



Syslog

- [Syslog, on page 1](#)
- [Enabling Syslog Messages to Store In a Local File, on page 2](#)

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.

Enabling Syslog Messages to Store In a Local File

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # { enable disable } syslog console | Enables or disables the sending of syslogs to the console. |
| Step 3 | (Optional) UCS-A /monitoring # set syslog console level { emergencies alerts critical } | Select the lowest message level that you want displayed. If syslogs are enabled, the system displays that level and above on the console. The level options are listed in order of decreasing urgency. The default level is Critical. |
| Step 4 | UCS-A /monitoring # { enable disable } syslog monitor | Enables or disables the monitoring of syslog information by the operating system. |
| Step 5 | (Optional) UCS-A /monitoring # set syslog monitor level { emergencies alerts critical errors warnings notifications information debugging } | Select the lowest message level that you want displayed. If the monitor state is enabled, the system displays that level and above. The level options are listed in order of decreasing urgency. The default level is Critical. Note Messages at levels below Critical are displayed on the terminal monitor only if you have entered the terminal monitor command. |
| Step 6 | UCS-A /monitoring # { enable disable } syslog file | Enables or disables the writing of syslog information to a syslog file. |
| Step 7 | UCS-A /monitoring # set syslog file name <i>filename</i> | The name of the file in which the messages are logged. Up to 16 characters are allowed in the file name. |
| Step 8 | (Optional) UCS-A /monitoring # set syslog file level { emergencies alerts critical | Select the lowest message level that you want stored to a file. If the file state is enabled, the system stores that level and above in the syslog |

| | Command or Action | Purpose |
|----------------|--|--|
| | errors warnings notifications information debugging} | file. The level options are listed in order of decreasing urgency. The default level is Critical. |
| Step 9 | (Optional) UCS-A /monitoring # set syslog file size <i>filesize</i> | The maximum file size, in bytes, before the system begins to write over the oldest messages with the newest ones. The range is 4096 to 4194304 bytes. |
| Step 10 | UCS-A /monitoring # {enable disable} syslog remote-destination {server-1 server-2 server-3} | Enables or disables the sending of syslog messages to up to three external syslog servers. |
| Step 11 | (Optional) UCS-A /monitoring # set syslog remote-destination {server-1 server-2 server-3} level {emergencies alerts critical errors warnings notifications information debugging} | Select the lowest message level that you want stored to the external log. If the remote-destination is enabled, the system sends that level and above to the external server. The level options are listed in order of decreasing urgency. The default level is Critical. |
| Step 12 | UCS-A /monitoring # set syslog remote-destination {server-1 server-2 server-3} hostname <i>hostname</i> | The hostname or IP address of the specified remote syslog server. Up to 256 characters are allowed in the hostname. |
| Step 13 | (Optional) UCS-A /monitoring # set syslog remote-destination {server-1 server-2 server-3} facility {local0 local1 local2 local3 local4 local5 local6 local7} | The facility level contained in the syslog messages sent to the specified remote syslog server. |
| Step 14 | UCS-A /monitoring # {enable disable} syslog source {audits events faults} | This can be one of the following: <ul style="list-style-type: none"> • audits—Enables or disables the logging of all audit log events. • events—Enables or disables the logging of all system events. • faults—Enables or disables the logging of all system faults. |
| Step 15 | UCS-A /monitoring # commit-buffer | Commits the transaction. |

Example

This example shows how to enable the storage of syslog messages in a local file and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # disable syslog console
UCS-A /monitoring* # disable syslog monitor
UCS-A /monitoring* # enable syslog file
UCS-A /monitoring* # set syslog file name SysMsgsUCSA
UCS-A /monitoring* # set syslog file level notifications
```

```
UCS-A /monitoring* # set syslog file size 4194304
UCS-A /monitoring* # disable syslog remote-destination server-1
UCS-A /monitoring* # disable syslog remote-destination server-2
UCS-A /monitoring* # disable syslog remote-destination server-3
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```