Call Home Faults

- About Call Home Messages, on page 1
- Cisco UCS Faults that Raise Call Home Alerts, on page 1
- Cisco UCS Faults and Call Home Priority Levels, on page 13

About Call Home Messages

When you configure Call Home to send messages, Cisco UCS Manager executes the appropriate command line interface (CLI) show command and attaches the command output to the message.

Cisco UCS delivers Call Home messages in the following formats:

- The short text format—A one- or two-line description of the fault that is suitable for pagers or printed reports.
- Full text format—Fully formatted message with detailed information that is suitable for human reading.
- XML machine readable format—Uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). The AML XSD is published on the Cisco.com website at https://www.cisco.com/. The XML format enables communication with the Cisco Systems Technical Assistance Center.

Cisco UCS Faults that Raise Call Home Alerts

If Smart Call Home is configured in the Cisco UCS instance, every fault listed in this section raises a Smart Call Home event to the Cisco Smart Call Home system.

Note All Cisco UCS Manager faults that raise Call Home alerts are documented in “Cisco UCS Faults” The type of Call Home alert is included in the CallHome line of the Fault Details section for each fault.

You can also find additional information about Call Home faults in the Unified Computing System (UCS) section of Monitoring Details for Cisco SMARTnet Service with Smart Call Home.

Faults Raised by a Fabric Interconnect

Diagnostic Faults Raised by a Fabric Interconnect

TestFabricPort

Details

Severity: Major

Customer Notification: Yes

Service Request: Yes, if ports_failed > 25%

Cisco UCS Manager CLI: show diagnostic result module all

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs because one or more of the ports have failed this diagnostic test either during the Power-On-Self-Test or during the run time monitoring. As a result, the Cisco UCS Manager shuts down the affected ports. The network connectivity to the devices connected on the failed ports is affected.

Recommended Action

If you see this fault, take the following actions:

1. If the failed port or ports are located in an expansion module, remove and re-insert the module.

   Follow the instructions outlined in the hardware installation guide for the fabric interconnect on how to insert the modules.
2. Remove and re-insert the SFP or SFP+ and ensure the SFP or SFP+ is seated properly.
3. Insert the suspected faulty SFP or SFP+ into a working port. If the working port becomes faulty, then the SFP or SFP+ is faulty. Consider replacing the faulty SFP or SFP+.
4. If the SFP or SFP+ is working, then the module hardware is faulty.
   a. a. If the fixed module is affected, consider replacing the fabric interconnect.
   b. b. If an expansion module is affected, consider replacing the faulty module.

   Schedule a downtime for the Cisco UCS instance to replace the hardware.

TestForwardingEngine

Details

Severity: Major

Customer Notification: Yes

Service Request: Yes, if ports_failed > 25%

Cisco UCS Manager CLI: show diagnostic result module all

Call Home Support: 3.0, 3.1

Explanation

One or more ports have failed this diagnostic test either during the Power-On-Self-Test or during the run time monitoring. As a result, the Cisco UCS Manager shuts down the affected ports. The network connectivity to the devices connected on the failed ports is affected.

Recommended Action

If you see this fault, take the following actions:

1. If the failed port or ports are located in an expansion module, remove and re-insert the module.

   Follow the instructions outlined in the hardware installation guide for the fabric interconnect on how to insert the modules.

2. Remove and re-insert the SFP or SFP+ and ensure the SFP or SFP+ is seated properly.
3. Insert the suspected faulty SFP or SFP+ into a working port. If the working port becomes faulty, then the SFP or SFP+ is faulty. Consider replacing the faulty SFP or SFP+.
4. If the SFP or SFP+ is working, then the module hardware is faulty.
   a. If the fixed module is affected, consider replacing the fabric interconnect.
   b. If an expansion module is affected, consider replacing the faulty module.

   Schedule a downtime for the Cisco UCS instance to replace the hardware.

TestForwardingEnginePort

Details

Severity: Major

Customer Notification: Yes

Service Request: Yes, if ports_failed > 25%

Cisco UCS Manager CLI: show diagnostic result module all

Call Home Support: 3.0, 3.1

Explanation

One or more ports have failed this diagnostic test either during the Power-On-Self-Test or during the run time monitoring. As a result, the Cisco UCS Manager shuts down the affected ports. the network connectivity to the devices connected on the failed ports is affected.

Recommended Action

If you see this fault, take the following actions:

1. If the failed port or ports are located in an expansion module, remove and re-insert the module.

   Follow the instructions outlined in the hardware installation guide for the fabric interconnect on how to insert the modules.

2. Remove and re-insert the SFP or SFP+ and ensure the SFP or SFP+ is seated properly.
3. Insert the suspected faulty SFP or SFP+ into a working port. If the working port becomes faulty, then the SFP or SFP+ is faulty. Consider replacing the faulty SFP or SFP+.
4. If the SFP or SFP+ is working, then the module hardware is faulty.
   a. If the fixed module is affected, consider replacing the fabric interconnect.

b. If an expansion module is affected, consider replacing the faulty module.

Schedule a downtime for the Cisco UCS instance to replace the hardware.

TestFrontPort

Details

Severity: Major

Customer Notification: Yes

Service Request: Yes, if ports_failed > 25%

Cisco UCS Manager CLI: show diagnostic result module all

Call Home Support: 3.0, 3.1

Explanation

One or more ports have failed this diagnostic test either during the Power-On-Self-Test or during the run time monitoring. As a result, the Cisco UCS Manager shuts down the affected ports. The network connectivity to the devices connected on the failed ports is affected.

Recommended Action

If you see this fault, take the following actions:

1. Move the devices connected on the affected ports to other functional ports of the fabric interconnect or to another fabric interconnect.
2. If the failed port or ports are located in an expansion module, do the following:
   a. Remove and re-insert the module.

      Follow the instructions outlined in the hardware installation guide for the fabric interconnect on how to insert the modules.

   b. If the problem persists and if all of the ports are required to be functional on the fabric interconnect, schedule a downtime and replace the expansion module.
3. If the failed port or ports are located in the fixed module and all ports are required to be functional on the fabric interconnect, schedule a downtime and replace the fabric interconnect.

TestInbandPort

Details

Severity: Major

Customer Notification: Yes

Service Request: Yes

Cisco UCS Manager CLI: show diagnostic result module all

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs because the inband connectivity to the fabric interconnect is experiencing a failure. The fabric interconnect uses inband connectivity for the control plane protocols to connect to

peers such as servers, LAN switches, and SAN switches. Examples of these control plane protocols include DCX, STP, LACP, and FSPF. If a fabric interconnect cannot run the appropriate control plane protocols, it can no longer function and the Cisco UCS Manager shuts down all of the ports on the fabric interconnect to avoid topology problems.

Recommended Action

If you see this fault, schedule a downtime and replace the fabric interconnect.

TestFabricEngine

Details

Severity: Major

Customer Notification: Yes

Service Request: Yes

Cisco UCS Manager CLI: show diagnostic result module all

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs because the fabric ASIC has reported a major failure. Connectivity among all of the ports depends upon the fabric ASIC. Therefore, the Cisco UCS Manager shuts down all ports on the fabric interconnect.

Recommended Action

If you see this fault, schedule a downtime and replace the fabric interconnect.

TestSPROM

Details

Severity: Major

Customer Notification: Yes

Service Request: Yes

Cisco UCS Manager CLI: show diagnostic result module all

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs when the Cisco UCS Manager cannot bring the affected module online because the module type is unidentified. For the expansion modules, the Cisco UCS Manager determines the module type from information stored in the module SPROM. If you see this error, the checksum calculation for the SPROM content has most likely failed.

This fault can only occur on the expansion modules. It cannot occur on the fixed module.

Recommended Action

If you see this fault, take the following actions:

1. Move the devices connected on the affected ports to other functional ports of the fabric interconnect or to another fabric interconnect:
2. Remove and re-insert the module to ensure that all pins are in good contact with the backplane.

Follow the instructions outlined in the hardware installation guide for the fabric interconnect on how to insert the modules.

3. If the problem persists after multiple re-insertions, schedule a downtime and replace the faulty module.

TestOBFL

Details

Severity: Minor

Customer Notification: Yes

Service Request: Yes

Cisco UCS Manager CLI: show diagnostic result module all

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs because the onboard fault logging (OBFL) flash has failed. The Cisco UCS Manager logs hardware failure messages to this flash component. That logging function is lost. However, other logs, such as the syslog, are not affected and can continue to work normally.

This fault does not affect the normal operation of the fabric interconnect. The fault can only occur on the fixed module. It cannot occur on the expansion modules.

Recommended Action

Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. Also refer to the *Release Notes for Cisco UCS Manager and the Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the **show tech-support** command and contact Cisco Technical Support.

TestLED

Details

Severity: Minor

Customer Notification: Yes

Service Request: No

Cisco UCS Manager CLI: show diagnostic result module all

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs when the Cisco UCS Manager cannot access the LED controls on a module. However, because the LED control uses the same transport mechanism that controls other key components on a module, this fault can indicate other failures. This fault can be caused by a bent pin on the module or fabric interconnect.

This fault can only occur on the expansion modules. It cannot occur on the fixed module.

Recommended Action

If you see this fault, take the following actions:

1. Move the devices connected on the affected ports to other functional ports of the fabric interconnect or to another fabric interconnect:

2. Remove and re-insert the module to ensure that all pins are in good contact with the backplane.

   Follow the instructions outlined in the hardware installation guide for the fabric interconnect on how to insert the modules.

3. If this failure continues after re-insertion, insert this module into a known good fabric interconnect to determine whether the same failure occurs.

4. If the problem persists, schedule a downtime and replace the faulty module.

Environmental Faults Raised by a Fabric Interconnect

Temperature Alarm

Details

Severity: Major

Customer Notification: Yes

Service Request: No

Cisco UCS Manager CLI: show environment

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs because the temperature sensor reports that the affected chassis has exceeded the major or minor threshold value and is at a dangerously high temperature. If the operating temperature is not reduced, the system shuts down the affected chassis to avoid causing permanent damage. The chassis is powered back on after the temperature returns to a reasonable level.

Each chassis needs at least seven functional fans to maintain operating temperature.

Recommended Action

If you see this fault, take the following actions:

1. If the fault report includes **fan_failure_found**, do the following:

   a. In either the Cisco UCS Manager CLI or the Cisco UCS Manager GUI, check the status of the affected fan to determine whether the temperature-related alarm is due to the failure of a fan.

   b. Ensure that a minimum of seven fans are installed in the chassis and are functioning properly.

   c. Check the fan-related syslog messages to see the exact reason for the failure. For example, the fan may have become non-operational.

   d. Replace the faulty fan to resolve the issue.

2. If the fault report includes **temp_current >= maj_threshold or temp_current =< min_threshold**, do the following:

   a. In either the Cisco UCS Manager CLI or the Cisco UCS Manager GUI, view the acceptable temperature and voltage parameters and determine how much of the outlet or inlet temperature has reached or exceeded over the major or minor threshold value.

   b. Verify the following to ensure that the site where the chassis is installed meets the site guidelines:

      - The area is dry, clean, well-ventilated and air-conditioned.

- The air conditioner is working correctly and maintains an ambient temperature of 0 to 40 degrees C.
- The chassis is installed in an open rack whenever possible. If the installation on an enclosed rack is unavoidable, ensure that the rack has adequate ventilation.
- The ambient airflow is unblocked to ensure normal operation. If the airflow is blocked or restricted, or if the intake air is too warm, an over temperature condition can occur.
- The clearance around the ventilation openings of the chassis are at least 6 inches (15.24 cm).
- The chassis is not in an overly congested rack or is not directly next to another equipment rack. Heat exhaust from other equipment can enter the inlet air vents and cause an over temperature condition.
- The equipment near the bottom of a rack is not generating excessive heat that is drawn upward and into the intake ports of the chassis. The warm air can cause an over temperature condition.
- The cables from other equipment does not obstruct the airflow through the chassis or impair access to the power supplies or the cards. Route the cables away from any field-replaceable components to avoid disconnecting cables unnecessarily for equipment maintenance or upgrades.

PowerSupplyFailure

Details

Severity: Major

Customer Notification: Yes

Service Request: Yes

Cisco UCS Manager CLI: show environment

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs because a failure was recorded in the affected power supply unit and the affected component is working with only one power supply unit.

Recommended Action

If you see this fault, take the following actions:

1. Check the power supply unit that has the problem, as follow:
   - In the Cisco UCS Manager CLI, execute the show environment power command
   - In the Cisco UCS Manager GUI, view the PSUs tab of the Chassis node on the Equipment tab.
2. Verify that the power cord is properly connected to the power supply and to the power source.
3. Ensure that the fabric interconnect is supplied with 220V (this is the only supported power supply configuration).
4. Ensure that the power supply is properly inserted and plugged in.

5. If problem persists, remove and re-insert the power-supply unit.
6. If the power supply light is still not green and the status continues to show fail or shutdown, replace the faulty power supply unit.

TEMPERATURE_ALARM --- Sensor

Details

Severity: Major

Customer Notification: Yes

Service Request: Yes

Cisco UCS Manager CLI: show environment

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs because the Cisco UCS Manager cannot access a temperature sensor. As a result, the Cisco UCS Manager cannot monitor or regulate the temperature for the affected component. The affected temperature sensor could be for a chassis, power supply, or module.

Recommended Action

If you see this fault, take the following actions:

1. View the logs to determine the set of sensors that has failed, as follow:
   - In the Cisco UCS Manager CLI, execute the show logging command
   - In the Cisco UCS Manager GUI, view the logs under the Faults, Events, and Audit Log node on the Admin tab.
2. If the failed sensors are on an expansion module or a power supply, do the following:
   a. Remove and re-insert the power supply or module.

      Follow the instructions outlined in the hardware installation guide for the fabric interconnect on how to insert the modules.

   b. If the failure continues to persist after multiple re-insertions, replace the faulty power supply unit or the module.
3. If the failed sensors are on the fixed module, replace the fabric interconnect as it can no longer regulate and monitor the chassis temperature.

TestFAN -- fan speed speed out of range >= expected. speed rpm

Details

Severity: Major

Customer Notification: Yes

Service Request: No

Cisco UCS Manager CLI: show environment

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs because the Cisco UCS Manager has detected a fan that is running at a speed that is too slow or too fast. A malfunctioning fan can affect the operating temperature of the chassis.

Recommended Action

If you see this fault, take the following actions:

1. If the fan is running below the expected speed, ensure that the fan blades are not blocked.
2. If the fan is running above the expected speed, remove and re-insert the fan.

Multiple fans missing or failed

Details

Severity: Major

Customer Notification: Yes

Service Request: No

Cisco UCS Manager CLI: show environment

Explanation

This fault typically occurs because the Cisco UCS Manager has detected multiple fan failures. The malfunctioning fans can result in high operating temperatures, affect performance, and cause the Cisco UCS Manager to shut down the affected component.

Recommended Action

If you see this fault, take the following actions:

1. If the chassis fans have failed, do the following:
   a. Check the fan status.
   b. Ensure that at least seven fans are installed and functioning properly.
   c. Check the fan-related syslog messages to see the exact reason for the failure. The fans may have become non-operational.
   d. Replace the faulty fans to resolve the issue.
2. If the power supply fans have failed and the power supply is operational, do the following:
   a. Check the fan status.
   b. Remove and re-insert the power supply and verify whether the fan is operational.
   c. If the problem persists, replace the power-supply.

One fan missing or failed

Details

Severity: Minor

Customer Notification: Yes

Service Request: No

Cisco UCS Manager CLI: show environment

Call Home Support: 3.0, 3.1

Explanation

This fault typically occurs because the Cisco UCS Manager has determined that a single fan is missing or has failed. A single missing or malfunctioning fan does not affect performance. A minimum of seven fans are required for a chassis to be operational.

Recommended Action

If you see this fault, take the following actions:

1. If the chassis fans have failed, do the following:
   a. Check the fan status.
   b. Ensure that at least seven fans are installed and functioning properly.
   c. Check the fan-related syslog messages to see the exact reason for the failure. The fan may have become non-operational.
   d. Replace the faulty fan to resolve the issue.
2. If the power supply fans have failed and the power supply is operational, do the following:
   a. Check the fan status.
   b. Remove and re-insert the power supply and verify whether the fan is operational.
   c. If the problem persists, replace the power-supply.

Faults Raised by Syslog

No license installed for feature, is on grace license, will expire in DD HH

Details

Severity: Major

Customer Notification: Yes

Service Request: No

Cisco UCS Manager CLI: show logging

Call Home Support: 3.0, 3.1

Explanation

The evaluation license installed for the affected feature is running under a grace period. The grace period expires on the date shown in the log at which time the Cisco UCS Manager disables the feature. To obtain more details, follow the instructions in the licensing chapter of the *Cisco UCS Manager CLI Configuration Guide* or the *Cisco UCS Manager GUI Configuration Guide*.

The impact on performance depends upon whether the affected feature is implemented.

Recommended Action

If you see this fault, obtain a permanent license for the affected feature through one of the following channels:

- Contact your local Cisco sales representative.
- Use the ordering tool at https://www.cisco.com/c/en/us/buy.html.

License for feature, will expire in HH MM

Details

Severity: Major

Customer Notification: Yes

Service Request: No

Cisco UCS Manager CLI: show logging

Call Home Support: 3.0, 3.1

Explanation

The evaluation license installed for the affected feature expires within the number of hours and minutes listed in the alert. When that period expires, the Cisco UCS Manager disables the feature. To obtain more details, follow the instructions in the licensing chapter of the *Cisco UCS Manager CLI Configuration Guide* or the *Cisco UCS Manager GUI Configuration Guide*.

Recommended Action

If you see this fault, obtain a permanent license for the affected feature through one of the following channels:

- Contact your local Cisco sales representative.
- Use the ordering tool at https://www.cisco.com/c/en/us/buy.html.

License has expired for feature

Details

Severity: Major

Customer Notification: Yes

Service Request: No

Cisco UCS Manager CLI: show logging

Call Home Support: 3.0, 3.1

Explanation

The evaluation license installed for the affected feature has expired, and the Cisco UCS Manager has disabled the feature. To obtain more details, follow the instructions in the licensing chapter of the *Cisco UCS Manager CLI Configuration Guide* or the *Cisco UCS Manager GUI Configuration Guide*.

Recommended Action

If you see this fault, obtain a permanent license for the affected feature through one of the following channels:

- Contact your local Cisco sales representative.

- Use the ordering tool at https://www.cisco.com/c/en/us/buy.html.

License file is missing for feature

Details

Severity: Major

Customer Notification: Yes

Service Request: No

Cisco UCS Manager CLI: show logging

Call Home Support: 3.0, 3.1

Explanation

The previously installed license for the affected feature is missing from the fabric interconnect configuration storage, and the Cisco UCS Manager has disabled the feature. This issue can occur in rare circumstances such as flash corruption. To obtain more details, follow the instructions in the licensing chapter of the *Cisco UCS Manager CLI Configuration Guide* or the *Cisco UCS Manager GUI Configuration Guide*.

Recommended Action

If you see this fault, re-install the license from the license backup.

Cisco UCS Faults and Call Home Priority Levels

Because Call Home is present across several Cisco product lines, Call Home has developed its own standardized priority levels. The following table describes how the underlying Cisco UCS fault levels map to the Call Home priority levels.

Table 1: Mapping of Cisco UCS Faults and Call Home Priority Levels

dsfdsUCS Fault	Call Home Priority	SCH Priority
—	(9) Catastrophic	—
—	(8) Disaster	—
—	(7) Fatal	—
(6) Critical	(6) Critical	Major
(5) Major	(5) Major	Major
(4) Minor	(4) Minor	Minor
(3) Warning	(3) Warning	Minor
—	(2) Notification	Minor
(1) Info	(1) Normal	Minor

When Call Home information is communicated in an e-mail format, the priority levels and faults appear in the following places.

- The SCH priority is communicated in the e-mail subject line.
- The Call Home priority is communicated as a “Severity Level:” header to the e-mail message.
- The UCS fault information is attached in the body of the e-mail.
- The UCS fault severity is identified within the attachment as “severity=”.