Log File Exporter

Log File Exporter

Cisco UCS Manager generates log files for each executable. The log files can be up to 20 MB in size, and up to five backups can be stored on the server. The log file exporter allows you to export the log files to a remote server before they are deleted. The log file names contain the following information:

- The name of the process
- Timestamp
- The name and ID of the fabric interconnect

Note If you do not enable log exporting, the oldest log files are deleted whenever the maximum backup file limit is reached.

Guidelines and Limitations

- We recommend that you use tftp or password-less scp or sftp for log export. When standard scp or sftp is used, the user password is stored in the configuration file in encrypted format.
- On a HA setup, the log files from each side are exported separately. If one side fails to export logs, the other side does not compensate.

Exporting Log Files to a Remote Server

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.

	Command or Action	Purpose
Step 2	UCS-A /monitoring # **scope sysdebug**	Enters monitoring system debug mode.
Step 3	UCS-A /monitoring/sysdebug # **scope log-export-policy**	Enters log file export mode.
Step 4	UCS-A /monitoring/sysdebug/log-export-policy # **set admin-state** {**disabled** | **enabled**}	Whether log file exporting is enabled.
Step 5	(Optional) UCS-A /monitoring/sysdebug/log-export-policy # **set desc** *description*	Provides a description for the log export policy
Step 6	UCS-A /monitoring/sysdebug/log-export-policy # **set hostname** *hostname*	Specifies the hostname of the remote server.
Step 7	UCS-A /monitoring/sysdebug/log-export-policy # **set passwd**	After you press Enter, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.
Step 8	UCS-A /monitoring/sysdebug/log-export-policy # **set passwordless-ssh** {**no** | **yes**}	Enables SSH login without a password.
Step 9	UCS-A /monitoring/sysdebug/log-export-policy # **set proto** {**scp** | **ftp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 10	UCS-A /monitoring/sysdebug/log-export-policy # **set path** *path*	Specifies the path on the remote server where the log file is to be saved.
Step 11	UCS-A /monitoring/sysdebug/log-export-policy # **set user** *username*	Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 12	UCS-A /monitoring/sysdebug/log-export-policy # **commit-buffer**	Commits the transaction.

Example

The following example shows how to enable the log file exporter, specify the remote server hostname, set the protocol to scp, enable passwordless login, and commit the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # scope log-export-policy
UCS-A /monitoring/sysdebug/log-export-policy # set admin-state enable
UCS-A /monitoring/sysdebug/log-export-policy* # set hostname 10.10.1.1
```

```
UCS-A /monitoring/sysdebug/log-export-policy* # set path /
UCS-A /monitoring/sysdebug/log-export-policy* # set user testuser
UCS-A /monitoring/sysdebug/log-export-policy* # set proto scp
UCS-A /monitoring/sysdebug/log-export-policy* # set passwd
password:
UCS-A /monitoring/sysdebug/log-export-policy* # set passwordless-ssh yes
UCS-A /monitoring/sysdebug/log-export-policy* # commit-buffer
UCS-A /monitoring/sysdebug/log-export-policy #
```