Configuring Settings for Faults, Events, and Logs

This chapter includes the following sections:

Configuring Settings for the Fault Collection Policy

Fault Collection Policy

The fault collection policy controls the lifecycle of a fault in a Cisco UCS instance, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).

A fault in Cisco UCS 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 is cleared if the time between the fault being raised and the condition being cleared is greater than the flapping interval, otherwise, the fault remains raised but its status changes to soaking-clear. 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 remains raised and its status changes to flapping. If the condition does not reoccur during the flapping interval, the fault is cleared.
4. When a fault is cleared, it is deleted if the clear action is set to delete, or if the fault was previously acknowledged, otherwise, it is retained until either the retention interval expires, or if the fault is acknowledged.
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.

Configuring the Fault Collection Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **scope fault policy**	Enters monitoring fault policy mode.
Step 3	UCS-A /monitoring/fault-policy # **set clear-action** {**delete** | **retain**}	Specifies whether to retain or delete all cleared messages. If the **retain** option is specified, then the length of time that the messages are retained is determined by the **set retention-interval** command.
Step 4	UCS-A /monitoring/fault-policy # **set flap-interval** *seconds*	Specifies the time interval (in seconds) the system waits before changing a fault state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change state until the flapping interval has elapsed after the last state change. If the fault is raised again during the flapping interval, it returns to the active state, otherwise, the fault is cleared.
Step 5	UCS-A /monitoring/fault-policy # **set retention-interval** {*days hours minutes seconds* | **forever**}	Specifies the time interval the system retains all cleared fault messages before deleting them. The system can retain cleared fault messages forever, or for the specified number of days, hours, minutes, and seconds.
Step 6	UCS-A /monitoring/fault-policy # **commit-buffer**	Commits the transaction.

This example configures the fault collection policy to retain cleared fault messages for 30 days, sets the flapping interval to 10 seconds, and commits the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
UCS-A /monitoring/fault-policy # set clear-action retain
UCS-A /monitoring/fault-policy* # set flap-interval 10
UCS-A /monitoring/fault-policy* # set retention-interval 30 0 0 0
UCS-A /monitoring/fault-policy* # commit-buffer
UCS-A /monitoring/fault-policy #
```

Configuring Settings for the Core File Exporter

Core File Exporter

Cisco UCS Manager uses the Core File Exporter to export core files as soon as they occur to a specified location on the network through TFTP. This functionality allows you to export the tar file with the contents of the core file.

Configuring the Core File Exporter

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **scope sysdebug**	Enters monitoring system debug mode.
Step 3	UCS-A /monitoring/sysdebug # **enable core-export-target**	Enables the core file exporter. When the core file exporter is enabled and an error causes the server to perform a core dump, the system exports the core file via TFTP to the specified remote server.
Step 4	UCS-A /monitoring/sysdebug # **set core-export-target path** *path*	Specifies the path to use when exporting the core file to the remote server.
Step 5	UCS-A /monitoring/sysdebug # **set core-export-target port** *port-num*	Specifies the port number to use when exporting the core file via TFTP. The range of valid values is 1 to 65,535.
Step 6	UCS-A /monitoring/sysdebug # **set core-export-target server-description** *description*	Provides a description for the remote server used to store the core file.
Step 7	UCS-A /monitoring/sysdebug # **set core-export-target server-name** *hostname*	Specifies the hostname of the remote server to connect with via TFTP.
Step 8	UCS-A /monitoring/sysdebug # **commit-buffer**	Commits the transaction.

The following example enables the core file exporter, specifies the path and port to use when sending the core file, specifies the remote server hostname, provides a description for the remote server, and commits the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # enable core-export-target
UCS-A /monitoring/sysdebug* # set core-export-target path /root/CoreFiles/core
UCS-A /monitoring/sysdebug* # set core-export-target port 45000
UCS-A /monitoring/sysdebug* # set core-export-target server-description CoreFile102.168.10.10
UCS-A /monitoring/sysdebug* # set core-export-target server-name 192.168.10.10
UCS-A /monitoring/sysdebug* # commit-buffer
UCS-A /monitoring/sysdebug #
```

Disabling the Core File Exporter

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **scope sysdebug**	Enters monitoring system debug mode.
Step 3	UCS-A /monitoring/sysdebug # **disable core-export-target**	Disables the core file exporter. When the core file exporter is disabled core files are not automatically exported.
Step 4	UCS-A /monitoring/sysdebug # **commit-buffer**	Commits the transaction.

The following example disables the core file exporter and commits the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # disable core-export-target
UCS-A /monitoring/sysdebug* # commit-buffer
UCS-A /monitoring/sysdebug #
```

Configuring the Syslog

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **set syslog console state** {**enabled** | **disabled**}	Enables or disables the sending of syslogs.
Step 3	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 # **set syslog monitor state** {**enabled** | **disabled**}	Enables or disables the monitoring of syslog information by the operating system.
Step 5	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.

	Command or Action	Purpose
		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 # **set syslog file state** {**enabled** | **disabled**}	Enables or disables the writing of syslog information to a syslog file.
Step 7	UCS-A /monitoring # **set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	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 file. The level options are listed in order of decreasing urgency. The default level is Critical.
Step 8	UCS-A /monitoring # **set syslog file name** *filename*	The name of the file in which the messages are logged. Up to 16 characters are allowed in the file name.
Step 9	UCS-A /monitoring # **set syslog file size** *filesize*	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 # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **state** {**enabled** | **disabled**}	Enables or disables up to three external logs that can store messages generated by the components in the system.
Step 11	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 state is enabled, the system stores that level and above in the external log. 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** *hostname*	The host name or IP address on which the remote log file resides. Up to 256 characters are allowed in the host name.
Step 13	UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **facility** {**level0** | **level1** | **level2** | **level3** | **level4** | **level5** | **level6** | **level7**}	The facility level contained in the syslog messages.
Step 14	UCS-A /monitoring # **commit-buffer**	Commits the transaction.

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 # set syslog console state disabled
UCS-A /monitoring* # set syslog monitor state disabled
UCS-A /monitoring* # set syslog file state enabled
UCS-A /monitoring* # set syslog file name Messages
UCS-A /monitoring* # set syslog file level notifications
UCS-A /monitoring* # set syslog file size 4194304
UCS-A /monitoring* # set syslog remote-destination server-1 state disabled
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```