CHAPTER 4

Utilities

Revised: February 07, 2014, OL-30621-02

Introduction

This chapter describes the following utilities:

Working with Cisco SCE Platform Files

The CLI commands include a complete range of file management commands. These commands allow you to create, delete, copy, and display both files and directories

Note Regarding disk capacity: While performing disk operations, the user should take care that the addition of new files that are stored on the Cisco SCE disk do not cause the disk to exceed 70%.

Working with Directories

How to Create a Directory

mkdir

From the SCE# prompt, type:

Command	Purpose
mkdir *directory-name*	Creates a directory.

How to Delete a Directory

There are two different commands for deleting a directory, depending on whether the directory is empty or not.

How to Delete a Directory and All its Files

delete

From the SCE# prompt, type:

Command	Purpose
delete *directory-name* **/recursive**	The recursive flag deletes all files and sub-directories contained in the specified directory.

How to Delete an Empty Directory

rmdir

From the SCE# prompt, type:

Command	Purpose
rmdir *directory-name*	Use this command only for an empty directory.

How to Change Directories

Use this command to change the path of the current working directory. **cd**

From the SCE# prompt, type:

Command	Purpose
cd *new path*	Changes the path of the current working directory.

How to Display your Working Directory

pwd

From the SCE# prompt, type:

Command	Purpose
pwd	Displays the working directory.

How to List the Files in a Directory

You can display a listing of all files in the current working directory. This list may be filtered to include only application files. The listing may also be expanded to include all files in any sub-directories.

- How to List the Files in the Current Directory, page 4-3
- How to List the Applications in the Current Directory, page 4-4
- How to Include Files in Sub-Directories in the Directory Files List, page 4-4

How to List the Files in the Current Directory

From the SCE# prompt, type:

Command	Purpose
dir	Lists the files in the current directory.

How to List the Applications in the Current Directory

From the SCE# prompt, type:

Command	Purpose
dir applications	Lists the applications in the current directory.

How to Include Files in Sub-Directories in the Directory Files List

From the SCE# prompt, type:

Command	Purpose
dir -r	Includes files in the sub-directories in the directory files list.

Working with Files

How to Rename a File

From the SCE# prompt, type:

Command	Purpose
rename *current-file-name new-file-name*	Renames a file.

How to Delete a File

From the SCE# prompt, type:

Command	Purpose
delete *file-name*	Deletes a file.

Copying Files

You can copy a file from the current directory to a different directory. You can also copy a file (upload/download) to or from an FTP site.

To copy a file using passive FTP, use the **copy-passive** command.

How to Copy a File

From the SCE# prompt, type:

Command	Purpose
copy *source-file-name destination-file-name*	Copies a file.

Copying a File: Example

The following example copies the local analysis.sli file located in the root directory to the applications directory.

```
SCE#copy analysis.sli applications/analysis.sli
sce#
```

How to Download a File from an FTP Site

Use the copy command to upload and download commands from and FTP site. In this case, either the source or destination filename must begin with *ftp://*.

Step 1 From the SCE# prompt, type **copy** *ftp://username:password@ip-address/path:/source-file destination-file-name* and press **Enter**.

To upload a file to an FTP site, specify the FTP site as the destination (*ftp://username:password@ip-address/path:/destination-file*)

How to Upload a File to a Passive FTP Site

Step 1 From the SCE# prompt, type **copy-passive** *source-file-name ftp:/username:password@10.10.10.10/h:/destination-file* and press **Enter**.

To download a file from a passive FTP site, specify the FTP site as the source (*ftp://username:password@ip-address/path:/source-file*)

Uploading a File to a Passive FTP Site: Example

The following example uploads the analysis.sli file located on the local flash file system to the host 10.1.1.1, specifying Passive FTP.

```
SCE#copy-passive /appli/analysis.sli ftp://myname:mypw@10.1.1.1/p:/appli/analysis.sli
sce#
```

How to Display File Contents

From the SCE# prompt, type:

Command	Purpose
more *file-name*	Displays file contents.

How to Unzip a File

From the SCE# prompt, type:

Command	Purpose
unzip *file-name*	Unzips a file.

The User Log

The user log is an ASCII file that can be viewed in any editor. It contains a record of system events, including startup, shutdown and errors. You can use the Logger to view the user log to determine whether or not the system is functioning properly, as well as for technical support purposes.

The Logging System

Events are logged to one of two log files. After a file reaches maximum capacity, the events logged in that file are then temporarily archived. New events are then automatically logged to the alternate log file. When the second log file reaches maximum capacity, the system then reverts to logging events to the first log file, thus overwriting the temporarily archived information stored in that file.

Basic operations include:

- Copying the User Log to an external location
- Viewing the User Log
- Clearing the User Log
- Viewing/clearing the User Log counters

Copying the User Log

You can view the log file by copying it to an external location or to disk. This command copies both log files to the local Cisco SCE platform disk or any external host running a FTP server.

Copying the User Log to an External Location

From the SCE# prompt, type:

Command	Purpose
logger get user-log file-name *ftp://username:password@ipaddress/path*	Copies user log to an external location.

Copying the User Log to an Internal Location

From the SCE# prompt, type:

Command	Purpose
logger get user-log file-name *target-filename*	Copies the user log to an internal location.

Enabling and Disabling the User Log

By default, the user log is enabled. You can disable the user log by configuring the status of the logger.

- Disabling the User Log, page 4-8
- Enabling the User Log, page 4-8

Disabling the User Log

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logger device User-File-Log disabled** and press **Enter**.

Enabling the User Log

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logger device User-File-Log enabled** and press **Enter**.

Viewing the User Log Counters

- Viewing the user log counters for the current session, page 4-8
- Viewing the non-volatile counter for the user-file-log, page 4-9

There are two types of log counters:

- User log counters—Count the number of system events logged from the Cisco SCE platform last reboot.
- Non-volatile counters—These are not cleared during boot time

Viewing the user log counters for the current session

From the SCE# prompt, type:

Command	Purpose
show logger device user-file-log counters	Displays the user log counters for the current session.

Viewing the non-volatile counter for the user-file-log

From the SCE# prompt, type:

Command	Purpose
show logger device user-file-log nv-counters	Displays the non-volatile counter for the user-file-log.

Viewing the User Log

Note This command is not recommended when the user log is large. Copy a large log to a file to view it (see Copying the User Log, page 4-7)

From the SCE# prompt, type:

Command	Purpose
more user-log	Displays the user log.

Clearing the User Log

Step 1 From the SCE# prompt, type **clear logger device user-file-log** and press **Enter**.

Step 2 The system asks **Are you sure?**

Step 3 Type **Y** and press **Enter**.

Generating a File for Technical Support

In order for technical support to be most effective, the user should provide them with the information contained in the system logs. Use the logger get support-file command to generate a support file via FTP for the use of Cisco technical support staff.

From the SCE# prompt, type:

Command	Purpose
logger get support-file *filename*	Creates a support file. The support information file is created using the specified filename. The specified file must be a file located on an FTP site, not on the local file system. This operation may take some time.

Generating a File for Technical Support: Example

```
SCE#logger get support-file ftp://user:1234@10.10.10.10/c:/support.zip
```

Managing Syslog

System messages are also written to the Syslog server. When enabled, all user-log messages are sent to the configured Syslog servers as well as to the Cisco SCE user logs.

You can configure the following options for syslog support:

- Up to five remote syslog hosts
- Port number
- Minimum severity level to be logged
- Logging rate limit
- Syslog facility (such as system daemon, local printer, or user process)
- Time stamp format

Transport protocol is not configurable, since the Cisco SCE platform supports Syslog over UDP, only.

Enabling and Disabling Syslog

By default, logging to the syslog server is disabled.

Enabling Syslog

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging on** and press **Enter**.

Disabling Syslog

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging on** and press **Enter**.

Configuring Remote Syslog Hosts

You can configure up to five remote syslog hosts. You can also assign a UDP port to each host.

Guidelines

- You can define the host using either the hostname or the IP address.
- To assign a port, you must use the **transport udp** option. If you are not assigning a port, this is not required, since UDP is the only transport protocol supported for Syslog on the Cisco SCE platform.
- Each host requires a separate command.

Options

The following options are available:

- **hostname**—Logical name of the remote host
- **ip-address**—IP address of the remote host
- **port-number**—Number of the UDP port (1 – 65535)
  - default = 514

How to Add a Remote Syslog Host

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging host (*hostname* | *ip-address*) [transport udp [port *port-number*]]** and press **Enter**.

How to Remove a Remote Syslog Host

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging host (*hostname* | *ip-address*)** and press **Enter**.

Configuring the Minimum Severity Level to be Logged to Syslog

By default, all messages are logged to the Syslog server when it is enabled, with the exception of debug messages. However, you can configure the minimum severity level of the messages to logged to Syslog.

Table 4-1 lists the syslog severity levels and the corresponding SCOS severity levels. Not all syslog severity levels are supported on the Cisco SCE platform.

Table 4-1 Syslog and SCOS Severity Levels

Syslog Severity	Level	SCOS Severity	SCOS Definition
emergency	0	Not defined	SEVERITY_EMERGENCY_LEVEL
alert	1	Not defined	SEVERITY_ALERT_LEVEL
critical	2	Fatal	SEVERITY_FATAL_LEVEL
error	3	Error	SEVERITY_ERROR_LEVEL
warning	4	Warning	SEVERITY_WARNING_LEVEL
notice	5	Not defined	SEVERITY_NOTICE_LEVEL
informational	6	Info	SEVERITY_INFORMATIONAL_LEVEL
debug	7	Not defined	SEVERITY_DEBUG_LEVEL

Options

The following option is available:

- **severity-level**—The name of the desired severity level at which messages should be logged. Messages at or lower than the specified level are logged. Severity levels supported on the Cisco SCE platform are as follows:
  - **fatal**
  - **error**
  - **warning**
  - **info**

  Default = info

How to Configure the Minimum Severity Level for Syslog Messages

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging trap** ***severity-level*** and press **Enter**.

How to Restore the Default Minimum Severity Level for Syslog Messages

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging trap** and press **Enter**.

Configuring the Syslog Facility

You can assign Syslog messages to a specified facility.

Options

The following option is available:

- **facility-type**—Syslog facility. See Table 4-2
  - default = local7

Table 4-2 logging facility types

Facility-type keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-local7	Reserved for locally defined messages
lpr	Line printer system

Table 4-2 logging facility types (continued)

Facility-type keyword	Description
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

How to Configure the Syslog Facility

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging facility** ***facility-type*** and press **Enter**.

How to Restore the Default Syslog Facility

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging facility** and press **Enter**.

Configuring the Syslog Logging Rate Limit

You can configure a maximum number of messages logged per second. In addition, you can specify a severity level above which the rate is unlimited. For example, you can configure a rate limit for all messages below the **fatal** severity level.

Options

The following options are available:

- **rate**—Number of messages to be logged per second (1 to 10000).
  - default = 10
- **severity-level**—Excludes messages of this severity level and higher. Severity levels supported on the Cisco SCE platform are as follows:
  - **fatal**
  - **error**
  - **warning**
  - **info**

How to Configure the Syslog Rate Limit

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging rate-limit** *rate* **[except** *severity-level***]** and press **Enter**.

How to Restore the Default Syslog Rate Limit

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging rate-limit** and press **Enter**.

Configuring the Syslog Time Stamp Format

You can configure the format of the the time stamp on the messages on the Syslog server. You can use the **no** form of this command to specify the default Syslog time stamp format (uptime).

Options

The following time stamp format options are available:

- **uptime** (default)—Time stamp shows time since the system was last rebooted. For example "4w6d" (time since last reboot is 4 weeks and 6 days).
- **datetime**—Time stamp shows date and time.

  The following additional options are available for the **datetime option:**
  - **msec—**Include milliseconds in the date-time format.
  - **localtime—**Time stamp relative to the local time zone.
  - **show-timezone—**Include the time zone name in the date-time format.
  - **year—**Include the year in the date-time format.

  If the **datetime** keyword is used without additional keywords, time stamps will be shown using UTC, without the year, without milliseconds, and without a time zone name.

Tip The optional **msec**, **localtime**, **show-timezone**, and **year** keywords, if present, must be in the order shown in the command syntax. All keywords up to the last specified keyword must be present
Incorrect: **service timestamps log datetime msec year**
Correct: **service timestamps log datetime msec localtime show-timezone year**

How to Configure the Syslog Time Stamp Format

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **service timestamps log (uptime | (datetime [msec] [localtime] [show-timezone] [year]))** and press **Enter**.

How to Restore the Default Syslog Time Stamp Format

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no service timestamps log** and press **Enter**.

Enabling and Disabling the Syslog Message Counter

By default, the syslog message counter is enabled. You can use this command to disable the syslog message counter. When it is disabled, no line count appears in the syslog messages.

Disabling the Syslog Message Counter

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **no logging message-counter** and press **Enter**.

Enabling the Syslog Message Counter

Step 1 From the SCE# prompt, type **configure** and press **Enter**.

Step 2 From the SCE (config)# prompt, type **logging message-counter** and press **Enter**.

Monitoring Syslog

You can display the following Syslog information:

- Current Syslog server configuration.
- Syslog counters

How to Display the Syslog Configuration

From the SCE# prompt, type:

Command	Purpose
show logging	Displays the syslog configuration.

How to Display the Syslog Counters

From the SCE# prompt, type:

Command	Purpose
show logging counters	Displays the syslog counters.

Flow Capture

The flow capture utility is a CLI-controlled utility that is used to capture traffic according to Layer 4 attributes.

The traffic flow captured by this utility is accumulated in a cap format file. Traffic that is identified by the capture mechanism is not available for traffic control or any other service for the duration of the capture. When flow capture is configured, the traffic that matches the rules are bypassed on Cisco SCE. After the completion of a capture, normal service to all the traffic is resumed.

The recorded data is sent online to a distant location using FTP. The data is sent in a standard format, with a maximum file size of 128 MB on the Cisco SCE 8000 platform (configurable by a const DB).

In Cisco SCE 8000 that has two SCM modules, a separate cap file is created by each SCM module, each with a maximum file size of 64 MB.

Note Flow capture is used for troubleshooting. Enabling the flow capture may impact the CPU performance. We recommend that you avoid enabling flow capture in a production environment.

Limitations

Note the following known limitations of the flow capture utility:

- The actual capture starts only for newly opened flows. Therefore, already opened flows cannot be captured by this utility.
- The termination of a capture flow is verified for every new relevant packet that is being captured. As long as no packets matching the capturing attributes arrives after the time is exceeded, the capturing is not stopped and must be stopped manually.
- File size limitation: the maximum captured file size is limited on Cisco SCE 8000 platform to 128MB (configurable by a const DB). In this platform the FTP connection is opened when the capturing starts, but the data is first kept on the system disk and is transferred to the FTP destination only when the capturing procedure is concluded.
- In a system with two Cisco SCE 8000-SCM modules, which creates two capture files, the maximum file size for each file is 64MB, for a total of 128MB.
- FTP timeout: As the recorded traffic might be sparse, and since on the Cisco SCE 8000 platform the data is sent only upon termination of the capture, it is required to disable any connection timeout on the destination FTP server.
- Capture may end prematurely due to a shortage event on the Cisco SCE platform.
- Capturing throughput is limited by the following:
  - system architectural limitations
  - line capacity to the remote FTP destination (for non-Linux platforms only, such as the Cisco SCE 2000 platform).

  The approximated throughput on a live setup is 2Mbps. When this throughput is exceeded, packets are absent from the cap file and the appropriate field in the consequent captured packet is updated to note the number of lost packets. The maximum allowed number of sequential lost packets is configurable by a const DB.

The Flow Capture Process

There are three main steps in the overall flow capture process:

1. Configure the traffic rules to define the traffic to be captured. ("Configuring a Flow Capture Traffic Rule" section on page 4-18)
2. Configure the flow capture settings. (Optional) ("Configuring the Flow Capture Settings" section on page 4-18)
3. Perform the actual flow capture. ("Performing the Flow Capture" section on page 4-20)

Configuring a Flow Capture Traffic Rule

The flow capture traffic rules define the traffic to be captured. You can configure a flow capture traffic rule by specifying the **flow-capture** action for the relevant flows.

For example, in order to capture all the traffic sent to or coming from subscribers whose IP addresses are in the range.2.3.0-1.2.3.255, define a traffic rule as follows:

```
SCE(config if)# traffic-rule name flowcapturerule IP-addresses subscriber-side 1.2.3.0/24
network-side all protocol all direction both traffic-counter none action flow-capture
```

Multiple rules can be configured, but note that all configured flow capture rules are in effect during the flow capture process. It is not possible to apply only a subset of the configured rules.

For more information regarding configuring traffic rules, see "Configuring Traffic Rules and Counters" section on page 7-26.

Configuring the Flow Capture Settings

The flow capture settings control aspects of the flow capture process, as opposed to defining the flow to be captured. These settings limit the scope of the process to maximize the recorded information while minimizing the effect on traffic.

- Maximum duration of the capture: By limiting the duration of the capture, you can limit the effect of the capture on live traffic.

  You can stop the capture at any time before the maximum duration has been reached.

- Maximum length of the L4 payload of each captured packet: If you want to capture mainly the L2-L4 headers, you need only a small portion of the payload of each packet. Setting a limit on the length of the payload makes the capture more efficient, as it allows more packets to be captured within a given time frame and for a given throughput.

  Guidelines and Information:

  – If maximum L4 payload length is not configured, all bytes of each captured packet are recorded.

  – If maximum L4 payload length is configured, each captured packet will contain the entire L2/L3/L4 headers and no more than the configured maximum bytes of L4 payload.

  – Only one maximum L4 payload length value can be configured. This value applies to all recorded packets.

- If the maximum L4 payload length value is changed while recording is performed, it will not take effect until the next recording session.
- The cap file contains marking for packets which had TCP or UDP checksum error when received in the Cisco SCE platform, since the validity of the TCP and UDP checksum cannot be checked for the captured packets due to missing bytes.
- The cap file contains the information to retrieve the original length of each packet that was truncated.

How to Configure the Maximum Flow Capture Duration

The following options are available:

- **duration—**The maximum duration of the flow capture in seconds.

  Default = 3600 seconds
- **unlimited—**There is no time limit to the flow capture, and it will continue until stopped by the operator.

From the SCE(config if)# prompt, type:

Command	Purpose
flow-capture controllers time (*duration* | **unlimited**)	Configures the maximum flow capture duration.

How to Configure the Maximum Length of the L4 Payload

The following options are available:

- **length—**The maximum number of L4 payload bytes to capture from each packet.
- **unlimited**—There is no limit on the number of L4 payload bytes. (Default)

From the SCE(config if)# prompt, type:

Command	Purpose
flow-capture controllers max-l4-payload-length (*length* | **unlimited**)	Configures the maximum length of the L4 payload.

How to Restore the Default Flow Capture Settings

From the SCE(config if)# prompt, type:

Command	Purpose
default flow-capture controllers (time | max-l4-payload-length)	Restores the default flow capture settings.

Performing the Flow Capture

The flow capture begins when you execute the flow-capture command. You can stop the capture at any time. If the capture is not stopped, it continues for the configured maximum duration ("Configuring the Flow Capture Settings" section on page 4-18).

How to Start a Flow Capture

The following option is available:

- **filename**—Name and FTP location to which to record the flow capture data in the format *ftp://<username>:<password>@<IP_address>/<path>/<file_name>*. (Do not include the ".cap" file extension; it is appended automatically.)

  In a system with two Cisco SCE 8000-SCM modules, which creates two capture files, an indicator is appended to this prefix to indicate which Cisco SCE 8000-SCM module created the file. For example, if you assign the filename "myCapFile", the system creates *myCapFile1.cap* and *myCapFile2.cap*.

From the SCE# prompt, type:

Command	Purpose
flow-capture start format cap file-name-prefix *filename*	Starts a flow capture.

How to Stop a Flow Capture

From the SCE# prompt, type:

Command	Purpose
flow-capture stop	Stops a flow capture.

Monitoring the Flow Capture

Use the following command to monitor the flow capture process. It displays the following information:

- status of the recording process
- current target file size
- number of packets captured
- number of packets lost
- configured values of the different controllers

How to Monitor the Flow Capture

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 flow-capture	Monitors the flow capture.