CHAPTER 25

System Maintenance

Revised: April 5, 2007, OL-14647-02

Much of the system maintenance information for the MARS Appliance is provided exclusively in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System.*

The MARS Appliance requires little maintenance. To perform maintenance tasks, you can use the CLI or the web interface as needed. Some hardware maintenance tasks require physical access to the MARS Appliance.

This chapter contains the following sections:

For information about upgrading, backing up, and restoring data on the MARS Appliance, see the following sections of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*:

Setting Runtime Logging Levels

To set the appliance's runtime logging levels, navigate to **Admin > System Maintenance > Set Runtime Logging Levels**. For typical use, it is best to leave this page set to its defaults.

When you have made your selections, click the **Change Logging Levels** button.

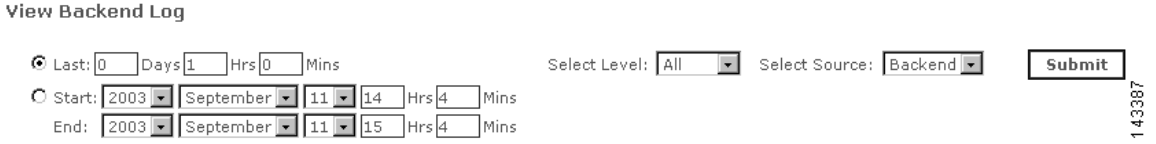
The following log levels are available:

- **Fatal**. Enables fatal logging messages. Fatal messages record very severe error events that will likely lead the application to abort.
- **Error**. Enables error and fatal logging messages. Error messages record error events that might still allow the application to continue running.
- **Warn**. Enables warning, error, and fatal logging messages. Warning messages record potentially harmful situations.
- **Info**. Enables informational, warning, error, and fatal logging messages. Informational messages highlight the progress of the application at coarse-grained level.
- **Debug**. Enables debug, informational, warning, error, and fatal logging messages. Debug messages record fine-grained informational events that are most useful to debug an application.
- **Trace**. Enables trace, debug, information, warning, error, and fatal logging messages. Trace messages record finer-grained informational events than debug messages.

Viewing the MARS Backend Log Files

To view the appliance's log files or to change their levels or source, navigate to **Admin > System Maintenance > View Log Files**.

Figure 25-1 Backend log viewing options



You can view the appliance's back-end logs either by selecting a number of days, hours, and minutes or you can view logs by selecting a start and ending date and time.

You can select the levels of logs that you want. Your choices are: All, Fatal, Error, Warn, Info, and Debug.

You can also choose the source of the files that you want to view. Select either Backend or GUI.

View the Backend Log

Step 1 Click the appropriate radio button:

- **Last**: The present time minus the number of days, hours, and minutes entered.
- **Start/End:** Absolute literal time ranges defined by the date to the minute.

Step 2 Select user, group, etc.

Step 3 Select the source.

Step 4 Click **Submit**.

Viewing the Audit Trail

You can track the activities of the appliance's users by analyzing the appliance's log files. To set the appliance's audit trail logs, navigate to **Admin > System Maintenance > View Audit Trail**. For typical use, it is best to leave this page set to its defaults.

You can view the user audit trails either by selecting a number of days, hours, and minutes, or you can view a specific interval by selecting a start and ending date and time.

View an Audit Trail

Step 1 Click the appropriate radio button:

- Last: DD-HH-MM
- Start/End: YY-MM-DD-HH-MM

Step 2 From the list, select the user or user group.

Step 3 Click **Submit**.

Retrieving Raw Messages

You can retrieve raw messages from either an archive server (see Configuring and Performing Appliance Data Backups, page 6-26) or from thedatabase running on the Local Controller. These two method offer different advantages:

- **Archive server.** Retrieving raw messages, or event data, from an archive server is much faster than retrieving from the database. Therefore, it is the recommended option if it is available and it covers the time period you are investigating. However, this option is only available if you have enabled data archiving and waited the requisite time for the initial archival operation to occur; it is a scheduled operation that runs nightly around 2:00 a.m. Once the initial archive is performed, the event data is written to the archive server frequently, often within 5 to 8 minutes after the MARS Appliance receives the message. That data is not archived in real-time identifies another limitation to this option, and that is the historical period that can be studied. If you need to view data that is more current than an hour old, you should select the Database option to ensure that correct data is retrieved. For all other periods, the archive server option is recommended. To enable archiving, see Configuring and Performing Appliance Data Backups, page 6-26.
- **Database**. Retrieving event data from the local files provides slower performance than the archive server. However, it provides access to the most current data received. When you select this option, you can specify where you want the retrieved records to be written: in the default local directory or the a remote server, if one is available.

This section contains the following topics:

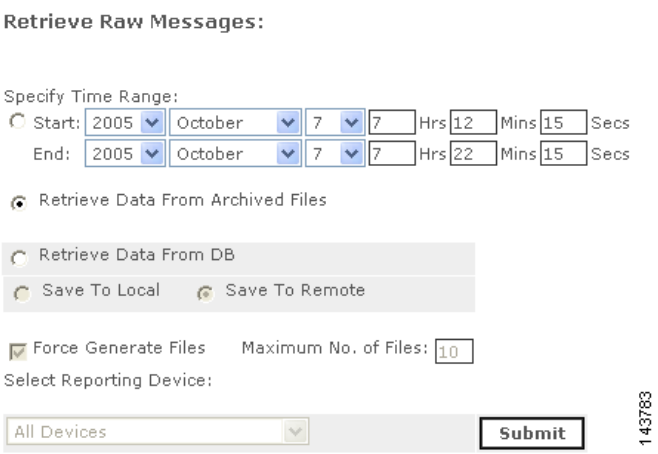
Retrieve Raw Messages From Archive Server

Use this selection if archiving is enabled.

To retrieve event data from an archive server, follow these steps:

Step 1 Click **Admin > System Maintenance > Retrieve Raw Messages**.

Figure 25-2 Retrive Raw Messages Page (4.2.x)



Step 2 Specify the time range by specifying values in the Start and End fields.

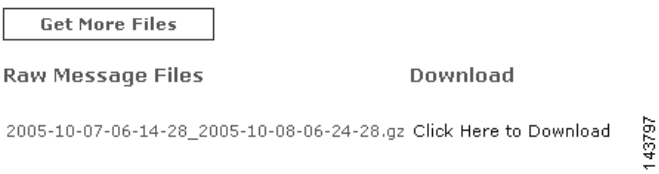
Step 3 Verify that **Retrieve Data From Archived Files** is selected.

The data will be retrieved from the server identified under Admin > System Maintenance > Data Archiving.

Step 4 Click **Submit**.

Note While MARS is generating your files, you can still use the system for other tasks.

Result: The Retrieving Progress 0% screen appears. When the operation is complete, the Raw Message Files screen appears, identifying a new Gzip archive file with a filename based on specified time range.



Step 5 To download and view the generated raw message file, click Click Here to Download next to the filename.

The filename adheres to the following syntax: YYYY-MM-DD-HH-MM-SS_YYYY-MM-DD-HH-MM-SS.gz.

Step 6 Use WinZip or another archive expansion program to extract the contents of the Gzip archive file.

Step 7 Once the textfile is extracted from the GNU Zip archive format, its contents resemble the following:

```
33750»Wed Jul 27 16:16:06 PDT 2005»BR-FW-1»10.4.1.1 Mon Jan 6 11:05:34 2003 <134>Jan 06
2003 11:03:53: %PIX-6-302001: Built inbound TCP connection 21000 for faddr 10.1.2.4/9000
gaddr 10.1.5.20/80 laddr 10.1.5.20/80
```

where it reads: *device ID>>date>>device name>>raw message*.

Note If you see Chinese or other unfamiliar characters in the resulting text file, please use Microsoft Internet Explorer to view the file and verify that the Western European ISO or Western European Windows encoding value is selected (View > Encoding). The "»" sign appears correctly as a separator when a compatible encoding is selected.

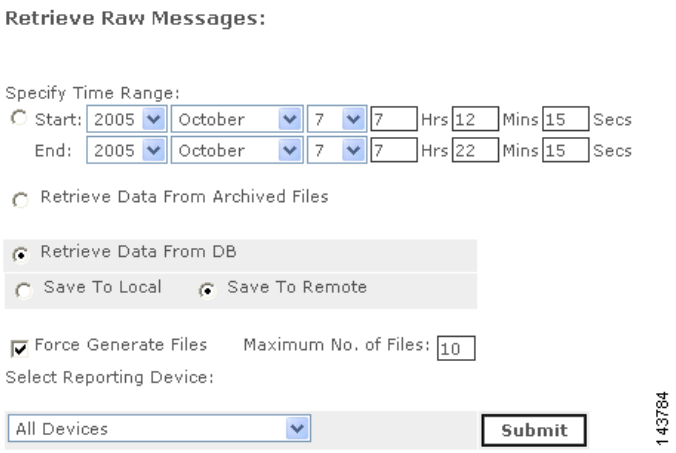
Retrieve Raw Messages From a Local Controller

Use this selection if archiving is not enabled or if you need to view event data that was received within the past hour.

To retrieve event data from the Local Controller, follow these steps:

Step 1 Click **Admin > System Maintenance > Retrieve Raw Messages**.

Figure 25-3 Retrive Raw Messages Page (4.2.x)



Step 2 Specify the time range by specifying values in the Start and End fields.

Step 3 Select **Retrieve Data from DB**

Step 4 Select one of the following options:

- **Save to Local**. This option retrieves the data from the database and stores it on the local appliance.
- **Save to Remote**. This option retrieves the data from the database and stores it on the archive server, as identified under Admin > System Maintenance > Data Archiving.

Step 5 Review the Cached Files time range information, and then do one of the following:

- If you want data from within this time range, you do not need for Force Generate Files.

- If you want data that does not fall within the Cached Files time range, select the **Force Generate Files** check box.
- If there is no cached file information, select the **Force Generate Files** check box.

If no cached file data is shown, then no previous queries have been performed and stored. For example, if you preform three separate queries, using time range *A*, from the database sing the time range, saving the files to the local MARS Appliance. If you later specify the same time range *A* and do the retrieval again but you do not clear the Force generate files check box, the system performs the query, generating the file again. However, if you have already retrieved and stored some data before, you can specify to retrieve them from those saved files by clearing the Force generate files check box.

Step 6 Enter the maximum number of retrieved files to retain in the Maximum No. of Files field.

This value refers to the maximum number of event files to be generated for this query.

Note Requesting large numbers of files can take some time.

Step 7 Select the list of devices for which you want to pull event data in the Reporting Devices list.

You can select a specific device by name or All Devices.

Step 8 Click **Submit**.

Note While MARS is generating your files, you can still use the system for other tasks.

Result: The Retrieving Progress 0% screen appears. When the operation is complete, the Raw Message Files screen appears, identifying a new Gzip archive file with a filename based on specified time range.

Step 9 To download and view the generated raw message file, click Click Here to Download next to the filename.

The filename adheres to the following syntax:
YYYY-MM-DD-HH-MM-SS_YYYY-MM-DD-HH-MM-SS.gz.

Step 10 Use WinZip or another archive expansion program to extract the contents of the Gzip archive file.

Step 11 Once the textfile is extracted from the GNU Zip archive format, its contents resemble the following:

```
33750»Wed Jul 27 16:16:06 PDT 2005»BR-FW-1»10.4.1.1 Mon Jan 6 11:05:34 2003 <134>Jan 06
2003 11:03:53: %PIX-6-302001: Built inbound TCP connection 21000 for faddr 10.1.2.4/9000
gaddr 10.1.5.20/80 laddr 10.1.5.20/80
```

where it reads: *device ID>>date>>device name>>raw message*.

Note If you see Chinese or other unfamiliar characters in the resulting text file, please use Microsoft Internet Explorer to view the file and verify that the Western European ISO or Western European Windows encoding value is selected (View > Encoding). The "»" sign appears correctly as a separator when a compatible encoding is selected.

Change the Default Password of the Administrator Account

Good security practices require that you change the default password. We recommend using strong passwords for the MARS Appliance appliances.

Login names and passwords:

- can be alphanumeric characters
- are case sensitive
- can contain special characters (!, @, #, etc.)
- **cannot** contain single or double quotes (‘or “)

Login names can contain up to 20 characters. Passwords can contain up to 64 characters.

To change the default password and setup administrator notification, follow these steps:

Step 1 Click the **Management > User Management** tab.

Step 2 Check the box next to Administrator, and click **Edit**.

Step 3 Enter the new Administrator password and the Administrator e-mail address.

Step 4 Click **Submit**.

Understanding Certificate and Fingerprint Validation and Management

Many reporting devices use certificates or fingerprints to enable secure communications over SSL or SSH respectively. Beginning in 4.2.3, MARS performs a strict check of the certificate or fingerprint of the device or server to which it is attempting to connect.

Note Certificate validation does not follow the convention of presenting the client with a list of certificate authorities and using the selected one to validate individual certificates. Instead, the MARS Appliance compares the certificate presented by the reporting device with a previously stored instance of the certificate. If the two match, the presented certificate is considered valid. This approach allows MARS to validate certificates without knowledge of revocation lists and to operate in a network without an Internet connection.

Three options exist for specifying how MARS should respond during attempts to establish a secure connection. The three options are as follows:

- **Automatically always accept.** This option, which is compatible with previous releases, allows a MARS Appliance to connect to reporting devices regardless of how frequently the certificate or fingerprint changes because MARS automatically accepts and stores the replacement certificate or fingerprint for all devices. However, this option does not provide an opportunity to inspect and authorize the changes to the certificates or fingerprints. When a conflict is detected or when a new certificate or fingerprint is accepted, the event is logged to the internal log. The internal log entry includes the name of the process that detected the conflict and the IP address of the reporting device. The logs can be retrieved by queries and reports. See Monitoring Certificate Status and Changes, page 25-10 for more information on studying these events.
- **Accept first time and prompt on change (default).** This option accepts and stores a new certificate or fingerprint the first time MARS Appliance connects to a device. For subsequent connection attempts, the appliance checks the presented certificate or fingerprint against the stored value. If a conflict is detected, the session is refused unless the new certificate or fingerprint is manually accepted by the administrator. This option enables initial topology discovery to proceed without administrator intervention. Internal system logs of the initial acceptance, conflict detection, and acceptance of new change are created. The internal logs include the name of the process that detected the conflict, the IP address of the reporting device, and the username of the account used to accept the change.

  If, when a change is detected by a web interface process, the session times out before administrative intervention, the communication fails but no internal system log is generated to record the failure to accept the changed certificate or fingerprint. Also, if a back-end process initiates the request, such as auto discovery, then the session attempt always fails and no attempt to obtain administrative acceptance is initiated. In such cases, any data the MARS Appliance would normally ascertain from the device during such a session is not collected. This delay of data retrieval does not apply to syslogs forward to the MARS Appliance by the reporting device and it resumes once the new certificate is accept. The recommended method for manually kicking off the change detections is to use the Test Connectivity or Discover button on the reporting device.
- **Always prompt on new and changed.** This options requires an administrator to manually accept the certificate or fingerprint before MARS can establish the desired communications each time the certificate or fingerprint changes. During changes, the internal log includes the username of the account used to accept the change. If the communication times out before administrative intervention, the communication fails and an internal system log records the failure to accept the changed certificate or fingerprint.

The implication of each option varies based on which MARS service is attempting the connection, not in the enforcement of the option, but in the ability of the service to prompt for immediate administrative intervention. In other words, if the service is a GUI-based services, you will be prompted to accept the changed certificate or fingerprint. If the service is a backend service, the communications with the target device will fail and the event will be logged.

The following services and operations are affected by the global certificate/fingerprint response setting:

- Upgrade (SSL). When MARS uses the HTTPS option to download the upgrade package from the remote server specified on the Admin > System Maintenance > Upgrade page.
- Discovery operation. (SSH)
- Test Connectivity operation. (SSL)
- Cisco IDS, IPS, and IOS IPS router Event Processing (RDEP or SDEE over SSH)
- CSM Policy Query Integration (SSL)
- Qualys Report Discovery. (SSL)

- Graphgen process for mitigation operation (SSH and SSL)
- Device Monitor process for resource monitoring feature (SSH)
- DTM process (SSH)

Setting the Global Certificate and Fingerprint Response

The default response is to accept the certificate or fingerprint the first time MARS attempts to connect to the device, after which if a conflict is detected, then administrative intervention is required to update to the new certificate or fingerprint.

If this option is not the one that you wish to use, you can select from three options. The global setting for the conflict detection responses is located on the **Admin > System Parameters > SSL/SSH Settings** page.

To change the default certificate and fingerprint response, follow these steps:

Step 1 Log into the web interface using an account with Administrative privilege.

Step 2 Click the **Admin > System Parameters > SSL/SSH Settings**.

Step 3 Select one of the following options to define the global behavior that you require:

- Automatically always accept
- Accept first time and prompt when changed
- Always prompt on new and changed

For details on these options, see Understanding Certificate and Fingerprint Validation and Management, page 25-7.

Step 4 Click **Submit**.

Upgrading from an Expired Certificate or Fingerprint

If you have selected a global response option other than Automatically always accept (see Setting the Global Certificate and Fingerprint Response, page 25-9), you will at some time be required to update an expired certificate or fingerprint.

Two options exist for upgrading from an expired certificate or fingerprint. If you are logged in to the web interface when a GUI process detects a certificate or fingerprint conflict, you will be prompted to accept or reject the new value. Otherwise, if you are not logged in or a backend process detects the conflict, you must manually initiate a communication with the device. To determine the list of devices for which you must manually update the certificates or fingerprints, review the Activity: CS-MARS Detected Conflicting Certificates/Fingerprints report (see Monitoring Certificate Status and Changes, page 25-10).

The following procedures explain how to upgrade under the specific circumstances:

- Upgrade a Certificate or Fingerprint Interactively, page 25-10
- Upgrade a Certificate Manually, page 25-10
- Upgrade a Fingerprint Manually, page 25-10

Upgrade a Certificate or Fingerprint Interactively

An interactive upgrade refers to responding to a web interface prompt to update the certificate. This type of upgrade is available when you are logged into the GUI and a process, such as graphgen, prompts you to upgrade a certificate or fingerprint that conflicts with the previously accepted value. Click Yes to accept the new fingerprint or certificate.

Upgrade a Certificate Manually

A manual upgrade allows you to upgrade any certificate at any time due to any reason: session time out during interactive prompt, user error, detection of conflict by a backend process.

To manually upgrade to a new certificate, follow these steps:‘

Step 1 Log into the web interface using an account with Administrative privilege.

Step 2 Select the reporting device on the Admin > System Setup > Security and Monitor Devices page for which MARS has detected a certificate conflict. and click **Edit**.

Step 3 Click **Test Connectivity**.

The dialog box displays stating “Do you want to accept following certificate for the device named: <device_name>?.

Step 4 Verify the certificate value.

Step 5 If the value is correct. click **Yes**.

Upgrade a Fingerprint Manually

A manual upgrade allows you to upgrade any fingerprint at any time due to any reason: session time out during interactive prompt, user error, detection of conflict by a backend process.

To manually upgrade a fingerprint, follow these steps:

Step 1 Log into the web interface using an account with Administrative privilege.

Step 2 Select the reporting device on the Admin > System Setup > Security and Monitor Devices page for which MARS has detected a fingerprint conflict and click **Edit**.

Step 3 Click **Discover**.

The dialog box displays stating “Do you want to accept following fingerprint for the device named: <device_name>?.

Step 4 Verify the fingerprint value.

Step 5 If the value is correct, click **Yes**.

Monitoring Certificate Status and Changes

To support the certificate management features in MARS, the following system inspection rule exists:

- **System Rule: CS-MARS Failure Saving Certificates/Fingerprints.** This inspection rule indicates that MARS has failed to save a new or changed device SSL certificate or SSH key fingerprint based on either explicit user action or automatic accept as specified on the SSL/SSH Settings page.

In addition, the following reports appear under the System: CS-MARS Issue category.

- Activity: CS-MARS Accepted New Certificates/Fingerprints
- Activity: CS-MARS Accepted Conflicting Certificates/Fingerprints
- Activity: CS-MARS Detected Conflicting Certificates/Fingerprints
- Activity: CS-MARS Accepted New Certificates/Fingerprints'
- Activity: CS-MARS Failure Saving Certificates/Fingerprints
- Activity: CS-MARS Device Connectivity Errors

Hardware Maintenance Tasks—MARS 100E, 100, 200, GCM, and GC

Replacing the Lithium Cell CMOS Battery

This section pertains only to the MARS 100, 100E, 200, GCM, and GC appliances.

Note Take proper electrostatic discharge (ESD) measures before physically touching the appliance.

If the CMOS battery needs replacement, follow these steps:

Step 1 Turn the appliance's power off.

Step 2 Unplug the appliance from the wall electrical socket.

Step 3 Locate the lithium cell CMOS battery.

Step 4 Remove it.

Step 5 Set the new battery in its place.

Step 6 Plug the appliance into the electrical socket in the wall.

Step 7 Turn the appliance's power on.

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

Hard Drive Troubleshooting and Replacement

This section comprises the following subsections:

Note The term HDD is sometimes used throughout this section in place of hard disk drive, disk, or hard drive.

Status Lights

Depending on the model of the appliance, each hard drive has two status lights under or next to the drive. The following states can be determined based on the status lights:

- A steady green light indicates that the drive is functioning normally.
- A blinking orange light indicates that the drive is performing I/O operations.
- No light indicates that the disk has no power.

Partition Checking

The appliance automatically runs checks on different partitions of the hard drive after the system has been re-booted 25 to 30 times, or if the appliance has not been re-booted in 180 days.

Hotswapping Hard Drives

If a hard drive fails in the MARS 50, 100, 100e, 200, GC, or GCm appliance models, the MARS administrator receives an e-mail notification. The notification identifies the slot number of the failed hard drive.

Overview of MARS RAID 10 Subsystem

This section pertains only to the MARS 100, 100E, 200, GCM, and GC appliances.

The following MARS Appliances are equipped with a Parallel IDE/ATA Redundant Array of Inexpensive Disks (RAID) controller card:

- CS-MARS-100E-K9
- CS-MARS-100-K9
- CS-MARS-200-K9
- CS-MARS-GCM-K9
- CS-MARS-GC-K9

All other MARS appliances running software version 4.X or prior have software RAID controllers.

The MARS RAID controller cards operate the hard drives in a RAID 10 configuration, also called RAID 1+0 because it combines the data handling techniques of RAID 1 and RAID 0. For additional information on RAID concepts and terminology, access the following URL: http://en.wikipedia.org/wiki/RAID

RAID 0 Data Striping

In a MARS RAID 10 configuration, half the total number of drives are arrayed as a single logical drive, wherein a data block is distributed across all of the physical drives in the logical drive using RAID 0 striping techniques. Data striping results in better performance for a data intensive application such as MARS, because hard drive random access times are minimized when data is read and written simultaneously from more than one physical hard drive.

RAID 1 Mirroring and Subunits

The remaining drives in the MARS RAID 10 array mirror the RAID 0 virtual drive. Each physical drive in the RAID 0 array is mirrored by an identical physical drive using RAID 1 techniques. Data written to one of the drives within the RAID 0 array is simultaneously written to its dedicated RAID 1 partner, thereby providing fault tolerance through data redundancy.

A RAID 1 pair is termed a subunit. For example, an 8-drive Local Controller 200 has 4 RAID 1 subunits (8 drives in total), a 6-drive Local Controller 100 has 3 subunits (6 drives in total).

A subunit always comprises the same two hard drive slots. For instance, a MARS 110 or GC2 will always have the same pairings in a subunit, Slots 0 and 1, physical hard drive pairings

Rebuilding a Degraded Array

Either drive in a subunit can serve in place of its partner should either drive become degraded (unavailable, physically inoperative, or data corrupted). A physical drive degraded but still physically operative can be rebuilt from the data of its undegraded partner and rejoin the array. An inoperative physical drive can be replaced with an operative one which is then rebuilt to join the array.

When any physical drive of the RAID 10 array is degraded, the entire array is considered degraded. While the array still functions, it is not working to its optimal throughput or redundancy capacity.

In a degraded RAID 10 array, data destined for degraded physical drives are written to available space on other subunits until the degraded drives are rebuilt or replaced. Degraded drives are rebuilt in sequence, one rebuilding process must complete before the next process can begin. Between 90 minutes and 2 hours are required to rebuild a MARS subunit. The more data to rebuild, the more time is consumed.

Hotswapping and Field-Replaceable Hard Drives

A physical hard drive can be hotswapped, that is, replaced without rebooting the MARS appliance. Use the **hotswap** CLI command before removing or inserting a new hard drive.

Note To match original performance, hotswapped hard drives should be the same make, model and size as the original hard drives.

RAID Procedures for MARS Appliances 100E, 100, 200, GCM, and GC

This section pertains only to the MARS 100E, 100, 200, GCM, and GC appliances.

The raidstatus CLI command

The raidstatus CLI command reports the current status of the RAID 10 array. Example 25-1 displays the output of the raidstatus command executed on a Local Controller 200. Table 25-1 describes the relevant output fields.

Example 25-1 Example of raidstatus CLI Command Output

```
[PNADMIN]$ raidstatus

CONTROLLER: C0
-------------
DRIVER:   1.02.00.037
MODEL:    7506-8
FW:       FE7X 1.05.00.068
BIOS:     BE7X 1.08.00.048
MONITOR:  ME7X 1.01.00.040
SERIAL #: L14104A5090383
PCB:      REV4
PCHIP:    1.30-66
ACHIP:    3.20


# OF UNITS: 1
UNIT 0: RAID 10 931.54 GB ( 1953580032 BLOCKS): REBUILDING (75%)

# OF PORTS: 8
PORT 0: WDC WD2500JB-19GVA0 WD-WCAL73129135 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 1: WDC WD2500JB-19GVA0 WD-WCAL73291174 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 2: WDC WD2500JB-19GVA0 WD-WCAL73157538 232.88 GB (488397168 BLOCKS)
: OK(NO UNIT)
PORT 3: WDC WD2500JB-98GVA0 WD-WMAL72243570 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 4: WDC WD2500JB-00GVA0 WD-WCAL73883655 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 5: WDC WD2500JB-19GVA0 WD-WCAL73290905 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 6: WDC WD2500JB-98GVA0 WD-WCAL73693347 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
PORT 7: WDC WD2500JB-98GVA0 WD-WMAL72244432 232.88 GB (488397168 BLOCKS)
: OK(UNIT 0)
UNIT /C0/U0
---------------------
STATUS:        REBUILDING
UNIT TYPE:     RAID 10
STRIPE SIZE:   64K
SIZE:          931.54 GB (1953580032 BLOCKS)
# OF SUBUNITS: 4

SUBUNIT 0:    RAID 1: OK

SUBUNIT 0:    CBOD: OK
PHYSICAL PORT: 7
LOGICAL  PORT: 0

SUBUNIT 1:    CBOD: OK
PHYSICAL PORT: 4
LOGICAL  PORT: 1

SUBUNIT 1:    RAID 1: REBUILDING (1%)
```

```
SUBUNIT 0:    CBOD: DEGRADED
PHYSICAL PORT: 6
LOGICAL  PORT: 0

SUBUNIT 1:    CBOD: OK
PHYSICAL PORT: 3
LOGICAL  PORT: 1

SUBUNIT 2:    RAID 1: DEGRADED

SUBUNIT 0:    CBOD: OK
PHYSICAL PORT: 5
LOGICAL  PORT: 0

SUBUNIT 1:    CBOD: OK
PHYSICAL PORT: 0
LOGICAL  PORT: 1
SUBUNIT 3:    RAID 1: OK

SUBUNIT 0:    CBOD: OK
PHYSICAL PORT: 1
LOGICAL  PORT: 0

SUBUNIT 1:    CBOD: OK
PHYSICAL PORT: 0
LOGICAL  PORT: 1
```

Table 25-1 Explanation of Output Fields for raidstatus CLI Command

Output Field	Description
`FW:  FE7X 1.05.00.068`	Indicates version of controller card firmware.
`STATUS:  REBUILDING`	Current status of entire array. • **OK**—The array and subunits are in good order and operating at optimal efficiency. • **Rebuilding**—A subunit is being rebuilt. Array efficiency is not yet optimal. • **Degraded**—At least one physical disk in the array cannot be accessed.
`# OF UNITS: 1 UNIT 0: RAID 10 931.54 GB ( 1953580032 BLOCKS): REBUILDING (75%)`	**Units**—Indicates the number of virtual drives the entire RAID configuration represents. In this case, the array acts as one virtual hard drive or unit. **Unit**—Identifies the RAID level, array size, and array status statistics of the specified unit. The total array size does not include the RAID overhead bytes. The status may be as follows: • **OK**—The array and subunits are in good order and operating at optimal efficiency. • **Rebuilding**—A subunit is being rebuilt. Array efficiency is not yet optimal. • **Degraded**—At least one physical disk in the array cannot be accessed. Troubleshooting is advised to prevent possible data loss.

Table 25-1 Explanation of Output Fields for raidstatus CLI Command (continued)

Output Field	Description
`# OF PORTS: 8`	Indicates the number of hard drives in the array.
`PORT 0: WDC WD2500JB-19GVA0 WD-WCAL73129135 232.88 GB (488397168 BLOCKS) : OK(UNIT 0)`	Indicates the model, serial number, size, and operational status of a hard drive related to the port. If a hard drive is not present or cannot be accessed, this output does not appear for that port. Table 25-2 lists how hard drive bays map to the port numbers.

`SUBUNIT 1: RAID 1: REBUILDING (1%)`
 	
`SUBUNIT 0: CBOD: DEGRADED`
`PHYSICAL PORT: 6`
`LOGICAL PORT: 0`
 	
`SUBUNIT 1: CBOD: OK`
`PHYSICAL PORT: 3`
`LOGICAL PORT: 1`
	A MARS RAID 10 configuration comprises multiple RAID 1 subunits, each RAID 1 subunit configured with two drives. The MARS 100 and 100e appliances have subunits numbered 0,1, and 2. MARS 200 appliances and Global Controllers have subunits 0,1,2, and 3.
	
	The two drives in each RAID 1 subunits have unique physical port numbers.
	
	The RAID 1 subunit status values are as follows:
	• **OK**—The subunit is in good order and operating at optimal efficiency.
	• **Rebuilding**—The subunit is being rebuilt, efficiency is not yet optimal.
	• **Degraded**—At least one physical disk in the array cannot be accessed.
	
	The rebuild processes can take between 90 minutes and two hours to complete, depending on the amount of data on the disk. Subunits are rebuilt one subunit at a time. The percentage complete indicator tells you which subunit is currently being rebuilt.
	
	The **Physical Port** number appears as N/A when the associated drive bay is empty.
	
	Individual drive status is shown in the **CBOD:** field. CDBOD status can be OK or DEGRADED.

Correlating Hard Drive Slots to RAIDSTATUS Command Physical Port Numbers

This section pertains only to the MARS 100E, 100, 200, GCM, and GC appliances.

Figure 25-4 shows how the hard drive slot numbers are ordered in MARS LC-200, GC, or GCM. Hard drive slot numbers increase from left to right, and from top to bottom. Figure 25-5 shows slot numbering for the Local Controller 100 and 100E.

The MARS CLI identifies hard drives by port numbers or physical port numbers, which are logical designations assigned by the operating system. Table 25-2 shows how the hard drive slots in the chassis correspond to the port and physical port numbers as reported in the CLI.

Note A port number is the same as a physical port number.

Table 25-2 Mapping Hard Drive Slot Number to CLI Physical Port Number

MARS Appliance	Storage Capacity[1]	Hard Drive Slot to Port Number
MARS 100E, 100	• 750 GB • RAID 10 6 x 250 GB Drives • Hot-swappable	Slot **6** is Port **0** Slot **5** is Port **1** Slot **4** is Port **2** Slot **3** is Port **3** Slot **2** is Port **4** Slot **1** is Port **5**
MARS 200, GCM, GC	• 1 TB • RAID 10 8 x 250 GB Drives • Hot-swappable	Slot **8** is Port **0** Slot **7** is Port **1** Slot **6** is Port **2** Slot **5** is Port **3** Slot **4** is Port **4** Slot **3** is Port **5** Slot **2** is Port **6** Slot **1** is Port **7**

1. The stated storage capacity is the sum of the rated capacity of all the hard drives and does reflect bytes reserved for the RAID overhead on each drive.

Figure 25-4 Hard Drive Slot Numbering for MARS Local Controller 200 and Global Controllers

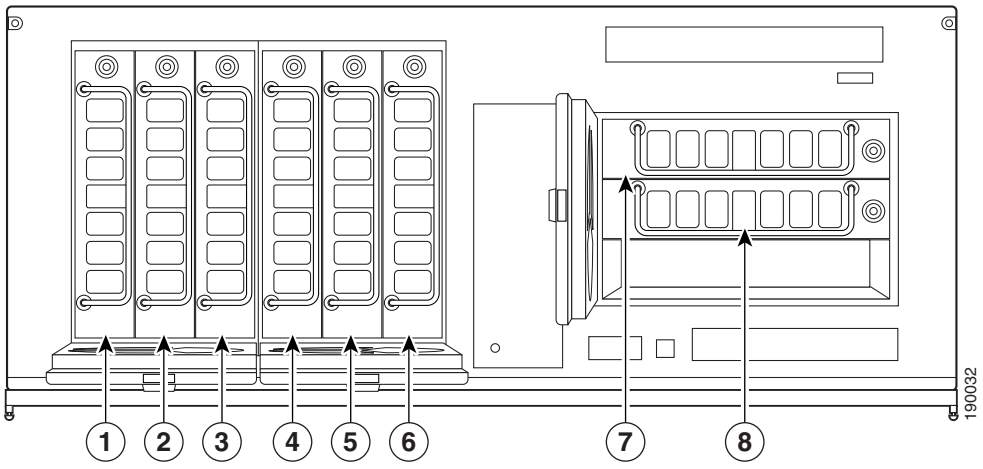
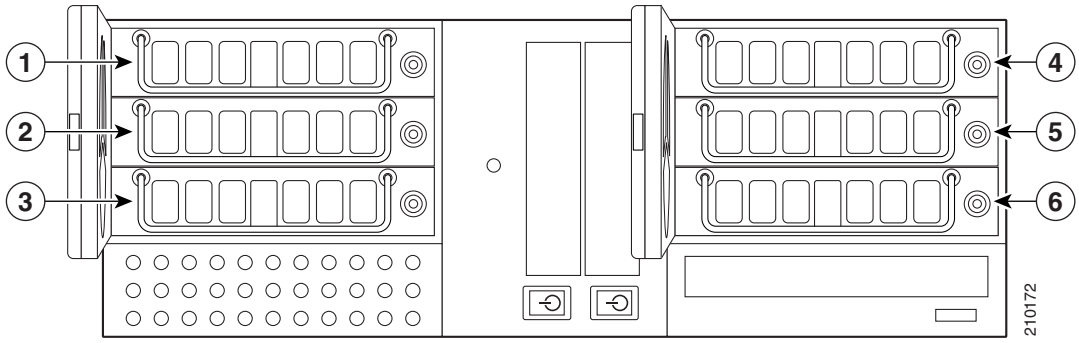


Figure 25-5 Hard Drive Slot Numbering for the Local Controller 100 and 100E



Hotswap Procedure To Remove and Add a Hard Drive

This section pertains only to the MARS 100E, 100, 200, GCM, and GC appliances.

Use the **hotswap** {**add** | **remove**} *disk* CLI command before you remove and before you insert a hard drive.

Note The **hotswap** command specifies the hard drive slot number in the chassis. The **raidstatus** CLI command refers to port numbers and physical port numbers. See Table 25-2 to map hard drive slot numbers to port numbers (a port number is the same as a physical port number).

Step 1 Establish a console connection with MARS.

Step 2 At the CLI prompt, enter **hotswap remove** *disk,* where *disk* is the hard drive slot number of the hard drive to remove.

A message informs you that it is safe to remove the hard drive.

Note Make sure that you remove the correct physical hard drive. If you remove the wrong one accidently then reinsert it, that drive will register as a degraded drive.

Step 3 Unlock the MARS drive bay door with the supplied key.

Note A ring with two keys is supplied in the MARS 100, 100e, 200, and Global Controller accessory kits, one key is for the hard drives and one is for the drive bay doors.

Step 4 Unlock the drive you want to replace with the supplied key.

Step 5 Pull out the hard drive.

Step 6 At the CLI prompt, enter **hotswap add** *disk*. Be sure to use the same slot number (*disk*) as in Step 2.

A message informs you that the hard drive (disk) is added successfully (to the logical array).

Step 7 Insert the new Cisco field-replaceable hard drive unit.

Step 8 Lock the hard drive into place.

Step 9 Close and lock the drive bay door.

Step 10 From the CLI, enter **raidstatus**.

The subunit with the slot number of the replaced hard drive should indicate that the RAID subunit is rebuilding, though the physical port number indicates the drive is degraded. This process can last from 90 minutes and 2 hours depending on the amount of data.

Note Verify the system has completed rebuilding the new hard drive before you hotswap another hard drive. The RAID subsystem rebuilds only one disk at a time. If the hotswapped drive does not rebuild after a couple of hours, rebuild the array with the RAID Controller utility, as explained in the section, "Rebuilding an Array with the RAID Utility."

This ends the Hotswap Procedure To Remove and Add a Hard Drive.

Hotswap CLI Example

This section pertains only to the MARS 100E, 100, 200, GCM, and GC appliances.

The following CLI output example hotswaps a hard drive in drive slot 6 (port 2) of a MARS 200. Physical port 2 remains degraded until RAID subunit 2 is rebuilt.

Example 25-2 Hotswap Procedure, CLI Output Example

```
[pnadmin]$ hotswap remove 6
removing port /c0/p2 ... Done.
Disk 6 can now be safely removed from the system.

pnadmin]$ hotswap add 6
rescanning controller /c0 for units and drives ...Done.
Rebuild started on unit /c0/u0
Disk 6 has been added to the system successfully.


[pnadmin]$ raidstatus
Controller: c0
--------------
Driver:   1.02.00.037
Model:    7506-8
FW:       FE7X 1.05.00.068
BIOS:     BE7X 1.08.00.048
Monitor:  ME7X 1.01.00.040
Serial #: L14104A5090383
PCB:      Rev4
PCHIP:    1.30-66
ACHIP:    3.20


# of units: 1
Unit 0: RAID 10 931.54 GB ( 1953580032 blocks): REBUILDING (64%)

# of ports: 8
Port 0: WDC WD2500JB-19GVA0 WD-WCAL73129135 232.88 GB (488397168 blocks)
: OK(unit 0)
Port 1: WDC WD2500JB-19GVA0 WD-WCAL73291174 232.88 GB (488397168 blocks)
: OK(unit 0)
Port 2: WDC WD2500JB-19GVA0 WD-WCAL73157538 232.88 GB (488397168 blocks)
: OK(unit 0)
Port 3: WDC WD2500JB-98GVA0 WD-WMAL72243570 232.88 GB (488397168 blocks)
```

```
: OK(unit 0)
Port 4: WDC WD2500JB-00GVA0 WD-WCAL73883655 232.88 GB (488397168 blocks)
: OK(unit 0)
Port 5: WDC WD2500JB-19GVA0 WD-WCAL73290905 232.88 GB (488397168 blocks)
: OK(unit 0)
Port 6: WDC WD2500JB-98GVA0 WD-WCAL73693347 232.88 GB (488397168 blocks)
: OK(unit 0)
Port 7: WDC WD2500JB-98GVA0 WD-WMAL72244432 232.88 GB (488397168 blocks)
: OK(unit 0)
Unit /c0/u0
---------------------
Status:        REBUILDING
Unit Type:     RAID 10
Stripe Size:   64k
Size:          931.54 GB (1953580032 blocks)
# of subunits: 4

Subunit 0:    RAID 1: OK

    Subunit 0:    CBOD: OK
    Physical Port: 7
    Logical  Port: 0

    Subunit 1:    CBOD: OK
    Physical Port: 4
    Logical  Port: 1

Subunit 1:    RAID 1: OK

    Subunit 0:    CBOD: OK
    Physical Port: 6
    Logical  Port: 0

    Subunit 1:    CBOD: OK
    Physical Port: 3
    Logical  Port: 1

Subunit 2:    RAID 1: REBUILDING (6%)

    Subunit 0:    CBOD: OK
    Physical Port: 5
    Logical  Port: 0

    Subunit 1:    CBOD: DEGRADED
    Physical Port: 2
    Logical  Port: 1

Subunit 3:    RAID 1: OK

    Subunit 0:    CBOD: OK
    Physical Port: 1
    Logical  Port: 0

    Subunit 1:    CBOD: OK
    Physical Port: 0
    Logical  Port: 1
```

Procedures for the MARS RAID Utility

This section pertains only to the MARS 100E, 100, 200, GCM, and GC appliances.

MARS Appliances equipped with a hardware RAID controller can configure the RAID 10 array with the 3ware Disk Array Configuration Utility, referred to as the RAID Utility in this document.

To access the RAID Utility you must have a direct console connection to MARS with an attached keyboard and external monitor.

Press **Alt-3** when the ***** <Press Alt-3 to access 3ware Configuration Screen ***>** message appears at the beginning of the bootup process. Table 25-3 briefly describes only those tasks that are relevant to the MARS RAID 10 hard drive arrays.

Table 25-3 RAID Utility Tasks and Procedures

Task Scenario	Procedure
If the **hotswap** command fails when replacing a drive, rebuild the array with the RAID utility.	Rebuilding an Array with the RAID Utility
If the **hotswap** command fails *and* the RAID utility rebuild fails, add the replacement drive with the RAID Utility.	Add a Replacement Drive to the Array with the RAID Utility
If during a reboot, MARS cannot find available drives, rebuild the array with the RAID Utility.	Delete and Create the RAID 10 Array

Caution Creating a disk array overwrites all data on those disks.

Rebuilding an Array with the RAID Utility

Perform this procedure when the **raidstatus** command indicates that MARS has not completed rebuilding a subunit of the RAID array after two hours. This procedure assumes the replacement hard drive is free of physical defects that prevent its operation.

Step 1 Establish a direct console connection to MARS with a keyboard and an external monitor.

Note You can access the RAID utility only with a direct console connection.

Step 2 Reboot the MARS Appliance. Press **Alt-3** to access the RAID utility when the following message appears:

***** <Press Alt-3 to access 3ware Configuration Screen ***>**

The 3ware Disk Array Configuration utility (RAID Utility) home screen appears.

Step 3 Read the help bar at the bottom of the screen for instructions on how to use the interface.

Step 4 Select **Array Unit 0**. The status of the array is Degraded if one of the drives in an array is degraded.

A selected item is marked with an asterisk in the leftmost column.

Step 5 Select **Rebuild Array** then press **F8** to complete.

Tip Within the RAID utility, you can use the following keystrokes to highlight the corresponding GUI button:
Alt-C—Create Array
Alt-D—Delete Array
Alt-M—Maintain Array
Alt-R—Rebuild Array

Step 6 Press **Y** to confirm. MARS exits the RAID utility and resumes the bootup process.

Step 7 At the CLI prompt, verify with the **raidstatus** command that the RAID array subunit is rebuilding.

If the subunit does not rebuild within two hours, delete the array and add the replacement drive with the RAID utility as described in the section "Add a Replacement Drive to the Array with the RAID Utility."

This ends the Rebuilding an Array with the RAID Utility procedure.

Add a Replacement Drive to the Array with the RAID Utility

This section pertains only to the MARS 100E, 100, 200, GCM, and GC appliances.

Perform this procedure when a hotswap attempt and the RAID Utility Rebuild procedure have failed.

Step 1 Insert the replacement drive into the hard drive slot.

Step 2 Establish a direct console connection to MARS with a keyboard and an external monitor.

Note You can access the RAID Utility only with a direct console connection.

Step 3 Reboot the MARS Appliance. Press **Alt-3** to access the RAID utility when the following message appears:

***** <Press Alt-3 to access 3ware Configuration Screen ***>**

The 3ware Disk Array Configuration utility (RAID Utility) home screen appears.

Step 4 Read the help bar at the bottom of the screen for instructions on how to use the RAID Utility interface.

Step 5 Select **Array Unit 0**—position the cursor over the text and press Enter.

A selected item is marked with an asterisk in the leftmost column.

Step 6 Select **Delete Array**, and press Enter.

A screen appears listing the ports and the hard drives of the array that will be deleted.

Tip Within the RAID utility, you can use the following keystrokes to highlight the corresponding GUI button:
Alt-C—Create Array
Alt-D—Delete Array
Alt-M—Maintain Array
Alt-R—Rebuild Array

Note When an array is deleted, the data is lost.

Step 7 Select **OK** and press Enter.

The "Available Drives:" screen appears listing all hard drives available to include in an array. The replacement drive should appear in this list.

Step 8 Select all the drives—position the cursor over the text and press Enter.

Step 9 Select **Create Array** and press Enter.

The RAID configuration options appear.

Step 10 Select the following RAID options:

- RAID Configuration—**10**
- Write Cache Status—**disable**
- Stripe Size—**64 KB**

Step 11 Select **OK** then press Enter.

The "Disk Arrays:" screen appears listing all the ports and drives in Array Unit 0.

Step 12 Press **F8** to complete.

Step 13 Press **Y** to confirm.

MARS exits the RAID utility and resumes the bootup process.

Step 14 At the MARS CLI prompt, use the **raidstatus** command to verify the following conditions:

- The full complement of ports are reported
- All RAID 0 subunits are shown as OK or REBUILDING
- All RAID 1 subunits are OK

A degraded physical port at this stage can indicate a defective hard drive, and improperly inserted hard drive, a loose hard drive cable connection, or a defective RAID controller card.

An array that has not completed rebuilding in two hours could indicate a defective RAID controller card.

This ends the Add a Replacement Drive to the Array with the RAID Utility procedure.

Delete and Create the RAID 10 Array

This section pertains only to the MARS 100E, 100, 200, GCM, and GC appliances.

Perform this procedure if MARS indicates that it cannot find the hard drives, you are reimaging MARS with a DVD, or the RAID Utility failed to add a replacement drive.

Step 1 Establish a direct console connection to MARS with a keyboard and an external monitor.

Note You cannot access the RAID utility with any other type of console connection.

Step 2 Shutdown the MARS Appliance with the **shutdown** CLI command.

Step 3 Powerup the MARS Appliance. Press **Alt-3** to access the RAID utility when the following message appears:

***** <Press Alt-3 to access 3ware Configuration Screen ***>**

The 3ware Disk Array Configuration utility home screen appears.

Step 4 Read the help bar at the bottom of the screen for instructions on how to use the RAID Utility interface.

Step 5 Select **Array Unit 0**.

A selected item is marked with an asterisk in the leftmost column.

Step 6 Select **Delete Array**.

A message appears listing the ports of the array that will be deleted.

Tip Within the RAID utility, you can use the following keystrokes to highlight the corresponding GUI button:
Alt-C—Create Array
Alt-D—Delete Array
Alt-M—Maintain Array
Alt-R—Rebuild Array

Note When an array is deleted, the data is lost.

Step 7 Select **OK** and press Enter.

The "Available Drives" screen appears listing all drives available for inclusion in an array.

Step 8 Select all of the drives. To select a drive, move the cursor over a drive and press Enter.

An asterisk in the leftmost column indicates the drive is selected.

Step 9 Select **Create Array** and press Enter.

The RAID configuration options appear.

Step 10 Select the following RAID options:

- RAID Configuration—**10**
- Write Cache Status—**disable**
- Stripe Size—**64 KB**

Step 11 Select **OK** then press Enter.

The "Disk Arrays:" screen appears listing all the drives in Array Unit 0.

Step 12 If you are reimaging with a DVD, insert the DVD now.

Step 13 Press **F8** to complete.

Step 14 Press **Y** to confirm.

MARS exits the RAID utility and resumes the bootup or reconfiguration process.

Step 15 At the MARS CLI prompt, use the **raidstatus** command to verify the following conditions:

- The full complement of ports are reported
- All RAID 0 subunits are shown as OK or REBUILDING
- All RAID 1 subunits are OK

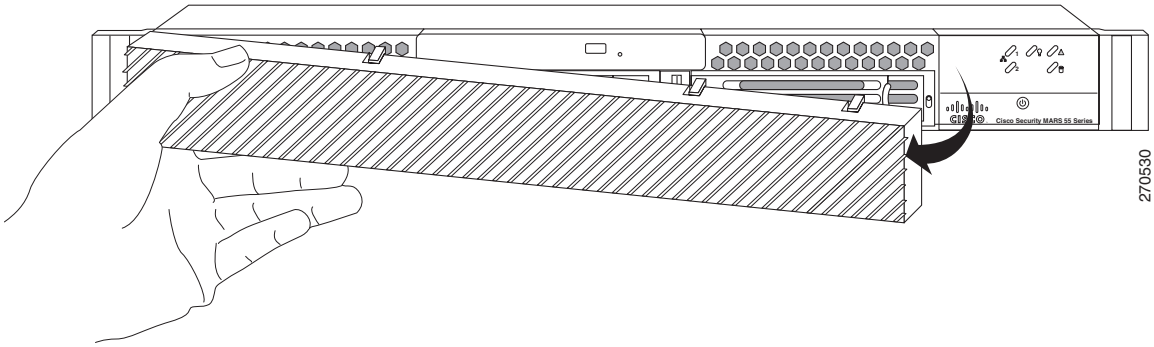
A degraded physical port at this stage can indicate a defective hard drive, and improperly inserted hard drive, a loose hard drive cable connection, or a defective RAID controller card.

An array that has not completed rebuilding in two hours could indicate a defective RAID controller card.

This ends the Delete and Create the RAID 10 Array procedure.

To remove the MARS 55 bezel, support the left-side hinge with your hand, pull the bezel from the right-hand side, swing open, then gently detach left-hand side from hinge, as shown in Figure 25-6.

Figure 25-6 Removing the Front Bezel from a MARS 55



Note The MARS 55 does not do RAID 0 striping. It is RAID 1 only.

Note MARS 55, one drive mirrors the other in a simple RAID 1 configuration. For Release 5.3.2 and more recent, the **hotswap list all** CLI command displays the physical slot number to PD and Port Number layout in ASCII art.

Figure 25-7 HDD Slot Numbers —