



CHAPTER 4

Performing Command Line Administration Tasks

Revised: August 28, 2008, OL-16776-01

This chapter describes details basic administrative tasks that you perform using a console connection to the MARS Appliance.

This chapter contains the following procedures:

- [Log In to the Appliance via the Console, page 4-1](#)
- [Reset the Appliance Administrator Password, page 4-2](#)
- [Shut Down the Appliance via the Console, page 4-3](#)
- [Log Off the Appliance via the Console, page 4-3](#)
- [Reboot the Appliance via the Console, page 4-3](#)
- [Determine the Status of Appliance Services via the Console, page 4-4](#)
- [Stop Appliance Services via the Console, page 4-6](#)
- [Start Appliance Services via the Console, page 4-6](#)
- [View System Logs via the Console, page 4-6](#)

For other MARS Appliance configuration and administration tasks, see the document roadmap for this release: [Cisco Security MARS Documentation Guide and Warranty](#).

Log In to the Appliance via the Console

After the MARS Appliance boots, the console service starts and prompts the user to log in. Successful login launches a command line application (shell) that operates the CLI.

To log in to the MARS Appliance via a console connection, follow these steps:

-
- Step 1** Establish a console connection to the MARS Appliance. For options and details, see [Establishing a Console Connection, page 2-4](#).
 - Step 2** At the `login:` prompt, enter the MARS Appliance administrator name.
 - Step 3** At the `password:` prompt, enter the MARS Appliance password.

Result: The system prompt appears in the following form:

```
Last login: Tue Jul 5 05:57:31 2005 from <host>.<domain>.com
```

```
Cisco Security MARS - Mitigation and Response System
```

```
? for list of commands
```

```
[pnadmin]$
```

**Note**

There is only one set of MARS Appliance login credentials (administrator name and password) that have the console connection privilege.

**Tip**

To exit the console connection, enter **exit** at the command prompt.

Reset the Appliance Administrator Password

There is always a single set of MARS Appliance administrator credentials consisting of the administrator name *pnadmin* and a corresponding password. Unlike other MARS administrative accounts, this unique administrative account is granted all privileges and cannot be deleted.

This procedure details how to reset the password after you log in with the existing credentials. If you do not have the existing MARS Appliance administrator login credentials with which to log in, the only method of recovery is to re-image the appliance, which resets the password to the factory defaults. For information on resetting the administrator login and password without first logging in, see [Recovery Management, page 6-16](#).

To reset the MARS Appliance administrator login credentials, follow these steps:

Step 1 Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).

Step 2 At the system prompt, type **passwd** and then press **Enter**.

Result: The MARS Appliance displays the following prompt:

```
New password:
```

Step 3 Type the new password, and then press **Enter**.

**Note**

The new password should not contain the administrator account name, must contain a minimum of 6 characters, and it should include at least 3 character types (numerals, special characters, upper case letters, and lowercase letters). Each of the following examples is acceptable: 1PaSsWoRd, *password44, Pass*word.

The MARS Appliance displays the following prompt:

```
Retype new password
```

Step 4 Type the new password again, and then press **Enter**.

Result: The MARS Appliance displays the command prompt, and the password is changed.

Shut Down the Appliance via the Console

You can shut down an appliance remotely via a console connection. However, to power up the appliance, you must have physical access to the device.

**Caution**

Powering off the MARS Appliance by using only the power switch may cause the loss or corruption of data. Use this procedure to shut down the MARS Appliance.

Summary Steps**1. shutdown**

use the console to shut down the MARS Appliance, follow these steps:

Step 1 Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).

Step 2 At the system prompt, type **shutdown**, and then press **Enter**.

Result: The following message appears and the MARS Appliance powers off.

```
[pnadmin]$ shutdown  
  
Broadcast message from root (pts/0) (Fri Mar 28 14:38:54 2008):  
  
The system is going down for system halt NOW!  
[pnadmin]$ Last login: Fri Mar 28 14:59:11 2008
```

Log Off the Appliance via the Console

Logging off via the console closes the administrative session at the appliance. Good security practices recommend logging off when you are not using the console.

Summary Steps**1. exit**

To log off the MARS Appliance via the console, follow these steps:

Step 1 At the system prompt, type **exit**.

Step 2 Press **Enter**.

Result: The console connection closes, and the `login:` prompt reappears.

Reboot the Appliance via the Console

From time to time, you may need to manually reboot the appliance. For example, if a service seems to be hung, rebooting may resolve the issue. Rebooting ensures that the services are shut down safely before the appliance restarts.

Summary Steps**1. reboot**

To reboot the MARS Appliance via the console, follow these steps:

Step 1 Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).

Step 2 At the system prompt, type **reboot**, and then press **Enter**.

Result: The MARS Appliance displays the following message:[pnadmin]\$ reboot

```
Broadcast message from root (pts/0) (Fri Mar 28 15:33:31 2008):
```

```
The system is going down for reboot NOW!
[pnadmin]$
```

The MARS Appliance reboots. When the reboot is finished, the `login:` prompt reappears.

Determine the Status of Appliance Services via the Console

You can use the console connection to obtain system and service status information.

Summary Steps**1. pnstatus****Detailed Steps**

To determine the status of the MARS Appliance's services, follow these steps:

Step 1 Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).

Step 2 At the system prompt, type **pnstatus**, and then press **Enter**.

The system displays list of services and status information. Possible states are:

- **RUNNING.** The service is operational.
- **STOPPED.** The service is not running.

**Note**

All services should be running on a Local Controller. However, a Global Controller only has five services running: autoupdate, graphgen, pnarchiver, securesyslog, and superV—all other services are stopped.

Examples

The expected results for **pnstatus** run on a Global Controller:

```
Last login: Tue Jul 15 08:39:14 2008 from <hostname>
```

```
CS MARS - Mitigation and Response System
```

? for list of commands

```
[pnadmin]$ pnstatus
Module                               State      Uptime
DbIncidentLoaderSrv                 STOPPED
KeywordQuerySrv                     STOPPED
autoupdate                           RUNNING    11-03:47:01
csdam                                 STOPPED
csiosips                             STOPPED
csips                                 STOPPED
cswin                                 STOPPED
device_monitor                       STOPPED
discover                             STOPPED
graphgen                             RUNNING    10:20:31
pnarchiver                           RUNNING    11-03:47:02
pndbpurger                           STOPPED
pnesloader                           STOPPED
pnmac                                 STOPPED
pnparser                              STOPPED
process_event_srv                    STOPPED
process_inlinerep_srv                STOPPED
process_postfire_srv                 STOPPED
process_query_srv                    STOPPED
securesyslog                         RUNNING    11-03:47:02
superV                               RUNNING    11-03:47:02
```

The expected results for **pnstatus** run on a Local Controller:

Last login: Tue Jul 15 08:11:56 2008 from <hostname>

CS MARS - Mitigation and Response System

? for list of commands

```
[pnadmin]$ pnstatus
Module                               State      Uptime
DbIncidentLoaderSrv                 RUNNING    41-19:20:54
KeywordQuerySrv                     RUNNING    41-19:20:54
autoupdate                           RUNNING    41-19:20:54
csdam                                 RUNNING    41-19:20:54
csiosips                             RUNNING    41-19:20:54
csips                                 RUNNING    41-19:20:54
cswin                                 RUNNING    41-19:20:54
device_monitor                       RUNNING    41-19:20:54
discover                             RUNNING    41-19:20:54
graphgen                             RUNNING    10:17:26
pnarchiver                           RUNNING    3-08:19:55
pndbpurger                           RUNNING    41-19:20:54
pnesloader                           RUNNING    41-19:20:54
pnmac                                 RUNNING    41-19:20:54
pnparser                              RUNNING    22:01:45
process_event_srv                    RUNNING    41-19:20:54
process_inlinerep_srv                RUNNING    41-19:20:54
process_postfire_srv                 RUNNING    41-19:20:54
process_query_srv                    RUNNING    41-19:20:54
securesyslog                         RUNNING    41-19:20:54
superV                               RUNNING    41-19:20:55
```

Stop Appliance Services via the Console

You can stop all MARS Appliance services from the console. To list the services and their status, you can use the **pnstatus** command. For more information, see [Determine the Status of Appliance Services via the Console, page 4-4](#).

To stop all services on the MARS Appliance, follow these steps:

-
- Step 1** Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).
 - Step 2** Type **pnstop**.
 - Step 3** Press **Enter**.

Result: The system immediately shows the message:

```
Please Wait . . .
```

Followed by the return of the prompt, indicating the command has completed.

- Step 4** To verify the status of the services, enter **pnstatus**.
The superV service does not stop. This service monitors and restarts the other services as needed.
-

Start Appliance Services via the Console

If the services are stopped, you can manually start all MARS Appliance services from the console. To list the services and their status, you can use the **pnstatus** command. For more information, see [Determine the Status of Appliance Services via the Console, page 4-4](#).

Summary Steps

1. **pnstart**

To start all stopped MARS services, follow these steps:

-
- Step 1** Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).
 - Step 2** Type **pnstart**.
 - Step 3** Press **Enter**.
Result: The system prompt disappears and then returns, indicating the services are restarted.
 - Step 4** To verify the status of the services, enter **pnstatus**.
-

View System Logs via the Console

This section details the procedure for running the **pnlog show** command. This command displays the log status and can be used by support personnel for analysis.

For more information on the **pnlog** command, see [pnlog show, page 1-53](#). The syntax for the **pnlog show** command is as follows:

```
pnlog show <gui|backend|cpdebug>
```

These options do a running output of a particular log file in the backend. There are three different logs that you can view: the web interface logs, the backend logs (shows logs for processes that the **pnstatus** command reports on), and CheckPoint debug logs. Use Ctrl+C or ^C to stop this command.

When using **cpdebug**, you should have `pnlog setlevel` set to more than 0, which is the default value and turns off the CPE Debug messages.

To generate a .cab file of log and system Registry information, follow these steps:

-
- Step 1** Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).
- Step 2** Type **pnlog show** and the appropriate argument.
- Step 3** Press **Enter**.
Result: The console begins scrolling the output of the executed command.
- Step 4** To stop the output at any time, press **Ctrl+C**.
Result: The system returns to the system prompt.
-

Determining the Version Running on an Appliance

Before you upgrade an appliance, you must determine the version you are running. You can determine this in one of two ways:

- **web interface.** To determine the version in the web interface, select **Help > About**.
- **CLI.** To determine the version from the CLI, enter **version** at the MARS command prompt.

The format of the version appears as `x.y.z (build_number) data_version`, for example, `6.0.1 (2992) 30`.

Result: You have identified the version running on your appliance and know whether you must contact Cisco support or continue with this checklist.

■ Determining the Version Running on an Appliance