Syslog

Syslog

Cisco UCS Manager generates system log, or syslog messages to record the following incidents that take place in the Cisco UCS Manager system:

- Routine system operations
- Failures and errors
- Critical and emergency conditions

There are three kinds of syslog entries: Fault, Event, and Audit.

Each syslog message identifies the Cisco UCS Manager process that generated the message and provides a brief description of the operation or error that occurred. The syslog is useful both in routine troubleshooting, incident handling, and management.

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.

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.

Cisco devices can send their log messages to a Unix-style syslog service. A syslog service simply accepts messages, then stores them in files or prints them according to a simple configuration file. This form of logging is the best available for Cisco devices because it can provide protected long-term storage of logs.

Configuring the Syslog Using Cisco UCS Manager GUI

Procedure

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

Step 2 Expand **All** > **Faults, Events, and Audit Log**.

Step 3 Click **Syslog**.

Step 4 In the **Global Settings**, choose to enable/disable **RFC 5424 Compliance**.

- **Enabled**—Syslog messages are displayed as per RFC 5424 format.
- **Disabled**—Syslog messages are displayed in the original format. By default, it is disabled.

Note This option is applicable only for Cisco UCS 6400 and 6500 series Fabric Interconnects.

Step 5 In the **Local Destinations** area, complete the following fields:

Name	Description
Console Section	
Admin State field	Indicate whether Cisco UCS displays Syslog messages on the console. This can be one of the following: • **Enabled**—Syslog messages are displayed on the console as well as added to the log. • **Disabled**—Syslog messages are added to the log but are not displayed on the console.
Level field	If this option is **enabled**, select the lowest message level that you want displayed. Cisco UCS displays that level, and above, on the console. This level can be one of the following: • **Emergencies** • **Alerts** • **Critical**
Monitor Section	

Name	Description
Admin State field	Indicate whether Cisco UCS displays Syslog messages on the monitor. This state can be one of the following: • **Enabled**—Syslog messages are displayed on the monitor as well as added to the log. • **Disabled**—Syslog messages are added to the log but not displayed on the monitor. If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.
Level drop-down list	If this option is **enabled**, select the lowest message level that you want displayed. The system displays that level, and above, on the monitor. This level can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
File Section	
Admin State field	Indicates whether Cisco UCS stores messages in a system log file on the fabric interconnect. This state can be one of the following: • **Enabled**—Messages are saved in the log file. • **Disabled**—Messages are not saved. If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.

Name	Description
Level drop-down list	Select the lowest message level that you want the system to store. Cisco UCS stores that level, and above, in a file on the fabric interconnect. This level can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
Name field	The name of the file in which the messages are logged. This name can be up to 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period). The default is name is **'messages'**.
Size field	The maximum size, in bytes, that the file can be before Cisco UCS Manager begins to write over the oldest messages with the newest ones. Enter an integer between 4096 and 4194304.

Step 6 In the **Remote Destinations** area, complete the following fields to configure up to three external logs that can store messages generated by the Cisco UCS components:

Name	Description
Admin State field	This can be one of the following: • **Enabled** • **Disabled** If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.

Name	Description
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level, and above, in the remote file. This level can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
Hostname field	The hostname or IP address on which the remote log file resides. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Facility drop-down list	This can be one of the following: • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

Step 7 In the **Local Sources** area, complete the following fields:

Name	Description
Faults Admin State field	If this field is **Enabled**, Cisco UCS logs all system faults.
Audits Admin State field	If this field is **Enabled**, Cisco UCS logs all audit log events.

Name	Description
Events Admin State field	If this field is **Enabled**, Cisco UCS logs all system events.

Step 8 Click **Save Changes**.