



CHAPTER 6

Backup, Recover, Restore, and Standby Server Options

Revised: November 7, 2008, OL-16776-01

This chapter describes the backup and recovery components of MARS, as well as how to configure a secondary standby server.

- [Configuring and Performing Appliance Data Backups, page 6-1](#)
- [Recovery Management, page 6-16](#)
- [Configuring a Standby or Secondary MARS Appliance, page 6-23](#)
- [Guidelines for Restoring, page 6-23](#)
- [Configure the Cygwin SFTP Server on Windows, page 6-11](#)

Configuring and Performing Appliance Data Backups

You can archive data from a MARS Appliance and use that data to restore the operating system (OS), system configuration settings, dynamic data (event data), or the complete system. The appliance archives and restores data to and from an external network-attached storage (NAS) system using the network file system (NFS) or Secure FTP (SFTP) protocols. While you cannot schedule when the data backup occurs, the MARS Appliance performs a configuration backup every morning at 2:00 a.m. and events are archived every hour. The configuration backup can take several hours to complete.

When archiving is enabled, dynamic data is written twice: once to the local database and once to the archive server. As such, the dynamic data that is archived includes only the data that is received or generated *after* you enable the data archive setting. Therefore, we recommend that you enable archiving before configuring your appliance to receive audit events from reporting devices.

You can use the same server to archive the data for more than one MARS Appliance; however, you must specify a unique directory in the path for each appliance that you want archive. If you use the same base directory, the appliances overwrite each others' data, effectively corrupting the images.



Note

For the complete list of supported NFS and SFTP servers, see:

- http://www.cisco.com/en/US/products/ps6241/products_device_support_tables_list.html

Each MARS Appliance seamlessly archives data using an expiration date that you specify. When the MARS internal storage reaches capacity, it automatically purges the data in the oldest partition of the local database, roughly 10% of the stored event and session data. The data in the NFS or SFTP file share has a life span specified in days. Therefore, to keep a year's worth of data, you would specify 365 days as the value for the Remote Storage Capacity (in Days) field. All data older than 365 days is purged from the archive file.

When planning for space requirements, use the following guidance: Estimate 6 GB of storage space for one year's worth of data, received at a sustained 10 events/second. This estimate assumes an average of 200 Bytes/event and a compression factor of 10, both realistic mean values. In addition to capacity planning, plan the placement of your archive server to ensure a reliable network connection that can transmit 10 MB/second exists between the archive server and the MARS Appliance. You should consider using the eth1 interface to avoid high-traffic networks that might introduce latency and to ensure that the backup operation is not competing with other operations in the MARS Appliance. Also, define a default route to the archive server on the MARS Appliance and that you verify any intermediate routers and firewalls allow for multi-hour NFS or SFTP connections to prevent session timeouts during the backup operation.

**Note**

Data archiving is local to a given appliance. When you configure data archiving on a Global Controller, you are archiving the data for that appliance; you cannot configure the Global Controller to archive data from Local Controllers that it monitors.

For more information on the uses and format of the archived data, see the following topics:

- [Typical Uses of the Archived Data, page 6-2](#)
- [Format of the Archive Share Files, page 6-3](#)
- [Archive Intervals By Data Type, page 6-4](#)
- [Guidelines for Restoring, page 6-23](#)
- [pnrestore, page 1-57](#)

To configure data archiving, you must perform the following procedures:

1. Configure the NFS server or SFTP server
 - [Configure the NFS Server on Windows, page 6-5](#)
 - [Configure the NFS Server on Linux, page 6-9](#)
 - [Configure the NetApp NFS Server, page 6-9](#)
 - [Configure the Cygwin SFTP Server on Windows, page 6-11](#)
2. (NFS only) [Configure Lookup Information for the NFS Server, page 6-11](#)
3. [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#)
4. [Access the Data Within an Archived File, page 6-15](#)
5. [Troubleshooting Data Archiving, page 6-16](#)

Typical Uses of the Archived Data

While the primary use of an archive is to restore the appliance in response to a catastrophic software failure, the archived data provides the following alternate uses:

- Use **Admin > System Maintenance > Retrieve Raw Messages** to analyze historical raw messages from periods that exceed the capacity of the local database. The data returned from raw message retrieval is simply the audit message provided by the reporting device. The raw message is just the message as sent by the reporting device, such as a syslog message. For more information, see [Retrieving Raw Messages, page 13-3](#).
- Manually view the archived event records, which are compressed using gzip. Viewing the data in this manner is faster than retrieving raw messages from either the local database or the archive. However, the record format is more complicated than the simple raw event returned by the Retrieve Raw Messages operation. It includes all the data necessary to restore the incidents and dependent data, including the raw message and the system data required to correlate that message with the session, device type, five tuple (source IP, destination IP, protocol, source port, and destination port), and all other data points. For more information, see [Format of the Archive Share Files, page 6-3](#) and [Access the Data Within an Archived File, page 6-15](#).
- Image a standby or secondary MARS Appliance to either swap into the network in the event of a hardware failure or to access full query and report features for historical time periods. For more information, see [Configuring a Standby or Secondary MARS Appliance, page 6-23](#), and [Guidelines for Restoring, page 6-23](#).

Format of the Archive Share Files

The MARS archive process runs daily at 2:00 a.m., and it creates a dated directory for its data. You cannot specify a different time to archive the data.

The `pnos` directory is where the operating system backup is stored.

```
06/12/2005 11:32p <DIR> .
06/12/2005 11:32p <DIR> ..
07/09/2005 01:30a <DIR> pnos      <-- OS Backup Directory
07/08/2005 04:49p <DIR> 2005-07-08<-- Daily Data Backup Directory
07/10/2005 12:09a <DIR> 2005-07-10
07/11/2005 12:12a <DIR> 2005-07-11
07/12/2005 12:12a <DIR> 2005-07-12
07/13/2005 12:16a <DIR> 2005-07-13
07/14/2005 02:02a <DIR> 2005-07-14
07/15/2005 02:02a <DIR> 2005-07-15
07/16/2005 02:02a <DIR> 2005-07-16
07/17/2005 02:02a <DIR> 2005-07-17
07/18/2005 02:02a <DIR> 2005-07-18
07/19/2005 02:02a <DIR> 2005-07-19
07/19/2005 09:46p <DIR> 2005-05-26
07/20/2005 07:16a <DIR> 2005-05-27
07/20/2005 07:17a <DIR> 2005-07-20
07/22/2005 12:13a <DIR> 2005-07-22
07/21/2005 12:09a <DIR> 2005-07-21
07/23/2005 12:15a <DIR> 2005-07-23
      0 File(s)          0 bytes
     58 Dir(s)  4,664,180,736 bytes free
```

Within each daily directory, subdirectories are created for each data type. The following example identifies the directory type in the comments.

Directory of D:\MARSBackups\2005-07-08

```
07/08/2005 04:49p <DIR> .
07/08/2005 04:49p <DIR> ..
07/08/2005 04:49p <DIR> CF<-- Configuration Data
07/08/2005 05:00p <DIR> IN<-- Incident Data
07/08/2005 05:16p <DIR> AL<-- Audit Logs
```

```

07/08/2005 05:16p <DIR> ST<-- Statistics Data
07/08/2005 05:16p <DIR> RR<-- Report Results
07/08/2005 05:49p <DIR> ES<-- Raw Event Data
          0 File(s)          0 bytes
          8 Dir(s)  4,664,180,736 bytes free

```

The .gz filename in the raw event data directory identifies the period of time that the archived data spans in a YYYY-MM-DD-HH-MM-SS format. The filename includes the following data [dbversion]-[productversion]-[serialno]_[StartTime]_[EndTime].gz. The following examples illustrate this format:

```

ix-5248-524-1171238692_2007-02-12-00-04-46_2007-02-12-01-04-51.gz
rm-5248-524-1171238692_2007-02-12-00-04-46_2007-02-12-01-04-51.gz

```



Note Files starting with “ix” are index files and those starting with “rm” contain the raw messages.

Directory of D:\MARSBackups\2005-07-08\ES

```

07/08/2005 05:49p <DIR> .
07/08/2005 05:49p <DIR> ..
07/08/2005 05:49p          34,861 es-3412-342_2005-07-08-16-49-52_2005-07-08-17-49-47.gz
07/08/2005 05:49p          31,828 rm-3412-342_2005-07-08-16-49-52_2005-07-08-17-49-47.gz
07/08/2005 06:49p          49,757 es-3412-342_2005-07-08-17-49-49_2005-07-08-18-49-40.gz
07/08/2005 06:49p          48,154 rm-3412-342_2005-07-08-17-49-49_2005-07-08-18-49-40.gz
07/08/2005 07:49p          24,420 es-3412-342_2005-07-08-18-49-45_2005-07-08-19-49-52.gz
07/08/2005 07:49p          22,346 rm-3412-342_2005-07-08-18-49-45_2005-07-08-19-49-52.gz
07/08/2005 08:50p          44,839 es-3412-342_2005-07-08-19-49-47_2005-07-08-20-50-04.gz
07/08/2005 08:50p          41,534 rm-3412-342_2005-07-08-19-49-47_2005-07-08-20-50-04.gz
07/08/2005 09:50p          58,988 es-3412-342_2005-07-08-20-49-55_2005-07-08-21-50-06.gz
07/08/2005 09:50p          54,463 rm-3412-342_2005-07-08-20-49-55_2005-07-08-21-50-06.gz
07/08/2005 10:50p         130,604 es-3412-342_2005-07-08-21-49-58_2005-07-08-22-50-08.gz
07/08/2005 10:50p          85,437 rm-3412-342_2005-07-08-21-49-58_2005-07-08-22-50-08.gz
07/08/2005 11:50p         114,445 es-3412-342_2005-07-08-22-49-55_2005-07-08-23-50-10.gz
07/08/2005 11:50p          58,240 rm-3412-342_2005-07-08-22-49-55_2005-07-08-23-50-10.gz
07/09/2005 12:50a         110,556 es-3412-342_2005-07-08-23-50-02_2005-07-09-00-50-14.gz
07/09/2005 12:50a          53,977 rm-3412-342_2005-07-08-23-50-02_2005-07-09-00-50-14.gz
          16 File(s)          964,449 bytes
           2 Dir(s)  4,664,164,352 bytes free

```

The following is an example of the data found in the configuration data directory.

Directory of D:\MARSBackups\2005-07-08\CF

```

07/08/2005 04:49p <DIR> .
07/08/2005 04:49p <DIR> ..
07/08/2005 02:02a          2,575,471 cf_2005-07-08-02-02-02.pna
          1 File(s)          2,575,471 bytes
          2 Dir(s)  4,664,164,352 bytes free

```

Archive Intervals By Data Type

MARS archives data either daily or in near real time based on the type of data. Therefore, all the data in the MARS internal storage (local database) should be in the archive server storage as well, give or take a day’s worth of specific types of data.

MARS data consists of four types:

1. configuration data, such as topology and device settings, which is archived daily

2. audit trails of MARS web interface activity and MARS report results, which are archived daily
3. MARS statistics, such as charts in Summary/Dashboard, which are archived hourly
4. dynamic and event data, such as events, sessions, and incidents, which are archived quickly so they do not tax the MARS Appliance's local storage.

Configuration data, audit trails, and static data is written to database first. During archival time, data is written to local files and archived from those files. However, dynamic and event data is written in parallel to both the database and to local files. Therefore, even if the data has been archived, it is likely to still be in the database.

In other words, dynamic and event data is initially stored in two locations: the archive server and MARS database. Later, when the MARS database partition becomes full, the database purge operation occurs to make room for new events—but those events and incidents were archived prior to the purge operation.

**Note**

Once data is purged from the MARS local database, it can not be queried. Queries and reports operate only on the data in the MARS database.

To account for temporarily unavailable archive servers, the files for all data types are stored locally on the MARS Appliance for one day before they are purged. When you enable archiving in the web interface, you must also define the parameters for retaining the data in the archive server. As a result, MARS performs simple data maintenance on the archive server by purging data outside the range specified in the Remote storage capacity in Days field of the Data Archiving page. For example, the storage capacity value is 365 days, then all data older than one year is purged from the archive server.

Refer to [Table 6-1](#) for the archive interval for each type of data.

Table 6-1 Archive Interval Description(4.3.1 and 5.2.4 and later)

Archive Folder and Data Type Description	Archive Interval	Max. Interval (in minutes)	Schedule
AL: Audit log information	Once per day at 2:00 a.m.	n/a	Daily at 2 a.m.
CF: Configuration information	Once per day at 2:00 a.m.	n/a	Daily at 2 a.m.
ES: Events, sessions, and raw messages	Every 10 minutes or when 3 MB (compressed) file size is reached, whichever threshold is met first.	10 minutes	n/a
IN: Incidents	Immediately	1 minute ¹	n/a
RR: Report results	Once per day at 2:00 a.m.		n/a
ST: Statistical data/counters information	Hourly.		n/a

1. If event rate is higher, archive interval for real time can be shorter than Max Interval.

Configure the NFS Server on Windows

Windows Services for UNIX (WSU) allows an NFS mount to be created on a Windows file server. This option is convenient and is often useful in a lab environments or when UNIX expertise is unavailable. The following URLs support the configuration of this complimentary download from Microsoft Corporation:

Windows Services for UNIX 3.5 Download and Resources (System Requirements, Reviewer's Guide, etc.)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=896c9688-601b-44f1-81a4-02878ff11778&DisplayLang=en>

Performance Tuning Guidelines for Microsoft Services for Network File System

<http://technet.microsoft.com/en-us/library/bb463205.aspx>

To install and configure the WSU 3.5 to operate with a MARS Appliance, perform the following tasks:

- [Install Windows Services for UNIX 3.5, page 6-6](#)
- [Configure a Share using Windows Services for UNIX 3.5, page 6-7](#)

Install Windows Services for UNIX 3.5

To configure the NFS server on a Windows server, follow these steps:

- Step 1** Log in to the Windows server using an account with either local or domain-level administrative privileges.



Note If you install the services using an account without administrative privileges, the archive process fails.

- Step 2** Download the Windows Services for UNIX 3.5.
- Step 3** To install the Windows Services for UNIX, double-click **SFU35SEL_EN.exe**.
- Step 4** Enter the folder where the program files should be extracted in the Unzip to folder field, and click **Unzip**. We recommend defining a new folder, not using the temp folder under the local profile. The unzip process can take several minutes.
- Step 5** Open the folder where you extracted the files, and double-click **SfuSetup.msi**.
- Step 6** Click **Next** to continue.
The Customer Information panel appears.
- Step 7** Enter values for the User name and Organization fields, and click **Next**.
The License and Support Information panel appears.
- Step 8** Select the **I accept the agreement** option, and click **Next**.
- Step 9** Select the **Custom Installation** option, and click **Next**.
- Step 10** At a minimum, you must select **Entire feature (including any subfeatures if any) will be installed on local hard drive** for the following components Under Windows Services for UNIX in the Components list, and then click **Next**:
- **NFS** (This option includes the Client for NFS and Server for NFS subfeatures.)
 - **Authentication tools for NFS** (This option includes the User Name Mapping, Server for NFS Authentication, and Server for PCNFS subfeatures.)



Note This procedure assumes that you have selected **Entire feature will not be available** for all components other than NFS and Authentication tools for NFS.

The Security Settings panel appears.

- Step 11** Verify that the Change the default behavior to case sensitive check box is *not selected*, and then click **Next**.
- As the MARS Appliance does not use a special account for NFS authentication, you do not need to change the default settings.
- Step 12** The User Name Mapping panel appears.
- Step 13** Verify that the Local User Name Mapping Server and Network Information Service (NIS) options are selected, and then click **Next**.
- A second User Name Mapping panel appears.
- Step 14** Enter values for the following fields, and then click **Next**:
- **Windows domain name.** We recommend accepting the default value, which is the local host name.
 - (Optional) **NIS domain name**
 - (Optional) **NIS server name**
- The Installation Location panel appears.
- Step 15** Enter the desired installation location and click **Next**.
- The Installing panel appears, presenting the progress of the installation. When the installation completes, the Completing the Microsoft Windows Services for UNIX Setup Wizard panel appears.
- Step 16** Click **Finish** to complete the installation and close the Setup Wizard.
- Step 17** Reboot the computer.
- You have successfully installed the required NFS components. Now you must define and configure a share to be used by the MARS Appliance for backups and archiving. For more information, see [Configure a Share using Windows Services for UNIX 3.5, page 6-7](#).
-

Configure a Share using Windows Services for UNIX 3.5

Configuring the share involves identifying the folder to share and specifying the correct permissions and access.

To configure WSU 3.5 as an NFS server for a MARS Appliance, follow these steps:

-
- Step 1** Start Windows Explorer on the Window host where you installed WSU 3.5.
- Step 2** Create the folder where you want the MARS archives to be stored.
- An example folder is *C:\MARSBackups*.
- Step 3** Right-click on the folder you created and click the **NFS Sharing** tab.
- Step 4** Select the **Share this folder** option, and enter a name in the Share name field.
- An example share name can be the same as the folder name, *MARSBackups*.
- Step 5** Select the **Allow Anonymous Access** check box.
- As the Windows server cannot directly authenticate the MARS Appliance, you *must* select this option.
- Step 6** Click **Permission**.
- The NFS Share Permissions dialog box appears.
- Step 7** Select **ALL MACHINES** under Name, and then select **No Access** from the Type of Access list.

- Step 8** Click **Add**.
- Step 9** Enter the IP address of the MARS Appliance, and click **OK**.
- Step 10** Select the IP address of the MARS Appliance, then select **Read-Write** from the Type of Access list. Ensure that **ANSI** is selected from the Encoding list.
- Step 11** Click **OK** to save your changes and close the NFS Share Permissions dialog box.
- Step 12** Click **Apply** to enable your changes.



Note If the Apply does not work, you did not reboot the server after installing WSU 3.5. To work around this issue, you must reboot the server and repeat this procedure.

- Step 13** From the DOS command window, enter the following commands:

```
cd <PathToParentOfShareFolder>
```

```
cacls <ShareFolderName> /E /G everyone:F
```

These commands modify the shared folder the permissions so that **Everyone** has local filesystem access to the folder. Example usage:

```
cd C:\archive
cacls MARSBackups /E /G everyone:F
```

- Step 14** Click **Start > Control Panel > Administrative Tools > Local Security Policy**
- Step 15** Under Local Security Policy > Security Options, double-click **Network Access: Let Everyone permissions apply to anonymous users**, select **Enabled**, and click **OK**.
- This option equates the Anonymous user to the Everyone user.
- Step 16** Configure exceptions for the required NFS ports in the Windows Firewall or other firewall application running on the server.
- Step 17** Reboot the server.
- You have completed the NFS configuration settings for the Windows server. To enable logging for debug purposes, continue with [Enable Logging of NFS Events, page 6-8](#). Otherwise, continue with [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#).
-

Enable Logging of NFS Events

For troubleshooting purposes, you can enable NFS Server logging on a Windows host that is running the Microsoft Windows Services for UNIX 3.5.

To enable NFS server logging on the Windows host, follow these steps:

-
- Step 1** Click **Start > All Programs > Services for UNIX Administration > Services for UNIX Administration**.
- Step 2** Under Services for UNIX, select **Server for NFS**.
- Step 3** Specify the folder where you want the log file to appear under Log events in this file:
By default the log file appears in C:\SFU\log directory.
- Step 4** Verify that all the check boxes are selected.

- Step 5** Click **Apply** to save your changes.
- Step 6** Continue with [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#).
-

Configure the NFS Server on Linux

NFS is supported natively on Linux file systems, which requires that you have a Linux box. Because a Linux file server can be built inexpensively, it is highly recommended that a file server be built and dedicated for MARS archived data.

This section presents an example configuration as guidance for configuring your NFS to archive the data for a MARS Appliance. For each MARS Appliance that you want to archive for a given NFS server, you must set up a directory on the NFS server to which the appliance can read and write. The following procedure identifies the steps required to accomplish this task.

To prepare a Linux NFS Server for archiving from a MARS Appliance, follow these steps:

- Step 1** Log in to the NFS server using an account with root permissions.
- Step 2** Create a directory for archiving data.

For example:

```
mkdir -p /archive/nameOfYourMARSBoxHere
chown -R nobody.nobody /archive
chmod -R 775 /archive
```



Note

Mode 770 works only for MARS Appliances running the same software generation (4.x or 5.x). Use 775 to support a mixed environment of 4.x to 5.3.x software and when performing migrations from 4.x to 5.3.x. Due to difference of UID/GID between the 4.x to 5.x releases, you must allow r-x so an appliance running 5.3.x can import from files exported by a 4.x appliance.

- Step 3** In the `/etc/exports` file, add the following line:
- ```
/archive/nameOfYourMARSBoxHere MARS_IP_Address(rw)
```
- Step 4** Restart the NFS service.
- ```
/etc/init.d/nfs restart
```
-

Configure the NetApp NFS Server

The NetApp NFS server differs from other Linux/UNIX NFS servers in that NetApp restricts the functionality of the shell environment running on the server. As such, you must use an external UNIX/Linux administrative host to change the permissions and ownership of the exported NFS directory.

Before You Begin

- To perform the tasks in this procedure, you must configure an external Linux/UNIX administrative host. For information on configuring such a host, refer to the documentation for your Network Appliance server.

To prepare the NetApp NFS server so that the MARS Appliance can archive to it, follow these steps:

Step 1 If you have not exported a directory on the NetApp NFS appliance, and perform the following task from the NetApp's web GUI.

- Connect to the NetApp administrative host (http://hostname/na_admin/).
- Click **FileView**, then click **NFS** on the menu in the left pane.
- If the exported directory already exists, click **Manage Exports** under NFS. Otherwise, click **Add Export** under NFS.
- Select the following options on the NFS Export Wizard page, and click **Next**:
 - Read-Write Access
 - Root-Access
 - Security

The NFS Export Wizard - Path page appears.



Note If you are using a temporary NetApp administrative host, you can disable the host's access to the exported directory. To do so, do not select the Root-Access option. This configuration disables access by the host to the exported NFS directory.

- Enter the path to the desired export directory in the Export Path field, and click **Next**.
The NFS Export Wizard - Read-Write Access page appears.
- Click **Add**, and enter the IP address of the MARS Appliance in the Host to Add field, and click **OK**.
- Click **Add**, and enter the IP address of the NetApp administrative host in the Host to Add field, click **OK**, and then click **Next**.
The NFS Export Wizard - Root Access page appears.
- Click **Add**, then enter the IP address of the NetApp appliance (or the IP address of the Linux/Unix server to serve this purpose) in the Host to Add field, click **OK**, and then click **Next**.
The NFS Export Wizard - Security page appears.
- Select the **Unix Style** option, and click **Next**.
The NFS Export Wizard - Commit page appears.
- Verify that the settings are correct, and then **Commit**.

Step 2 To change the permissions of the exported directory, enter the following commands on the NetApp administrative host:

```
mount NetAppIP:/PathToExport /mnt/YourMountPoint
```

```
chown nobody.nobody /mnt/YourMountPoint
```

```
chmod 775 /mnt/YourMountPoint
```

**Note**

Mode 770 works only for MARS Appliances running the same software generation (4.x or 5.x). Use 775 to support a mixed environment of 4.x to 5.3.x software and when performing migrations from 4.x to 5.3.x. Due to difference of UID/GID between the 4.x to 5.x releases, you must allow r-x so an appliance running 5.3.x can import from files exported by a 4.x appliance.

Step 3 To verify that `/mnt/YourMountPoint` directory is writable by anyone, enter the following command:

```
ls -l /mnt
```

Step 4 To unmount the directory, enter the following command:

```
umount /mnt/YourMountPoint
```

Step 5 Configure the MARS Appliance to use the path as archiving directory as described in [Configure the Data Archive Setting for the MARS Appliance](#), page 6-13.

Configure Lookup Information for the NFS Server

**Note**

These common guidelines apply to NFS servers running on either Linux or Windows.

Many services in the current Linux system, such as ssh and the NFS server, use nslookup to obtain the hostname of the client. If the nslookup operation fails, the connection may fail or take a long time to finish the negotiation.

For the pnarchive and pnrestore operations to succeed, the NFS server must obtain the hostname of the MARS Appliance using its IP address. You can ensure that it obtains this information by doing one of the following:

- Add the NFS client (MARS Appliance) info in `/etc/hosts` file on the NFS server. The hosts file is located at `WINDOWS\system32\drivers\etc\` on Windows servers.
- Add the MARS Appliance information to your DNS server.

During a typical restore process, the MARS Appliance is first re-imaged from the DVD, upgraded to the correct version of software, and then the restore operation is performed. During the DVD re-image process, the name of the appliance is changed to the factory default, which is **pnmars**. If you do not wish to change the name of the appliance *before* you attempt to restore it from the NFS server, be sure to add an entry for **pnmars** to the DNS server or in the `/etc/hosts` file on the NFS server so that during the restore operation, the NFS server can perform an IP address-to-hostname lookup for the MARS Appliance.

After the restore operation completes, the MARS Appliance will be restored to the name saved in the archived OS package. You should have included this name already in the DNS server or `/etc/host` file of the NFS server. Otherwise, this archive/restore operations may not function properly.

Configure the Cygwin SFTP Server on Windows

Cisco Security MARS supports SFTP servers as a storage medium for archiving or for data migration from 4.x to 6.0.1. This topic presents the steps require to configure Cygwin and OpenSSH on Windows. It targets Cygwin SFTP server on Windows XP.

**Note**

You must be logged in using an account with Administrator privileges on the Windows host to perform the tasks in this section.

Install the following packages as part of Cygwin:

- cygwin 1.5.25-12
- cygrunsrv 1.34-1
- openssh 5.0p1-1
- tcp_wrappers 0-7.6-4
- zlib 1.2.3-2

Once these packages are installed, perform the following steps:

Step 1 To CYGWIN as a System variable in Windows, right-click My Computer and select **Properties** on the shortcut menu.

Step 2 Click the **Advanced** tab, and then click **Environment Variables**.

Step 3 Do the following:

- Set value of CYGWin variable to **ntsec tty**
- Add **;c:\cygwin\bin** to end of PATH System variable.

Step 4 From a Command Prompt shell, enter the following command:

```
cygwin
```

Result: The Cygwin command prompt appears.

Step 5 At the Cygwin command prompt, enter the following command:

```
ssh-host-config -y
```

Step 6 You are prompted to enter the value of environment variable CYGWIN.

```
ntsec tty
```

Step 7 To verify the sshd service is installed, enter the following command:

```
cygrunsrv -L
```

Step 8 To start sshd, enter the following command:

```
cygrunsrv -S sshd
```

Step 9 To verify that sshd is running, enter the following command:

```
sftp <username>@localhost
```

Where *username* is the administrative account used to install Cygwin.

Step 10 Enter the password for the administrative user account.

Step 11 Enter the following command:

```
pwd
```

The working directory should be `/home/<username>`.



Note

When performing a migration from a MARS Appliance (or configuring the archive settings in the web interface), use the Windows user account used to install Cygwin to authenticate to the SFTP server. For details on performing the migration, see the **pnexp** and **pnimp** commands in the [Migrating Data from Cisco Security MARS 4.x to 6.0.1](#) document.

Configure the Data Archive Setting for the MARS Appliance

You can archive the data and the system software that is running on a MARS Appliance to a remote server. This data archival includes operating system (OS) and upgrade/patch data, system configuration settings, and dynamic data, such as system logs, incidents, generated reports, and the audit events received by the appliance. The feature provides a snapshot image of the appliance.



Note

While complete system configuration data is archived, the dynamic data that is archived includes only the data that is received or generated *after* you enable the data archive setting. Therefore, we recommend that you enable archiving before configuring your appliance to receive audit events from reporting devices.

Using archived data, you can restore your appliance in the event of a failure, as long as the data is not corrupted. In this capacity, data archiving provides an alternative to re-imaging your appliance with the Recovery DVD.

Before You Begin

You must set up the NFS server correctly to archive the appliance's data. See [Configure the NFS Server on Windows, page 6-5](#) or [Configure the NFS Server on Linux, page 6-9](#).

You must configure the basic network settings for the appliance.

To configure the data archive settings for a given MARS Appliance, follow these steps:

Step 1 Select **Admin > System Maintenance > Data Archiving**.

Step 2 Specify values for the following fields:

- **Archiving Protocol**—Select either NFS or SFTP
- **Remote Host IP**—enter the IP address of the remote server.
- **Remote Path**—Enter the export path on the remote SFTP server, NFS server, or a NAS system where you want to store the archive files.

For example, `/MARSBackups` would be a valid value for a Windows host with an NFS share named `MARSBackups`. The forward slash is required to resolve the UNC share name.


For SFTP Data Archiving, the **Remote Path** field can take an absolute or a relative path. An absolute path has a leading forward slash that specifies the absolute directory structure from the root directory of the archive server (for example, `/storage/jcn1a/5_3_5/PNARCHIVE`). Omitting the leading forward slash specifies a directory relative to the user's home directory on the archive server.

- **Remote storage capacity in Days**—enter one of the following values:

- The maximum number of days for which you want the archive server to retain data. The server keeps your data for the number of days previous to the current date.
- The number of days of data that the archive server can maximally retain. In other words, you are identifying the upward capacity of the archive server.
- **Username**—(SFTP only) Enter the Windows user account used to install Cygwin to authenticate to the SFTP server.
- **Password/Re-enter password**—(SFTP only) Enter the password associated with the account specified in the Username field.

Figure 6-1 Configuring SFTP Data Archiving

Data Archiving
 Status: **Running** ([less info](#))


Archiving Service: **Enabled**
 Remote Server: **Available** (Click  to check remote host current status)

Remote Server Settings (* denotes required field)

→ *Archiving Protocol:	SFTP
→ *Remote Host IP:	10 . 2 . 3 . 7
→ *Remote Path:	/storage/jonla/5_3_5/PNAR0
→ *Remote Storage Capacity in Days:	10
→ *Username:	
→ *Password:	
→ *Re-enter password:	

Figure 6-2 Configuring NFS Data Archiving

Data Archiving
 Status: **Running** ([less info](#))

Archiving Service: **Enabled**
 Remote Server: **Available** (Click  to check remote host current status)

Remote Server Settings (* denotes required field)

→ *Archiving Protocol:	NFS
→ *Remote Host IP:	10 . 2 . 3 . 7
→ *Remote Path:	/storage/jonla/5_3_5/PNAR0
→ *Remote Storage Capacity in Days:	10

Step 3 Click **Start** to enable archiving for this appliance.

**Note**

After starting archiving, if you see an error message such as “invalid remote IP or path,” your archive server is not correctly configured. If you receive these messages, consult [Configure the NFS Server on Windows, page 6-5](#), [Configure the NFS Server on Linux, page 6-9](#), or [Configure the Cygwin SFTP Server on Windows, page 6-11](#).

Result: A status page appears. Click **Back** to return to the Data Archiving page.

Step 4

If you need to change any values on this page, enter the value and click **Change**.

**Tip**

To stop archiving data, return to the Data Archiving page and click **Stop**.

Access the Data Within an Archived File

You can access the event data in an archived file allows to review the events contained therein. You may want to perform this task to verify the archive settings, to look at a particular time range of events, or to perform post processing on the data.

**Tip**

For other options on accessing archived data, see [Typical Uses of the Archived Data, page 6-2](#)

To access the data within an archived file, follow these steps:

Step 1

Perform the following command at the command line interface of the archive server:

```
cd <archive_path>
```

where *archive_path* is the remote path value specified in [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#).

Step 2

To select the archive to review, enter the following command:

```
cd <YYYY-MM-DD>
```

where *YYYY-MM-DD* is the date that the archive file was created.

Step 3

To view the list of archive files for the selected data, enter the following command:

```
cd ES ls -l
```

Step 4

To extract the data from the archive file, enter the following command:

```
gunzip <filename>
```

where *filename* is the name of the file to extract. The list of available files are based on a timestamp for when they were created.

Step 5

To view the file's contents, enter the following command:

```
vi <filename>
```

You can use any text editor or run scripts against the data in these files. However, you should not change the contents of these zipped files or leave extracted data or additional files in the archive folders. MARS cannot process new or extracted files when performing a restore operation.

Troubleshooting Data Archiving

Table 6-2 identifies possible errors and likely causes and solutions.

Table 6-2 Error Table for Archive Server and MARS Integration

Error/Symptom	Workaround/Solution
<p>Connection to remote archive server fails! (archive server IP: <address>, exported path: /<archive_server_path>)</p> <p>CS-MARS appliance cannot connect to the remote archive server that is set up for archiving the configuration and event data.</p> <p>Please verify that the connection of the archive server at IP: '<address>' to the CS-MARS appliance is OK and CS-MARS appliance has the write permission to the exported path: '/<archive_server_path>' on the archive server!</p>	<ul style="list-style-type: none"> The connection between the MARS Appliance and the archive server has failed. Verify the route is allowed between the two devices (ping the archive server from the MARS Appliance CLI) and verify the archive server is running. Verify that the exported path value is correct under Admin > System Maintenance > Data Archiving. <p>Note You will receive an e-mail every two minutes until the NFS connection issue is resolved.</p> <ul style="list-style-type: none"> Configure exceptions for required NFS ports in any firewall or port blocking software running on the archive server.

Recovery Management

MARS Appliance functionality includes two procedures that you can perform using the MARS Appliance Recovery DVD-ROM. The approach you should take to recover your appliance depends upon whether or not you have archived data that you want to recover as well. Two decisions affect how you will recover your MARS Appliance:

- **Re-Image a Global Controller or Local Controller.** The procedure for recovering an appliance is unique to the role that the appliance has in the STM system. Global Controllers require an additional operation on each monitored Local Controller.
- **Archived Data.** If you have been archiving data for the appliance that you wish to recover, there is an additional step following recovery of the appliance.



Caution

The recovery process erases the MARS Appliance hard disk drive. You permanently lose all configuration and event data that you have not previously archived or backed up. If possible, write down your license key before you re-image the appliance. You must provide this license key during the initial configuration following any re-image operation, and it is not restored as part of archived data.

The procedures, detailed in this section, are as follows:

- [Recovering a Lost Administrative Password, page 6-17](#)
- [Downloading and Burning a Recovery DVD, page 6-17](#)
- [Recovery the MARS Operating System, page 6-17](#)
- [Re-Imaging a Local Controller, page 6-19](#)
- [Re-Imaging a Global Controller, page 6-20](#)
- [Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-22](#)

Recovering a Lost Administrative Password

If you lose the password associated with the *pnadmin* account, you cannot recover the password. You must re-image the appliance, which resets the password to the factory defaults, as described in [Re-Imaging a Local Controller, page 6-19](#), and [Re-Imaging a Global Controller, page 6-20](#). If you have configured the MARS Appliance to archive data, as described in [Configuring and Performing Appliance Data Backups, page 6-1](#), you can also recover the configuration and event data using the procedure in [Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-22](#).

Downloading and Burning a Recovery DVD

If you do not have the MARS Appliance Recovery DVD-ROM that shipped with your MARS Appliance or you want to use a new image to expedite the post recovery upgrade process, you can download the current recovery image from the Cisco.com software download pages dedicated to MARS. You can access these pages at the following URLs, assuming you have a valid Cisco.com account and that you have registered your SMARTnet contract number for your MARS Appliance.

- Recovery images: <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-recovery>

After you download the ISO image, for example, *csmars-6.0.1.iso*, you must burn that file on to a DVD-ROM. The files are typically 1.42 GB or larger.

The following guidelines are defined:

- Use DVD+R, DVD+RW, or DVD-R and the correct media for either of those standards.
- Do not burn the DVD at a speed higher than 4X.
- To make a bootable DVD, you must burn the *.iso file onto the DVD using the bootable ISO DVD format; just copying the file to DVD does not make it bootable. Do not copy the *.iso file to a DVD; instead, you must extract it onto the DVD using your burner software. Most DVD burner software has a burn image function that extracts the files and makes the DVD bootable.

Recovery the MARS Operating System

For MARS 25, 55, 110, 210, GC2, and their variant models, the MARS operating system (OS) is stored separate from the MARS application and event data. It is stored on a flash disk-on-module (DOM) drive in the appliance. With the OS and application separation, if the MARS application hangs due to a RAID failure, you can login from a remote host and still retrieve log and trace data to assist in identifying the root cause of the failure.

The flash drive corrupts when, for example, system libraries or executable files are missing or are the wrong sizes as reported during a consistency checks or when the previous configuration is lost. When a corruption occurs, you will see symptoms like a failure to boot or to deploy the previous configuration, not able to execute certain commands, failures during the file system consistency check, or errors reporting missing files.

If the flash becomes corrupted, you can restore the OS using a Recovery DVD. For information on creating a Recovery DVD, see [Downloading and Burning a Recovery DVD, page 6-17](#). The recovery operation restores the MARS OS without prompting for installation option information, such as the model or role (Global Controller vs. Local Controller). The flash drive is also stores the system configuration data (IP addresses, DNS configuration settings, host name, and license file). During an OS recovery, the daily backup of the configuration data is copied from the hard drive to the flash drive so you configuration can be reapplied, eliminating any appliance configuration or licensing.

Before You Begin

- Ensure that the release number of the Recovery DVD matches the operating system running on your appliance. Issues may result if a DVD of an earlier release is used to recover a appliance running a newer release. The DVD does not checks the versions to prevent this issue.
- During the OS recovery operation, the system configuration data is copied from the hard drive to the flash drive. The system configuration data is created as part of the daily backup operation and is created nightly at 2:00 A.M. If your appliance has not been running long enough to back up the system configuration, then the OS is restored but the configuration is not.
- If you changed your system network settings (DNS, IP address, or hostname) after the last nightly backup, you must manually (using the [ifconfig, page 1-29](#), [hostname, page 1-25](#), and the [dns, page 1-11](#) commands) correct the settings once the OS recovery operation completes.

To recovery the operating system for your MARS Appliance, follow these steps:

-
- Step 1** Connect your monitor to the MARS Appliance's VGA port and your keyboard to the PS/2 keyboard port. (To view a diagram of the MARS Appliance VGA and serial ports, refer to the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide*.)
- Step 2** Disconnect any connected network cables from the eth0 and eth1 ports.
- Step 3** Put the Recovery DVD in the MARS Appliance DVD-ROM drive.
- Step 4** Do one of the following:
- Log in to the MARS Appliance as pnaadmin and reboot the system using the **reboot** command
 - Power cycle the MARS Appliance
- Result:* The following message displays on the console:
- ```
Please Choose A MARS Model To Install...
1. Distributed Mars - Local Controller
2. Distributed Mars - Global Controller
3. Mars Operating System Recovery
4. Quit
```
- Step 5** Using the arrow keys, select **3. Mars Operating System Recovery** at the Recover menu and press **Enter**.
- Result:* The OS binary download to the appliance begins. This process takes approximately 15 minutes. After the image download is complete, the Recovery DVD is ejected and the following message appears on the console:
- ```
Please remove the installation CD and press Reboot to finish the installation.
```
- Step 6** Remove the Recovery DVD from the MARS Appliance.

Step 7 Press **Enter** to restart the MARS Appliance.

Result: The MARS Appliance reboots and synchronizes the configuration information between the flash drive and the hard drive.

Step 8 Reconnect any network cables to the eth0 and eth1 ports.

Because the OS recovery does not affect configuration data or event data, the system should be accessible with no further configuration requirements.

Re-Imaging a Local Controller

Use the MARS Appliance Recovery DVD-ROM to re-image the Local Controller if necessary. This operation destroys all data and installs a new image. In addition to preparing the device and later restoring any archived data, you must also perform three time-consuming appliance recovery phases:

- Image downloading from the CD (about 30 minutes)
- Image installation after the download (about 90 minutes)
- Basic system configuration (about 5 minutes)



Caution

Performing this procedure destroys all data stored on the MARS Appliance.

Before You Begin

- (Models 20/20R, 50, 100/100e, 200, GC/GCm) Write down your license key before you re-image the appliance. You must provide this license key during the initial configuration following the re-image operation.
- (Models 25/25R, 55, 110/110R, 210, GC2/GC2R) You must provide the license file during the initial configuration following the re-image operation.

To re-image your Local Controller, follow these steps:

Step 1 Connect your monitor to the MARS Appliance VGA port and your keyboard to the PS/2 keyboard port. (To view a diagram of the MARS Appliance VGA and serial ports, refer the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide*.)

Step 2 Disconnect any connected network cables from the eth0 and eth1 ports.

Step 3 Put the Recovery DVD in the MARS Appliance DVD-ROM drive.

Step 4 Do one of the following:

- Log in to the MARS Appliance as padmin and reboot the system using the **reboot** command
- Power cycle the MARS Appliance

Result: The following message displays on the console:

```
Please Choose A MARS Model To Install...
1. Distributed Mars - Local Controller
2. Distributed Mars - Global Controller
3. Mars Operating System Recovery
4. Quit
```

Step 5 Using the arrow keys, select **1. Distributed MARS — Local Controller** at the Recover menu and press **Enter**.

Step 6 (100/100e or 110/110R only) Do one of the following:

- If you are re-imaging a MARS 100 or 100e, the following message appears on the console.

```
Please Choose Which MARS 100 Model To Install...
1. MARS100
2. MARS100E
3. Quit
```

Using the arrow keys, select the proper model based on the license you purchased and press **Enter**.

- If you are re-imaging a MARS 110 or 110R, the following message appears on the console.

```
Please Choose Which MARS 110 Model To Install...
1. MARS110
2. MARS110R
3. Quit
```

Using the arrow keys, select the proper model based on the license you purchased and press **Enter**.

Result: The image download to the appliance begins. This process takes approximately 15 minutes. After the image download is complete, the Recovery DVD is ejected and the following message appears on the console:

```
Please remove the installation CD and press Reboot to finish the installation.
```

Step 7 Remove the Recovery DVD from the MARS Appliance.

Step 8 Press **Enter** to restart the MARS Appliance.

Result: The MARS Appliance reboots, performs some configurations, including building the Oracle database. The configurations that occur after the first reboot take a significant amount of time (between an hour and an hour and a half), during which there is no feedback; this is normal system behavior.

Step 9 Reconnect any network cables to the eth0 and eth1 ports.



Note

After re-imaging the appliance, you must once again perform initial configuration of the MARS Appliance. For detailed instructions, see [Chapter 2, “Initial MARS Appliance Configuration.”](#)

Step 10 After the initial configuration is complete, do one of the following:

- Add any devices to be monitored to the Local Controller. For more information, see *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*.
- Recover the previously archived data using the procedure in [Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-22](#)

Re-Imaging a Global Controller

Use the MARS Appliance Recovery DVD ROM to re-image the Global Controller if necessary. This operation destroys all data and installs a new image. In addition to preparing the device and later restoring any archived data, you must also perform four time-consuming appliance recovery phases:

- Purge all Global Controller data from each monitored Local Controller. (See [Before You Begin, page 6-21](#).)
- Image downloading from the CD (about 30 minutes)
- Image installation after the download (about 45 minutes)

- Basic system configuration (about 5 minutes)

To re-image your Global Controller, follow these steps:



Caution

Performing this procedure destroys all data stored on the MARS Appliance.

Before You Begin

- (Models 20/20R, 50, 100/100e, 200, GC/GCm) Write down your license key before you re-image the appliance. You must provide this license key during the initial configuration following the re-image operation.
- (Models 25/25R, 55, 110/110R, 210, GC2/GC2R) You must provide the license file during the initial configuration following the re-image operation.
- Before you can re-image a Global Controller, you must purge the data that the Global Controller pushed down to the Local Controllers that it monitors. For each Local Controller that is monitored by the Global Controller that you want to recover, execute the following command at the command line interface of each Local Controller.

```
pnreset -g
```

This command clears the global inspection rules and user accounts from the Local Controller, which prepares it to be managed by the re-imaged Global Controller. However, it does not remove the global user groups; instead they are renamed (appended with a date) and converted to local user groups. You can edit or delete these empty groups after the reset. Because user groups are often used as recipients for rule notifications, they are not deleted to avoid invalidating the Action definition of such rules.

- Step 1** After you have executed the **pnreset -g** command on each Local Controller as described in [Before You Begin, page 6-21](#), connect your monitor to the MARS Appliance VGA port and your keyboard to the PS/2 keyboard port. (To view a diagram of the MARS Appliance VGA and serial ports, refer to the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide*.)
- Step 2** Disconnect any connected network cables from the eth0 and eth1 ports.
- Step 3** Put the Recovery DVD in the MARS Appliance DVD-ROM drive.
- Step 4** Do one of the following:
- Log in to the MARS Appliance as pndadmin and reboot the system using the **reboot** command
 - Power cycle the MARS Appliance

Result: The following message displays on the console:

```
Please Choose A MARS Model To Install...
1. Distributed Mars - Local Controller
2. Distributed Mars - Global Controller
3. Mars Operating System Recovery
4. Quit
```

- Step 5** Using the arrow keys, select **2. Distributed MARS — Global Controller** at the Recover menu and press **Enter**.

Result: The image download to the appliance begins. After the image download is complete, the Recovery DVD is ejected and the following message appears on the console:

```
Please remove the installation DVD and press Reboot to finish the installation.
```

Step 6 Remove the Recovery DVD from the MARS Appliance.

Step 7 Press **Enter** to restart the MARS Appliance.

Result: The MARS Appliance reboots, performs some configurations, including building the Oracle database. The configurations that occur after the first reboot take a significant amount of time, during which there is no feedback; this is normal system behavior.

Step 8 Reconnect any network cables to the eth0 and eth1 ports.



Note

After re-imaging the appliance, you must once again perform initial configuration of the MARS Appliance. For detailed instructions, see [Chapter 2, “Initial MARS Appliance Configuration.”](#)

Step 9 After the initial configuration is complete, do one of the following:



Note

You cannot add or monitor a Local Controller using the Global Controller until the Global Controller is running the same MARS software version as the Local Controllers it will be used to monitor.

- Add all Local Controllers back into the Global Controller. All devices and topology information are pulled up from each Local Controller into the Global Controller. For more information, see *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*.
- **(Recommended)** Recover the previously archived data using the procedure described in [Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-22](#).

Restoring Archived Data after Re-Imaging a MARS Appliance

When you restore a MARS Appliance using archived data, you are restoring the system to match the data and configuration settings found in the archive. The configuration data includes the operating system, MARS software, license key, user accounts, passwords, and device list in effect at the time the archive was performed.



Caution

The version of MARS software running on the appliance to be restored must match the version recorded in the archive. For example, if the data archive is for version 4.1.4, you must reimage the MARS Appliance to version 4.1.4, not older or newer, before using the **pnrestore** command to recover the system configuration and events.

For additional information on how the archives are restored, see [Guidelines for Restoring, page 6-23](#).



Note

If you choose to restore from your archived data, you must re-enter all devices on the Local Controller that are missing from the archive file. To restore existing cases, you must restore incident and session data. See [pnrestore, page 1-57](#), for more information on types of data and restore modes.

If you have archived your data and you have recovered your MARS Appliance as described in either [Re-Imaging a Local Controller, page 6-19](#), or [Re-Imaging a Global Controller, page 6-20](#), perform the following steps:

Step 1 When the recovery process is complete, restore the MARS Appliance from the last archived data by executing the following command:

```
pnrestore -p <ArchiveServerIP>:/<archive_path>
```

Where *ArchiveServerIP* is the value specified in the Remote Host IP field and *archive_path* is the value specified in the Remote Path field in the settings found in the web interface at **Admin > System Maintenance > Data Archiving**. You must identify the archive server by IP address, separated by a */* and then the pathname *ArchiveServerIP:/archive_path*. For more information on these settings, see [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#).

Step 2 When the restore operation completes, you may need to delete, re-enter, and re-discover all the devices that are missing from the MARS archive file.

Configuring a Standby or Secondary MARS Appliance

You cannot run queries and reports or perform incident investigation over archived data directly. To perform any kind of investigation using archived data, you must restore that data to a MARS Appliance. Therefore, we recommend that you configure a secondary appliance for this purpose. The reason to use a separate appliance to study old data is that you must restore the period data to the appliance, and the restore re-images all configuration and event data based on the archive settings for the defined period.

To restore to a secondary appliance, you must restore to an appliance of the same model or higher. For example, you can restore an image from a MARS 20 to a MARS 20, MARS 50, MARS 100, or MARS 100e; however, you *cannot* restore a MARS 50 to a MARS 20. Restoring to a secondary appliance differs from restoring to the actual appliance that performed the archive. The following issues must be addressed when restoring to a secondary appliance:

- You must purchase a new license key for the secondary appliance. Each license key is associated with the serial number of the appliance to which it is assigned.
- You must enter that new license key on the restored image before you can log into the secondary appliance.
- When restoring the image to the secondary appliance, you need to take the primary appliance off the network or perform the operation behind a gateway that can perform NAT. When the secondary appliance comes up and you are on the same network, you receive an IP address conflict error, because the IP address assigned to the secondary appliance exactly matches that of the primary.

Because a single image of the complete system configuration data is archived and updated daily, no matter what period you select from an archive, the system configuration data includes the most recent changes. In other words, selecting a period that is 365 days old affects only the event data. The system configuration that is restored mirrors that of the most current archive.

For more guidance, see [Guidelines for Restoring, page 6-23](#).

Guidelines for Restoring

When you do restore to an appliance, keep in mind the following guidelines:

- The version of MARS software running on the appliance to be restored must match the version recorded in the archive. For example, if the data archive is for version 4.1.4, you must reimage the MARS Appliance to version 4.1.4, not older or newer, before using the **pnrestore** command to recover the system configuration and events.

**Caution**

The **pnrestore** command does not check to ensure that the same version requirement is met, and it will attempt to restore an incorrect version match.

- All restore operations take a long time. Time varies based on the options you select. See [pnrestore, page 1-57](#).
- A restore of configuration data only takes less time.
- A restore operation does not allow for incremental restores of event data only. It always performs a complete reimage of the harddrive in the target appliance.
- All configuration information, including the license key, IP addresses, hostname, stored certificates and fingerprints, user accounts, passwords, and DNS settings, are always restored.
- If restoring to an appliance other than the one that created the archive, see [Configuring a Standby or Secondary MARS Appliance, page 6-23](#).
- When restoring to an appliance different from the one that archived the data, you must enter the license key assigned to the serial number of the new appliance before you access the restored data.
- A restore is performed from the day you specify forward until the archive dates are exhausted. The date argument of the **pnrestore** command should be the name of the daily data backup directory that identifies the start of the time range to be restored. See [Format of the Archive Share Files, page 6-3](#).
- To restore a specific range of days, we recommend temporarily moving the unwanted days at the end of the range out of the archive folder. This technique of trimming out unwanted days can also speed up the restore, although you do lose the dynamic data from those dates.
- If the data contained in the selected restore range of the archive exceeds the capacity of the local database on the target MARS Appliance, the MARS Appliance automatically purges the data in the oldest partition of the local database and then resumes the restore operation. As such, you should select a reasonable range of dates when performing the restore. Nothing is gained from restoring ranges that exceed the local database limits, and the overall restore operation is slowed by the intermittent purging of the oldest partition until the most current date is restored.
- Mode 5 of the **pnrestore** command restores from a backup in the local database; you cannot use it to restore from a NFS or SFTP archive. As such, you do not need to have archiving enabled to perform this restore operation. The configuration data is backed up every night on the appliance. Beware that if you upgrade to a newer release and attempt a restore before that configuration has been backed up, the restore will fail. See [pnrestore, page 1-57](#), for more information on types of data and restore modes.
- If a Global Controller requires re-imaging, you should perform a **pnrestore** operation to recover the data after it is reimaged (assuming you have archived it). This approach is recommended because:
 - All global data defined on the Global Controller and propagated to each managed Local Controller is not pushed back to the Global Controller, so restoring it from an archived configuration file is the only method of recovering these configuration settings and accounts.
 - Incidents and report results that were pushed to the Global Controller before it was reimaged are not pushed back after reimaging. When running on a Global Controller, the archive operation only archives reports, which can be restored. However, all old incidents are permanently lost on the Global Controller, as they are not archived.

- Regardless of how the Global Controller is restored, re-image or restore, the Local Controllers must be cleaned of Global Controller configuration data, which is accomplished by performing a **pnreset -g** operation on each Local Controller.
 - The **pnreset -g** operation must be completed on each Local Controller before attempting to restore the Global Controller.
-

