General Troubleshooting Solutions

This chapter includes the following sections:

Guidelines for Troubleshooting

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

Table 1: Troubleshooting Guidelines

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

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

Faults

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

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

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

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

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

Fault Severities

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

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

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

Fault States

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

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

Fault Types

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

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

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

Fault Properties

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

Property Name	Description
Severity	Current severity level of the fault, which can be any of the severities described in Fault Severities, on page 2 .
Last Transition	Day and time on which the severity for the fault last changed. If the severity has not changed since the fault was raised, this property displays the original creation date.
Affected Object	Component that is affected by the condition that raised the fault.
Description	Description of the fault.

Property Name	Description
ID	The unique identifier associated with the message.
Type	Type of fault that has been raised, which can be any of the types described in Fault Types, on page 3 .
Cause	Unique identifier associated with the condition that caused the fault.
Created at	Day and time when the fault occurred.
Code	The unique identifier assigned to the fault.
Number of Occurrences	Number of times the event that raised the fault occurred.
Original Severity	Severity assigned to the fault the first time it occurred.
Previous Severity	Previous severity level. This property is only used if the severity of a fault changes during its lifecycle.
Highest Severity	Highest severity encountered for this issue.

Lifecycle of Faults

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

A fault has the following lifecycle:

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

Faults in Cisco UCS Manager GUI

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

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

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

Faults in Cisco UCS Manager CLI

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

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

Fault Collection Policy

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

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

Events

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

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

Properties of Events

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

Table 2: Event Properties

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

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

Events in the Cisco UCS Manager GUI

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

Events in the Cisco UCS Manager CLI

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

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

Audit Log

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

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

Audit Log Entry Properties

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

Table 3: Audit Log Entry Properties

Property Name	Description
ID	Unique identifier associated with the audit log message.
Affected Object	Component affected by the user action.
Severity	Current severity level of the user action associated with the audit log message. These severities are also used for the faults, as described Fault Severities, on page 2.
Trigger	User role associated with the user that raised the message.
User	Type of user that created the event, as follows: • admin • internal • blank
Indication	Action indicated by the audit log message, which can be one of the following: • creation—A component was added to the system. • modification—An existing component was changed.
Description	Description of the user action.

Audit Log in the Cisco UCS Manager GUI

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

Audit Log in the Cisco UCS Manager CLI

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

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

System Event Log

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

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

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

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

SEL File

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

SEL Policy

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

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

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

Syslog

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

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

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

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

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

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

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

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

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

Syslog Entry Format

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

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

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

Syslog Entry Severities

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

Table 4: Syslog Entry Severities in Cisco UCS

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

Syslog Entry Parameters

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

Table 5: Syslog Message Content

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

Syslog Services

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

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

Technical Support Files

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

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

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

Creating a Tech Support File in the Cisco UCS Manager GUI

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

Procedure

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

Step 2 Expand **All**.

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

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

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

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

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

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

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

Step 6 Click **OK**.

Creating a Technical Support File in the Cisco UCS Manager CLI

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt** {**a** | **b**}	Enters local management mode.
Step 2	UCS-A(local-mgmt) # **show tech-support** {**chassis** *chassis-id* {**all** | **cimc** *slot* [**adapter** *adapter-id*] | **iom** *iom-id*} | **fex** *fex-id* | **server** *server-id* [**adapter** *adapter-id*] | **server-memory** {*server-list* | **all**} | **ucsm** | **ucsm-mgmt**} [**brief** | **detail**]	Outputs information about the selected objects in a file that you can send to Cisco Technical Assistance Center. The following options are available: • **chassis**—Creates file containing technical support data for either the CIMCs or I/O modules in a given chassis. • **fex**—Creates a file containing technical support data for a fabric extender. • **server**—Creates a file containing technical support data for a C-Series server. • **server-memory**—Creates a technical support file with all server memory related information. You can run the **server-memory** command for the following: • One blade server or rack-mount server • Multiple blade servers • Multiple rack-mount servers • A mix of blade and rack-mount servers • All servers **Important** Multiple servers specified in the *server-list* must be separated by commas. You cannot run this command for a range of servers. If you use the **server-memory** option with the **detail** option, detailed information about the memory is saved into a file and the file name and path are displayed.

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

Powering Down a Cisco UCS Domain

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

Procedure

Step 1 Create a configuration backup.

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

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

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

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

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

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

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

Verification of LDAP Configurations

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

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

Verifying the LDAP Provider Configuration

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

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

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

Procedure

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

Example

The following is an example of the response:

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

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

Verifying the LDAP Provider Group Configuration

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

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

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

Procedure

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

Example

The following is an example of the response:

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