Cisco UCS Manager B-Series Troubleshooting Guide

First Published: October 26, 2011

Last Modified: June 04, 2012

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

Text Part Number: OL-20137-11

CONTENTS

Preface

CHAPTER 1

Preface

This preface includes the following sections:

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

Organization

This document includes the following chapters:

Chapter	Title	Description
Chapter 1	Overview of Troubleshooting in Cisco UCS Manager, on page 1	Provides an overview of where to find faults, events, and other information that can help you troubleshoot issues with Cisco Unified Computing System (Cisco UCS) servers and Cisco UCS Manager.

Chapter	Title	Description
Chapter 2	Finite State Machine, on page 15	Describes the finite state machine (FSM) and how to use it to troubleshoot issues with Cisco UCS.
Chapter 3	General Troubleshooting Solutions, on page 19	Describes solutions that you can implement when you troubleshoot issues with Cisco UCS.
Chapter 4	Troubleshooting Issues with Cisco UCS Manager, on page 25	Describes solutions that you can implement when you troubleshoot issues with Cisco UCS Manager.
Chapter 5	Troubleshooting SAN Boot and SAN Connectivity Issues, on page 43	Describes how to troubleshoot SAN boot and SAN connectivity issues, including the Storage Area Network (SAN) configuration in Cisco UCS Manager and the SAN array.
Chapter 6	Troubleshooting Server Hardware Issues , on page 45	Describes how to troubleshoot hardware issues not specific to a given model of Cisco UCS B-Series server.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`courier`font	Terminal sessions and information that the system displays appear in `courier` font.
[ ]	Elements in square brackets are optional.
{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.

Convention	Indication
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*.

Tip Means *the following information will help you solve a problem*.

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

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

Warning Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

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: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc .

Other Documentation Resources

An ISO file containing all B and C-Series documents is available at the following URL: http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821. From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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

CHAPTER 1

Overview of Troubleshooting in Cisco UCS Manager

This chapter includes the following sections:

Troubleshooting Information in Cisco UCS Manager GUI

Cisco UCS Manager GUI provides several tabs and other areas that you can use to find troubleshooting information for a Cisco UCS domain. For example, you can view faults and events for specific objects or for all objects in the system.

The **Admin** tab in the **Navigation** pane provides access to faults, events, core files, and other information that can help you troubleshoot issues.

If you select **Faults, Events and Audit Log** in the **Filter** field on the **Admin** tab, Cisco UCS Manager GUI limits the tree browser so that you can only access the following:

- The faults for all components in the system
- The events for all components in the system
- The audit log for the system
- Any core files created by the fabric interconnects in the system

- The fault collection and core file export settings

Note Fault thresholds might need to be modified. See the "Statistics Threshold Policy" section in the *Cisco UCS Manager GUI Configuration Guide* for the release of Cisco UCS Manager that you are using.

Troubleshooting Information in Cisco UCS Manager CLI

The Cisco UCS Manager CLI includes several **show** commands that you can execute to find troubleshooting information for a Cisco UCS domain. These **show** commands are scope-aware, which means that if you enter the **show fault** command from the top scope, it displays all faults in the system. However, if you scope to a specific object, the **show fault** command displays faults that are related to that object only.

Note Fault thresholds might need to be modified. See the "Statistics Threshold Policy" section in the *Cisco UCS Manager CLI Configuration Guide* for the release of Cisco UCS Manager that you are using.

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.

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.
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.
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.

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 #unique_32.
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.
ID	Unique identifier assigned to the fault.
Type	Type of fault that has been raised, which can be any of the types described in #unique_33.
Cause	Unique identifier associated with the condition that caused the fault.
Created at	Day and time when the fault occurred.
Code	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 1: Event Properties

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

Core Files

Critical failures in Cisco UCS Manager and some of the Cisco UCS components, such as a fabric interconnect or an I/O module, can cause the system to create a core file. Each core file contains a large amount of data about the system and the component at the time of the failure.

Cisco UCS Manager manages the core files from all of the components. You can configure Cisco UCS Manager to export a copy of a core file to a location on an external TFTP server as soon as that core file is created.

Core Files in the Cisco UCS Manager GUI

You can find out if a component in the Cisco UCS domain generated a core file by navigating to the **Core Files** node on the **Admin** tab under the **Faults, Events and Audit Log** node.

Core Files in the Cisco UCS Manager CLI

You can find out if a component in the Cisco UCS domain generated a core file by entering the following commands:

1. **scope monitoring**
2. **scope sysdebug**
3. **show cores**

Core File Exporter

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

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

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 2: 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 3.
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 GUI

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.

Tip For more information about the SEL, including how to view the SEL for each server and configure the SEL policy, see the Cisco UCS Manager configuration guides, which are accessible through the Cisco UCS B-Series Servers Documentation Roadmap.

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 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 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 3: 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 4: 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.

CHAPTER 2

Finite State Machine

This chapter includes the following sections:

Overview of the FSM

An FSM is a workflow model, similar to a flow chart, that is composed of the following:

- A finite number of stages (states)
- Transitions between those stages
- Operations

The current stage in an FSM is determined by past stages and the operations performed to transition between the stages. A transition from one stage to another is dependent on the success or failure of an operation.

Cisco UCS Manager uses FSM tasks that run in the Data Management Engine (DME) to manage end points in the Cisco UCS object model, including the following

- Physical components (chassis, I/O module, servers)
- Logical components (LAN cloud, policies)
- Workflows (server discovery, service profile management, downloads, upgrades, backups)

The DME manages the FSM stages and transitions and instructs the Application Gateway (AG) to perform operations on the managed end points. Therefore, each stage can be considered to be an interaction between the DME, AG, and managed end point. The AGs do the real work in interacting with managed end points, such as the CIMC, adapter, or I/O module.

When all of the FSM stages have run successfully, Cisco UCS considers the FSM to be successful.

If the FSM encounters an error or timeout at a stage, the FSM retries that stage at scheduled intervals. When the retry count has been reached for that stage, the FSM stops and Cisco UCS Manager declares the change to have failed. If an FSM task fails, Cisco UCS Manager raises faults and alarms.

Multiple FSM tasks can be associated to an end point. However, only one FSM task at a time can run. Additional FSM tasks for the same end point are placed in a queue and are scheduled to be run when the previous FSM task is either successfully completed or fails.

You can view the FSM details for a particular end point to determine if a task succeeded or failed. You can also use the FSM to troubleshoot any failures.

FSM Stage Names

The FSM stage names are usually constructed using the following notation:

Fsm*ObjectWorkflowOperationWhere-is-it-executed*

where:

- *Object* is the object the FSM is running, such as Blade/Chassis.
- *Workflow* is the overall task being performed by the FSM, such as Discover or Association.
- *Operation* is the task being performed at a particular stage, such as Pnuos-Config.
- *Where-is-it-executed* is generally “”, or “A” or “B” or “Local” or “Peer”. If not specified, it is executed on the managingInst node.

Each FSM stage name has a prefix that identifies the FSM and a suffix that identifies a stage within the FSM. The prefix notation is **Fsm***ObjectWorkflow* and the suffix notation is *OperationWhere-is-it-executed*. For example, if the FSM name is **FsmComputeBladeDiscoverCimcInventory**, the prefix is **FsmComputeBladeDiscover** and the suffix is **CimcInventory**.

FSM in the Cisco UCS Manager GUI

The Cisco UCS Manager GUI displays FSM information for an end point on the FSM tab for that end point. You can use the FSM tab to monitor the progress and status of the current FSM task and view a list of the pending FSM tasks.

The information about a current FSM task in the Cisco UCS Manager GUI is dynamic and changes as the task progresses. You can view the following information about the current FSM task:

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

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

FSM in Cisco UCS Manager CLI

The Cisco UCS Manager CLI can display the FSM information for an endpoint when you are in the command mode for that end point.

You can use the **show fsm status** command in the appropriate mode to view the current FSM task for an end point. The information displayed about a current FSM task in the command-line interface (CLI) is static. You must reenter the command to see progress updates.

The following example shows how to display information about the current FSM task for the server in chassis 1, slot 6:

```
)
UCS-A# scope server 1/6

UCS-A /chassis/server # show fsm status
Slot: 6
Server: sys/chassis-1/blade-6
    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Discover Blade Boot Wait
        Previous Status: Discover Blade Boot Wait
        Timestamp: 2006-01-26T23:31:36
        Try: 0
        Flags: 0
        Progress (%): 33
        Current Task: Waiting for system reset on server 1/6
(FSM-STAGE:sam:dme:ComputeBladeDiscover:BladeBootWait)
```

You can use the **show fsm task** command in the appropriate mode to view all pending tasks in the FSM queue.

The following example shows how to display the FSM task queue for the server in chassis 1, slot 6:

```
UCS-A# scope server 1/6
UCS-A /chassis/server # show fsm task

FSM Task:
    Item             ID       Completion   FSM Flags
    ---------------- -------- ------------ ---------
    Powercycle        1154858 Scheduled
    BiosRecovery      1154860 Scheduled
```

CHAPTER 3

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 5: 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.
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.

Guideline	Description
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.

Technical Support Files

When you encounter an issue that requires troubleshooting or a request for assistance to the Cisco Technical Assistance Center (Cisco TAC), 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.
- 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.

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 TAC.

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*} | **ucsm**} [**brief** | **detail**]	Outputs information about the selected objects in a file that you can send to Cisco TAC.
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 '~'.

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 the **Admin** tab.

Step 2 On the **Admin** tab, click **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.

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

Option	Description
ucsm	Saves a file containing technical support data for the entire Cisco UCS domain in the specified directory.
ucsm-mgmt	Saves a file containing technical support data for the Cisco UCS management services, excluding the fabric interconnects, in the specified directory.
chassis	Saves 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 I/O module within the chassis, enter that module's ID in the **IOM ID** field. To get the data for all I/O modules in the chassis, enter all in this field.
fabric-extender	Saves a file containing technical support data for a fabric extender in the specified directory. 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.

Option	Description
rack-server	Saves a file containing technical support data for a C-Series server to the specified directory. When you select this option, Cisco UCS Manager GUI displays the following fields: • **Rack Server ID** field—The unique identifier of the rack server for which you want technical support data. • **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.

Step 6 Click **OK**.

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.

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.

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 4

Troubleshooting Issues with Cisco UCS Manager

This chapter includes the following sections:

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 the **Servers** tab, 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 the **Equipment** tab, 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 the **Servers** tab.

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

	Command or Action	Purpose
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:	
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:	

Troubleshooting Cisco UCS Manager Issues

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 TAC 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**.

Forcing a Fabric Interconnect Failover

This operation can only be performed in the Cisco UCS Manager CLI.

You must force the failover from the primary fabric interconnect.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show cluster state**	Displays the state of fabric interconnects in the cluster and whether the cluser is HA ready.
Step 2	UCS-A# **connect local-mgmt**	Enters local management mode for the cluster.
Step 3	UCS-A (local-mgmt) # **cluster** {**force primary** | **lead** {**a** | **b**}}	Changes the subordinate fabric interconnect to primary using one of the following commands: **force** Forces local fabric interconnect to become the primary. **lead** Makes the specified subordinate fabric interconnect the primary.

The following example changes fabric interconnect b from subordinate to primary:

```
UCS-A# show cluster state
Cluster Id: 0xfc436fa8b88511e0-0xa370000573cb6c04

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
UCS-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-A(local-mgmt)# cluster lead b
UCS-A(local-mgmt)#
```

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 as described in Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script.

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*

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.

CHAPTER 5

Troubleshooting Server Disk Drive Detection and Monitoring

This chapter includes the following sections:

Support for Disk Drive Monitoring

Disk drive monitoring only supports certain blade servers and a specific LSI storage controller firmware level.

Supported Cisco UCS Servers

Through Cisco UCS Manager, you can monitor disk drives for the following servers:

- B-200 blade server
- B-230 blade server
- B-250 blade server
- B-440 blade server

Cisco UCS Manager cannot monitor disk drives in any other blade server or rack-mount server.

Storage Controller Firmware Level

The storage controller on a supported server must have LSI 1064E firmware.

Cisco UCS Manager cannot monitor disk drives in servers with a different level of storage controller firmware.

Prerequisites for Disk Drive Monitoring

In addition to the supported servers and storage controller firmware version, you must ensure that the following prerequisites have been met for 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 a Disk Drive in the Cisco UCS Manager GUI

Procedure

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

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.

Step 3 Click the server for which you want to view the status of the disk drive.

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

Step 5 Click the **Storage** subtab.

Step 6 Click the down arrows to expand the **Disks** bar and view the following fields in the **States** section for each disk drive:

Name	Description
Operability field	The operational state of the disk drive. This can be the following: • **Operable**—The disk drive is operable. • **Inoperable**—The disk drive is inoperable, possibly due to a hardware issue such as bad blocks. • **N/A**—The operability of the disk drive cannot be determined. This could be due to the server or firmware not being support for disk drive monitoring, or because the server is powered off. **Note** The **Operability** field may show the incorrect status for several reasons, such as if the disk is part of a broken RAID set or if the BIOS POST (Power On Self Test) has not completed.

Name	Description
Presence field	The presence of the disk drive, and whether it can be detected in the server drive bay, regardless of its operational state. This can be the following: • **Equipped**—A disk drive can be detected in the server drive bay. • **Missing**—No disk drive can be detected in the server drive bay.

Viewing the Status of a Disk Drive in the Cisco UCS Manager CLI

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope server** *server-num*	Enters server chassis mode.
Step 3	UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}	Enters RAID controller server chassis mode.
Step 4	UCS-A /chassis/server/raid-controller #	Displays the following local disk statistics:

	Command or Action	Purpose	
		Name	**Description**
	show local-disk [*local-disk-id* | **detail** | **expand**]	**Operability** field	The operational state of the disk drive. This can be the following: • **Operable**—The disk drive is operable. • **Inoperable**—The disk drive is inoperable, possibly due to a hardware issue such as bad blocks. • **N/A**—The operability of the disk drive cannot be determined. This could be due to the server or firmware not being support for disk drive monitoring, or because the server is powered off. **Note** The **Operability** field may show the incorrect status for several reasons, such as if the disk is part of a broken RAID set or if the BIOS POST (Power On Self Test) has not completed.
		Presence field	The presence of the disk drive, and whether it can be detected in the server drive bay, regardless of its operational state. This can be the following: • **Equipped**—A disk drive can be detected in the server drive bay. • **Missing**—No disk drive can be detected in the server drive bay.

The following example shows the status of a disk drive:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 6
UCS-A /chassis/server # scope raid-controller 1 sas
UCS-A /chassis/server/raid-controller # show local-disk 1

Local Disk:
    ID: 1
    Block Size: 512
    Blocks: 60545024
    Size (MB): 29563
    Operability: Operable
    Presence: Equipped
```

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 disk 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 property values.

Operability Status	Presence Status	Interpretation
Operable	Equipped	No fault condition. The disk drive is in the server and can be used.
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 may show the incorrect status for several reasons, such as if the disk is part of a broken RAID set or if the BIOS POST (Power On Self Test) 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 TAC.

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.

CHAPTER 6

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 44?

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 7

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 error 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

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 and service notes 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 and service notes to verify that you are adding the DIMMs appropriately for a given server type.
- Most DIMMs are sold in matched pairs. They are intended to be added two at a time, paired with each other. Splitting the pairs can cause memory problems.
- If the replacement DIMMs have a maximum speed lower than those previously installed, all DIMMs in a server run at the slower speed or not work at all. All of the DIMMs in a server should be of the same type.
- The number and size of DIMMs should be the same for all CPUs in a server. Mismatching DIMM configurations can damage system performance.

Known DIMM Memory Issues

Cisco UCS Manager GUI Incorrectly Reports Bad DIMMs

The Cisco UCS Manager GUI can incorrectly report "inoperable memory" when the Cisco UCS Manager CLI indicates no failures. This problem has occurred when running Cisco UCS Manager, Release1.0(1e).

Upgrade to Cisco UCS Manager, Release1.0(2d) or a later release. If that is not possible, to confirm memory is OK, enter the following CLI commands in order (where x=chassis# and y=server# and z=memory array ID#):

- scope server x/y show memory detail
- scope server x/y show memory-array detail -> provides memory-array ID
- scope server x/y scope memory-array z show stats history memory-array-env-stats detail

Resetting the BMC to Clear DIMM Error

Correctable DIMM errors report a DIMM as “Degraded” in Cisco UCS Manager, but the DIMMs are still available to the OS on the blade.

To correct this problem, use the following commands to clear the SEL logs from the BMC, then reboot the BMC of the affected blade, or just remove and reseat the blade server from the chassis.

Procedure

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

The following example resets the SEL logs from the BMC on server x/y:

```
SAM-FCS-A# scope server x/y
UCS-A /chassis/server # scope bmc
UCS-A /chassis/server/bmc # reset
UCS-A /chassis/server/bmc* # commit-buffer
```

Cisco UCS Manager Incorrect Report of Effective Memory

When running Cisco UCS Manager, Release 1.0(1e), Cisco UCS Manager can misread the SMBIOS table, and not be able to read it without a server reboot.

Upgrade to Cisco UCS Manager, Release 1.2(0) or a later release.

Memory Misreported in Cisco UCS Manager

Memory arrays show more memory sockets than are physically on the system board.

Upgrade to Cisco UCS Manager, release 1.0(2j) or later.

Single DIMM Causes Other DIMMs To Get Marked as Bad and POST Fails

The server does not complete its boot cycle, and the FSM remains stuck at 54 percent.

Upgrade to Cisco UCS Manager, Release 1.2.(1b) or a later release.

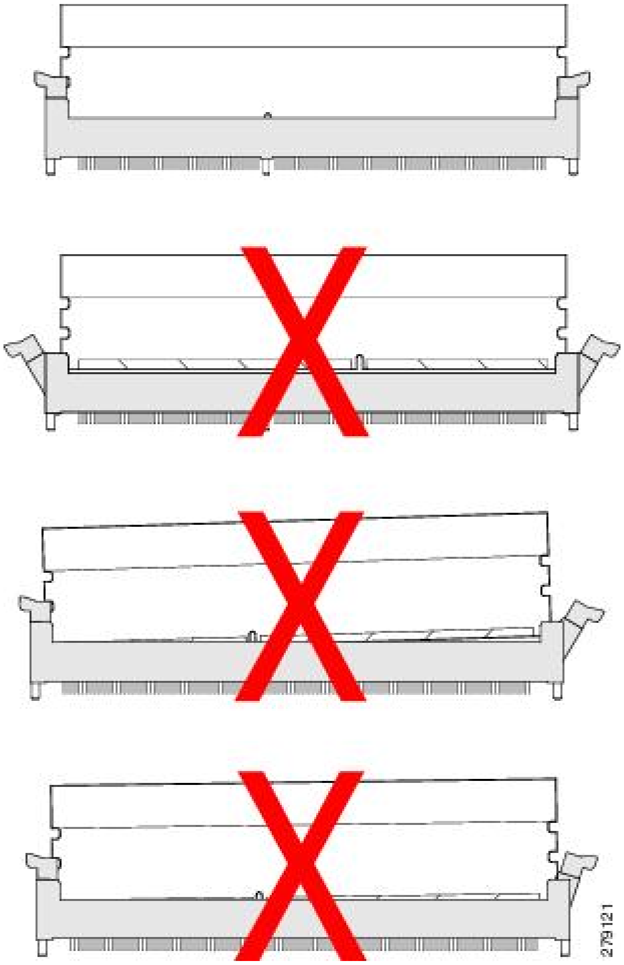
Troubleshooting DIMM Errors

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.

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 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.

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. Cisco UCS Manager shows the DIMMs as inoperable in the case of uncorrectable DIMM errors. These errors are not correctable using the software. You can identify a bad DIMM and remove it to allow the server to boot. For example, the BIOS fails to pass the POST due to one or more bad DIMMs.

In situations where BIOS POST failures occur due to suspected memory issues and the particular DIMMs or DIMM slots are not identifiable, follow these steps to further isolate a particular failed part:

Procedure

Step 1 Remove all DIMMs from the system.

Step 2 Install a single DIMM (preferably a tested good DIMM) or a DIMM pair in the first usable slot for the first processor (minimum requirement for POST success). For example, On a B200 blade it is DIMM slot A1. Refer to the published memory population rules to determine which slot to use.

Step 3 Re-attempt to boot the system.

Step 4 If the BIOS POST is still unsuccessful, repeat steps 1 through 3 using a different DIMM in step 2.

Step 5 If the BIOS POST is successful and the blade can associate to a service profile, continue adding memory. Follow the population rules for that server model. If the system can successfully pass the BIOS POST in some memory configurations but not 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 6: 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.

Issue	Recommended Solution
The DIMM is reported as bad in the SEL, POST, or LEDs, or the DIMM is reported as inoperable in Cisco UCS Manager.	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. Upgrade to Cisco UCS Manager, Release 1.2.(1b) or a later release. 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 blade server in the chassis. Verify that all DIMMs can run at the same speed. If a slower DIMM is added to a system that had used faster DIMMs, all DIMMs on a server run at the slower speed.
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. (B440 servers use these for unused CPU slots.)

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.
- f 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.
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.

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 CPU Issues

The following table lists guidelines and recommended solutions that can assist you in troubleshooting CPU issues.

Issue	Recommended Solution
The CPU does not fit in slot.	Verify that the CPU is supported on that server model. Verify that the CPU 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 UCS Manager.	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. Upgrade to Cisco UCS Manager, Release 1.2.(1b) or a later release. Reset the BMC.
The DIMM is reported as degraded in the GUI or CLI.	Reset the BMC. Reseat the blade server in the chassis. Verify that all DIMMs are running at the same speed. If a slower DIMM is added to a system that has faster DIMMs, all of the DIMMs on a server run at the slower speed.

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 of the empty HDD bays, server slots, and power supply bays use blanking covers to assure that the air flows move as designed. Verify that the server air baffles are installed to assure that the air flows move as designed.

CPU CATERR Details

The system event log (SEL) contains events related to the processor's catastrophic error (CATERR) sensor. A CATERR message indicates a failure, while a CATERR_N message indicates that the sensor is not in a failure state.

A CATERR_N message indicates an assertion of a no-fault bit that indicates that a predictive failure was deasserted. The no-fault bit was turned on to indicate that there is no failure.

When the sensor is initialized, the BMC sends out a SEL event with the initial state of the sensor in order to stay in synchronization with the server manager software, which monitors when the sensors are active and the state of the sensors. In most cases, the initial reading of the sensor is that a predictive failure has been deasserted, resulting in a CATERR_N message being sent.

Transitions from a nonfault state to a fault state turn off a no-fault bit and turn on a fault bit. In this case, you can expect two events to occur:

- No-fault (predictive failure deasserted) bit has been deasserted,
- Fault (predictive failure asserted) bit has been asserted.

These events indicate that the no-fault bit is turned OFF (deasserted) and the fault bit (predictive failure asserted) is turned ON.

Transitions from a fault state to a nonfault state often are redundant and not generally logged, as they indicate a condition that is not an error or a false positive case. These messages state that a reading was received from the sensor and the no-failure bit in the sensor is turned ON. The initial sensor state readings are logged for synchronization reasons with the management software.

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.

Documentation About RAID Controllers and LSI Utilities

The LSI utilities have help documentation. For basic information on RAID and how to use the LSI utilities, see the following documentation:

- LSI MegaRAID SAS Software User’s Guide (for LSI MegaRAID)
- LSI Fusion-MPT Device Management User’s Guide (for LSI 3081E)
- LSI SAS2 Integrated RAID Solution User Guide (for LSI SAS1064E)

Moving a RAID Cluster Using UCS Software Version 1.4(1)

You can set a server to recognize a RAID cluster created on another server. This procedure is useful when upgrading from the M1 version of a server to the M2 version of a server. You can also use this procedure whenever data on a RAID cluster needs to be moved between servers.

Note Both the old and new servers for the cluster must be in the same LSI controller. For example, migration from a server with an LSI 1064E to a server with an LSI MegaRAID is not supported.

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 Put both the start and destination servers for the RAID cluster in the associated state.

Step 2 Shut down both servers.

Note When using this procedure during an M1 to M2 upgrade or a direct replacement within a slot, at this point in process the destination server is not yet associated and does not have a disk policy. When the destination server is inserted into the slot where the start server was located, the destination server inherits policies from the start server. The RAID controller and the PnuOS will read the disk and RAID volume details during the subsequent association (when PnuOS boots).

Step 3 After the servers power off, physically move the drives in the array to the destination server. If you are changing servers but keeping the drives in the same slots, insert the new server into the slot of the original server.

Step 4 Connect the KVM dongle.

Step 5 Connect a monitor, keyboard, and mouse to the destination server.

Step 6 Boot the destination 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 57.)

Step 7 Wait for the LSI Configuration Utility banner.

Step 8 To enter the LSI Configuration Utility, press Ctrl-C.

Step 9 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 57.

Step 10 Choose **RAID Properties**.
The **View Array** screen appears.

Step 11 Choose **Manage Array**.
The **Manage Array** screen appears.

Step 12 Choose **Activate Array**.
When the activation is complete, the RAID status changes to Optimal.

Step 13 On the **Manage Array** screen, choose **Synchronize Array**.

Step 14 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 15 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 16 Choose the reboot option to implement the changes.

Moving a RAID Cluster Using UCS Software Version 1.4(2) and Forward

You can set a server to recognize a RAID array created on another server. This procedure is useful when upgrading from the M1 version of a server to the M2 version of a server. You can also use this procedure whenever data on a RAID array needs to be moved between servers.

Note Both the old and new servers for the cluster must be in the same LSI controller family. For example, migration between a server with an LSI 1064 to a server with an LSI MegaRAID is not supported.

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 Decommission both the source and destination servers from UCS Manager.

Step 2 Wait for the servers to shut down (Decommission Server prompts you to shut down the server).

Note When you use this procedure during an M1 to M2 upgrade or a direct replacement within a slot, at this point in the process the destination server is not yet associated and does not have a disk policy. When the destination server is inserted into the slot where the start server was located, the destination server inherits policies from the start server. The RAID controller and the PnuOS will read the disk and RAID volume details during the subsequent association (when PnuOS boots).

Step 3 After the servers power off, physically move the drives in the array to the destination server.
If you are changing servers but keeping the drives in the same slots, insert the new server into the slot of the original server.

Step 4 Power on the servers by pressing the front power button of each of the servers.

Step 5 Choose **Reacknowledge Slot** for each of the slots (Source and Destination). If UCS Manager prompts you to `Resolve Slot Issue`, then choose the **here** link in the **Resolve Slot** screen and resolve the slot issue before server discovery begins.

Step 6 Wait for server discovery and association to complete for each server.
If each of the preceding steps runs without issues, the servers boot up with the OS that was installed on the respective RAID volumes prior to the RAID Cluster Migration.

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 Connect the KVM dongle to the server with the failed drive.

Step 2 Connect a monitor, keyboard, and mouse to the destination server.

Step 3 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 4 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 57.)

Step 5 Wait for the LSI Configuration Utility banner.

Step 6 To enter the LSI Configuration Utility, press Ctrl-C.

Step 7 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 57.

Step 8 Choose **RAID Properties**.
The **View Array** screen appears.

Step 9 Choose **Manage Array**.
The **Manage Array** screen appears.

Step 10 Choose **Activate Array**.
When the activation is complete, the RAID status changes to Optimal.

Step 11 On the **Manage Array** screen, choose **Synchronize Array**.

Step 12 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 13 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 14 Choose the reboot option to implement the changes.

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
Cisco UCS B440	All except 82598KR-CI	M72KR-Q or -E + M81KR

Known Adapter Issues

There are a number of known issues and open bugs with adapters. These problems are called out in the Release Notes. The release notes are accessible through the Cisco UCS B-Series Servers Documentation Roadmap.

Specifically, the bugs CSCtd32884 and CSC71310 track a persistent known condition in which the type of the adapter in a server affects the maximum transmission unit (MTU) supported. The network MTU that is above the maximum can cause the packet to be dropped for the following adapters:

- The Cisco UCS CNA M71KR adapter supports an MTU of 9216.
- The Cisco UCS 82598KR-CI adapter supports an MTU of 14000.

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. See Diagnostics Button and LEDs, on page 45.

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**]	

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 #
```

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.

Recommended Solutions for Adapter Issues

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

Table 7: 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 20.

Related B-Series Server Documentation

Individual server models are documented in the Cisco UCS Blade Server Installation and Service Notes.

INDEX