specific object, scope to that object and then execute the **show fault** command.

If you want to view all available details about a fault, enter the **show fault detail** command.

Fault Collection Policy

The fault collection policy controls the lifecycle of a fault in the Cisco UCS domain, including the length of time that each fault remains in the flapping and retention intervals.

Tip For information on how to configure the fault collection policy, see the Cisco UCS Manager configuration guides, which are accessible through the Cisco UCS B-Series Servers Documentation Roadmap.

Events

In Cisco UCS, an event is an immutable object that is managed by Cisco UCS Manager. Each event represents a nonpersistent condition in the Cisco UCS domain. After Cisco UCS Manager creates and logs an event, the event does not change. For example, if you power on a server, Cisco UCS Manager creates and logs an event for the beginning and the end of that request.

You can view events for a single object, or you can view all events in a Cisco UCS domain from either the Cisco UCS Manager CLI or the Cisco UCS Manager GUI. Events remain in the Cisco UCS until the event log fills up. When the log is full, Cisco UCS Manager purges the log and all events in it.

Properties of Events

Cisco UCS Manager provides detailed information about each event created and logged in a Cisco UCS domain. The following table describes the fault properties that you can view in Cisco UCS Manager CLI or Cisco UCS Manager GUI.

Table 2: Event Properties

Property Name	Description
Affected Object	Component that created the event.
Description	Description of the event.

Property Name	Description
Cause	Unique identifier associated with the event.
Created at	Date and time when the event was created.
User	Type of user that created the event, such as one of the following: • admin • internal • blank
Code	Unique identifier assigned to the event.

Events in the Cisco UCS Manager GUI

If you want to view events for a single object in the system, navigate to that object in the Cisco UCS Manager GUI and click the Events tab in the Work pane. If you want to view events for all objects in the system, navigate to the Events node on the Admin tab under the Faults, Events and Audit Log.

Events in the Cisco UCS Manager CLI

If you want to view events for all objects in the system, enter the **show event** command from the top-level scope. If you want to view events for a specific object, scope to that object and then enter the **show event** command.

If you want to view all available details about an event, enter the **show event detail** command.

Audit Log

The audit log records actions performed by users in Cisco UCS Manager, including direct and indirect actions. Each entry in the audit log represents a single, non-persistent action. For example, if a user logs in, logs out, or creates, modifies, or deletes an object such as a service profile, Cisco UCS Manager adds an entry to the audit log for that action.

You can view the audit log entries in the Cisco UCS Manager CLI, Cisco UCS Manager GUI, or in a technical support file that you output from Cisco UCS Manager.

Audit Log Entry Properties

Cisco UCS Manager provides detailed information about each entry in the audit log. The following table describes the fault properties that you can view in the Cisco UCS Manager GUI or the Cisco UCS Manager CLI.

Table 3: Audit Log Entry Properties

Property Name	Description
ID	Unique identifier associated with the audit log message.
Affected Object	Component affected by the user action.
Severity	Current severity level of the user action associated with the audit log message. These severities are also used for the faults, as described Fault Severities, on page 4.
Trigger	User role associated with the user that raised the message.
User	Type of user that created the event, as follows: • admin • internal • blank
Indication	Action indicated by the audit log message, which can be one of the following: • creation—A component was added to the system. • modification—An existing component was changed.
Description	Description of the user action.

Audit Log in the Cisco UCS Manager GUI

In the Cisco UCS Manager GUI, you can view the audit log on the **Audit Log** node on the **Admin** tab under the **Faults, Events and Audit Log** node.

Audit Log in the Cisco UCS Manager CLI

In the Cisco UCS Manager CLI, you can view the audit log through the following commands:

- **scope security**
- **show audit-logs**

System Event Log

The system event log (SEL) resides on the CIMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes.

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

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

The backup file is automatically generated. The filename format is sel-*SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp*; for example, sel-UCS-A-ch01-serv01-QCI12522939-20091121160736.

SEL File

The SEL file is approximately 40 KB. No further events can be recorded when the SEL file is full. It must be cleared before additional events can be recorded.

SEL Policy

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

Cisco UCS Manager automatically generates the SEL backup file, according to the settings in the SEL policy. The filename format is `sel-SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp`

For example, a filename could be `sel-UCS-A-ch01-serv01-QCI12522939-20091121160736`.

Syslog

The syslog provides a central point for collecting and processing system logs that you can use to troubleshoot and audit a Cisco UCS domain. Cisco UCS Manager relies on the Cisco NX-OS syslog mechanism and API, and on the syslog feature of the primary fabric interconnect to collect and process the syslog entries.

Cisco UCS Manager collects and logs syslog messages internally. You can send them to external syslog servers running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Some syslog messages to monitor include, DIMM problems, equipment failures, thermal problems, voltage problems, power problems, high availability (HA) cluster problems, and link failures.

Note The FSM faults, threshold faults, and unresolved policy events are not sent to syslog server. However, SNMP traps are generated for the threshold fault events.

Cisco UCS Manager manages and configures the syslog collectors for a Cisco UCS domain and deploys the configuration to the fabric interconnect or fabric interconnects. This configuration affects all syslog entries generated in a Cisco UCS domain by Cisco NX-OS or by Cisco UCS Manager.

You can configure Cisco UCS Manager to do one or more of the following with the syslog and syslog entries:

- Display the syslog entries in the console or on the monitor
- Store the syslog entries in a file

- Forward the syslog entries to up to three external log collectors where the syslog for the Cisco UCS domain is stored

Syslog messages contain an event code and fault code. To monitor syslog messages, you can define syslog message filters. These filters can parse the syslog messages based on the criteria you choose. You can use the following criteria to define a filter:

- By event or fault codes: Define a filter with a parsing rule to include only the specific codes that you intend to monitor. Messages that do not match these criteria are discarded.
- By severity level: Define a filter with a parsing rule to monitor syslog messages with specific severity levels. You can set syslog severity levels individually for OS functions, to facilitate logging and display of messages ranging from brief summaries to detailed information for debugging.

Syslog Entry Format

Each syslog entry generated by a Cisco UCS component is formatted as follows:

```
Year month date hh:mm:ss hostname %facility-severity-MNEMONIC description
```

For example: `2007 Nov 1 14:07:58 excal-113 %MODULE-5-MOD_OK: Module 1 is online`

Syslog Entry Severities

A syslog entry is assigned a Cisco UCS severity by Cisco UCS Manager. The following table shows how the Cisco UCS severities map to the syslog severities.

Table 4: Syslog Entry Severities in Cisco UCS

Cisco UCS Severity	Syslog Severity
CRIT	CRIT
MAJOR	ERR
MINOR	WARNING
WARNING	NOTICE
INFO	INFO

Syslog Entry Parameters

The following table describes the information contained in each syslog entry.

Table 5: Syslog Message Content

Name	Description
Facility	Logging facility that generated and sent the syslog entry. The facilities are broad categories that are represented by integers. These sources can be one of the following standard Linux facilities: • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7
Severity	Severity of the event, alert, or issue that caused the syslog entry to be generated. The severity can be one of the following: • emergencies • critical • alerts • errors • warnings • information • notifications • debugging
Hostname	Hostname included in the syslog entry that depends upon the component where the entry originated, as follows: • The fabric interconnect, Cisco UCS Manager, or the hostname of the Cisco UCS domain • For all other components, the hostname associated with the virtual interface (VIF)
Timestamp	Date and time when the syslog entry was generated.
Message	Description of the event, alert, or issue that caused the syslog entry to be generated.

Syslog Services

The following Cisco UCS components use the Cisco NX-OS syslog services to generate syslog entries for system information and alerts:

- I/O module—All syslog entries are sent by syslogd to the fabric interconnect to which it is connected.
- CIMC—All syslog entries are sent to the primary fabric interconnect in a cluster configuration.
- Adapter—All syslog entries are sent by NIC-Tools/Syslog to both fabric interconnects.
- Cisco UCS Manager—Self-generated syslog entries are logged according to the syslog configuration.

Technical Support Files

When you encounter an issue that requires troubleshooting or a request for assistance to the Cisco Technical Assistance Center (Cisco Technical Assistance Center), collect as much information as possible about the affected Cisco UCS domain. Cisco UCS Manager outputs this information into a tech support file that you can send to Cisco.

You can create a tech support file for the following components of a Cisco UCS domain:

- UCSM—Contains technical support data for the entire Cisco UCS domain.
- UCSM management services—Contains technical support data for the Cisco UCS Manager management services, excluding Fabric Interconnects.
- Chassis—Contains technical support data for the I/O module or the CIMCs on the blade servers in a given chassis only.
- Fabric extender—Contains technical support data for the given FEX.
- Rack server—Contains technical support data for the given rack-mount server and adapter.
- Server memory—Contains server memory technical support data for the given rack-mount servers and blade servers.

Creating a Tech Support File in the Cisco UCS Manager GUI

Note In releases earlier than Cisco UCS Manager Release 1.4(1), you can create a technical support file only in the Cisco UCS Manager CLI.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All**.

Step 3 In the **Work** pane, click **Create and Download Tech Support**.

Step 4 In the **Path** field in the **Create and Download a Tech Support File** dialog box, enter the full path where the technical support file should be saved.

This path must be locally accessible. If you do not know the path, click the **Browse** button to navigate to it.

Name	Description
Path field	The full path where the technical support file should be saved. This path must be locally accessible.

Step 5 In the **Options** area, click one of the following radio buttons:

Option	Description
ucsm	Creates a file containing technical support data for the entire Cisco UCS domain. If you select **ucsm**, Cisco UCS Manager GUI displays the following options: • **Exclude Commands**—Reduces the size of the tech support file by excluding all CLI commands. • **Include Fabric Interconnect Trace Logs**—Includes any trace logs generated by the fabric interconnects. You should only check these options if directed to do so by Cisco Technical Assistance Center.
ucsm-mgmt	Creates a file containing technical support data for the Cisco UCS management services, excluding the fabric interconnects. If you select **ucsm-mgmt**, Cisco UCS Manager GUI displays the following options: • **Exclude Commands**—Reduces the size of the tech support file by excluding all CLI commands. • **Include Fabric Interconnect Trace Logs**—Includes any trace logs generated by the fabric interconnects. You should only check these options if directed to do so by Cisco Technical Assistance Center.

Option	Description
chassis	Creates a file containing technical support data for either the CIMCs or I/O modules in a given chassis. When you select this option, Cisco UCS Manager GUI displays the following fields: • **Chassis ID** field—The chassis for which you want technical support data. • **CIMC** radio button—Select this option to get CIMC technical support data. To get the data for a single server within the chassis, enter that server's ID in the **CIMC ID** field. To get the CIMC data for all servers in the chassis, enter **`all`** in this field. • **IOM** radio button—Select this option to get I/O module technical support data. To get the data for a single server within the chassis, enter that server's ID in the **IOM ID** field. To get the I/O module data for all servers in the chassis, enter **`all`** in this field.
fabric-extender	Creates a file containing technical support data for a fabric extender. When you select this option,Cisco UCS Manager GUI displays the **FEX ID** field that lets you enter the unique identifier of the FEX for which you want technical support data.
rack-server	Creates a file containing technical support data for a C-Series server. When you select this option, Cisco UCS Manager GUI displays the following fields: • **Rack Server ID** field—The unique identifier of the rack server, or the rack server number for which you want technical support data. For example, 4 or 7. • **Rack Server Adapter ID** field—The unique identifier of the adapter for which you want technical support data. To get the data for all adapters in the server, enter **`all`** in this field.
server-memory	Saves a file containing server memory technical support data for B-Series and C-Series servers to the specified directory. When you select this option, Cisco UCS Manager GUI displays the following field: **Server IDs** field—The comma-separated list of unique identifiers of the blade servers and rack servers for which you want detailed server memory technical support data. For blade servers, each server ID is in the following form—*chassis-num*/*blade-server-num*. For example, 1/3 or 4/5. For rack servers, each server ID is the following form—*rackserver-num*. For example, 4 or 7.

Step 6 Click **OK**.

Creating a Technical Support File in the Cisco UCS Manager CLI

Use the **show tech-support** command to output information about a Cisco UCS domain that you can send to Cisco Technical Assistance Center.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt** {**a** | **b**}	Enters local management mode.

Step 2	UCS-A(local-mgmt) # **show tech-support** {**chassis** *chassis-id* {**all** | **cimc** *slot* [**adapter** *adapter-id*] | **iom** *iom-id*} | **fex** *fex-id* | **server** *server-id* [**adapter** *adapter-id*] | **server-memory** {*server-list* | **all**} | **ucsm** | **ucsm-mgmt**} [**brief** | **detail**]	Outputs information about the selected objects in a file that you can send to Cisco Technical Assistance Center. The following options are available:
		• **chassis**—Creates file containing technical support data for either the CIMCs or I/O modules in a given chassis.
		• **fex**—Creates a file containing technical support data for a fabric extender.
		• **server**—Creates a file containing technical support data for a C-Series server.
		• **server-memory**—Creates a technical support file with all server memory related information. You can run the **server-memory** command for the following:
		  • One blade server or rack-mount server
		  • Multiple blade servers
		  • Multiple rack-mount servers
		  • A mix of blade and rack-mount servers
		  • All servers
		Important Multiple servers specified in the *server-list* must be separated by commas. You cannot run this command for a range of servers.
		If you use the **server-memory** option with the **detail** option, detailed information about the memory is saved into a file and the file name and path are displayed.

	Command or Action	Purpose
		• **ucsm**—Creates a file containing technical support data for the entire Cisco UCS domain. • **ucsm-mgmt**—Creates a file containing technical support data for the Cisco UCS management services, excluding the fabric interconnects.
Step 3	UCS-A (local-mgmt) # **copy workspace:techsupport/***filename.tar* {**scp** | **ftp**}: *user_name@IP_address* Enter *username*'s password: *password*	Copies the output file to an external location through SCP or FTP. The SCP and FTP commands require an absolute path for the target location. The path to your home directory cannot include special symbols, such as '~'.

Powering Down a Cisco UCS Domain

You can decommission an entire Cisco UCS domain, for example as part of a planned power outage.

Procedure

Step 1 Create a configuration backup.

For more information, see the Cisco UCS Manager configuration guides for the release of Cisco UCS Manager that you are using. The configuration guides are accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Step 2 Gracefully power down all of the blades or rack servers from their installed operating system.

You can power down the servers from the OS on the server or through Cisco UCS Manager.

Step 3 Unplug the chassis power or the power to the rack servers after all of the servers are powered down.

When the servers are powered down, the power LEDs are amber rather than green.

Step 4 Power down each fabric interconnect by unplugging the power cords in the following order:

- Unplug the subordinate fabric interconnect.
- Unplug the primary fabric interconnect.

Verification of LDAP Configurations

Note This procedure can be performed only through the Cisco UCS Manager CLI.

The Cisco UCS Manager CLI **test** commands verify the configuration of the Lightweight Directory Access Protocol (LDAP) provider or the LDAP provider group.

Verifying the LDAP Provider Configuration

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

You can enter the **test aaa server ldap** command to verify the following information if Cisco UCS Manager is able to communicate with the LDAP provider as follows:

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

Procedure

	Command or Action	Purpose
Step 1	**connect nxos**	Enters nxos mode.
Step 2	**test aaa server ldap**	Tests the LDAP provider configuration.

Example

The following is an example of the response:

```
UCS-A# /security # connect nxos
UCS-A#(nxos)# test aaa server ldap 10.193.23.84 kjohn Nbv12345
user has been authenticated
Attributes downloaded from remote server:
User Groups:
CN=g3,CN=Users,DC=ucsm  CN=g2,CN=Users,DC=ucsm  CN=group-2,CN=groups,DC=ucsm
CN=group-1,CN=groups,DC=ucsm  CN=Domain Admins,CN=Users,DC=ucsm
CN=Enterprise Admins,CN=Users,DC=ucsm  CN=g1,CN=Users,DC=ucsm
CN=Administrators,CN=Builtin,DC=ucsm
User profile attribute:
shell:roles="server-security,power"
shell:locales="L1,abc"
Roles:
```

```
server-security power
Locales:
L1 abc
```

Verifying the LDAP Provider Group Configuration

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

You can enter the **test aaa group** command to verify the following information if Cisco UCS Manager is able to communicate with the LDAP group as follows:

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

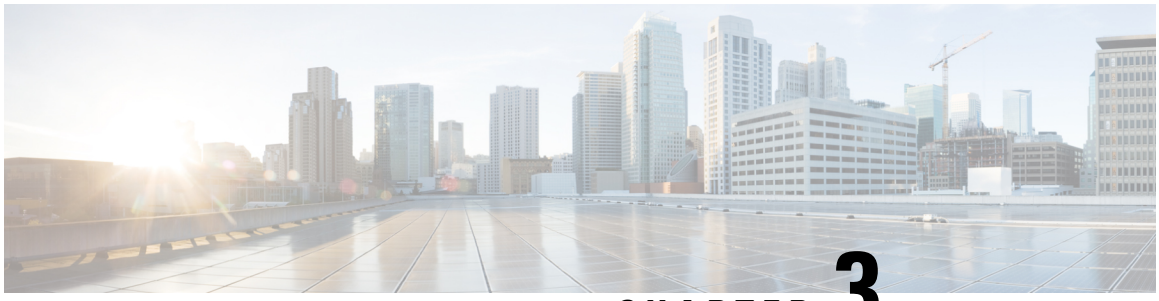
Procedure

	Command or Action	Purpose
Step 1	**connect nxos**	Enters nxos mode.
Step 2	**test aaa group**	Tests the LDAP group configuration.

Example

The following is an example of the response:

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



CHAPTER 3

Troubleshooting Issues with Cisco UCS B-Series Operation

This chapter includes the following sections:

Troubleshooting Cisco UCS Manager Initial Configuration

Verify Console Setup

You can verify that both fabric interconnect configurations are complete by logging into the fabric interconnect via SSH and verifying the cluster status through CLI. For this procedure, you can watch Cisco UCS Manager Initial Setup part 3.

Use the following commands to verify the cluster state:

Command	Purpose	Sample Output

show cluster state	Displays the operational state and leadership role for both fabric interconnects in a high availability cluster.	The following example displays that both fabric interconnects are in the Up state, HA is in the Ready state, fabric interconnect A has the primary role, and fabric interconnect B has the subordinate role:
		`UCS-A# show cluster state`
		`Cluster Id:`
		`0x4432f72a371511de-0xb97c000de1b1ada4`
		
		`A: UP, PRIMARY`
		`B: UP,`
		`SUBORDINATE HA READY`

show cluster extended-state	Displays extended details about the cluster state and typically used when troubleshooting issues.	The following example shows how to view the extended state of a cluster:
		`UCSC# show cluster`
		`extended-state`
		`0x2e95deadbd0f11e2-0x8ff35147e84f3de2Start`
		` time: Thu May 16 06:54:22`
		`2013Last election time: Thu`
		`May 16 16:29:28 2015System`
		`Management`
		`Viewing the Cluster State`
		`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`
		`HA READY`
		`Detailed state of the device`
		`selected for HA quorum data:`
		`Device 1007, serial:`
		`a66b4c20-8692-11df-bd63-1b72ef3ac801,`
		` state: active`
		`Device 1010, serial:`
		`00e3e6d0-8693-11df-9e10-0f4428357744,`
		` state: active`
		`Device 1012, serial:`
		`1d8922c8-8693-11df-9133-89fa154e3fa1,`
		` state: active

Troubleshooting Boot Issues

Reboot Warning Does Not Display

Problem—The system fails to produce a reboot warning that lists any dependencies.

Possible Cause—This problem can be caused by changes to a vNIC template or a vHBA template. Reboot warnings occur when the back-end returns a list of dependencies. When you update the template type for a vNIC or vHBA template and make changes to any boot-related properties without applying changes between steps, the back-end systems are not triggered to return a list of dependencies.

Procedure

Step 1 Launch the Cisco UCS Manager GUI.

Step 2 In the vNIC template or vHBA template included in the service profile, do the following:

a) Change the template type from **Initial Template** to **Updating Template**.
b) Click **Save Changes**.

Step 3 Make any additional changes to the reboot-related values and click **Save Changes**.

A reboot warning and the list of dependencies are displayed.

Server Does Not Boot from OS Installed on eUSB

Problem—The eUSB embedded inside the Cisco UCS server includes an operating system. However, the server does not boot from that operating system.

Possible Cause—This problem can occur when, after associating the server with the service profile, the eUSB is not at the top of the actual boot order for the server.

Procedure

Step 1 Launch the Cisco UCS Manager GUI.

Step 2 On **Servers**, do the following to verify the boot policy configuration:

a) Navigate to the service profile associated with the server.
b) In the **Work** pane, click the **Boot Order** tab
c) Ensure that **Local Disk** is configured as the first device in the boot policy.

Step 3 On **Equipment**, do the following to verify the actual boot order for the server:

a) Navigate to the server.
b) On the **General** tab, expand the **Boot Order Details** area and verify that the eUSB is listed as the first device on the **Actual Boot Order** tab.

For example, the first device should be **VM eUSB DISK**.

Step 4 If the eUSB is not the first device in the actual boot order, do the following:

a) On the **General** tab for the server, click the following links in the **Actions** area:

- Click **KVM Console** to launch the KVM console.
- Click **Boot Server** to boot the server.

b) In the KVM console, while the server is booting, press **F2** to enter the BIOS setup.
c) In the BIOS utility, click on the **Boot Options** tab.
d) Click **Hard Disk Order**.
e) Configure **Boot Option #1** to the eUSB.

For example, set this option to **VM eUSB DISK**.

f) Press **F10** to save and exit.

Server Does Not Boot After RAID1 Cluster Migration

Problem—The server does not boot from the operating system after a RAID1 cluster migration. The RAID LUN remains in "inactive" state during and after service profile association. As a result, the server cannot boot.

Possible Cause—This problem can occur if the local disk configuration policy in the service profile on the server is configured with **Any Configuration** mode rather than RAID1.

Procedure

Step 1 In Cisco UCS Manager GUI, click **Servers**.

Step 2 Navigate to the service profile associated with the server and click the **Storage** tab.

Step 3 Do one of the following:

- Change the local disk configuration policy included in the service profile to the same policy included in the service profile associated with the server prior to the migration, as follows:
  - In the **Actions** area, click **Change Local Disk Configuration Policy**.
  - From the **Select the Local Disk Configuration Policy** drop-down list, choose the appropriate policy.
  - Click **OK**.
- Change the mode property in the local disk configuration policy included in the service profile, as follows:
  - In the **Local Disk Configuration Policy** area of the **Storage** tab, click the link in the **Local Disk Policy Instance** field.
  - In the **Mode** field, ensure that the **Raid 1 Mirrored** option is chosen.
  - Click **Save Changes**.

Troubleshooting KVM Issues

BadFieldException When Launching the KVM Viewer

Problem—The BadFieldException error appears when the KVM viewer is launched.

Possible Cause—This problem can occur because the Java Web Start disables the cache by default when it is used with an application that uses native libraries.

Procedure

Step 1 Choose **Start** > **Control Panel** > **Java**.
Step 2 Click on the **General** tab.
Step 3 In the **Temporary Internet Files** area, click **Settings**.
Step 4 Click the **Keep temporary files on my computer** check box.
Step 5 Click **OK**.

KVM Console Failure

Problem—The KVM console fails to launch and the JRE displays the following message:

```
Unable to launch the application.
```

Possible Cause—This problem can be caused if several KVM consoles are launched simultaneously.

Procedure

Step 1 If possible, close all of the open KVM consoles.
Step 2 Relaunch the KVM consoles one at a time.

KVM Fails to Open

Problem—The first time you attempt to open the KVM on a server, the KVM fails to launch.

Possible Cause—This problem can be caused by a JRE version incompatibility.

Procedure

Step 1 Upgrade to JRE 1.6_11.
Step 2 Reboot the server.

Step 3 Launch the KVM console.

Troubleshooting VM issues

No Ports Available for Distributed Virtual Switch

Problem—The following error displays:

```
Currently connected network interface x uses Distributed Virtual Switch (uusid:y) which is
accessed on the host via a switch that has no free ports.
```

Possible Cause—This problem can be caused by one of the following issues:

- After powering off or migrating a VM from one host to another, the vSphere server fails to recompute the numPortsAvailable property in the hostProxySwitch object.
- The cumulative number of vNICs for the VMs powered on an ESX host matches or exceeds the number of dynamic nVINCs configured in the server's service profile.
- After migrating a VM from one data-store to another data-store on the same server, the server incorrectly detects an increase in the number of DVS ports being used by all of the VMs powered on the host.

Procedure

Step 1 Identify what you were doing when the error displayed.

Step 2 If the error resulted from powering off a VM, or from migrating a VM from one host to another, do the following:

a) Migrate a second VM from the ESX host to another system.
b) When a second port is made available, do one of the following:
   - Power on a VM.
   - Migrate a VM back to the ESX host.

Step 3 If the error resulted from migrating a VM instance from one data-store to another data-store on the same server, do the following:

a) Shut down all of the VMs on the ESX host.
b) Retry the migration.

Troubleshooting Cisco UCS Manager Issues

DME Process Timed Out

Problem—When you run Cisco UCS Manager CLI commands, Cisco UCS Manager CLI displays the following message:

```
Software Error: Exception during execution: [Error: Timed out communicating with DME]
```

Possible Cause—This problem occurs when the DME process on the primary fabric interconnect is either unresponsive or has crashed, and is not in the running state. Other symptoms that appear when the DME is down are:

- Cisco UCS Manager GUI becomes unresponsive
- Connectivity to Virtual IP goes down

Procedure

Step 1 Gather information on the sequence of events, such as upgrade of Cisco UCS Manager and configuration changes, that lead the system to this state.

Step 2 Connect to each fabric interconnect by using its individual IP address, and verify the cluster status, process and core dumps by using the following commands:

a) UCS-A# **connect local-mgmt**

Enters local management mode for the cluster.

b) UCS-A (local-mgmt) # **show cluster extended-state**

Displays the state of fabric interconnects in the cluster and whether the cluster is HA ready.

c) UCS-A(local-mgmt)# **show pmon state**

Displays the state of all processes within Cisco UCS Manager.

d) UCS-A(local-mgmt)# **ls workspace:/cores**

Displays a list of all core dumps in workspace.

Step 3 Identify the primary fabric interconnect, and whether HA election is incomplete.

Step 4 Review NXOS logs for fabric interconnect hardware issues by using the following commands:

a) UCS-A# **connect nxos {a | b}**

Enters NX-OS mode for the fabric interconnect.

b) UCS-A(nxos)# **show logg**

Displays details about log files.

Step 5 Collect technical support information for Cisco UCS Manager from local-mgmt CLI by using the following commands:

a) UCS-A# **connect local-mgmt**

Enters local management mode for the cluster.

b) UCS-A(local-mgmt)# **show tech-support ucsm detail**

Displays technical support information for Cisco UCS Manager.

What to do next

Contact TAC with these logs and information to further investigate the failure.

Event Sequencing Fatal Error

Problem—After coming back from sleep mode, the Cisco UCS Manager GUI displays the following message:

```
Fatal error: event sequencing is skewed.
```

Possible Cause—This problem can be caused if the Cisco UCS Manager GUI was running when the computer went to sleep. Since the JRE does not have a sleep detection mechanism, the system is unable to retrack all of the messages received before it went into sleep mode. After multiple retries, this event sequencing error is logged.

Note Always shut down Cisco UCS Manager GUI before putting your computer to sleep.

Procedure

In Cisco UCS Manager GUI, if a **Connection Error** dialog box is displayed, click one of the following:

- Click **Re-login** to log back in to the Cisco UCS Manager GUI.
- Click **Exit** to exit the Cisco UCS Manager GUI.

Troubleshooting Fabric Interconnect Issues

Recovering a Fabric Interconnect from the Boot Loader Prompt

If the fabric interconnect fails to start, you may have one of the following issues:

- The kickstart image is corrupted or non-functional for other reasons
- The file system on the bootflash memory is corrupted

If either of these issues exist, you might need to use the boot loader prompt to recover the fabric interconnect.

Procedure

Contact Cisco Technical Assistance Center to obtain the firmware recovery images and information about how to recover the fabric interconnect from the boot loader prompt.

Resolving Fabric Interconnect Cluster ID Mismatch

Problem—When you set up two fabric interconnects to support a high availability cluster and connect the L1 ports and L2 ports, a fabric interconnect cluster ID mismatch can occur. This type of mismatch means that the cluster fails and Cisco UCS Manager cannot be initialized.

Procedure

Step 1 In Cisco UCS Manager CLI, connect to fabric interconnect B and execute **erase configuration**.

All configuration on the fabric interconnect is erased.

Step 2 Reboot fabric interconnect B.

After rebooting, fabric interconnect B detects the presence of fabric interconnect A and downloads the cluster ID from fabric interconnect A. You need to configure the subordinate fabric interconnect for the cluster configuration.

Step 3 When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.

Note The fabric interconnect should detect the peer fabric interconnect in the cluster. If it does not, check the physical connections between the L1 and L2 ports, and verify that the peer fabric interconnect has been enabled for a cluster configuration.

Step 4 Enter **y** to add the subordinate fabric interconnect to the cluster.

Step 5 Enter the admin password of the peer fabric interconnect.

Step 6 Enter the IP address for the management port on the subordinate fabric interconnect.

Step 7 Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings.

If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

Troubleshooting Server Disk Drive Detection and Monitoring

Support for Local Storage Monitoring

The type of monitoring supported depends upon the Cisco UCS server.

Supported Cisco UCS Servers for Local Storage Monitoring

Through Cisco UCS Manager, you can monitor local storage components for the following servers:

- Cisco UCS B200 M3 blade server
- Cisco UCS B420 M3 blade server
- Cisco UCS B22 M3 blade server
- Cisco UCS B200 M4 blade server
- Cisco UCS B260 M4 blade server
- Cisco UCS B460 M4 blade server
- Cisco UCS C460 M2 rack server
- Cisco UCS C420 M3 rack server
- Cisco UCS C260 M2 rack server
- Cisco UCS C240 M3 rack server
- Cisco UCS C220 M3 rack server
- Cisco UCS C24 M3 rack server
- Cisco UCS C22 M3 rack server
- Cisco UCS C220 M4 rack server
- Cisco UCS C240 M4 rack server
- Cisco UCS C460 M4 rack server

Note Not all servers support all local storage components. For Cisco UCS rack servers, the onboard SATA RAID 0/1 controller integrated on motherboard is not supported.

Supported Cisco UCS Servers for Legacy Disk Drive Monitoring

Only legacy disk drive monitoring is supported through Cisco UCS Manager for the following servers:

- Cisco UCS B200 M1/M2 blade server
- Cisco UCS B250 M1/M2 blade server

Note In order for Cisco UCS Manager to monitor the disk drives, the 1064E storage controller must have a firmware level contained in a UCS bundle with a package version of 2.0(1) or higher.

Prerequisites for Local Storage Monitoring

These prerequisites must be met for local storage monitoring or legacy disk drive monitoring to provide useful status information:

- The drive must be inserted in the server drive bay.
- The server must be powered on.
- The server must have completed discovery.
- The results of the BIOS POST complete must be TRUE.

Viewing the Status of a Disk Drive

Viewing the Status of Local Storage Components in the Cisco UCS Manager GUI

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.

Step 3 Click the server for which you want to view the status of your local storage components.

Step 4 In the **Work** pane, click the **Inventory** tab.

Step 5 Click the **Storage** subtab to view the status of your RAID controllers and any FlexFlash controllers.

Step 6 Click the down arrows to expand the **Local Disk Configuration Policy**, **Actual Disk Configurations**, **Disks**, and **Firmware** bars and view additional status information.

Interpreting the Status of a Monitored Disk Drive

Cisco UCS Manager displays the following properties for each monitored disk drive:

- Operability—The operational state of the drive.
- Presence—The presence of the disk drive, and whether it can be detected in the server drive bay, regardless of its operational state.

You need to look at both properties to determine the status of the monitored disk drive. The following table shows the likely interpretations of the combined property values.

Operability Status	Presence Status	Interpretation
Operable	Equipped	No fault condition. The disk drive is in the server and can be used.

Operability Status	Presence Status	Interpretation
Inoperable	Equipped	Fault condition. The disk drive is in the server, but one of the following could be causing an operability problem: • The disk drive is unusable due to a hardware issue such as bad blocks. • There is a problem with the IPMI link to the storage controller.
N/A	Missing	Fault condition. The server drive bay does not contain a disk drive.
N/A	Equipped	Fault condition. The disk drive is in the server, but one of the following could be causing an operability problem: • The server is powered off. • The storage controller firmware is the wrong version and does not support disk drive monitoring. • The server does not support disk drive monitoring.

Note The **Operability** field might show the incorrect status for several reasons, such as if the disk is part of a broken RAID set or if the BIOS power-on self-test (POST) has not completed.

HDD Metrics Not Updated in Cisco UCS Manager GUI

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

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

Procedure

Reboot the server.

Disk Drive Fault Detection Tests Fail

Problem—The fault LED is illuminated or blinking on the server disk drive, but Cisco UCS Manager does not indicate a disk drive failure.

Possible Cause—The disk drive fault detection tests failed due to one or more of the following conditions:

- The disk drive did not fail, and a rebuild is in progress.
- Drive predictive failure
- Selected drive failure on Disk 2 of a B200, B230 or B250 blade
- Selected drive failure on Disk 1 of a B200, B230 or B250 blade

Procedure

Step 1 Monitor the fault LEDs of each disk drive in the affected server(s).

Step 2 If a fault LED on a server turns any color, such as amber, or blinks for no apparent reason, create technical support file for each affected server and contact Cisco Technical Assistance Center.

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

Problem—Cisco UCS Manager reports that a server has more disks than the total disk slots available in the server. For example, Cisco UCS Manager reports three disks for a server with two disk slots as follows:

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

Possible Cause—This problem is typically caused by a communication failure between Cisco UCS Manager and the server that reports the inaccurate information.

Procedure

Step 1 Upgrade the Cisco UCS domain to the latest release of Cisco UCS software and firmware.

Step 2 Decommission the server.

Step 3 Recommission the server.

Troubleshooting Post-Upgrade IQN Issues

Clearing the Duplicate IQN Fault and Reconfiguring IQN Initiator Names

Problem—After an upgrade from Cisco UCS, Release 2.0(1) to Release 2.0(2), Cisco UCS Manager raises an IQN-related fault on one or more service profiles when you attempt to perform an action on a service profile, such as modifying the host firmware package.

Possible Cause—One or more iSCSI vNICS used within a single service profile or across multiple service profiles did not have a unique IQN initiator name.

Procedure

Step 1 Log into the Cisco UCS Manager CLI.

Step 2 Run the following command to view a list of the IQNs in the Cisco UCS domain:

UCS-A# **show identity iqn** | **include** *iqn name*

Step 3 In Cisco UCS PowerTool, run the script to identify the iSCSI vNICs which include the duplicate IQNs.

Step 4 In the service profile to which the IQN initiator name is not registered, change the initiator identity to the default IQN pool or manually assign a unique IQN.

Step 5 In the service profile in which you changed the initiator identity, change the initiator assignment to the name or pool you assigned, as follows:

a) UCS-A # **scope org** *org-name*

Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.

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

Enters service profile organization mode for the service profile.

c) UCS-A/org# scope vnic-iscsi *iscsi_vnic_name*

Enters the mode for the specified iSCSI vNIC.

Note This vNIC is not registered or visible through **show identity iqn**.

d) UCS-A /org/service-profile/vnic-iscsi* # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}

Specifies the name of the iSCSI initiator or the name of an IQN pool from which the iSCSI initiator name will be provided. The iSCSI initiator name can be up to 223 characters.

e) UCS-A /org/service-profile/vnic-iscsi # **commit-buffer**

Commits the transaction to the system configuration.

Note Changing initiator names also involves storage side configuration, which is beyond the scope of this document.

Step 6 Perform an action on the service profile to register the initiator names in the Cisco UCS database.

For example, you can upgrade the firmware on the associated server or modify the description or label of the service profile.

Step 7 Run the following command to verify that the IQN changes were registered:

UCS-A**show identity iqn** | **include** *iqn name*

Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script

If a Cisco UCS domain is configured for iSCSI boot, before you upgrade from Cisco UCS, Release 2.0(1) to Cisco UCS, Release 2.0(2) or higher, you must ensure that all iSCSI vNICs used across multiple service profile have unique initiator names.

You can use a script that runs in the Cisco UCS PowerTool to determine whether a Cisco UCS configuration for iSCSI boot includes duplicate IQNs.

Procedure

Step 1 To download Cisco UCS PowerTool, do the following:

a) In your web browser, navigate to the following website:
http://developer.cisco.com/web/unifiedcomputing/microsoft

b) Scroll down to the **Cisco UCS PowerTool (PowerShell Toolkit) Beta Download** area.

c) Download the `CiscoUcs-PowerTool-0.9.6.0.zip` file.

d) Unzip the file and follow the prompts to install Cisco UCS PowerTool.

You can install Cisco UCS PowerTool on any Windows computer. You do not need to install it on a computer used to access Cisco UCS Manager.

Step 2 To launch Cisco UCS PowerTool, enter the following at a command line:

C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUc sPS.ps1

Example:

The following example shows what happens when you launch Cisco UCS PowerTool:

```
C:\Program Files (x86)\Cisco\Cisco UCS
PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe
-NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPS.ps1
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

Step 3 In Cisco UCS PowerTool, do the following:

a) Connect to Cisco UCS Manager, as follows:

PS C:\> **Connect-Ucs** *IP_address*

b) Enter your username and password when prompted for your credential as shown in the following example:

```
cmdlet Connect-Ucs at command pipeline position 1
Supply values for the following parameters:
Credential
```

Cisco UCS PowerTool outputs the following to your screen after you log in.

```
Cookie               : 1331303969/2af0afde-6627-415c-b85f-a7cae6233de3
Domains              :
LastUpdateTime       : 3/9/2012 6:20:42 AM
Name                 : 209.165.201.15
NoSsl                : False
NumPendingConfigs    : 0
NumWatchers          : 0
Port                 : 443
Priv                 : {admin, read-only}
RefreshPeriod        : 600
SessionId            : web_49846_A
TransactionInProgress : False
Ucs                  : ucs-4
Uri                  : https://209.165.201.15
UserName             : admin
VirtualIpv4Address   : 209.165.201.15
Version              : 2.0(2i)3.0(1a)
WatchThreadStatus    : None
```

Step 4 In the Cisco UCS PowerTool, run the following script to validate your iSCSI boot configuration and check for duplicate IQNs :

PS C:\> **Get-UcsServiceProfile -type instance | Get-UcsVnicIScsi | ? { $_.InitiatorName -ne "" } | select Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj | Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name; $obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn }); $obj** }

Cisco UCS PowerTool outputs the results to your screen, as follows:

```
Count InitiatorName              Dn
----- -------------              --
    2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_1_6/is...
    2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_1/is...
    2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_41/i...
    4 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_7/is...
    2 iqn.2012-01.cisco.com:s... {org-root/org-sub1/ls-...
    2 iqn.2012-01.cisco.com:s... {org-root/org-sub2/ls-...
```

Step 5 (Optional) If you have .NET Frame work 3.5 Service Pack 1 installed, you can use the following script to view the output in the GUI:

PS C:\> **Get-UcsServiceProfile -type instance | Get-UcsVnicIScsi | ? { $_.InitiatorName -ne "" } | select Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj | Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name; $obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn }); $obj } | ogv**

Step 6 Disconnect from Cisco UCS Manager, as follows:

PS C:\>**Disconnect-Ucs**

What to do next

If duplicate IQNs exist across multiple service profiles in the Cisco UCS domain, reconfigure the iSCSI vNICs with unique IQNs in Cisco UCS Manager before you upgrade to Cisco UCS, Release 2.1 or greater.

If you do not ensure that all iSCSI vNICs are unique across all service profiles in a Cisco UCS domain before you upgrade, Cisco UCS Manager raises a fault on the iSCSI vNICs to warn you that duplicate IQNs are present. Also, if you do not ensure that there are no duplicate IQN names within a service profile (for example, the same name used for both iSCSI vNICs), Cisco UCS reconfigures the service profile to have a single IQN. For information on how to clear this fault and reconfigure the duplicate IQNs, see the Cisco UCS B-Series Troubleshooting Guide.

Reconfiguring IQN Initiator Names on a Service Profile Bound to an Updating Service Profile Template

Problem—After an upgrade from Cisco UCS, Release 2.0(1) to Release 2.0(2), Cisco UCS Manager raises an IQN-related fault on one or more service profiles and you cannot reconfigure the duplicate IQN initiator name on the service profile.

Possible Cause—The service profile that does not have a unique IQN initiator name is based on an updating service profile template.

Procedure

Step 1 Log into the Cisco UCS Manager CLI.

Step 2 UCS-A # **scope org** *org-name*

Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.

Step 3 UCS-A /org # **scope service-profile** *profile-name*

Enters service profile organization mode for the service profile.

Step 4 UCS-A/org# scope vnic-iscsi *iscsi_vnic1_name*

Enters the mode for the first iSCSI vNIC assigned to the service profile.

Step 5 UCS-A /org/service-profile/vnic-iscsi* # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}

Specifies the name of the iSCSI initiator or the name of an IQN pool from which the iSCSI initiator name will be provided. The iSCSI initiator name can be up to 223 characters.

Step 6 UCS-A /org/service-profile/vnic-iscsi* # **exit**

Exits the mode for the specified iSCSI vNIC

Step 7 UCS-A/org# scope vnic-iscsi *iscsi_vnic2_name*

Enters the mode for the second iSCSI vNIC assigned to the service profile.

Step 8 UCS-A /org/service-profile/vnic-iscsi* # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}

Specifies the name of the iSCSI initiator or the name of an IQN pool from which the iSCSI initiator name will be provided. The iSCSI initiator name can be up to 223 characters.

Step 9 UCS-A /org/service-profile/vnic-iscsi # **commit-buffer**

Commits the transaction to the system configuration.

Step 10 In the Cisco UCS Manager GUI, unbind the service profile from the updating service profile template.

Troubleshooting Issues with Registering Cisco UCS Domains in Cisco UCS Central

...

Date and time mismatch is the most common issue with registration.

To ensure that the date and time between Cisco UCS Central and Cisco UCS domains are in sync, try the following:

- Ensure that you have a valid NTP configuration with Cisco UCS Central and the Cisco UCS domains.
- Ensure that Cisco UCS Central is running behind the time for the Cisco UCS domains. This ensures that the start date of a certificate issued by Cisco UCS Central is not in the future.
- If the certificate is not valid, regenerate the default keyring certificate from Cisco UCS Central using the following commands:

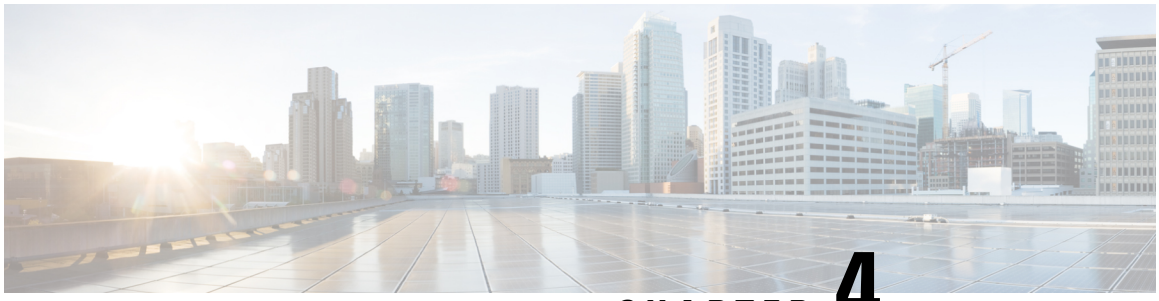
```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope keyring default
UCSC(policy-mgr) /org/device-profile/security/keyring* # set regenerate yes
UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer
```

- If you have issues after correcting the configuration, you may need to update the shared secret in Cisco UCS Manager.

```
UCSM# scope system
UCSM /system # scope control-ep policy
UCSM /system/control-ep # set shared-secret
     Shared Secret for Registration:
UCSM /system/control-ep* # commit-buffer
```

Important Before calling Cisco TAC, make sure that:

- You synchronize the date and time in Cisco UCS Central and registered Cisco UCS domains.
- Cisco UCS Domain is not in suspended or lost visibility state.
- The registration status for the domain displays **Registered**.



CHAPTER 4

Troubleshooting SAN Boot and SAN Connectivity Issues

This chapter includes the following sections:

SAN Connectivity Checklist

A problem with connectivity to the SAN array can cause issues with the SAN boot. If other solutions do not resolve your issue, consider the following:

- Are the fibre channel uplink ports configured in Cisco UCS Manager?
- Do the numbers assigned to the Virtual Storage Area Networks (VSANs) in Cisco UCS Manager match those configured in the fibre channel switch?
- Is the N-Port ID Virtualization (NPIV) enabled on the fibre channel switch?
- Is the Cisco UCS fabric interconnect logged into the fibre channel switch? The fibre channel switch displays the fabric interconnect as an NPIV device. For example, you can use the **show fcns data** command on a multi-layer director switch (MDS) to determine whether the Cisco UCS fabric interconnect is logged into it.
- Is the world wide name (WWN) in the correct format in Cisco UCS Manager?
- Have you upgraded the Cisco UCS domain, including the server adapters, to use the latest firmware?
- Have you verified that the SAN boot and SAN boot target configuration in the boot policy is included with the service profile associated with the server?
- Do the vNICs and vHBAs in the boot policy match the vNICs and vHBAs that are assigned to the service profile?
- Is the array active or passive?
- Are you booting to the active controller on the array?

- Is the array configured correctly? For example, have you verified the items in the SAN Array Configuration Checklist, on page 40?

SAN Array Configuration Checklist

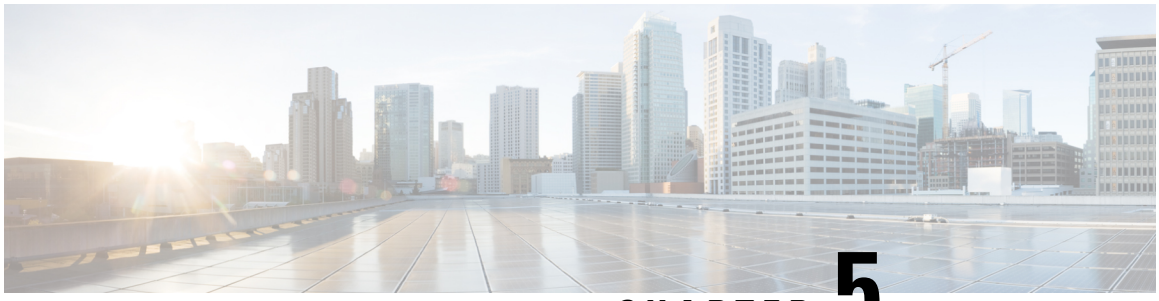
A misconfiguration or other issue with the SAN array can cause issues with the SAN boot. If other solutions do not resolve your issue, verify the following basic configurations in the SAN array:

- Has the host been acknowledged or registered by the array?
- Is the array configured to allow the host to access the logical unit number (LUN)? For example, is LUN security or LUN masking configured?
- Did you correctly configure the LUN allocation with the world wide port name (WWPN) assigned in the Cisco UCS domain? If you assign and configure with a world wide node name (WWNN), you could encounter issues.
- Did you map the backed LUN of the array to the same LUN number configured in the Cisco UCS boot policy?

Recommended Solutions for Issues During SAN Boot

contains a list of issues and recommended solutions that can assist you with troubleshooting a SAN boot issue. If an attempt to boot from a SAN array fails, you should implement these solutions.

Issue	Recommended Solution
The SAN boot fails intermittently.	Verify that the configuration of the SAN boot target in the boot policy is included in the service profile. For example, make sure that the SAN boot target includes a valid WWPN.
The server tries to boot from local disk instead of SAN.	Verify that the configured boot order in the service profile has SAN as the first boot device. If the boot order in the service profile is correct, verify that the actual boot order for the server includes SAN as the first boot device. If the actual boot order is not correct, reboot the server.
The server cannot boot from SAN even though the boot order is correct.	For Windows and Linux, verify that the boot LUN is numbered as 0 to ensure that LUN is mounted as the first disk from which the server boots. For ESX, if more than one LUN is presented, verify that the boot LUN is the lowest numbered LUN.



CHAPTER 5

Troubleshooting Server Hardware Issues

This chapter includes the following sections:

Diagnostics Button and LEDs

At the blade start-up, the POST diagnostics test the CPUs, DIMMs, HDDs, and adapter cards. Any failure notifications are sent to Cisco UCS Manager. You can view these notification in the system event log (SEL) or in the output of the show tech-support command. If errors are found, an amber diagnostic LED lights up next to the failed component. During run time, the blade BIOS, component drivers, and OS monitor for hardware faults. The amber diagnostic LED lights up for any component if an uncorrectable error or correctable errors (such as a host ECC error) over the allowed threshold occurs.

The LED states are saved. If you remove the blade from the chassis, the LED values persist for up to 10 minutes. Pressing the LED diagnostics button on the motherboard causes the LEDs that currently show a component fault to light up for up to 30 seconds. The LED fault values are reset when the blade is reinserted into the chassis and booted.

If any DIMM insertion errors are detected, they can cause the blade discovery to fail and errors are reported in the server POST information. You can view these errors in either the Cisco UCS Manager CLI or the Cisco UCS Manager GUI. The blade servers require specific rules to be followed when populating DIMMs in a blade server. The rules depend on the blade server model. Refer to the documentation for a specific blade server for those rules.

The HDD status LEDs are on the front of the HDD. Faults on the CPU, DIMMs, or adapter cards also cause the server health LED to light up as a solid amber for minor error conditions or blinking amber for critical error conditions.

DIMM Memory Issues

Types of DIMM Errors

Cisco UCS Servers can detect and report correctable and uncorrectable DIMM errors.

Correctable DIMM Errors

DIMMs with correctable errors are not disabled and are available for the OS to use. The total memory and effective memory are the same (memory mirroring is taken into account). These correctable errors are reported in as degraded once they exceed pre-determined error thresholds.

Uncorrectable DIMM Errors

Uncorrectable errors generally cannot be fixed, and may make it impossible for the application or operating system to continue execution. The DIMMs with uncorrectable error will be disabled if DIMM blacklisting is enabled or if the DIMM fails upon reboot during BIOS POST and OS will not see that memory. **operState** will be inoperable for this DIMM in this case.

A problem with the DIMM memory can cause a server to fail to boot or cause the server to run below its capabilities. If DIMM issues are suspected, consider the following:

- DIMMs tested, qualified, and sold by Cisco are the only DIMMs supported on your system. Third-party DIMMs are not supported, and if they are present, Cisco technical support will ask you to replace them with Cisco DIMMs before continuing to troubleshoot a problem.
- Check if the malfunctioning DIMM is supported on that model of server. Refer to the server's installation guide and technical specifications to verify whether you are using the correct combination of server, CPU and DIMMs.
- Check if the malfunctioning DIMM seated correctly in the slot. Remove and reseat the DIMMs.
- All Cisco servers have either a required or recommended order for installing DIMMs. Refer to the server's installation guide and technical specifications to verify that you are adding the DIMMs appropriately for a given server type.
- If the replacement DIMMs have a maximum speed lower than those previously installed, all DIMMs in a server run at the slower speed or not work at all. All of the DIMMs in a server should be of the same type. All of the DIMMs in a server should be of the same type for optimal performance.
- The number and size of DIMMs should be the same for all CPUs in a server. Mismatching DIMM configurations can degrade system performance.

Memory Terms and Acronyms

Table 6: Memory Terms and Acronyms

Acronym	Meaning
DIMM	Dual In-line Memory Module
DRAM	Dynamic Random Access Memory
ECC	Error Correction Code

LVDIMM	Low voltage DIMM
MCA	Machine Check Architecture
MEMBIST	Memory Built-In Self Test
MRC	Memory Reference Code
POST	Power On Self Test
SPD	Serial Presence Detect
DDR	Double Data Rate
CAS	Column Address Strobe
RAS	Row Address Strobe

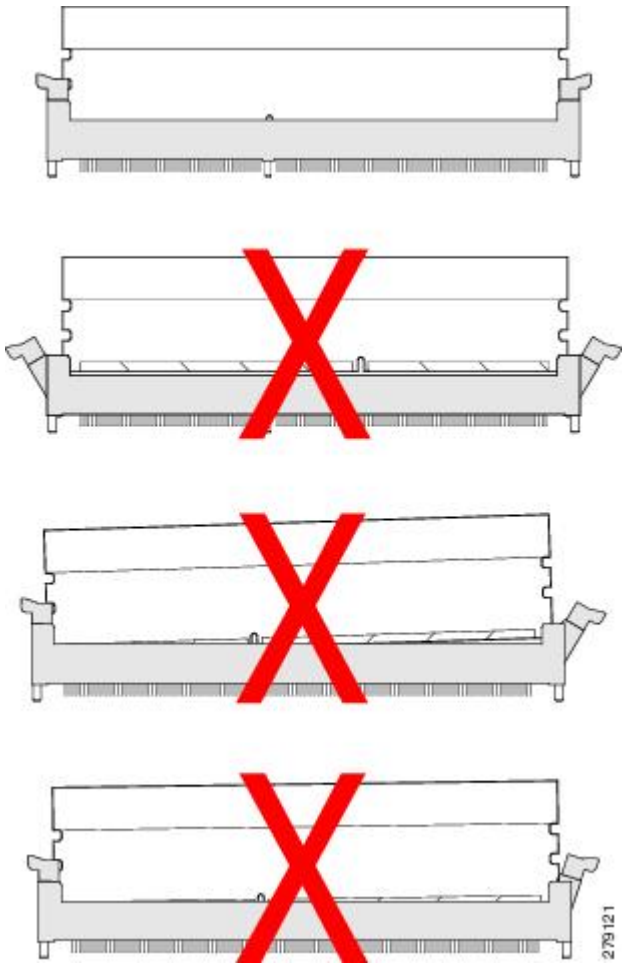
Troubleshooting DIMM Errors

Correct Installation of DIMMs

Verify that the DIMMs are installed correctly.

In the first example in the following figure, a DIMM is correctly inserted and latched. Unless there is a small bit of dust blocking one of the contacts, this DIMM should function correctly. The second example shows a DIMM that is mismatched with the key for its slot. That DIMM cannot be inserted in this orientation and must be rotated to fit into the slot. In the third example, the left side of the DIMM seems to be correctly seated and the latch is fully connected, but the right side is just barely touching the slot and the latch is not seated into the notch on the DIMM. In the fourth example, the left side is again fully inserted and seated, and the right side is partially inserted and incompletely latched.

Figure 1: Installation of DIMMs



Troubleshooting DIMM Errors Using the Cisco UCS Manager CLI

You can check memory information to identify possible DIMM errors in the Cisco UCS Manager CLI.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *x/y*	Enters server mode for the specified server.
Step 2	UCS-A /chassis/server # **show memory detail**	Shows memory information for the server.
Step 3	UCS-A /chassis/server # **show memory-array detail**	Shows detailed information about the memory arrays.
Step 4	UCS-A /chassis/server # **scope memory-array** *x*	Enters memory array mode for the specified array.
Step 5	UCS-A /chassis/server/memory-array # **show stats**	Shows statistics for memory array.

Example

The following example shows how to check memory information using the Cisco UCS Manager CLI:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # show memory detail
Server 1/5:
    Array 1:
        CPU ID: 1
        Current Capacity (GB): 393216
        Error Correction: Undisc
        Max Capacity (GB): 393216
        Max Devices: 48
        Populated: 48

        DIMMS:

        ID 1:
            Location: DIMM_A0
            Presence: Equipped
            Overall Status: Operable
            Operability: Operable
            Visibility: Yes
            Product Name: 8GB DDR3-1333MHz RDIMM/PC3-10600/dual rank 2Gb DRAM
            PID: N01-M308GB2
            VID: V01
            Vendor: 0xCE00
            Vendor Description: Samsung Electronics, Inc.
            Vendor Part Number: M393B1K70BH1-CH9
            Vendor Serial (SN): 0x46185EC2
            HW Revision: 0
            Form Factor: Dimm
            Type: Other
            Capacity (MB): 8192
            Clock: 1067
            Latency: 0.900000
            Width: 64
.
.
.
UCS-A /chassis/server # show memory-array detail

Memory Array:
    ID: 1
    Current Capacity (GB): 384
    Max Capacity (GB): 384
    Populated: 48
    Max Devices: 48
    Error Correction: Undisc
    Product Name:
    PID:
    VID:
    Vendor:
    Serial (SN):
    HW Revision: 0
    Threshold Status: N/A
    Power State: N/A
    Thermal Status: N/A
    Voltage Status: N/A
```

```
UCS-A /chassis/server # scope memory-array 1
UCS-A /chassis/server/memory-array # show stats

Memory Array Env Stats:
    Time Collected: 2011-09-27T20:15:52.858
    Monitored Object: sys/chassis-1/blade-5/board/memarray-1/array-env-stats
    Suspect: No
    Input Current (A): 62.400002
    Thresholded: 0

Memory Error Stats:
    Time Collected: 2011-09-27T20:15:43.821
    Monitored Object: sys/chassis-1/blade-5/board/memarray-1/mem-1/error-stats
    Suspect: No
    Address Parity Errors: 0
    Mismatch Errors: 0
    Ecc Multibit Errors: 0
    Ecc Singlebit Errors: 0
    Thresholded: 0

    Time Collected: 2011-09-27T20:15:43.821
    Monitored Object: sys/chassis-1/blade-5/board/memarray-1/mem-2/error-stats
    Suspect: No
    Address Parity Errors: 0
    Mismatch Errors: 0
    Ecc Multibit Errors: 0
    Ecc Singlebit Errors: 0
    Thresholded: 0

    Time Collected: 2011-09-27T20:15:43.821
    Monitored Object: sys/chassis-1/blade-5/board/memarray-1/mem-3/error-stats
    Suspect: No
    Address Parity Errors: 0
    Mismatch Errors: 0
    Ecc Multibit Errors: 0
    Ecc Singlebit Errors: 0
    Thresholded: 0
.
.
.
UCS-A /chassis/server/memory-array #
```

Troubleshooting DIMM Errors Using the Cisco UCS Manager GUI

You can determine the type of DIMM errors being experienced using the Cisco UCS Manager GUI.

Procedure

Step 1 In the navigation pane, expand the correct chassis and select the server.

Step 2 On the **Inventory** tab, click the **Memory** tab.

Memory errors on that server are displayed.

Step 3 On the **Statistics** tab for the server, click the **Chart** tab.

You can expand the relevant memory array for information about that array.

Step 4 Confirm that the amount of memory seen from the OS point-of-view matches that are listed for the server's associated service profile.

For example, does the OS see all the memory or just part of the memory? If possible, run a memory diagnostic tool from the OS.

Troubleshooting Degraded DIMM Errors

DIMMs with correctable errors are not disabled and are available for the OS to use. The total memory and effective memory are the same (memory mirroring is taken into account). These correctable errors are reported in Cisco UCS Manager as degraded.

If you see a correctable error reported that matches the information above, the problem can be corrected by resetting the BMC instead of reseating or resetting the blade server. Use the following Cisco UCS Manager CLI commands:

Note Resetting the BMC does not impact the OS running on the blade.

Procedure

	Command or Action	Purpose
Step 1	UCS1-A# **scope server** *x/y*	Enters server configuration mode.
Step 2	UCS1-A /chassis/server # **scope bmc**	Enters configuration mode for the BMC.
Step 3	UCS1-A /chassis/server/bmc # **reset**	Resets the BMC server.
Step 4	UCS1-A /chassis/server/bmc* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to reset the BMC:

```
UCS1-A# scope server x/y
UCS1-A /chassis/server # scope bmc
UCS1-A /chassis/server/bmc # reset
UCS1-A /chassis/server/bmc* # commit-buffer
```

Troubleshooting Inoperable DIMMs Errors

DIMMs with uncorrectable errors are disabled and the OS on the server does not see that memory. If a DIMM or DIMMs fail while the system is up, the OS could crash unexpectedly. shows the DIMMs as inoperable in the case of uncorrectable DIMM errors. These errors are not correctable using the software. You can identify a bad DIMM and remove it to allow the server to boot. For example, the BIOS fails to pass the POST due to one or more bad DIMMs.

Procedure

Step 1 Install a single DIMM (preferably a tested good DIMM) or a DIMM pair in the first usable slot for the first processor (minimum requirement for POST success).

Step 2 Re-attempt to boot the system.

Step 3 If the BIOS POST is still unsuccessful, repeat steps 1 through 3 using a different DIMM in step 2.

Step 4 If the BIOS POST is successful, continue adding memory. Follow the population rules for that server model. If the system can successfully pass the BIOS POST in some memory configurations but not others, use that information to help isolate the source of the problem.

Recommended Solutions for DIMM Issues

The following table lists guidelines and recommended solutions for troubleshooting DIMM issues.

Table 7: DIMM Issues

Issue	Recommended Solution
DIMM is not recognized.	Verify that the DIMM is in a slot that supports an active CPU. Verify that the DIMM is sourced from Cisco. Third-party memory is not supported in Cisco UCS.
DIMM does not fit in slot.	Verify that the DIMM is supported on that server model. Verify that the DIMM is oriented correctly in the slot. DIMMs and their slots are keyed and only seat in one of the two possible orientations.
The DIMM is reported as bad in the SEL, POST, or LEDs, or the DIMM is reported as inoperable in Cisco IMC.	Verify that the DIMM is supported on that server model. Verify that the DIMM is populated in its slot according to the population rules for that server model. Verify that the DIMM is seated fully and correctly in its slot. Reseat it to assure a good contact and rerun POST. Verify that the DIMM is the problem by trying it in a slot that is known to be functioning correctly. Verify that the slot for the DIMM is not damaged by trying a DIMM that is known to be functioning correctly in the slot. Reset the BMC.
The DIMM is reported as degraded in the GUI or CLI, or is running slower than expected.	Reset the BMC. Reseat the server in the chassis.

Issue	Recommended Solution
The DIMM is reported as overheating.	Verify that the DIMM is seated fully and correctly in its slot. Reseat it to assure a good contact and rerun POST. Verify that all empty HDD bays, server slots, and power supply bays use blanking covers to assure that the air is flowing as designed. Verify that the server air baffles are installed to assure that the air is flowing as designed. Verify that any needed CPU air blockers are installed to assure that the air is flowing as designed.

CPU Issues

All Cisco UCS servers support 1–2 or 1–4 CPUs. A problem with a CPU can cause a server to fail to boot, run very slowly, or cause serious data loss or corruption. If CPU issues are suspected, consider the following:

- All CPUs in a server should be the same type, running at the same speed and populated with the same number and size of DIMMs.
- If the CPU was recently replaced or upgraded, make sure the new CPU is compatible with the server and that a BIOS supporting the CPU was installed. Refer to the server's documentation for a list of supported Cisco models and product IDs. Use only those CPUs supplied by Cisco. The BIOS version information can be found in the release notes for a software release.
- When replacing a CPU, make sure to correctly thermally bond the CPU and the heat sink. An overheating CPU produces fault messages visible in Cisco UCS Manager. The CPU can also lower its performance in order to prevent damage to itself.
- If CPU overheating is suspected, check the baffles and air flow for all servers in a chassis. Air flow problems in adjacent servers can also cause improper CPU cooling in a server.
- The CPU speed and memory speed should match. If they do not match, the server runs at the slower of the two speeds.
- In the event of a failed CPU, the remaining active CPU or CPUs do not have access to memory assigned to the failed CPU.

Troubleshooting CPU Issues Using the CLI

You can check CPU information using Cisco UCS Manager CLI.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *x/y*	Enters server mode.
Step 2	UCS-A# **show cpu**	Shows CPU information for the server.

	Command or Action	Purpose
Step 3	UCS-A# **show bios**	Shows the BIOS information for the server.
Step 4	UCS-A# **show cimc**	Shows the CIMC information for the server.

Example

The following example shows how to display information about the CPU, BIOS, and CIMC on server 1/5.

```
jane-A# scope server 1/5
UCS-A /chassis/server # show cpu

CPU:
    ID  Presence             Architecture      Socket Cores       Speed (GHz)
    --- -------------------- ----------------- ------ ----------- -----------
      1 Equipped             Xeon              CPU1   6           3.333000
      2 Equipped             Xeon              CPU2   6           3.333000
UCS-A /chassis/server # show bios

Bios Firmware:

Server  Model      Vendor            Running-Vers Package-Vers
------- ---------- ----------------- ------------ ------------
1/5     N20-B6625-2 Cisco Systems, In S5500.1.3.1c.0.052020102031
UCS-A /chassis/server # show cimc

CIMC:
    PID              Serial (SN)      HW Revision
    ---------------- ---------------- -----------
    N20-B6625-2      QCI140200D4      0
UCS-A /chassis/server #
```

Troubleshooting CPU Issues Using the GUI

You can determine the type of CPU errors being experienced using the Cisco UCS Manager GUI.

Procedure

Step 1 In the navigation pane, expand the correct chassis and select the server.

Step 2 In the Inventory window, select the **CPU** tab.

CPU errors on that server are displayed.

Recommended Solutions for DIMM Issues

The following table lists guidelines and recommended solutions for troubleshooting DIMM issues.

Table 8: DIMM Issues

Issue	Recommended Solution
DIMM is not recognized.	Verify that the DIMM is in a slot that supports an active CPU. Verify that the DIMM is sourced from Cisco. Third-party memory is not supported in Cisco UCS.
DIMM does not fit in slot.	Verify that the DIMM is supported on that server model. Verify that the DIMM is oriented correctly in the slot. DIMMs and their slots are keyed and only seat in one of the two possible orientations.
The DIMM is reported as bad in the SEL, POST, or LEDs, or the DIMM is reported as inoperable in Cisco IMC.	Verify that the DIMM is supported on that server model. Verify that the DIMM is populated in its slot according to the population rules for that server model. Verify that the DIMM is seated fully and correctly in its slot. Reseat it to assure a good contact and rerun POST. Verify that the DIMM is the problem by trying it in a slot that is known to be functioning correctly. Verify that the slot for the DIMM is not damaged by trying a DIMM that is known to be functioning correctly in the slot. Reset the BMC.
The DIMM is reported as degraded in the GUI or CLI, or is running slower than expected.	Reset the BMC. Reseat the server in the chassis.
The DIMM is reported as overheating.	Verify that the DIMM is seated fully and correctly in its slot. Reseat it to assure a good contact and rerun POST. Verify that all empty HDD bays, server slots, and power supply bays use blanking covers to assure that the air is flowing as designed. Verify that the server air baffles are installed to assure that the air is flowing as designed. Verify that any needed CPU air blockers are installed to assure that the air is flowing as designed.

CPU CATERR_N Details

The CATERR_N signal indicates that one or more of the processors experienced a catastrophic memory error. It could mean an uncorrectable memory error occurred or represent a link error on QPI. The CATERR_N signal is monitored by the CATERR_N sensor, which will generate events in the system event log (SEL) if the signal is indicating normal operation or if a fault has occurred.

The CATERR_N sensor uses two bits to represent the sensor reading which indicate either normal operation or that a fault has occurred:

- Bit 0 set indicates: Predictive Failure Deasserted (Meaning there is no fault indicated by the sensor)
- Bit 1 set indicates: Predictive Failure Asserted (Meaning a fault has occurred)

When the sensor is initialized by the sensor scanning manager, you will typically see an event in the system event log (SEL) indicating the bit has been set to indicat e there is no failure. This is bit 0, and you will see an event that looks like this:

```
| CIMC | Processor CATERR_N #0x8e | Predictive
Failure Deasserted | Asserted
```

This says we asserted the bit which indicates there is no failure, the "Predictive Failure Deasserted" bit (which is Bit 0) has been asserted. This is a positive indication.

When the system encounters a catastrophic error, the sensor manager will transition the CATERR_N sensor from Bit0 set, to Bit1 set. This will deassert the "Predictive Failure Deasserted" bit (Bit 0), and assert the "Predictive Failure Asserted" bit (Bit 1). When this occurs you will see events in the system event log (SEL) that look like this:

```
| CIMC | Processor CATERR_N #0x8e | Predictive
Failure Deasserted | Deasserted
 | CIMC | Processor CATERR_N #0x8e | Predictive
Failure Asserted | Asserted
```

Meaning Bit 0 is "off" , and Bit 1 is now "On" . Some logs filter out the "turned off" (Deasserted) messages so you may only see the second event in the log. When the sensor returns to a normal state , you will see the fault bit (bit 1) deasserted and the no-fault bit (bit 0) asserted:

```
 | CIMC | Processor CATERR_N #0x8e | Predictive
Failure Asserted | Deasserted
| CIMC | Processor CATERR_N #0x8e | Predictive
Failure Deasserted | Asserted
```

Again, you may only see the event for the bit that is turning "On" (Predictive Failure Deasserted | Asserted) in the log file, which in this case indicates assertion of the non-fault bit (bit 0).

Disk Drive and RAID Issues

A problem with the disk drive or RAID controller can cause a server to fail to boot, or cause serious data loss or corruption. If drive issues are suspected, consider the following:

- Use OS tools regularly to detect and correct drive problems (for example, bad sectors). Cisco UCS Manager cannot correct drive problems as effectively as the server’s OS.
- Each disk drive has an activity LED that indicates an outstanding I/O operation to the drive and a health LED that turns solid amber if a drive fault is detected. Drive faults can be detected in the BIOS POST. SEL messages can contain important information to help you find these problems.
- Disk drives are the only major component that can be removed from the server without removing the blade from the system chassis.

- Disk drives are available in several sizes. If the disk drive performance is slow because the drive is full or there are issues with the drive that the OS cannot solve, you might need to back up the drive contents and install a larger or new hard drive.

RAID Controllers

You can order or configure the B-Series servers with the following RAID controller options:

- The Cisco UCS B200 and B250 servers have an LSI 1064E controller on the motherboard. The controller supports RAID 0 and 1 for up to two SAS or two SATA drives. The controller must be enabled in Cisco UCS Manager before configuring RAID. All RAID options can be configured from Cisco UCS Manager.
- The Cisco UCS B440 servers have the LSI MegaRAID controller (the model varies by server). Depending on the license key installed, these controllers provide RAID 0, 1, 5, 6, and 10 support for up to four SAS or SATA drives.
- The Cisco B200 M3 servers have an LSI SAS 2004 RAID controller on the motherboard. The controller supports RAID 0 and 1 for up to two SAS or two SATA drives.

Note If you ever need to move a RAID cluster from one server to another, both the old and new servers for the cluster must use the same LSI controller. For example, migration from a server with an LSI 1064E to a server with an LSI MegaRAID is not supported.

If there is no record of which option is used in the server, disable the quiet boot feature and read the messages that appear during system boot. Information about the models of installed RAID controllers appears as part of the verbose boot feature. You are prompted to press Ctrl-H to launch configuration utilities for those controllers.

Disabling Quiet Boot

When the quiet boot feature is disabled, the controller information and the prompts for the option ROM-based LSI utilities are displayed during bootup. To disable this feature, follow these steps:

Procedure

Step 1 Boot the server and watch for the **F2** prompt during the boot process.

Step 2 To enter the BIOS Setup Utility, press **F2** when prompted.

Step 3 On the Main page of the **BIOS Setup Utility**, set **Quiet Boot** to disabled.

This allows non-default messages, prompts, and POST messages to display during bootup instead of the Cisco logo screen.

Step 4 Press **F10** to save the changes and exit the utility.

Accessing ROM-Based Controller Utilities

To change the RAID configurations on your hard drives, use the host-based utilities that were installed on top of the host OS. You can also use the LSI option ROM-based utilities that are installed on the server.

Procedure

Step 1 Boot the server with Quiet mode is disabled. (See the "Disabling Quiet Boot" section on page 6-11)

Information about the controller appears along with the prompts for the key combination to launch the LSI option ROM-based utilities for your controller.

Step 2 During the verbose boot process, enter one of the following control commands when the prompt for the desired controller appears.

- When the prompt appears, enter **`Ctrl-H`** (for an LSI 1064E controller), or **`Ctrl-C`** (for an LSI MegaRAID controller), or **`Ctrl-M`** (for an Intel ICH10R) to enter the controller card utility.

Moving a RAID Cluster Between B200 M3 Servers

You can set a server to recognize a RAID cluster created on another server. You can also use this procedure whenever data on a RAID cluster needs to be moved between servers.

Before you begin

Verify that the service profiles for both the source and destination servers have an identical local disk configuration policy and can boot successfully.

Procedure

Step 1 Shut down the source server's operating system from within that operating system.

Before proceeding, verify that the OS has shut down completely and not restarted itself.

Step 2 Disassociate the service profile currently applied to the B200M3 server.

Step 3 Physically move the drives in the array to the destination server.

If you are changing servers you must keep the drives in the same slot in the new server as they were in the original server.

Step 4 Reassociate the service profile to the new blade, keeping the same LD Config Policies as were previously used.

Step 5 Power on the servers by pressing the front power button of each of the servers.

Step 6 Open a KVM connection to the new server and wait for the Storage Web BIOS Utility.

Step 7 Follow the Web BIOS Utility prompts to "migrate" the RAID LUN.

Replacing a Failed Drive in a RAID Cluster

We recommend following industry standard practice of using drives of the same capacity when creating RAID volumes. If drives of different capacities are used, the useable portion of the smallest drive will be used on all drives that make up the RAID volume.

Before you begin

Replace a failed HDD or SSD with a drive of the same size, model, and manufacturer. Before changing an HDD in a running system, check the service profile in UCS Manager to make sure that the new hardware configuration is within the parameters allowed by the service profile.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to view the status of your local storage components.

Step 4 In the **Work** pane, click the **Inventory** tab.

Step 5 Click the **Storage** subtab to view the status of your RAID controllers and any FlexFlash controllers.

Step 6 Click the down arrows to expand the **Local Disk Configuration Policy**, **Actual Disk Configurations**, **Disks**, and **Firmware** bars and view additional status information.

Step 7 Physically replace the failed drive.

If needed, refer to the service note for your server model. In general, the steps are similar for most models.

Step 8 Boot the server, using the power switch on the front of the server.

If necessary, disable the quiet boot feature and boot again. (See Disabling Quiet Boot, on page 53.)

Step 9 Wait for the LSI Configuration Utility banner.

Step 10 To enter the LSI Configuration Utility, press **`Ctrl-C`**.

Step 11 From the **SAS Adapter List** screen, choose the SAS adapter used in the server.

To determine which RAID controller is being used, refer to RAID Controllers, on page 53.

Step 12 Choose **RAID Properties**.

The **View Array** screen appears.

Step 13 Choose **Manage Array**.

The **Manage Array** screen appears.

Step 14 Choose **Activate Array**.

When the activation is complete, the RAID status changes to Optimal.

Step 15 On the **Manage Array** screen, choose **Synchronize Array**.

Step 16 Wait for the mirror synchronization to complete, and monitor the progress bar that comes up.

Note The time to complete the synchronization can vary depending upon the size of the disks in the RAID array.

Step 17 When the mirror synchronization is complete, press the **ESC** key several times to go back through each of the screens (one at a time) and then exit the LSI Configuration Utility.

Step 18 Choose the reboot option to implement the changes.

Local Storage Check Consistency Operation Fails

Problem—The Check Consistency operation fails on a Virtual Drive with the error message:

```
Adapter 0: Check Consistency is not possible on Virtual Drive at this time
```

Cause—The Check Consistency operation is not supported on RAID 0 volume.

Workaround—Run Check Consistency on a Virtual Disk configured as a RAID 1 volume.

Adapter Issues

A problem with the Ethernet or FCoE adapter can cause a server to fail to connect to the network and make it unreachable from Cisco UCS Manager. All adapters are unique Cisco designs and non-Cisco adapters are not supported. If adapter issues are suspected, consider the following:

- Check if the Cisco adapter is genuine.
- Check if the adapter type is supported in the software release you are using. The Internal Dependencies table in the Cisco UCS Manager Release Notes provides minimum and recommended software versions for all adapters.
- Check if the appropriate firmware for the adapter has been loaded on the server. In Release versions 1.0(1) through 2.0, the Cisco UCS Manager version and the adapter firmware version must match. To update the Cisco UCS software and the firmware, refer to the appropriate Upgrading Cisco UCS document for your installation.
- If the software version update was incomplete, and the firmware version no longer matches the Cisco UCS Manager version, update the adapter firmware as described in the appropriate Cisco UCS Manager configuration guide for your installation.
- If you are deploying two Cisco UCS M81KR Virtual Interface Cards on the Cisco UCS B250 Extended Memory Blade Server running ESX 4.0, you must upgrade to the patch 5 (ESX4.0u1p5) or later release of ESX 4.0.
- If you are migrating from one adapter type to another, make sure that the drivers for the new adapter type are available. Update the service profile to match the new adapter type. Configure appropriate services to that adapter type.
- If you are using dual adapters, note that there are certain restrictions on the supported combinations. The following combinations are supported:

Server	Dual card same type	Dual card mixed type
Cisco UCS B250	All	M71KR-Q or -E + M81KR M72KR-Q or -E + M81KR

Server	Dual card same type	Dual card mixed type
Cisco UCS B440	All except 82598KR-CI	M72KR-Q or -E + M81KR

Troubleshooting Adapter Errors Using the GUI

The link LED on the front of the server is off if the adapter cannot establish even one network link. It is green if one or more of the links are active. Any adapter errors are reported in the LEDs on the motherboard. See the "Diagnostics Button and LEDs" section on page 6-1.

Use the following procedure to determine the type of adapter errors being experienced:

Procedure

Step 1 In the navigation pane, expand the chassis and choose the desired server.

Step 2 In the Inventory window, choose the **Interface Cards** tab.

Any adapter errors on that server are displayed on the screen.

Troubleshooting Adapter Errors Using the CLI

The link LED on the front of the server is off if the adapter cannot establish even one network link. It is green if one or more of the links are active. Any adapter errors are reported in the LEDs on the motherboard.

You can check adapter state information in the CLI by using the following procedure:

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id/server-id*	
Step 2	UCS-A /chassis/server #**show adapter** [**detail**]	

Example

The following example shows how to show adapter details for chassis ID 1, server ID 5:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # show adapter detail

Adapter:
    Id: 2
    Product Name: Cisco UCS 82598KR-CI
    PID: N20-AI0002
    VID: V01
    Vendor: Cisco Systems Inc
    Serial: QCI132300GG
    Revision: 0
```

```
    Mfg Date: 2009-06-13T00:00:00.000
    Slot: N/A
    Overall Status: Operable
    Conn Path: A,B
    Conn Status: Unknown
    Managing Instance: B
    Product Description: PCI Express Dual Port 10 Gigabit Ethernet Server Adapter
UCS-A /chassis/server #
```

Recommended Solutions for Adapter Issues

The following table lists guidelines and recommended solutions that can help you in troubleshooting adapter issues.

Table 9: Adapter Issues

Issue	Recommended Solution
The adapter is reported as bad in the SEL, POST or LEDs or is reported as inoperable in Cisco UCS Manager.	Verify that the adapter is supported on that server model. Verify that the adapter has the required firmware version to work with your version of Cisco UCS Manager. Verify that the adapter is seated fully and correctly in the slot on the motherboard and in the midplane connections. Reseat it to ensure a good contact, reinsert the server, and rerun POST. Verify that the adapter is the problem by trying it in a server that is known to be functioning correctly and that uses the same adapter type.
The adapter is reported as degraded in the GUI or CLI.	Reseat the blade server in the chassis.
The adapter is reported as overheating.	Verify that the adapter is seated fully and correctly in the slot. Reseat it to assure a good contact and rerun POST. Verify that all empty HDD bays, server slots, and power supply bays use blanking covers to ensure that the air is flowing as designed. Verify that the server air baffles are installed to ensure that the air is flowing as designed.

Power Issues

A problem with a server's onboard power system can cause a server to shut down without warning, fail to power on, or fail the discovery process.

Troubleshooting a FET Failure in a Cisco UCS B440 Server

The failure of a field effect transistor (FET) in a Cisco UCS B440 server's power section can cause the server to shut down, fail to power on, or fail the discovery process. When the server has detected the failure, you are unable to power on the server, even using the front panel power button.

To determine whether a FET failure has occurred, perform the following steps:

Procedure

Step 1 Using the procedure in the "Faults" section on page 1-2, check the reported faults for Fault Code F0806, "Compute Board Power Fail." This fault will cause the server's overall status to be Inoperable.

Step 2 Check the system event log (SEL) for a power system fault of the type in this example:

```
58f | 06/28/2011 22:00:19 | BMC | Power supply POWER_SYS_FLT #0xdb | Predictive Failure
deasserted | Asserted
```

Step 3 From the CLI of the fabric interconnect, access the CIMC of the failed server and display the fault sensors by entering **connect cimc** *chassis/server*.

Example:

The following example shows how to connect to the CIMC on chassis 1, server 5:

```
Fabric Interconnect-A# connect cimc 1/5
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '^]'.
CIMC Debug Firmware Utility Shell
[ help ]# sensors fault
HDD0_INFO | 0x0 | discrete | 0x2181| na | na | na | na | na | na
HDD1_INFO | 0x0 | discrete | 0x2181| na | na | na | na | na | na
.
.[lines removed for readability]
.
LED_RTC_BATT_FLT | 0x0 | discrete | 0x2180| na | na | na | na | na | na
POWER_SYS_FLT | 0x0 | discrete | 0x0280| na | na | na | na | na | na
[ sensors fault]#
```

For the POWER_SYS_FLT sensor, a reading of 0x0280 confirms the FET failure. In normal operation, this sensor will have reading of 0x0180.

Step 4 If you determine that a FET failure has occurred, perform the following steps:

a) In the Cisco UCS Manager CLI, collect the output of the following commands:

- **show tech-support ucsm detail**
- **show tech-support chassis** *chassis-id* **all detail**

b) Contact the Cisco Technical Assistance Center (TAC) to confirm the failure.

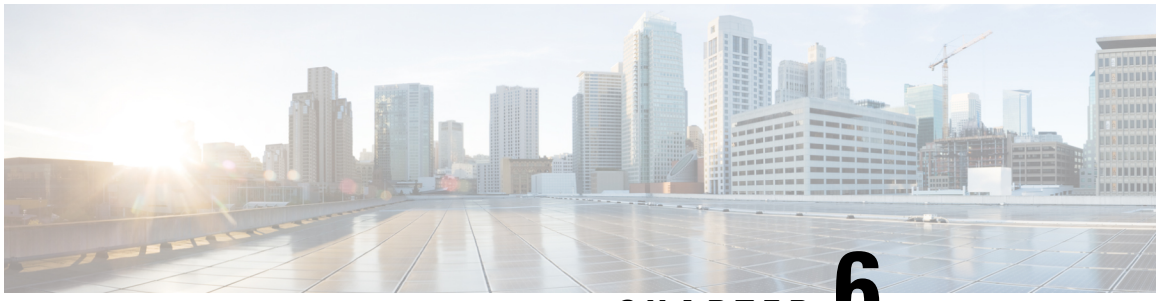
c) Install a replacement server using the Recover Server action in Cisco UCS Manager.

Information Needed Before Calling Cisco TAC

If you cannot isolate the issue to a particular component, consider the following questions. They can be helpful when contacting the Cisco Technical Assistance Center (TAC).

- Was the blade working before the problem occurred? Did the problem occur while the blade was running with a service profile associated?
- Was this a newly inserted blade?
- Was this blade assembled on-site or did it arrive assembled from Cisco?
- Has the memory been re-seated?
- Was the blade powered down or moved from one slot to another slot?
- Have there been any recent upgrades of Cisco UCS Manager. If so, was the BIOS also upgraded?

When contacting Cisco TAC for any Cisco UCS issues, it is important to capture the tech-support output from Cisco UCS Manager and the chassis in question. For more information, see Technical Support Files, on page 14.



CHAPTER 6

Troubleshoot Firmware

Recovering Fabric Interconnect During Upgrade

If one or both fabric interconnects fail during failover or firmware upgrade, you can recover them by using one of the following approaches:

- Recover a fabric interconnect when you do not have a working image on the fabric interconnect
- Recover a fabric interconnect when you have a working image on the fabric interconnect
- Recover an unresponsive fabric interconnect during upgrade or failover
- Recover fabric interconnects from a failed FSM during upgrade with Auto Install

Recovering Fabric Interconnects When You Do Not Have Working Images on The Fabric Interconnect or The Bootflash

You can perform these steps when both or any fabric interconnect goes down during firmware upgrade, gets rebooted, and is stuck at the loader prompt, and you do not have working images on the fabric interconnect.

Procedure

Step 1 Reboot the switch, and in the console, press **Ctrl+L** as it boots to get the loader prompt.

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

Example:

```
loader>
```

Step 2 Required: Configure the interface to receive the kickstart image through TFTP.

a) Enter the local IP address and subnet mask for the system at the loader> prompt, and press **Enter**.

Example:

```
loader> set ip 10.104.105.136 255.255.255.0
```

b) Specify the IP address of the default gateway.

Example:

```
loader> set gw 10.104.105.1
```

c) Boot the kickstart image file from the required server.

Example:

```
loader> boot
tftp://10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)#
```

Note You do not need to do this step if you already have a kickstart image in the bootflash.

Step 3 Enter the **init system** command at the switch(boot)# prompt.

This will reformat the fabric interconnect.

Example:

```
switch(boot)# init system
```

Step 4 Configure the management interface.

a) Change to configuration mode and configure the IP address of the mgmt0 interface.

Example:

```
switch(boot)# config t
switch(boot)(config)# interface mgmt0
```

b) Enter the **ip address** command to configure the local IP address and the subnet mask for the system.

Example:

```
switch(boot)(config-if)# ip address 10.104.105.136 255.255.255.0
```

c) Enter the **no shutdown** command to enable the mgmt0 interface on the system.

Example:

```
switch(boot)(config-if)# no shutdown
```

d) Enter the **ip default-gateway** command to configure the IP address of the default gateway.

Example:

```
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.104.105.1
```

e) Enter **exit** to exit to EXEC mode.

Example:

```
switch(boot)(config)# exit
```

Step 5 Copy the kickstart, system, and Cisco UCS Manager management images from the TFTP server to the bootflash.

Example:

```
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
 bootflash://
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
 bootflash://
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-manager-k9.3.0.2d56.bin bootflash://
```

Step 6 Create separate directories for installables and installables/switch in the bootflash.

Example:

```
switch(boot)# mkdir bootflash:installables
switch(boot)# mkdir bootflash:installables/switch
```

Step 7 Copy the kickstart, system, and Cisco UCS Manager images to the installables/switch directory.

Example:

```
switch(boot)# copy ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin bootflash:installables/switch/
switch(boot)# copy ucs-6300-k9-system.5.0.2.N1.3.02d56.bin bootflash:installables/switch/
switch(boot)# copy ucs-manager-k9.3.02d56.bin bootflash:installables/switch/
```

Step 8 Ensure that the management image is linked to nuova-sim-mgmt-nsg.0.1.0.001.bin.

nuova-sim-mgmt-nsg.0.1.0.001.bin is the name that the reserved system image uses, and it makes the management image Cisco UCS Manager-compliant.

Example:

```
switch(boot)# copy bootflash:installables/switch/ucs-manager-k9.3.02d56.bin
nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Step 9 Reload the switch.

Example:

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
```

Step 10 Boot from the kickstart image.

Example:

```
loader> dir
nuova-sim-mgmt-nsg.0.1.0.001.bin
ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
ucs-manager-k9.3.02d56.bin
loader> boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)#
```

Step 11 Load the system image.

The **Basic System Configuration Dialog** wizard appears after the system image is completely loaded. Use this wizard to configure the fabric interconnect.

Example:

```
switch(boot)# load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
Uncompressing system image: bootflash:/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin

...

---- Basic System Configuration Dialog ----

  This setup utility will guide you through the basic configuration of
  the system. Only minimal configuration including IP connectivity to
  the Fabric interconnect and its clustering mode is performed through these steps.

...

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

Configuration file - Ok
```

Step 12 Log in to Cisco UCS Manager and download the firmware.

Example:

```
UCS-A# scope firmware
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<infra bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<b-series bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<c-series bundle name>
Password:
UCS-A /firmware # show download-task
Download task:
    File Name Protocol Server          Userid          State
    --------- -------- --------------- --------------- -----
    ucs-k9-bundle-b-series.3.0.2.B.bin
              Scp      10.104.105.22   abcdefgh        Downloading
    ucs-k9-bundle-c-series.3.0.2.C.bin
              Scp      10.104.105.22   abcdefgh        Downloading
    ucs-k9-bundle-infra.3.0.2.A.bin
              Scp      10.104.105.22   abcdefgh        Downloading
UCS-A /firmware #
```

Step 13 After the firmware download is complete, activate the fabric interconnect firmware and Cisco UCS Manager firmware.

This step updates Cisco UCS Manager and the fabric interconnects to the version you want, and then reboots them.

Example:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect* # activate firmware kernel-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
```

```
UCS-A /fabric-interconnect* # activate firmware system-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect # exit

UCS-A# scope system
UCS-A /system # show image

Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-manager-k9.3.02d56.bin                  System              3.0(2d)
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system #
```

Recovering Fabric Interconnect During Upgrade When You have Working Images on the Bootflash

You can perform these steps when both or any fabric interconnect goes down during firmware upgrade, gets rebooted, and is stuck at the loader prompt.

Before you begin

You must have working images on the bootflash to perform these steps.

Procedure

Step 1 Reboot the switch, and in the console, press Ctrl+L as it boots to get the loader prompt.

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

Example:

```
loader>
```

Step 2 Run the **dir** command.

The list of available kernel, system, and Cisco UCS Manager images in the bootflash appears.

Example:

```
loader> dir
nuova-sim-mgmt-nsg.0.1.0.001.bin
ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
ucs-manager-k9.3.02d56.bin
```

Step 3 Boot the kernel firmware version from the bootflash.

Note Any kernel image available here will be a working image from which you can boot.

Example:

```
loader> boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
```

Step 4 Ensure that the management image is linked to nuova-sim-mgmt-nsg.0.1.0.001.bin.

nuova-sim-mgmt-nsg.0.1.0.001.bin is the name that the reserved system image uses, and it makes the management image Cisco UCS Manager-compliant.

Example:

```
switch(boot)# copy ucs-manager-k9.1.4.1k.bin nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Step 5 Load the system image.

Example:

```
switch(boot)# load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
```

Step 6 Log in to Cisco UCS Manager and update your fabric interconnect and Cisco UCS Manager software to the version that you want.

Recovering Unresponsive Fabric Interconnects During Upgrade or Failover

During upgrade or failover, avoid performing the following tasks because they introduce additional risk:

- Pmon stop/start
- FI reboots – power cycle or CLI
- HA failover

Procedure

Step 1 If the **httpd_cimc.sh** process is lost, as documented in CSCup70756, you lose access to the KVM. Continue with the failover or contact Cisco Technical Assistance.

Step 2 If you lose access to the KVM on the primary side, continue with the failover to resolve the issue.

Step 3 If KVM is needed or is down on the subordinate side, start only that service using the debug plugin. Contact TAC to run the debug image.

Step 4 If the /dev/null issue is encountered, as documented in CSCuo50049, fix the rights to 666 with the debug-plugin at both steps if required. Contact Cisco Technical Assistance to run debug commands.

Step 5 If both CSCup70756 and CSCuo50049 are encountered, it can cause VIP loss. If the VIP is lost, do the following:

1. Access the primary physical address through the GUI and use the GUI to verify all IO Module backplane ports recovered.
2. If the GUI is down, verify IO Module backplane ports with the NXOS **show fex detail** command.

3. Perform the workaround and verify that the cluster state is UP on both fabric interconnects.
4. If the cluster state is UP on both fabric interconnects, continue the upgrade by reacknowledging the primary fabric interconnect reboot using the SSH CLI syntax:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # acknowledge primary fabric-interconnect reboot
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

Recovering Fabric Interconnects From a Failed FSM During Upgrade With Auto Install

You can perform these steps when all the following occur:

- You are upgrading or downgrading firmware using Auto Install between Cisco UCS Manager Release 3.1(2) and Release 3.1(3) while a service pack is installed on the fabric interconnects.
- Both or any fabric interconnect goes down because of an FSM failure or multiple retries in the DeployPollActivate stage of the FSM

Procedure

Step 1 When the FSM fails, or when multiple retries are observed in the DeployPollActivate stage of the FSM on the subordinate fabric interconnect, do the following:

a) Clear the startup version of the default infrastructure pack and the service pack.

Example:

```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # set infra-bundle-version ""
UCS-A /org/fw-infra-pack* # commit-buffer
```

b) Remove the service pack from the subordinate fabric interconnect.

Example:

```
UCS-A# scope fabric-interconnect b
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

Step 2 Upgrade the infrastructure firmware using the force option through Auto Install.

Example:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 3.1(3a)A force
This operation upgrades firmware on UCS Infrastructure Components
(UCS manager, Fabric Interconnects and IOMs).
Here is the checklist of things that are recommended before starting Auto-Install
```

```
(1) Review current critical/major faults
(2) Initiate a configuration backup
(3) Check if Management Interface Monitoring Policy is enabled
(4) Check if there is a pending Fabric Interconnect Reboot activitiy
(5) Ensure NTP is configured
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no): yes
Triggering Install-Infra with:
Infrastructure Pack Version: 3.1(3a)A
```

Step 3 Acknowledge the reboot of the primary fabric interconnect.

Example:

```
UCS-A /firmware/auto-install # acknowledge primary fabric-interconnect reboot
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

Step 4 When the FSM fails, or when multiple retries are observed in the DeployPollActivate stage of the FSM on the current subordinate fabric interconnect, do the following:

a) Clear the startup version of the default infrastructure pack and the service pack.

Example:

```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # set infra-bundle-version ""
UCS-A /org/fw-infra-pack* # commit-buffer
```

b) Remove the service pack from the current subordinate fabric interconnect.

Example:

```
UCS-A# scope fabric-interconnect a
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

Both fabric interconnects will now reflect Release 3.1(3) firmware and the default service pack for Running and Startup versions.

Recovering IO Modules During Firmware Upgrade

You can recover an IO Module during firmware upgrade by resetting it from a peer IO Module. After it is reset, it can derive the configuration from the fabric interconnect.

Resetting an I/O Module from a Peer I/O Module

Sometimes, I/O module upgrades can result in failures or I/O modules can become unreachable from Cisco UCS Manager due to memory leaks. You can reboot an I/O module that is unreachable through its peer I/O module.

Resetting the I/O module restores the I/O module to factory default settings, deletes all cache files and temporary files, but retains the size-limited OBFL file.

Procedure

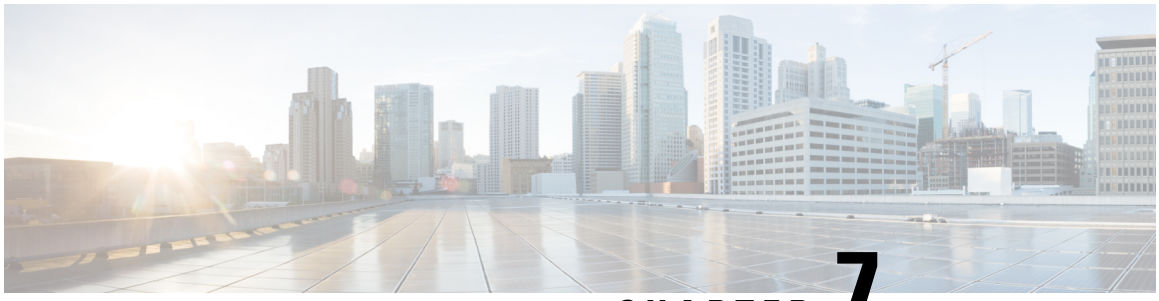
Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 3 Choose the peer I/O module of the I/O module that you want to reset.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the Actions area, click **Reset Peer IO Module**.



CHAPTER 7

Troubleshooting issues with Cisco IPMI Extensions

This chapter includes the following sections:

Introduction

Familiarity with the IPMI 2.0 specification is assumed in this chapter.

To offer greater ease of debugging, existing and future Cisco servers may offer more sensors than the 255 the current IPMI specification can handle. Thus, certain B-series and C-series Cisco servers extend the sensor and sensor related features of the IPMI 2.0 specification. This chapter describes these extensions so that IPMI tool users can use the extensions effectively.

For sensors whose sensor number is less than or equal to 255, Cisco remains compliant to IPMI specification. For sensors whose sensor number is greater than or equal to 256 (the extended sensor range or ESR), Cisco adds equivalent sensor-related IPMI commands as Cisco OEM IPMI commands. A sensor in the extended sensor range is referred to as a Cisco extended sensor (CES). Additionally, the IPMI specification does not constrain implementations to consecutively number all sensors. Thus, depending on the Cisco server and CIMC software version, there may be sensors in ESR that are not in the IPMI range even though there is room in the IPMI range.

The open source programs IPMITool and OpenIPMI will not be modified to integrate Cisco's ESR functionality. However, these tools provide the ability to issue raw IPMI commands and thus allow you to write a wrapper to process the ESR functionality.

Cisco ESR Details

Both SDR (sensor data record) and SEL formats are augmented to accommodate a 32-bit sensor ID beyond the existing IPMI standard 8-bit size. The Cisco Extended Sensor Range - Sensor Data Record (ESR-SDR) allows for more sensors, a larger record size and a longer string length. The ESR - Sensor Event Logs are enlarged and the ability to retrieve sensor readings in the new name is supported.

At the core, the operation of the CES and associated SDRs and SELs remain consistent with the behavior defined in the standard IPMI specification even though new formats are being introduced. In other words, the expected behavior of an IPMI sensor is no different than the expected behavior of a Cisco extended sensor.

The addition of the Cisco Extended SEL (ESR-SEL) repository operates slightly different than normally expected. To enhance overall debugging ease of the server, this repository contains both standard IPMI SEL events, reformatted to the ESR-SEL format, and SEL events of the Cisco Extended Sensors. In short, ESR-SEL can be regarded as the super set.

In a current UCS server, a sensor is provided to indicate, in percentage, the current usage of the IPMI SEL repositories and to generate a SEL event when the repository reaches a certain level of fullness. This sensor is named, "SEL_FULLNESS". Because ESR-SEL is a different repository, an equivalent sensor is provided. The traditional "SEL_FULLNESS" sensor always refers to the standard IPMI repository and the new "CISCO_SEL_FULLNESS" sensor refers to the ESR-SEL repository. The name of the sensor is the key in distinguishing between the repositories. Consequently, the "Clear-SEL-Event" SEL record and the "SEL-Full-Event" SEL record will also inherit the SEL usage sensor's name. By looking at the name of these sensors, one can determine the current percentage of usage, when the SEL was last cleared and when the SEL became full and to which repository those events refer.

When enabled, the UCS Manager SEL backup function will back up the SEL events from the server based on the SEL usage sensor. Prior to this implementation, this only sensor was the SEL_FULLNESS sensor. With ESR functionality, UCS Manager looks at both SEL usage sensors and backs up the events if either one reaches a certain usage level. UCS Manager will clear both repositories after the backup.

High Level Generic Algorithm

The following algorithm is provided to identify and use Cisco's Extended Sensors functionality. This algorithm can be safely applied to any Cisco and non-Cisco platform that implements IPMI.

1. Issue a **Get Device ID** IPMI command to the server. If the manufacturer ID is 0x168B, this is a Cisco B-series or C-series server. Please proceed to the next step. If the manufacturing ID is not 0x168B, do not proceed on with this algorithm any further. It may lead to undefined behavior.
2. Issue a **Cisco Get ESR Capabilities** IPMI command. Ensure that the first six bytes are as defined and all bytes are returned. If an error code is returned, a mismatch in the first six bytes or not all bytes are returned, then the Cisco B-Series or C-series server does not support ESR and do not proceed any further.
3. Check the remaining bytes in the **Cisco Get ESR Capabilities** command. If the ESR enabled flag is not set, do not proceed any further.
4. At this point, the Cisco B-series or C-series server is confirmed to support ESR and any of the Cisco ERS IPMI commands may be issued.

The following steps are recommended for retrieving sensor readings after support for ESR functionality has been established.

1. Retrieve all standard IPMI SDRs per the IPMI specification.

2. Retrieve all Cisco ESR Sensor Data Records (ESR-SDR) by issuing the **Get ESR-SDR** IPMI command.
3. Retrieve the desired sensor reading by issuing the standard IPMI **Get Sensor Reading** command or by issuing the **Get CES Reading** IPMI command as described later in this document. The **Get CES Reading** command can also be issued to retrieve IPMI sensors.
4. Use the corresponding SDR to decode the raw reading to a human readable format.

Byte Ordering

All multi-byte fields in IPMI are in little endian, meaning the least significant byte is placed in the least significant index of the request or response field. This is consistent with IPMI. For example, if there is a request field called *earth-age* and it is four bytes long at index 5 to 8. If the age of the earth is approximately 1 billion years, which is 0x3B9ACA00 in hexadecimal notation, then, index 5 of the request data is 0; index 6 should be 0xCA; index 7 is 0x9A and index 8 is 0x3B.

Cisco ESR IPMI Command Definitions

Get ESR Capabilities Command

Command Name:		Get ESR Capabilities
Net Function:		NF_STO
Command Number:		0xF5
Request Bytes	**Field Name**	**Description**
None		
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	
[2]	ID0	0x43: ASCII 'C'
[3]	ID1	0x49: ASCII 'I'
[4]	ID2	0x53: ASCII 'S'
[5]	ID3	0x43: ASCII 'C'
[6]	ID4	0x4F: ASCII 'O'
[7]	Flags	Bit 0: This is the ESR enable flag. If this bit is set, ESR functionality is supported. Bits [7:1]: Reserved. All 0's.

[8]	API Version	The current version is 1. This field determines the definition of the request and response byte for all Cisco ESR IPMI Commands. This field can be used by software to determine which API version of Cisco ESR is on this system. For example, a document update, such as a typo, will result in a revision number change but the API format may not change. Thus, software does not have to change.
[9]	Document Version, Minor	This is the minor version of this document to use for reference.
[10]	Document Version, Major	This is the major version of this document to use for reference. Both the major and minor version indicates which version of this document to use for reference. The revision is on the title page of this document.
[11:37]	Reserved	Should be all zeros.

Get ESR-SDR Repository Information Command

This command gets the repository information and is analogous to the **Get SDR Repository Info** IPMI command.

Command Name:		Get ESR-SDR Repository Info
Net Function:		NF_STO
Command Number:		0xF0
Request Bytes	**Field Name**	**Description**
None		
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	
[2]	State	0x1 still in initialization.
[3:6]	Starting Record ID	The record ID that marks the first ESR-SDR in the repository.
[7:10]	End Record ID	The record ID that marks the last ESR-SDR in the repository.
[11:14]	SDR Size	The size of the ESR-SDR Repository in bytes.

Get Cisco SDR Record

Command Name:	Get Cisco SDR Record
Net Function	NF_STO

Command Number:		0xF1
Request Bytes	**Field Name**	**Description**
[1:4]	Record ID	The record ID of the SDR whose data is to be retrieved.
[5:6]	Offset	The offset into the record
[7]	Read Bytes	The number of bytes to read. Should not exceed 33 bytes.
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	0xCA: Request read bytes and offset extends beyond the SDR's record length.
[2:5]	Next Record ID	The record id of the next SDR. 0xFFFFFFFF indicates the last record has been reached.
[6:N]		SDR Data.

Get ESR-SDR Command

This command retrieves the ESR-SDR records from the ESR-SDR Repository. Equivalent to the IPMI **Get SDR** command.

Command Name:		Get ESR-SDR
Net Function:		NF_STO
Command Number:		0xF1
Request Bytes	**Field Name**	**Description**
[1:4]	Record ID	The record ID of the SDR whose data is to be retrieved.
[5:6]	Offset	The offset into the record.
[7]	Read Bytes	The number of bytes to read. The maximum value is 33.
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	
[2:5]	Next Record ID	The record ID of the record that follows. The value, 0xFFFFFFFF, indicates the last record has been reached.

[6:N]	Data	The data of ESR-SDR record that is being retrieved.

Get CES Reading Command

This command retrieves the raw reading of the CES. Its equivalent command is the standard IPMI **Get Sensor Reading** command.

Command Name:		Get CES Reading
Net Function:		NF_SEN
Command Number:		0xF0
Request Bytes	**Field Name**	**Description**
[1:4]	CES number	The sensor number of the Cisco Extended Sensor
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	
[2]	Reading	See byte 2 of the standard IPMI Get Sensor Reading Command.
[3]	Sensor Status	See byte 3 of the standard IPMI Get Sensor Reading Command.
[4] Optional	Sensor Flags 1	See byte 4 of the standard IPMI Get Sensor Reading Command.
[5] Optional	Sensor Flags 2	See byte 5 of the standard IPMI Get Sensor Reading Command.

Get Cisco Extended SEL Repository Information

This command retrieves the raw reading regarding the SEL repository. Its equivalent command is the standard IPMI **Get SEL Info** command.

Command Name:		Get Cisco Extended SEL Repository Information
Net Function:		NF_STO
Command Number:		0xF2
Request Bytes	**Field Name**	**Description**
None		
Response Bytes	**Field Name**	**Description**

[1]	Completion Code	
[2:5]	Total Entries	Total Number of Cisco Extended SELs in the repository.
[6:9]	Free Space	Number of free bytes in the CESEL repository.
[10:13]	Add Timestamp	The timestamp of the latest Cisco SEL addition.
[14:17]	Erase Timestamp	The timestamp of the last Cisco SEL clear.
[18]	Flags	Bit 7: If set, SEL overflow occurred. Bits[6:0]: Reserved. All zeros.

Get Cisco SEL Repository Info

Command Name:		Get Cisco SEL Repository Info
Net Function		NF_STO
Command Number:		0xF2
Request Bytes	**Field Name**	**Description**
None		
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	
[2:5]	Total Entries	Number of Cisco SELs in repository
[6:9]	Free Space	Number of free bytes in repository
[10:13]	Add Timestamp	Last timestamp of Cisco SEL addition
[14:17]	Erase Timestamp	Last timestamp of Cisco SEL erase
[18]	SEL Flags	bit 7: If set, SEL overflow occurred.

Get Cisco Extended SEL Record Command

This command retrieves an entry from the SEL repository. Its equivalent command is the standard IPMI **Get SEL Entry** command.

Command Name:	Get Cisco Extended SEL Record Command

Net Function:		NF_SEN
Command Number:		0xF3
Request Bytes	**Field Name**	**Description**
[1:4]	Cisco SEL Record ID	The record ID of the Cisco Extended SEL to be retrieved.
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	
[2:5]	Next SEL Record ID	The record ID of the following SEL. The value, 0xFFFFFFFF, indicates the last SEL record has been reached.
[6:9]	SEL Record ID	The SEL ID that is being retrieved.
[10]	SEL Version	The version ID of the current SEL record. This field identifies how to interpret the remaining bytes in the SEL Record Data. Please see ESR-SEL record format section for more details.
[11:29]	SEL Record Data	The data of the Cisco Extended SEL.

Get Cisco SEL Entry

Command Name:		Get Cisco SEL Entry
Net Function:		NF_STO
Command Number:		0xF3
Request Bytes	**Field Name**	**Description**
[1:4]	SEL ID	SEL entry number to retrieve
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	0xCA: SEL ID does not exist
[2:5]	Next SEL ID	SEL ID of the next SEL. 0xFFFFFFFF indicates the last SEL record has been reached.
[6:9]	SEL ID	The SEL ID that is being retrieved.

[10]	Version	Cisco SEL Format Version. Currently it is version 1 and thus the following bytes are defined for version 1.
[11]	SEL Type	See the equivalent in IPMI Get SEL Entry Response
[12:13]	Reserved	Should be zero.
[14:17]	Time stamp	Time stamp of SEL
[18:19]	Generator ID	See the equivalent in IPMI Get SEL Entry Response
[20]	EvMRev	See the equivalent in IPMI Get SEL Entry Response
[21]	Sensor Type	See the equivalent in IPMI Get SEL Entry Response
[22:25]	Sensor Number	
[26]	Event Attribute	See the equivalent in IPMI Get SEL Entry Response
[27:29]	Event Data	See the equivalent in IPMI Get SEL Entry Response

Clear Cisco Extended SEL Repository

This command clears all existing SEL events in the repository. Equivalent to the IPMI **Clear SEL** command.

Command Name:		Clear Cisco Extended SEL Repository
Net Function:		NF_SEN
Command Number:		0xF4
Request Bytes	**Field Name**	**Description**
None		
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	

Get Cisco Sensor Reading

Command Name:	Get Cisco Sensor Reading
Net Function	NF_SEN

Command Number:		0xF0
Request Bytes	**Field Name**	**Description**
[1:4]	Sensor Number	The number of the sensor to obtain reading.
Response Bytes	**Field Name**	**Description**
[1]	Completion Code	
[2]	Reading	See byte 2 of IPMI Get Sensor Reading
[3]	Sensor Status	See byte 3 of IPMI Get Sensor Reading
[4] Optional	Sensor Flags	See byte 4 of IPMI Get Sensor Reading
[5] Optional	Sensor Flags	See byte 5 of IPMI Get Sensor Reading

Record Formats

SDR Format

Field Name	**IPMI 2.0 SDR Type 1 Byte**	**Cisco SDR Byte**	**Description**
Record ID	[1:2]	[1:4]	This will begin with the record ID of the last IPMI compliant SDR record plus one.
SDR Version	3	5	For Cisco SDR this will be 0x80.
Record Type	4	6	Will be fixed to 0xC1 for Cisco Sensor Full Data Record.
Record Length	5	[7:10]	
Sensor Owner ID	6	11	
Sensor Owner LUN	7	12	
Sensor Number	8	[13:16]	
Entity ID	9	17	
Entity Instance	10	18	

Sensor Initialization	11	19	
Sensor Capabilities	12	20	
Sensor Type	13	21	
Event/Reading Code	14	22	
Assertion Event Mask/Lower Threshold Reading Mask	[15:16]	[23:24]	
Deassertion Event Mask/Upper Threshold Reading Mask	[17:18]	[25:26]	
Discrete Reading Mask/Settable Threshold Mask/Readable Threshold Mask	[19:20]	[27:28]	
Sensor Units 1	21	29	
Sensor Units 2	22	30	
Sensor Units 3	23	31	
Linearization	24	32	
M	25	33	
M and Tolerance	26	34	
B	27	35	
B and Accuracy	28	36	
Accuracy, Accuracy exponent and Sensor Direction	29	37	
R and B exponents	30	38	
Analog Characteristic Flag	31	39	
Normal Reading	32	40	
Normal Maximum	33	41	
Normal Minimum	34	42	
Sensor Max Reading	35	43	
Senosr Min Reading	36	44	
Upper Non-Recoverable Threshold	37	45	
Upper Critical Threshold	38	46	

Upper Non-Critical Threshold	39	47	
Lower Non-Recoverable Threshold	40	48	
Lower Critical Threshold	41	49	
Lower Non-Critical Threshold	42	50	
Positive Going Threshold Hystersis	43	51	
Negative Going Threshold Hystersis	44	52	
reserved	[45:46]	N/A	Removed.
OEM	47	53	
ID String and Len Code	48	54	Bits[7:6] is per IPMI spec. Bits[5:0] is the ID String Length.
ID String	[49:64]	[55:N]	Now supports a maximum of 48 bytes. The maximum value for N is 102.

ESR-SEL Record Format

This section defines the format for the various standard IPMI SEL ranges in the ESR-SEL record format. The timestamp field, in general, indicates the number of seconds from epoch.

SEL Type 0x2 is the equivalent of the standard IPMI SEL Type 0x2 but with different indexes. The SEL record version and the SEL type field help identify this record type.

Byte Index	Field Name	Description
[1:4]	Record ID	The ID of this ESR-SEL record
[5]	Cisco SEL Record Version	Value is 0x1 for this definition.
[6]	SEL Type	Value is 0x2.
[7:8]	Reserved	Value is all 0.
[9:12]	Timestamp	Time stamp when the event was logged in the ESR-SEL repository.
[13:14]	Generator ID	Please refer to bytes 8 and 9 of the standard IPMI SEL Type 2.
[15]	EvMRev	Please refer to byte 10 of the standard IPMI SEL Type 2.

[16]	Sensor Type	Please refer to byte 11 of the standard IPMI SEL Type 2.
[17:20]	Sensor Number	The sensor number. This sensor number can be an IPMI sensor or a CES.
[21]	Event Attribute	Please refer to byte 13 of the standard IPMI SEL Type 2.
[22:24]	Event Data 1, 2 and 3	Please refer to byte 14 through 16 of the standard IPMI SEL Type 2.

SEL Type OEM Range 0xC0 to 0xDF functions as shown.

Byte Index	Field Name	Description
[1:4]	Record ID	The ID of this ESR-SEL record
[5]	Cisco SEL Record Version	Value is 0x1 for this definition.
[6]	SEL Type	Value: 0xC0 to 0xDF
[7:8]	Reserved	Value is all 0.
[9:12]	Timestamp	Time stamp when the event was logged in the ESR-SEL repository.
[13:15]	Manufacturer ID	Please refer to bytes 8 to 10 of the OEM SEL Record in the standard IPMI specification.
[16:22]	OEM Defined	Please refer to bytes 11 to 16 of the OEM SEL Record in the standard IPMI specification.
[23:24]	Reserved	Returns all 0s.

Under the IPMI specification, SEL Type OEM Range 0xE0 to 0xFF is a non-time-stamped OEM SEL record. However, when this event converts into the ESR-SEL record format, it will be time stamped.

Byte Index	Field Name	Description
[1:4]	Record ID	The ID of this ESR-SEL record
[5]	Cisco SEL Record Version	Value is 0x1 for this definition.
[6]	SEL Type	Value: 0xEO to 0xFF
[7]	OEM Defined Byte 1	Please refer to byte 4 of the OEM non-timestamped SEL event in the IPMI Specification.
[8]	Reserved	Value is 0.

[9:12]	Timestamp	Time stamp when the event was logged in the ESR-SEL repository.
[13:24]	OEM Defined Bytes 2 through 13	Please refer to bytes 5 to 16 of the OEM SEL Record format in the standard IPMI specification.

Recommended Solutions Based on IPMI Sensor Information

Overview

IPMI sensor information is available in the server event logs and in some error messages. This section presents some possible solutions for problems reported by IPMI sensors.

Power Sensors

Sensor Name	Recommended Action
	If the status shown for the voltage to any of these sensors is FAIL or anything other than OK, the server needs to be returned to Cisco for a replacement. The CPU, DIMMs, and drives can be moved to the replacement server.

Sensor Name	Recommended Action
P5V_STBY	
P3V3_STBY	
P1V1_SSB_STBY	
P1V8_STBY	
P1V0_STBY	
P1V5_STBY	
P0V75_STBY	
P12V	
P5V	
P3V3	
P1V5_SSB	
P1V1_SSB	
P1V8_SAS	
P1V5_SAS	
P1V0_SAS	
P1V0A_SAS	
P3V3_SAS	
P12V_SAS	
P0V75_SAS	
P1V05_VTT_P1	
P1V05_VTT_P2	
P1V05_VTT_P3	
P1V05_VTT_P4	
P0V9_PVSA_P1	
P0V9_PVSA_P2	
P0V9_PVSA_P3	
P0V9_PVSA_P4	
P1V8_PLL_P1	
P1V8_PLL_P2	
P1V8_PLL_P3	
P1V8_PLL_P4	
P1V1_VCCP_P1	
P1V1_VCCP_P2	

Sensor Name	Recommended Action
P1V1_VCCP_P3 P1V1_VCCP_P4 P1V5_VCC_AB P1V5_VCC_CD P1V5_VCC_EF P1V5_VCC_GH P1V5_VCC_IJ P1V5_VCC_KL P1V5_VCC_MN P1V5_VCC_OP P0V75_DDR3VTT_AB P0V75_DDR3VTT_CD P0V75_DDR3VTT_EF P0V75_DDR3VTT_GH P0V75_DDR3VTT_IJ P0V75_DDR3VTT_KL P0V75_DDR3VTT_MN P0V75_DDR3VTT_OP	
P3V_BAT_SCALED	Replace the motherboard battery if a failure is seen.
HP_MAIN_FET_FLT HP_STBY_FET_FLT HW_POWER_FLT POWER_ON_FAIL	Failure of one of these sensors indicates a failure in the blade power supplies, the server will need to be replaced.
P12V_CUR_SENS POWER_USAGE	If either of these sensors indicates a failure, reduce the load on the server. Check the power capping and budgeting options in UCS Manager.

Sensor Name	Recommended Action
VCCP_P1_CUR_SENS VCCP_P2_CUR_SENS VCCP_P3_CUR_SENS VCCP_P4_CUR_SENS PVSA_P1_CUR_SENS PVSA_P2_CUR_SENS PVSA_P3_CUR_SENS PVSA_P4_CUR_SENS VCCD_AB_CUR_SENS VCCD_CD_CUR_SENS VCCD_EF_CUR_SENS VCCD_GH_CUR_SENS VCCD_IJ_CUR_SENS VCCD_KL_CUR_SENS VCCD_MN_CUR_SENS VCCD_OP_CUR_SENS P1_CORE_VRHOT P2_CORE_VRHOT P3_CORE_VRHOT P4_CORE_VRHOT P1_MEM_VRHOT P2_MEM_VRHOT P3_MEM_VRHOT P4_MEM_VRHOT	A failure on one or more of these sensors may be seen intermittently for CPU activity spikes. Reduce the CPU load if this is seen too often.

Device Detection Sensors

Sensor Name	Recommended Action
	All of these indicate the corresponding component was discovered successfully. If an installed device fails discovery, try re-seating it in its socket, or replace it with a known working component of the same type.

Sensor Name	Recommended Action
HDD0_PRS	
HDD1_PRS	
HDD2_PRS	
HDD3_PRS	
MEZZ1_PRS	
MEZZ2_PRS	
MLOM_PRS	
TPM_CARD_PRS	
P1_PRESENT	
P2_PRESENT	
P3_PRESENT	
P4_PRESENT	
DDR3_P1_A0_PRS	
DDR3_P1_A1_PRS	
DDR3_P1_A2_PRS	
DDR3_P1_B0_PRS	
DDR3_P1_B1_PRS	
DDR3_P1_B2_PRS	
DDR3_P1_C0_PRS	
DDR3_P1_C1_PRS	
DDR3_P1_C2_PRS	
DDR3_P1_D0_PRS	
DDR3_P1_D1_PRS	
DDR3_P1_D2_PRS	
DDR3_P2_E0_PRS	
DDR3_P2_E1_PRS	
DDR3_P2_E2_PRS	
DDR3_P2_F0_PRS	
DDR3_P2_F1_PRS	
DDR3_P2_F2_PRS	
DDR3_P2_G0_PRS	
DDR3_P2_G1_PRS	
DDR3_P2_G2_PRS	

Sensor Name	Recommended Action
DDR3_P2_H0_PRS	
DDR3_P2_H1_PRS	
DDR3_P2_H2_PRS	
DDR3_P3_I0_PRS	
DDR3_P3_I1_PRS	
DDR3_P3_I2_PRS	
DDR3_P3_J0_PRS	
DDR3_P3_J1_PRS	
DDR3_P3_J2_PRS	
DDR3_P3_K0_PRS	
DDR3_P3_K1_PRS	
DDR3_P3_K2_PRS	
DDR3_P3_L0_PRS	
DDR3_P3_L1_PRS	
DDR3_P3_L2_PRS	
DDR3_P4_M0_PRS	
DDR3_P4_M1_PRS	
DDR3_P4_M2_PRS	
DDR3_P4_N0_PRS	
DDR3_P4_N1_PRS	
DDR3_P4_N2_PRS	
DDR3_P4_O0_PRS	
DDR3_P4_O1_PRS	
DDR3_P4_O2_PRS	
DDR3_P4_P0_PRS	
DDR3_P4_P1_PRS	
DDR3_P4_P2_PRS	
MAIN_POWER_PRS	
LSI_FLASH_PRSNT	
BBU_PRES	

POST Sensors

Sensor Name	Recommended Action
BIOS_POST_CMPLT	This sensor indicates BIOS POST has completed after the server powered up. Informational message, no further action is required.
BIOSPOST_TIMEOUT	POST took longer than expected and was unable to complete. Informational message, no further action is required.
BIST_FAIL	Indicates host CPU self test failure. Check the SEL to see which host CPU failed, and contact Cisco TAC. Replace the CPU.
WILL_BOOT_FAULT	The server will probably fail discovery, look for UCS Manager discovery problems.

Temperature Sensors

Sensor Name	Recommended Action
TEMP_SENS_FRONT	This is the intake temperature sensor. If this is too high, immediately verify that the ambient room temperature is within the desired range.
TEMP_SENS_REAR	This is the exhaust temperature sensor. If this is too high, verify that there are no obstructions to air intake or exhaust, and the air baffles in the server are installed as intended.
P1_TEMP_SENS P2_TEMP_SENS P3_TEMP_SENS P4_TEMP_SENS	These sensors indicate overheating CPUs. The CPUs might not have correctly applied thermal paste, or the heat sink might be damaged or not tightened properly. If these are still too high after replacing the thermal paste and checking the heat sink, also check that there are no obstructions to air intake or exhaust, and the air baffles in the server are installed as intended. If this condition has persisted too long you may need to replace the CPU.

Sensor Name	Recommended Action
	These sensors indicate overheating DIMMs. Check that there are no obstructions to air intake or exhaust, and the air baffles in the server are installed as intended. If the problem persists, the overheating DIMMs may become damaged and need to be replaced.

Sensor Name	Recommended Action
DDR3_P1_A0_TMP	
DDR3_P1_A1_TMP	
DDR3_P1_A2_TMP	
DDR3_P1_B0_TMP	
DDR3_P1_B1_TMP	
DDR3_P1_B2_TMP	
DDR3_P1_C0_TMP	
DDR3_P1_C1_TMP	
DDR3_P1_C2_TMP	
DDR3_P1_D0_TMP	
DDR3_P1_D1_TMP	
DDR3_P1_D2_TMP	
DDR3_P2_E0_TMP	
DDR3_P2_E1_TMP	
DDR3_P2_E2_TMP	
DDR3_P2_F0_TMP	
DDR3_P2_F1_TMP	
DDR3_P2_F2_TMP	
DDR3_P2_G0_TMP	
DDR3_P2_G1_TMP	
DDR3_P2_G2_TMP	
DDR3_P2_H0_TMP	
DDR3_P2_H1_TMP	
DDR3_P2_H2_TMP	
DDR3_P3_I0_TMP	
DDR3_P3_I1_TMP	
DDR3_P3_I2_TMP	
DDR3_P3_J0_TMP	
DDR3_P3_J1_TMP	
DDR3_P3_J2_TMP	
DDR3_P3_K0_TMP	
DDR3_P3_K1_TMP	
DDR3_P3_K2_TMP	

Sensor Name	Recommended Action
DDR3_P3_L0_TMP DDR3_P3_L1_TMP DDR3_P3_L2_TMP DDR3_P4_M0_TMP DDR3_P4_M1_TMP DDR3_P4_M2_TMP DDR3_P4_N0_TMP DDR3_P4_N1_TMP DDR3_P4_N2_TMP DDR3_P4_O0_TMP DDR3_P4_O1_TMP DDR3_P4_O2_TMP DDR3_P4_P0_TMP DDR3_P4_P1_TMP DDR3_P4_P2_TMP	
P1_PROCHOT P2_PROCHOT P3_PROCHOT P4_PROCHOT	These sensors indicate overheating CPUs. The CPUs might not have correctly applied thermal paste, or the heat sink might be damaged or not tightened properly. If these are still too high after replacing the thermal paste and checking the heat sink, also check that there are no obstructions to air intake or exhaust, and the air baffles in the server are installed as intended. If the problem persists, you may need to replace the CPU. This sensor also indicates the Intel Processor is trying to self-regulate its temperature by slowing its internal clock, which lowers its power draw and the heat it generates.

Sensor Name	Recommended Action
P1_THERMTRIP_N P2_THERMTRIP_N P3_THERMTRIP_N P4_THERMTRIP_N	These sensors indicate overheating CPUs. The CPUs might not have correctly applied thermal paste, or the heat sink might be damaged or not tightened properly. If these are still too high after replacing the thermal paste and checking the heat sink, also check that there are no obstructions to air intake or exhaust, and the air baffles in the server are installed as intended. If the problem persists, you may need to replace the CPU. This sensor indicates the Intel Processor is trying to self-regulate its temperature and prevent overheating damage by shutting down. Most likely this is seen after the processor has tried to self-regulate its temperature by slowing its internal clock, which lowers its power draw and the heat it generates.

Supercap Sensors

Sensor Name	Recommended Action
LSI_SCAP_FAULT	This sensor indicates the supercap needs to be replaced.
BBU_PRES	This sensor indicates the presence of a supercap. Informational, no action is required.
BBU_TEMP	This sensor reports temperature in degrees C of the supercap. Informational, no action is required unless overheating is indicated. If the supercap is overheating, power down the server.
BBU_PRED_FAIL	This sensor indicates the supercap is about to fail and should be replaced.
BBU_FAULT BBU_REPLACE_REQD	A failure has occurred in the supercap, replace the supercap immediately.
BBU_DEGRADED	The supercap needs attention. The LSI firmware will take care of this automatically and no action is required.
BBU_CAPACITANCE	Measures and reports the supercap charge state in % of design value.

Standard IPMI Sensors

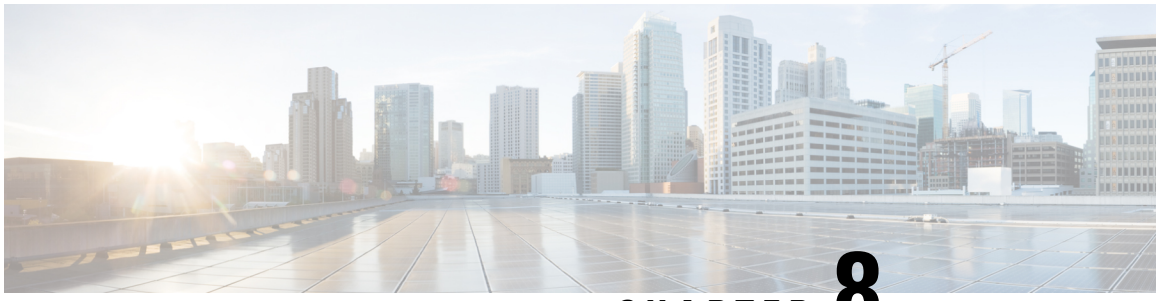
Sensor Name	Recommended Action
SEL_FULLNESS	Percentage full of the standard IPMI sensor log. No action is required, this is informational only.
CISCO_SEL_FULLNESS	Percentage full of the Cisco extended sensor log. No action is required, this is informational only.

Preventing Problems With IPMI Settings After Downgrade

Problem—IPMI settings fail.

Possible Cause—By default, IPMI over LAN is disabled in CIMC version at 2.2(2*) and above. If the system is downgraded to 2.2(1d), for example, IPMI over LAN is still disabled.

To prevent problems that sometimes occur after downgrading, follow the steps in this section before the downgrade to enable IPMI over LAN in Cisco UCS Manager: http://www.cisco.com/web/about/security/intelligence/IPMI_security.html#host.



CHAPTER 8

Troubleshooting IOM Issues

This chapter contains the following sections:

IOM Terminology

The following abbreviations and terms may be encountered while diagnosing IOM difficulties.

- HR - Host Receive Block
- NR - Network Receive Block
- SS- Switching Subsystem
- HI- Host Interface Block
- NI - Network Interface Block
- CI- CPU Interface Block
- BI- BMC Interface Block
- HIF- Host Interface
- NIF- Network Interface
- CIF- CPU Interface
- BIF- BMC Interface
- VIF- Virtual Interface
- VNTag- Virtual NIC Tag
- h2n- Host-to-Network direction. Used to describe traffic received on an HI, CI, or BI destined for an NI.
- n2h- Network-to-Host direction. Used to describe traffic received on an NI destined for an HI, CI, or BI

- Redwood - ASIC on the 2104 IOM. The basic functionality of the Redwood ASIC is to aggregate traffic to/from 8 host-facing 10G Ethernet ports connected to server adapter cards from/to 4 network-facing 10G Ethernet ports.
- Woodside - ASIC on the 2204 and 2208 IOM. Aggregates traffic to/from 32 host-facing 10G Ethernet ports from/to 4 or 8 network-facing 10G Ethernet ports.
- Chassis Management Switch (CMS) - a Marvell 88E6095 Ethernet switch integrated into the IOM.
- CMC- A CPU that controls the Redwood or Woodside ASIC and the CMS, runs the required IOM firmware, and perform other chassis management functionality.

Chassis Boot Sequence

The 2100 and 2200 series IOMs in the Cisco 5108 chassis are the only active components in the chassis itself. A single IOM is sufficient to bring the chassis up, though both would be needed in a cluster configuration.

Problems in the chassis and IOM can sometimes be traced by understanding the following boot sequence:

1. Power is applied.
2. The bootloader is invoked, the IOM memory is configured, scrubbed and ECC is enabled. The bootloader sets the IOM health LED to amber.
3. The kernel checksum and boot begins.

   An alternate kernel is booted if the selected kernel's checksum fails, or if the selected kernel failed to boot the user process "OHMS" for the last two boots.
4. If the kernel can't be booted the IOM health LED blinks amber. The IOM will not be recognized by Cisco UCS Manager. If this is the only active IOM, the entire chassis will not be recognized

   If the kernel boot is successful, the IOM Health LED is set to green. If the IOM is not recognized by Cisco UCS Manager, rule out a problem with the physical cabling between IOM and fabric interconnect. A single functioning physical connection should be enough for the chassis to be managed in Cisco UCS Manager. If the cabling is not the issue, the final possibility is that the firmware version on the IOM may be much older than the version of Cisco UCS Manager. This may or may not require the IOM be returned to Cisco.
5. Processes running on the Communications ASIC (either Redwood or Woodside) and the CMC Process Monitor (pmon) starts and restarts the following CMC platform processes:
   - platform_ohms - POST and run-time health monitoring
   - dmserver - device manager, caches seeprom data, scans I2C devices
   - ipmiserver - sends sensor and FRU data to UCS Manager
   - cmc_manager - set chassis info, respond to UCS Manager requests
   - cluster_manager - local cluster master and client data transfer
   - updated - listens for software update requests
   - thermal - chassis thermal management
   - pwrmgr- chassis power manager

- pppd - communication path to peer CMC over UART 2
- obfllogger - accepts client requests to log messages to OBFL flash
- rsyslogd - syslog, messages sent to UCS Manager controlled by level

If a failure at a stage 2 or 3 of the boot sequence is identified, the related components are the most likely causes and the IOM will almost certainly have to be returned. There is an HDMI console port on the IOMs that can directly monitor the IOM bootloader console, but its use is limited to Cisco's internal technicians, who would have access to the debugging software needed to make further changes such as loading in known functioning firmware images.

Table 10: Expected IOM and Chassis LED Behavior

LED	Status	LED State
IOM Health LED	Normal operation	Green
	Booting or minor error	Amber
	Major error	Blinking amber
Chassis OK LED	Booting	Off
	IOM Controlling	Green
Chassis FAIL LED	No error	Off
	Minor error	Amber
	Major error	Blinking amber

Link Pinning and Failover Behavior

Failures seen when a link between IOM and fabric interconnect (an IOM HIF port) goes down are more easily understood when the static route pinning applied to the servers in the chassis is understood. The quickest solution may be simply to reacknowledge the chassis, but understanding this topic will provide insight into when to apply that solution.

Table 11: Link Pinning on an IOM

Number of Active Fabric Links	Blade slot pinned to fabric link
1-Link	All the HIF ports are pinned to the active link
2-Link	1,3,5,7 to link-1 2,4,6,8 to link-2

Number of Active Fabric Links	Blade slot pinned to fabric link
4-Link	1,5 to link-1 2,6 to link-2 3,7 to link-3 4,8 to link-4
8-Link (Applies only to 2208XP)	1 to link-1 2 to link-2 3 to link-3 4 to link-4 5 to link-5 6 to link-6 7 to link-7 8 to link-8

Only 1,2,4 and 8 links are supported. 3,5,6, and 7 links are not valid configurations.

Here is an example of an expected behavior:

1. There are four active links on each IOM to their respective fabric interconnects.
2. Link 4 between IOM-1 and its fabric interconnect (currently Active) is accidentally unplugged by a datacenter worker.
3. Connectivity through IOM-1 from blade slots 3,4,7, and 8 fails over to IOM-2 and the standby fabric interconnect. While you might think that only slots 4 and 8 would be affected, link 3 fails administratively because 3 link configurations are not supported. Data throughput is not lost, but the failure is noted in Cisco UCS Manager.
4. At this point you can either:
   - Resolve the connectivity issue by plugging link 4 back in. Normal configured operation will resume.
   - Re-acknowledge the chassis, and the configuration will re-establish pinning to work over 2 fabric links. If at a later time the links are replaced or repaired, a second re-acknowledgement will be needed.

Recommended Solutions for IOM Issues

The following table lists guidelines and recommended solutions for troubleshooting IOM issues.

Table 12: IOM Issues

Issue	Recommended Solution
The IOM Health LED turns amber at initial bootup, and stays there.	Re-seat the affected IOM. Remove and replace the IOM. If both IOMs in a chassis are showing the same behavior, decommission the server or chassis and call Cisco TAC.
The IOM health LED blinks amber but never turns green.	Re-seat the affected IOM. Remove and replace the IOM. If both IOMs in a chassis are showing the same behavior, decommission the server or chassis and call Cisco TAC.
CMC receives chassis info from Cisco UCS Manager but one or more blades are either not responding or do not accept the chassis info.	Verify that the IOM firmware and Cisco UCS Manager are at the same software level. Re-seat the affected IOM. Check the POST results for the Redwood or Woodside ASIC in the IOM. Check for runtime link down status. Check for failed POST tests on the affected server. The most detail on chassis info is in the CMC Manager logs. The CMC Cluster state can be compared to the fabric interconnect with the following commands FI: show cluster state cmc connected directly to the IOM: show platform software cmcctrl dmclient all
CMC never receives chassis info from Cisco UCS Manager.	Verify that the IOM firmware and Cisco UCS Manager are at the same software level. Verify that at least one physical cable between the IOM and fabric interconnect is functioning properly. Check for runtime link down status. Re-seat the affected IOM.
The link to one or more servers has been lost.	Verify that the affected servers are in the same pinning group. Isolate and replace the downed link if possible. Re-seat the affected server. Re-seat the affected IOM. Re-establish pinning to the affected servers by reacknowledging the chassis.

Issue	Recommended Solution
IOM-1 does not seem to peer connect to IOM-2.	Re-seat both IOMs.

Checking POST results: a successful Woodside POST example

```
cmc-3-A# connect iom 1
fex-1# show platform software woodside post
PRBS passes: 0
+-------+--------+--------+--------+--------+
| Port  | Pat0   | Pat1   | Pat2   | Pat3   |
+-------+--------+--------+--------+--------+
+-------+--------+--------+--------+--------+

POST Results:
  legend:
        '.' PASSED
        'X' FAILED
        ' ' Not Run
        '/' Not applicable
              A C N N N N N N N N H H H H H H H H H H H H H H H H H H H H H H H H H H H H
              s I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I
              i   0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2
              c                                       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7
+-+----------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0| Register |
|1| MBIST
|2| CI lpbk
|3| Serdes   |/|/| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
 | | | |
|4| PHY BIST |/|/|.|.|.|.|.|.|.|.| | | | | | | | | | | | | | | | | | | | | | | | | | | | |
 | | | |
|5| PRBS
|6| PCS lpbk
|7| Runtime  |/|/| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
 | | | |
+-+----------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Checking POST results: a successful Redwood POST example

```
cmc-3-A# connect iom 1
fex-1# show platform software redwood post
Redwood POST Results:
  legend:
        '.' PASSED
        'X' FAILED
        ' ' Not Run
+-------------------+-+----+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   |A|    | | | | | | | | | | | | | | | |
|                   |S|ASIC| | |H|H|H|H|H|H|H|N|N|N|N|
|                   |I|LVL |C|B|I|I|I|I|I|I|I|I|I|I|I|
| POST Test         |C|RSLT|I|I|0|1|2|3|4|5|6|7|0|1|2|3|
+-------------------+-+----+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| 0. Register Test  |0|  . | | | | | | | | | | | | | | |
| 1. MBIST          |0|  . | | | | | | | | | | | | | | |
```

```
| 2. CI Loopback    |0|  . | | | | | | | | | | | | | | |
| 3. Serdes         |0|    | | |.|.|.|.|.|.|.|.|.|.|.|.|
| 4. PHY BIST       |0|    | | |.|.|.|.|.|.|.|.|.|.|.|.|
| 5. PRBS           |0|    | | |.|.|.|.|.|.|.|.|.|.|.|.|
| 6. PCS Loopback   |0|    | | |.|.|.|.|.|.|.|.|.|.|.|.|
| 7. IIF PRBS       |0|    | | | | | | | | | | | | | |
| 8. Runtime Failure|0|    | | | | | | | | | | | | | |
+-------------------+-+----+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
fex-1#
```

Verifying Chassis Management Switch Statistics

```
cmc-3-A# connect iom 1
fex-1# show platform software cmcctrl cms all
0        up <= iBMC slot 1
1        up <= iBMC slot 2
2        down <= iBMC slot 3
3        down <= iBMC slot 4
4        up <= iBMC slot 5
5        down <= iBMC slot 6
6        down <= iBMC slot 7
7        down <= iBMC slot 8
8        up <= CMS/CMC Processor link
9        no_phy <= Redwood link
10       no_phy <= Debug port link
IN_GOOD_OCTETS_LO (p0)  : [0x000290AA]
IN_GOOD_OCTETS_HI (p0)  : [0x00000000]
...
...
IN_FILTERED       (p10) : [0x0000]
OUT_FILTERED      (p10) : [0x0000]
```

Check for runtime link down status, Woodside ASICs.

- NI - network interface is to the switch
- HI - host interface is to the blades

```
cmc-3-A# connect iom 1
fex-1# show platform software woodside sts
Board Status Overview:
 legend:
        '  '= no-connect
        X   = Failed
        -   = Disabled
        :   = Dn
        |   = Up
        [$] = SFP present
        [ ] = SFP not present
        [X] = SFP validation failed
------------------------------

(FINAL POSITION TBD)     Uplink #:        1  2  3  4  5  6  7  8
                       Link status:       |  |  |  |  |  |  |  |
                                        +-+--+--+--+--+--+--+--+-+
                                SFP:     [$][$][$][$][$][$][$][$]
                                        +-+--+--+--+--+--+--+--+-+
                                        | N  N  N  N  N  N  N  N |
                                        | I  I  I  I  I  I  I  I |
                                        | 0  1  2  3  4  5  6  7 |
                                        |                        |
                                        |        NI (0-7)        |
                                        +------------+-----------+
                                                     |
```

```
+-------------------------+-------------+-------------+---------------------------+
             |                           |                           |
     |
+------------+-----------+ +-----------+------------+ +------------+-----------+
+-------------+----------+
|        HI (0-7)        | |        HI (8-15)       | |       HI (16-23)       | |
HI (24-31)      |
|                        | |                        | |                        | |
                 |
| H  H  H  H  H  H  H  H | | H  H  H  H  H  H  H  H | | H  H  H  H  H  H  H  H | | H  H  H
  H  H  H  H  H |
| I  I  I  I  I  I  I  I | | I  I  I  I  I  I  I  I | | I  I  I  I  I  I  I  I | | I  I  I
  I  I  I  I  I |
| 0  1  2  3  4  5  6  7 | | 8  9  1  1  1  1  1  1 | | 1  1  1  1  2  2  2  2 | | 2  2  2
  2  2  2  3  3 |
|                        | |       0  1  2  3  4  5 | | 6  7  8  9  0  1  2  3 | | 4  5  6
  7  8  9  0  1 |
+-+--+--+--+--+--+--+-+ +-+--+--+--+--+--+--+-+ +-+--+--+--+--+--+--+-+
+-+--+--+--+--+--+--+-+
 [ ][ ][ ][ ][ ][ ][ ][ ]   [ ][ ][ ][ ][ ][ ][ ][ ]   [ ][ ][ ][ ][ ][ ][ ][ ]   [ ][ ][
][ ][ ][ ][ ][ ]
+-+--+--+--+--+--+--+-+ +-+--+--+--+--+--+--+-+ +-+--+--+--+--+--+--+-+
+-+--+--+--+--+--+--+-+
  -  -  -  |  -  -  -  |     -  -  -  :  -  -  -  :     -  -  -  :  -  -  -  :     -  -  -
  |  -  -  -  |
  3  3  3  2  2  2  2  2     2  2  2  2  2  1  1  1     1  1  1  1  1  1  1  9     8  7  6
  5  4  3  2  1
  2  1  0  9  8  7  6  5     4  3  2  1  0  9  8  7     6  5  4  3  2  1  0
  \__\__/__/  \__\__/__/     \__\__/__/  \__\__/__/     \__\__/__/  \__\__/__/     \__\__/__/
  \__\__/__/
    blade8      blade7         blade6      blade5         blade4      blade3         blade2
      blade1
```

Check for runtime link down status, Redwood ASICs.

- NI - network interface is to the switch
- HI - host interface is to the blades

```
cmc-3-A# connect iom 1
fex-1# show platform software redwood sts
Board Status Overview:
 legend:
        ' '= no-connect
        X  = Failed
        -  = Disabled
        :  = Dn
        |  = Up
        ^  = SFP+ present
        v  = Blade Present
------------------------------

        +---+----+----+----+
        |[$]| [$]| [$]| [$]|
        +---+----+----+----+
          |    |    |    |
        +-+----+----+----+-+
        | 0    1    2    3 |
        | I    I    I    I |
        | N    N    N    N |
        |                  |
        |      ASIC 0      |
        |                  |
        | H H H H H H H H  |
```

```
        | I I I I I I I I  |
        | 0 1 2 3 4 5 6 7  |
        +-+-+-+-+-+-+-+-+--+
          | | : : - - : :
         +-+-+-+-+-+-+-+-+
         |v|v|v|v|-|-|v|v|
         +-+-+-+-+-+-+-+-+
Blade:    8 7 6 5 4 3 2 1

fex-1#
```

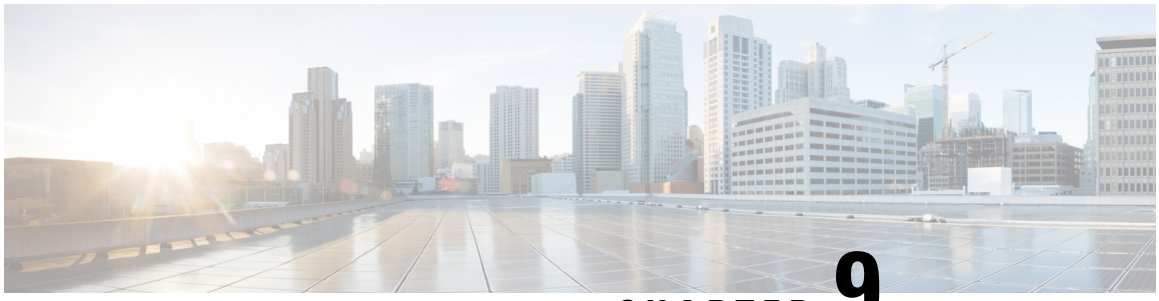
Check administrative control, MAC and PHY status, and SFP detected, Redwood example.

```
cmc-3-A# connect iom 1
fex-1# show platform software redwood oper

ASIC 0:
 +--+----+-+----+-----+-------------------------+-+
 |  |    | |    |MAC  |        PHY              | |
 |P | N  |A|    |-+-+-+----+-+-+-+--------+-----+ +
 |o | a  |d|    | | |A|    |X| | |        |     | |
 |r | m  |m|    |L|R|L|    |G|P|P|        |     |S|
 |t | e  |i|Oper|C|M|G|MDIO|X|C|M|        |     |F|
 |  |    |n| St |L|T|N|adr |S|S|D| u-code | Ver |P|
 +--+----+-+----+-+-+-+----+-+-+-+--------+-----+-+
 | 0| CI |E| Up | | | |  0 |0|0|0| n/a    | 0.00| |
 | 1| BI |E| Up | | | |  0 |0|0|0| n/a    | 0.00| |
 | 2| HI0|E| Up | | | | 18 |1|1|1| Ok     | 1.09| |
 | 3| HI1|E| Up | | | | 19 |1|1|1| Ok     | 1.09| |
 | 4| HI2|E| Dn |1| |1| 16 |0|0|0| Ok     | 1.09| |
 | 5| HI3|E| Dn |1| |1| 17 |0|0|0| Ok     | 1.09| |
 | 6| HI4|-| Dn | | |1| 14 |0|0|0| Ok     | 1.09| |
 | 7| HI5|-| Dn | | |1| 15 |0|0|0| Ok     | 1.09| |
 | 8| HI6|E| Dn |1| |1| 12 |0|0|0| Ok     | 1.09| |
 | 9| HI7|E| Dn |1| |1| 13 |0|0|0| Ok     | 1.09| |
 |10| NI0|E| Up | | | | 23 |1|1|1| Ok     | 1.39|*|
 |11| NI1|E| Up | | | | 22 |1|1|1| Ok     | 1.39|*|
 |12| NI2|E| Up | | | | 21 |1|1|1| Ok     | 1.39|*|
 |13| NI3|E| Up | | | | 20 |1|1|1| Ok     | 1.39|*|
 +--+----+-+----+-+-+-+----+-+-+-+--------+-----+-+
```

Check administrative control, MAC and PHY status, and SFP detected, Woodside example.

```
fex-1# show platform software woodside oper

ASIC 0:
 +---+-----+-+----+----------+----------------+
 |   |     | |    |    MAC   | |  PHY  | |    |
 |   |     | |    |          |S|---+---| |    |
 |   |     |A|    |-+-+-+-+-+-|e|XFI|SFI| |    |
 | P |     |d|    | |L|T|R|R|T|r|---+---| |    |
 | o |     |m|    |P|o|R|R|F|F|d|p|p|p|p|S|    |
 | r |
|i|Oper|C|c|d|d|l|l|e|m|c|c|m|F|ucode|---------------------------+----------------------------+-----+

 | t |Name |n| St |S|k|y|y|t|t|s|d|s|s|d|P| ver |    Time last came Up       |      Time
last went Down   |Flaps|

+---+-----+-+----+-+-+-+-+-+-+-+-+-+-+-+-+-----+---------------------------+----------------------------+-----+

 | 0 |HI0  |-| Dn |0|0|1|1|0|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 | 1 |HI1  |-| Dn |0|0|1|1|0|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 | 2 |HI2  |-| Dn |0|0|1|1|0|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
```

```
00:00:00.000000 |    0|
 | 3 |HI3  |E| Up |1|1|1|1|1|1|1|0|0|0|0| | 0.00| 02/03/2012 23:17:36.046137 | 02/03/2012
23:17:34.815303 |   24|
 | 4 |HI4  |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 | 5 |HI5  |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 | 6 |HI6  |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 | 7 |HI7  |E| Up |1|1|1|1|1|1|1|0|0|0|0| | 0.00| 02/03/2012 22:53:04.761879 | 02/03/2012
22:52:44.548148 |   17|
 | 8 |HI8  |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 | 9 |HI9  |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 |10 |HI10 |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 |11 |HI11 |E| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 02/03/2012 20:46:44.214237 | 02/03/2012
20:49:30.606932 |    3|
 |12 |HI12 |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 |13 |HI13 |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 |14 |HI14 |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 |15 |HI15 |E| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 02/03/2012 20:45:30.918631 | 02/03/2012
20:48:06.811009 |    3|
 |16 |HI16 |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
 |17 |HI17 |-| Dn |0|0|1|1|0|0|0|0|0|0|0| | 0.00| 01/01/1970 00:00:00.000000 | 01/01/1970
00:00:00.000000 |    0|
```



CHAPTER 9

Additional Troubleshooting Documentation

Additional Troubleshooting Documentation

Additional troubleshooting information is available in the following documents:

- Cisco UCS Manager Faults and Error Message Reference—Contains information about Cisco UCS Manager faults and System Event Log messages, including BIOS and CIMC messages.
- Cisco UCS C-Series Servers Integrated Management Controller Troubleshooting Guide—Contains information about how to troubleshoot issues with C-Series rack-mount servers.
- Cisco UCS Central Troubleshooting Reference Guide—Contains information about how to troubleshoot issues with Cisco UCS Central.

Additional Troubleshooting Documentation