CHAPTER 15

Maintaining Cisco E-DI

Several tools are provided for Cisco E-DI server maintenance and troubleshooting:

- Maintenance Submode—The Cisco E-DI maintenance shell can be used to perform routine maintenance tasks such as installing patches or rebooting the Cisco E-DI server.
- Viewing Server Information—Administrators can view Cisco E-DI related information such as device-packages, clock, netstat, interfaces, and thread pools.
- Viewing License Information—Used to get information about the Cisco E-DI license.
- Viewing Security Features—Administrators can check the transport method, either SNMP Write or Telnet/SSH, and the credential set.

Cisco E-DI provides an aggregate log of all database transactions with their respective time stamps.

Cisco E-DI provides CLI commands to display:

- Linux process information
- Cisco E-DI thread pool sizes and pending tasks in the queue
- System memory usage
- System CPU usage

Cisco E-DI also generates internal statistics which can be output to a file.

Viewing Server Information

Troubleshooting the server typically begins by looking at the server statistics and debug information. To enable administrators to view this information, Cisco E-DI provides options for the **show server** command. See Table 15-1.

Table 15-1 Commands to View Server Information

Action	Command
To display installed Cisco E-DI device packages.	`[SRV:/server]# show server device-packages`
To print a list of event queues.	`[SRV:/server]# show server event-queues`
To display the server log information.	`[SRV:/server]# show server log [bookmark name | log.1 | log.2 | log backup]`

Table 15-1 Commands to View Server Information (continued)

Action	Command
To display the known device types.	`[SRV:/server]# show server known-devices`
To print a list of all server software modules.	`[SRV:/server]# show server modules`
To display the server IP routing table.	`[SRV:/server]# show server routes`
To display the server running configuration for a module.	`[SRV:/server]# show server running-config module`
To display the server startup configuration.	`[SRV:/server]# show server startup-config`
To display the server statistics that include the aggregate count and the last occurrence for the following operations and events: • Database backup, database restore. • Discovery jobs. • Inventory jobs run. • SNMP—Traps sent, trap send failures. • Syslog—Message send failures, messages sent, receiver decode errors, messages received but dropped, messages received. • Server—Configuration change count, configuration load count, configuration save count. • TFTP—Authentication failed requests, get requests, put requests. • SNMP Traps—Traps received but dropped, known traps received, traps received, unknown traps received. • Triggers—Failed action implementations, successful action implementations, successful pattern matches. • XML API—Events sent, keep-alive requests received, XML requests received, XML responses sent out.	`[SRV:/server]# show server stats`
To print a list of thread pools.	`[SRV:/server]# show server thread-pools`
To print a list of all threads.	`[SRV:/server]# show server threads`
To show the server version.	`[SRV:/server]# show server version brief`

In addition, administrators can use the **show line** command to view information on the sessions currently in use, including the userId, IP Address, connection mode and the uptime.

Debug Logs

Debug logging can be enabled or altered or disabled on specific modules or on all the modules using the **debug** CLI command. When debug logging is enabled with a specific level, the messages that are generated by various modules at that level and above are logged into a log file.

Debug mode has the following levels of severity:

- fatal (5)
- error (4)
- warn (3)
- info (2)
- debug (1)

The debug log messages can be viewed using **show server log** command. The log output can be redirected to the terminal using the **terminal monitor** command. When the log file reaches the maximum size of 30MB, it is saved into a backup file.

These messages can be displayed on the terminal or logged to a file that you can access using the commands given in Table 15-2.

Table 15-2 Commands to Debug Cisco E-DI

Action	Command
To set the debugging level for all the Cisco E-DI modules.	`[SVR:/server]# debug all level {debug | error | fatal | info | warn}`
To set the debugging level for a specific Cisco E-DI module to a pre-defined state.	`[SVR:/server]# debug module {module-name} level {debug | error | fatal | info | warn}`
To set a bookmark in the log file to facilitate retrieval of log messages between desired Cisco E-DI states.	`[SVR:/server]# debug bookmark {begin | end} bookmark-name`
To show the contents of the log file for the specified bookmark.	`[SVR:/server]# show server log bookmark bookmark-name`
To print the logging messages to the terminal,	`[SVR:/server]# terminal monitor`
To clear the debug log. See Table A-1 for details of the options available with this command.	`[SVR:/server]# clear debug-log`

Viewing License Information

Choose option **J** to display the license file status information. This command provides information including the license type (either permanent or demo), the MAC address of the Cisco E-DI server, and if a demo license is installed, the remaining days before the license expires.

Viewing Security Features

Device authentication allows the administrator to choose between a centralized credential model (**non session based device authentication**) and a per user-session credential model (**session based device authentication**). Whichever mode is chosen is applied to all devices in the network. See Device Authentication for more details.

Table 15-3 details how to check the transport method, either SNMP Write or Telnet/SSH, and the credential set.

Table 15-3 Commands to View Security Setup

Action	Command
To view the IP address of Cisco E-DI and the users' login ID.	`[SRV:/server]# show line`
To view the syslog messages on the devices.	`[NET:/network]# show events`
To check the status of management operations in Cisco E-DI	`[NET:/network]# show devices manageability`

Synchronizing Information

Cisco E-DI has the most current information about all of the devices in the network in its database. In case of any discrepancies found in the information when troubleshooting, you can synchronize the information between the server and the network.

Synchronization can be done in the foreground or the background.

The command for configuration synchronization is context sensitive.

Table 15-4 gives the commands to synchronize information in Cisco E-DI.

Table 15-4 Commands to Synchronize Information

Action	Command
To synchronize the config-archives with the database for all offline and online devices, and server	`[NET:/network]# sync archives-with-db [all]`
To synchronize the file system with device. Synchronization can be done in the foreground or the background. The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-7 for a full explanantion of the command behavior.	`[NET:/network]# sync filesystem {bg | fg}`
To synchronize the startup and running config files with device. Synchronization can be done in the foreground or the background. The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-7 for a full explanantion of the command behavior.	`[NET:/network]# sync configuration {bg | fg}`
To synchronize the asset inventory information. Synchronization can be done in the foreground or the background.	`[NET:/network]# sync asset {bg | fg}`