Introduction to UCS Faults

Overview of Faults

About Faults in the Cisco UCS

In the Cisco UCS, a fault is a mutable object that is managed by the Cisco UCS Manager. Each fault represents a failure in the Cisco UCS instance 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, then the object transitions to a functional state.

A fault remains in the 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 the Cisco UCS instance 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 instance collects and retains faults.

Note All Cisco UCS faults can be trapped by SNMP.

Fault Severity

A fault raised in a Cisco UCS instance can transition through more than one severity during its lifecycle. Table describes the possible fault severity in alphabetical order.

Table 1: Fault Severities in Cisco UCS

Severity	Description
Cleared	A notification that the condition that caused the fault has been resolved, and the fault has been cleared.

Severity	Description
Condition	An informational message about a condition, possibly independently insignificant.
Critical	A 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.
Info	A basic notification or informational message, possibly independently insignificant.
Major	A 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	A non-service-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 currently degrading the capacity of the managed object.
Warning	A potential or impending service-affecting fault that currently has no significant effects in the system. Action should be taken to further diagnose, if necessary, and correct the problem to prevent it from becoming a more serious service-affecting fault.

Fault Types

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

Table 2: Types of Faults in Cisco UCS

fsm	An FSM task has failed to complete successfully, or the Cisco UCS Manager is retrying one of the stages of the FSM.
equipment	The Cisco UCS Manager has detected that a physical component is inoperable or has another functional issue.
server	The Cisco UCS Manager is unable to complete a server task, such as associating a service profile with a server.
configuration	The Cisco UCS Manager is unable to successfully configure a component.

environment	The Cisco UCS Manager has detected a power problem, thermal problem, voltage problem, or a loss of CMOS settings.
management	The Cisco UCS Manager has detected a serious management issue, such as one of the following: • Critical services could not be started. • The primary switch could not be identified. • Components in the instance include incompatible firmware versions.
connectivity	The Cisco UCS Manager has detected a connectivity problem, such as an unreachable adapter.
network	The 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.

Properties of Faults

The Cisco UCS Managerprovides detailed information about each fault raised in a Cisco UCS instance. The table describes the fault properties that can be viewed in the Cisco UCS Manager CLI or the Cisco UCS Manager GUI.

Table 3:

Property Name	Description
Severity	The current severity level of the fault. This can be any of the severity described in Table 1: Fault Severities in Cisco UCS, on page 1.
Last Transition	The 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	The component that is affected by the condition that raised the fault.
Description	The description of the fault.
ID	The unique identifier assigned to the fault.
Status	Additional information about the fault state. This can be any of the states described in Table 4: Fault Lifecycle States, on page 5.

Property Name	Description
Type	The type of fault that has been raised. This can be any of the types described in Table 2: Types of Faults in Cisco UCS, on page 2.
Cause	The unique identifier associated with the condition that caused the fault.
Created at	The day and time when the fault occurred.
Code	The unique identifier assigned to the fault.
Number of Occurrences	The number of times the event that raised the fault occurred.
Original Severity	The severity assigned to the fault on the first time that it occurred.
Previous Severity	If the severity has changed, this is the previous severity.
Highest Severity	The highest severity encountered for this issue.

Lifecycle of Faults

The faults in Cisco UCS are stateful, and a fault raised in a Cisco UCS instance transitions through more than one state during its lifecycle. In addition, only one instance of a given fault can exist on each object. If the same fault occurs a second time, the Cisco UCS increases the number of occurrences by one.

A fault has the following lifecycle:

1. A condition occurs in the system and the Cisco UCS raises a fault in the active state.
2. If the fault is alleviated within a short period of time know as the flap interval, the fault severity remains at its original active value but the fault enters the soaking state. The soaking state indicates that the condition that raised the fault has cleared, but the system is waiting to see whether the fault condition reoccurs.
3. If the condition reoccurs during the flap interval, the fault enters the flapping state. Flapping occurs when a fault is raised and cleared several times in rapid succession. If the condition does not reoccur during the flap interval, the fault is cleared.
4. Once cleared, the 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 that the fault is not 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. When a fault is active, the additional lifecycle state information listed in Table 1-4 may be provided in the Status field of the fault notification.

Table 4: Fault Lifecycle States

State	Description
Soaking	A fault was raised and then cleared within a short time known as the flap interval. Since this may be a flapping condition, the fault severity remains at its original active value, but this state indicates that the condition that raised the fault has cleared. If the fault does not reoccur, the fault moves into the cleared state. Otherwise, the fault moves into the flapping state.
Flapping	A fault was raised, cleared, and then raised again within a short time known as the flap interval.

Fault Collection Policy

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

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

Faults in Cisco UCS Manager

Faults in Cisco UCS Manager GUI

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

In addition, a summary of all faults can be viewed in a Cisco UCS instance. Go to 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 instance.

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. When 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, at the top-level scope, enter the **show fault** command. If you want to view faults for a specific object, scope to that object and then enter the **show fault** command.

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

Fault Suppression

Fault suppression allows you to suppress SNMP trap and Call Home notifications during a planned maintenance time. You can create a fault suppression task to prevent notifications from being sent whenever a transient fault is raised or cleared.

Faults remain suppressed until the time duration has expired, or the fault suppression tasks have been manually stopped by the user. After the fault suppression has ended, Cisco UCS Manager will send notifications for any outstanding suppressed faults that have not been cleared. *Cisco UCS Manager GUI System Monitoring Guide, Release 2.2* and *Cisco UCS Manager CLI System Monitoring Guide, Release 2.2* provide detailed information about fault suppression.

Syslog Message Example and Format

The following string is an example of a typical Cisco UCS Manager syslog message:

```
Apr 19 17:11:12 UTC: %UCSM-6-LOG_CAPACITY:
[F0461][info][log-capacity][sys/chassis-1/blade-7/mgmt/log-SEL-0] Log
capacity on Management Controller on server 1/7 is very-low
```

The following table lists the Syslog message parts and provides the definition of each part:

Syslog Message	Message Part	Definition
Apr 19 17:11:12 UTC	Date and Time	Provides the date and the time, in UTC format, and indicates when the event or fault occurred.
%UCSM	Facility	Refers to the message source. The message source is usually a hardware device, a protocol, or a module of the system software. **Note** Facility is Cisco-specific and is only relevant within the message string. It is different from facility as defined in RFC 3164 for the syslog protocol. For messages originating from Cisco UCS Manager, the facility will always be %UCSM.
6	Severity	Refers to the syslog severity code.
LOG_CAPACITY	Mnemonic	A device-specific code that uniquely identifies the message, and maps to a fault type in Cisco UCS Manager.

Syslog Message	Message Part	Definition
[F0461]	ID	A unique identifier assigned to the fault.
[info]	UCSM Severity	In this example, a basic notification or informational message, possibly independently insignificant.
[log-capacity]	Mnemonic	A device-specific code that uniquely identifies the message and maps to the fault type in Cisco UCS Manager.
[sys/chassis-1/blade-7/mgmt/log-SEL-0]	System	The specific Cisco UCS device in which the fault occurred.
Log capacity on Management Controller on server 1/7 is very-low	Description	A brief description of the fault.

Syslog Messages for Cisco UCS Manager Faults

A fault is an abnormal condition or defect at the component, equipment, or subsystem level which may lead to a failure. Faults are categorized by their severity, and the message part of the syslog entry contains text that lets you see the criticality of the fault. Faults can also be managed using SNMP. For more information about managing faults using SNMP, refer the http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html.

The following are a few examples of syslog messages generated for fault events:

- 2011 Apr 19 17:11:12 UTC: %UCSM-6-LOG_CAPACITY: [F0461][info][log-capacity][sys/chassis-1/blade-7/mgmt/log-SEL-0] Log capacity on Management Controller on server 1/7 is very-low
- 2011 Apr 20 14:33:14 UTC: %UCSM-3-CONFIGURATION_FAILURE: [F0327][major][configuration-failure][org-root/ls-test] Service profile test configuration failed due to insufficient-resources,mac-address-assignment,system-uuid-as
- 2011 Apr 20 20:50:25 UTC: %UCSM-3-THERMAL_PROBLEM: [F0382][major][thermal-problem][sys/chassis-1/fan-module-1-1] Fan module 1/1-1 temperature: lower-critical
- 2011 Apr 20 14:33:14 UTC: %UCSM-5-UNASSOCIATED: [F0334][warning][unassociated][org-root/ls-test] Service profile test is not associated

Syslog Messages for Cisco UCS Manager Events

Event messages are generated when an FSM transitions from one state to another. Event messages notify you of the transitions of all FSMs, and may contain information about a specific user when a user invokes a process that updates the state of an FSM.

Note All FSM event messages are delivered with the info security level in syslog.

The following are a few examples of syslog messages generated by system events:

- 2011 Apr 22 16:53:18 UTC: %UCSM-6-EVENT: [E4195931][456249][transition][ucs-username\username][] [FSM:BEGIN]: Hard-reset server sys/chassis-1/blade-7(FSM:sam:dme:ComputePhysicalHardreset)
- 2011 Apr 22 16:53:18 UTC: %UCSM-6-EVENT: [E4195931][456250][transition][ucs-username\username][] [FSM:STAGE:END]:(FSM-STAGE:sam:dme:ComputePhysicalHardreset:begin)
- 2011 Apr 22 16:53:18 UTC: %UCSM-6-EVENT: [E4195932][456251][transition][ucs-username\username][] [FSM:STAGE:ASYNC]: Preparing to check hardware configuration server sys/chassis-1/blade-7(FSM-STAGE:sam:dme:ComputePhysicalHa
- 2011 Apr 22 16:53:23 UTC: %UCSM-6-EVENT: [E4195932][456252][transition][internal][] [FSM:STAGE:STALE-SUCCESS]: Preparing to check hardware configuration server sys/chassis-1/blade-7(FSM-STAGE:sam:dme:ComputePhysicalHardres
- 2011 Apr 22 16:53:23 UTC: %UCSM-6-EVENT: [E4195932][456253][transition][internal][] [FSM:STAGE:END]: Preparing to check hardware configuration server sys/chassis-1/blade-7(FSM-STAGE:sam:dme:ComputePhysicalHardreset:PreSani
- 2011 Apr 25 18:27:01 UTC: %UCSM-6-EVENT: [E4196181][535831][transition][internal][] [FSM:END]: Hard-reset server sys/chassis-1/blade-7(FSM:sam:dme:ComputePhysicalHardreset)

Syslog Messages for Cisco UCS Manager Audit Logs

An audit log entry describes an activity that takes place in the Cisco UCS Manager system. It identifies what took place, when it took place, where it took place (in what physical resource), and who was responsible. Audit log entries track actions that are initiated by system users.

Note All audit log messages are delivered with the info security level in syslog.

The following are a few examples of system audit log messages that are logged to syslog:

- 2011 May 15 10:19:14 UTC: %UCSM-6-AUDIT: [session][internal][creation][] Web B: remote user ibm logged in from 172.25.206.73
- 2011 Apr 22 16:53:18 UTC: %UCSM-6-AUDIT: [admin][ucs-username\username][modification][] server 1/7 power-cycle/reset action requested: hard-reset-immediate
- 2011 Apr 20 14:33:14 UTC: %UCSM-6-AUDIT: [admin][username][creation][] service profile test created
- 2011 Apr 20 14:33:14 UTC: %UCSM-6-AUDIT: [admin][username][creation][] service profile Power MO created
- 2011 Apr 20 14:33:14 UTC: %UCSM-6-AUDIT: [admin][username][creation][] Ether vnic eth1 created
- 2011 Apr 20 14:33:14 UTC: %UCSM-6-AUDIT: [admin][username][creation][] Ethernet interface created