Maintaining Your Cisco WAAS System

This chapter describes the tasks to perform to maintain your Cisco WAAS system.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco WAAS Central Managers and Cisco Wide Area Application Engines (WAEs) in your network. The term WAE refers to WAE and WAVE appliances, and Cisco Virtual WAAS (vWAAS) instances.

This chapter contains the following sections:

Upgrading the Cisco WAAS Software

This section contains the following topics:

Operating Guidelines for Upgrading the Cisco WAAS Software

Consider the following guidelines when you upgrade your Cisco WAAS software:

- As shown in , upgrading is supported only from certain older releases to a particular release. If you have a Cisco WAAS device that is running a release from which upgrading to the desired release is not supported, first upgrade the device to an intermediate supported release and then to the final desired release.

When you perform a software upgrade using the Cisco WAAS Central Manager, there is only a limited system check to verify the support of the target Cisco WAAS version. To ensure that you have a successful Cisco WAAS upgrade, use Table 14-1 to verify that the target version is supported for your system.

For more information on Cisco WAAS software versions, see *Release Note for Cisco Wide Area Application Services*.

Table 1: Upgrade Paths to Cisco WAAS Version 6.4.3x

Current Cisco WAAS Version	Cisco WAAS Central Manager Upgrade Path	Cisco WAAS Upgrade Path
5.5.3 and later	Upgrade directly to 6.4.3x	Upgrade directly to 6.4.3x
4.3.x through 5.5.1	**1.** Upgrade to 5.5.3, 5.5.5x (5.5.5, 5.5.5a), or 5.5.7x **2.** Upgrade to 6.4.3x	**1.** Upgrade to 5.5.3, 5.5.5x, or 5.5.7x **2.** Upgrade to 6.4.3x
4.2.x	**1.** Upgrade to version 4.3.x through 5.4.x **2.** Upgrade to 5.5.3 or 5.5.5x (5.5.5, 5.5.5a), or 5.5.7x **3.** Upgrade to 6.4.3x	**1.** Upgrade to version 4.3.x through 5.4.x **2.** Upgrade to 5.5.3, 5.5.5x, or 5.5.7x **3.** Upgrade to 6.4.3x

- We recommend that all the devices in your Cisco WAAS network run the same version of the Cisco WAAS software. If some of your Cisco WAAS devices are running different software versions, the Cisco WAAS Central Manager should be the latest version. For details on Cisco WAAS version interoperability limitations, see the *Release Note for Cisco Wide Area Application Services*.
- If the Cisco WAAS Central Manager detects any registered Cisco WAE devices that are at a higher version level than the current one, it raises a minor alarm to alert you. Additionally, the Cisco WAE devices are shown in red on the device listing page.
- The Cisco WAAS Central Manager running Cisco WAAS Version 5.4.1 can manage Cisco WAE devices running Cisco WAAS Version 4.3.1 and later. However, some Cisco WAAS Central Manager windows with Cisco Version 5.4.1 features will not be applicable to Cisco WAAS devices that are running a version earlier than Cisco WAAS Version 5.4.1. If you modify this configuration, the configuration is saved, but it does not affect the earlier-version devices until these are upgraded to Cisco WAAS Version 5.4.1.
- If you are upgrading from a Cisco WAAS Version earlier than Cisco WAAS Version 6.1.1x to Cisco WAAS Version 6.x and use virtual blade, the upgrade procedure may get stuck in the Proceeding with Download phase. To remedy this scenario, follow these steps:

  1. To remove the Cisco WAAS device registration record and its configuration on the Cisco WAAS Central Manager, on the Cisco branch device, run the **cms degister** EXEC command.
  2. Wait ten minutes.
  3. To enable synchronization of the Cisco WAAS network configuration of the Cisco WAAS device with the local Cisco WAAS CLI configuration, on the Cisco WAAS branch device, run the **cms enable** EXEC command.

4. Using the Cisco WAAS Central Manager, install the specified Cisco WAAS 6.x version.

- Cisco WAAS Version 5.4.x is not supported running in a mixed-version Cisco WAAS network with any Cisco WAAS device that is running a Cisco WAAS version earlier than Cisco WAAS 4.3.1.

  Consider these upgrade guidelines:

  - If you have Cisco WAAS devices running versions earlier than Cisco WAAS Version 4.3.1, you must first upgrade these devices to Cisco WAAS Version 4.3.1, or a later version, before you install version Cisco WAAS Version 5.2 on the Cisco WAAS Central Manager.
  - Do not upgrade any Cisco WAAS device to a version later than the existing Cisco WAAS Central Manager version.
  - After all the Cisco WAAS devices are upgraded to Cisco WAAS Version 4.3.1 or later, you can begin the upgrade to Cisco WAAS Version 5.4.1 on the Cisco WAAS Central Manager.
  - Directly upgrading a device from Cisco WAAS Version 4.0, Version 4.1 or Version 4.2 to Cisco WAAS Version 5.4.1 is not supported.

Before Starting the Upgrade:

- Disable WCCP on all Cisco WAEs in an AppNav cluster. After upgrade is complete, confirm the following before you re-enable WCCP.
  - The Cisco WAEs are up and running.
  - The AppNav cluster is re-converged properly.
  - All disks are ready (not initializing).
  - There are no alarms on the device.
  - The **show accelerator** EXEC command shows all enabled Application Optimizers are healthy.

    After you have confirmed that each of these is complete, re-enable WCCP.

Checklist for Upgrading the Cisco WAAS Software

The Table 2: Checklist for Upgrading the Cisco WAAS Software table highlights the tasks needed to upgrade the Cisco WAAS software. In addition, consider these guidelines:

- To downgrade or roll back the Cisco WAAS software to a lower version, first downgrade or roll back the Cisco WAE devices' version, then the standby Central Manager (if applicable), and finally the primary Cisco WAAS Central Manager. For more information about downgrading, see the Release Note for Cisco Wide Area Application Services.
- You cannot downgrade an Cisco ENCS 5400-W device to a Cisco WAAS software version lower than 6.4.1, either from a device or a device group level. A warning message is displayed if you attempt to downgrade.

Table 2: Checklist for Upgrading the Cisco WAAS Software

Task	Additional Information and Instructions
1. Determine the current software version running on your Cisco WAAS network.	Check the software version that you are currently using so when you go to Cisco.com, you know if there is a newer version to download. For more information, see Determining the Current Software Version.
2. Obtain the new Cisco WAAS software version from **cisco.com**.	Visit **cisco.com** to download a newer software version and place this file on a local FTP or HTTP server. For more information, see Obtaining the Latest Cisco WAAS Software Version.
3. Register the new software version with the Cisco WAAS Central Manager.	Register the URL of the new software file so the Cisco WAAS Central Manager knows where to go to access the file. For more information, see Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI.
4. Upgrade all your Cisco WAAS Central Managers and Cisco WAAS devices.	Upgrade the Standby and Primary Cisco WAAS Central Managers. For more information, see Upgrading the Cisco WAAS Central Manager. After upgrading the Cisco WAAS Central Manager, upgrade all your Cisco WAAS devices that are members of a device group. For more information, see Upgrading Multiple Devices Using Device Groups.
5. Delete the software version file.	After completely upgrading your Cisco WAAS network, you can remove the software file if desired. For more information, see Deleting a Software File .

Determining the Current Software Version

To view the current software version running on a particular device, choose **Devices > All Devices**. The **All Devices** window displays the software version for each listed device.

You can also click **Devices >** *device-name* or the **Edit** icon next to the name of a device in the **Devices** window. The **Device Dashboard** window appears, listing the software version for that device.

Note The software version is not upgraded until a software upgrade is successfully completed. If a software upgrade is in progress, the version number displayed is the base version, not the upgraded version number.

Alternatively, in the device context, choose **Monitor > CLI Commands > Show Commands**. Choose the version and click **Submit**. A secondary window is displayed with the CLI output for the **show version** EXEC command.

Obtaining the Latest Cisco WAAS Software Version

Procedure

Step 1 Launch your web browser and access the Cisco Software Download page:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Choose **Application Networking Services > Wide Area Application Services > Cisco Wide Area Application Services (WAAS) Software** download area.

Step 3 Choose the Cisco WAAS software version that you want and download the appropriate software image.

Step 4 Register the location of the software file in the WAAS Central Manager GUI, as described in Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI, on page 5.

Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI

Before you begin

To upgrade your Cisco WAAS software, you must first specify the location of the Cisco WAAS software file in the Cisco WAAS Central Manager GUI and configure the software file settings.

There are two types of Cisco WAAS software files:

- **Universal**: Includes Cisco WAAS Central Manager, Application Accelerator, and AppNav Controller functionality. You can use this type of software file to upgrade a device operating in any mode.
- **Accelerator only**: Includes Application Accelerator and AppNav Controller functionality only. You can use this type of software file to upgrade only an Application Accelerator or AppNav Controller device. If you want to change an Application Accelerator or AppNav Controller to a Central Manager, you must install the Universal software file, reload the device, change the device mode to central-manager, and then reload the device again. Additionally, kdump analysis functionality is not included in the Accelerator only image.

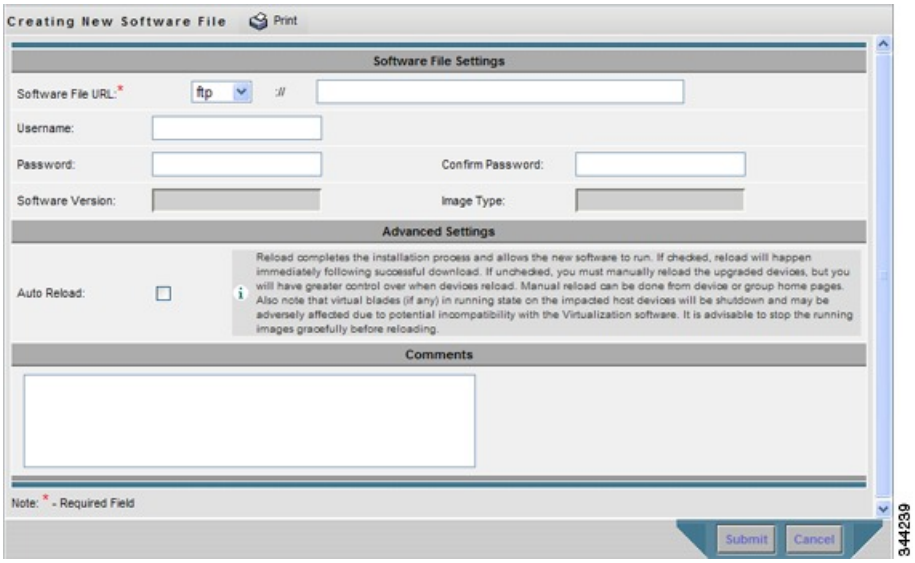
Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin > Version Management > Software Update**.

Step 2 Click the **Create New Software File** icon in the taskbar.

The **Creating New Software File** window appears.

Figure 1: Creating New Software File Window



Step 3 In the **Software File URL** field, specify the location of the new WAAS software file as follows:

a) From the **Software File URL** drop-down list, choose a protocol (**HTTP** or **FTP**).

b) Enter the URL for the **.bin** software file that you downloaded from Cisco.com. For example, a valid URL might look like the following:

http://internal.mysite.com/waas/*WAAS-xxxx-K9***.bin**

http://2012:3:3:3::8/waas/*WAAS-xxxx-K9***.bin**

Here, **WAAS- xxxx -K9.bin** is the name of the software upgrade file. (The filename typically includes the version number.)

Be sure that the URL identifies the correct type of software image for the devices you want to upgrade, either **Universal** or **Accelerator** only.

If the Central Manager has been configured with an IPV6 address, it can be accessed using **https://[CM ipv6 address]:8443/**

Software update configuration with IPv6 address will be filtered in the **device /device group** level usage pages for unsupported device models and versions.

Step 4 (Optional) If your server requires user login authentication, enter your username in the **Username** field and enter your login password in the **Password** field. Enter the same password in the **Confirm Password** field.

The **Software Version** and **Image Type** fields cannot be edited. They are filled in automatically after you submit the settings and the image is validated.

Step 5 To automatically reload a device when you upgrade the software, at the **Advanced Settings** pane, check the **Auto Reload** check box. If you do not check this check box, you should manually reload a device after you upgrade the software on it to complete the upgrade process.

Step 6 (Optional) Enter comments in the **Comments** field.

Step 7 Click **Submit**.

The software image file is validated and the **Software Version** and **Image Type** fields are filled in with the appropriate information extracted from the image file.

Caution If your browser is configured to save the username and password for the Cisco WAAS Central Manager GUI, the browser will autopopulate the **Username** and **Password** fields in the **Creating New Software File** window. You must clear these fields before you click **Submit**.

The software file that you want to use is now registered with the Cisco WAAS Central Manager. When you perform the software upgrade or downgrade, the URL that you just registered becomes one of the choices available in the **Update Software** window.

Step 8 To reload a device from the CLI, run the **reload** EXEC command.

Note When you are viewing the list of registered software files, if the **Image Type** column displays **Unknown** for a software file, it indicates that the software file was added under a Cisco WAAS version earlier than Cisco WAAS Version 4.2.1. These **Unknown** software files must be resubmitted if you want to use them. Click the Edit icon next to the file to open the **Modifying Software File** window, and then, to resubmit the file, click **Submit**.

Upgrading the Cisco WAAS Central Manager

Before you begin

When upgrading software in your Cisco WAAS network, begin with Cisco WAAS Central Manager before upgrading Cisco WAAS WAE devices.

Primary and Standby Cisco WAAS Central Manager devices must be running the same version of Cisco WAAS software. If they are not, the Standby Cisco WAAS Central Manager detects this and will not process any configuration updates it receives from the Primary Cisco WAAS Central Manager. If the Primary Cisco WAAS Central Manager sees that the Standby Cisco WAAS Central Manager has a different version level, it shows the Standby Cisco WAAS Central Manager in red on the device listing page.

If you use the primary Cisco WAAS Central Manager to perform the software upgrade, you need to upgrade your standby Cisco WAAS Central Manager first, and then upgrade your primary Cisco WAAS Central Manager. We also recommend that you create a database backup for the primary Cisco WAAS Central Manager and copy the database backup file to a safe place before you upgrade the software.

Use this upgrade procedure for Cisco WAAS Central Manager devices. You can also use this upgrade procedure to upgrade Cisco WAAS devices one at a time (after the Cisco WAAS Central Manager).

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.

The **Device Dashboard** window appears.

Step 2 Verify that the device is not already running the version to which you plan to upgrade.

Step 3 Click **Update**.

The **Software Update** window appears.

Step 4 To choose the software file URL from the **Software Files** list, click the radio button next to the corresponding filename.

The list displays only software files with an image type of **Universal**, because you are upgrading a Cisco WAAS Central Manager device. If no such images are available, you must create a software file, as described in Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI.

Step 5 To confirm you decision, click **Submit** and then click **OK**.

The **Devices Listing** window is displayed again. You can monitor the progress of your upgrade from this window.

Software upgrade status messages are displayed in the **Software Version** column. These intermediate messages are also written to the system log on the Cisco WAAS devices. See theTable 3: Upgrade Status Messages, on page 8 table for a description of upgrade status messages.

Step 6 Clear your browser cache, close the browser, and restart the browser session to the WAAS Central Manager.

What to do next

The Cisco WAAS Central Manager may reboot at the conclusion of the upgrade procedure (if **Auto Reload** is in the **Creating New Software File** window), causing you to temporarily lose contact with the device and the Cisco WAAS Central Manager GUI.

Table 3: Upgrade Status Messages

Upgrade Status Message	Status
Pending	The request has not yet been sent from the Cisco WAAS Central Manager to the device, or receipt of the request is yet to be acknowledged by the device.
Downloading	The download method for the software file is being determined.
Proceeding with Download	The download method for the software file is determined to be a direct download. Proceeding with the request for direct download of the software file.
Download in Progress (Completed...)	The direct download of the software file is being processed. **Completed** indicates the number of megabytes processed.
Download Successful	The direct download of the software file is successful.
Download Failed	The direct download of the software file cannot be processed. Further troubleshooting is required; see the device system message log. If you are upgrading several devices at once, the download may fail if the server hosting the software file becomes overloaded with requests. Retry the upgrade by clicking the **Retry** link if it is displayed.
Proceeding with Flash Write	A request has been made to write the software file to the device flash memory.
Flash Write in Progress (Completed...)	The write of the device flash memory is being processed. **Completed** indicates the number of megabytes processed.

Upgrade Status Message	Status
Flash Write Successful	The flash write of the software file has been successful.
Reloading	A request to reload the device has been made in order to complete the software upgrade. The device may be offline for several minutes.
Reload Needed	A request to reload the device has not been made. The device must be reloaded manually to complete the software upgrade.
Cancelled	The software upgrade request was interrupted, or a previous software upgrade request was bypassed from the Cisco WAAS CLI.
Update Failed	The software upgrade could not be completed. Troubleshooting is required; see the device system message log. If you are upgrading several devices at once, the upgrade may fail if the server hosting the software file becomes overloaded with requests. Retry the upgrade by clicking the **Retry** link if it is displayed.

Upgrading Multiple Devices Using Device Groups

Before you begin

This procedure is for Cisco WAE devices only. Cisco WAAS Central Manager devices cannot be upgraded using device groups.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** > *device-group-name*.

Step 2 Choose **Admin** > **Versioning** > **Software Update**.

The **Software Update for Device Group** window appears.

Step 3 To choose the software file URL from the **Software File URL** list, click the radio button next to the filename. If no images are available, create a software file, as described in Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI.

If you are updating many devices and you want to use a smaller size software file to save network bandwidth, specify a software file with an image type of Accelerator only, which is smaller than a Universal image. If you later want to change an **Accelerator-only** device to a **Cisco WAAS Central Manager**, you must install the **Universal software file**, reload the device, change the device mode to **central-manager**, and then reload the device again.

Step 4 Click **Submit**.

To view the progress of an upgrade, choose **Devices** > **All Devices** to display the **All Devices** window, and to view the software upgrade status message in the **Software Version** column. These intermediate messages are also written to the system log on Cisco WAAS devices. See the Table 3: Upgrade Status Messages, on page 8 table for a description of the upgrade status messages.

Upgrading Cisco WAAS Central Manager to New Hardware and Converting an Existing Cisco WAAS Central Manager to a Cisco WAE

Before you begin

Consider the following guidelines:

- To add a new piece of hardware as a primary Cisco WAAS Central Manager, and use the existing Cisco WAAS Central Manager as a Cisco WAE, it is important to first add it to the system and then configure it.
- To prevent the former Cisco WAAS Central Manager from later being used as a Cisco WAE, perform a database backup of the former Central Manager and restore it on the new device.

Procedure

Step 1 Add a hardware device as the new Cisco WAAS Central Manager and configure it as a Standby Cisco WAAS Central Manager. There may be multiple Standby Cisco WAAS Central Managers in the system. For more information, see Configuring the Cisco WAAS Central Manager Role.

Step 2 Enable the new hardware device to be the primary Cisco WAAS Central Manager after it is available online and has finished synchronizing with other systems. For more information, see Converting a Standby Cisco WAAS Central Manager to a Primary Cisco WAAS Central Manager.

Step 3 To remove the former Cisco WAAS Central Manager from the Cisco WAAS Central Manager database:

- Disable the CMS service.
- At the former Cisco WAAS Central Manager CLI interface, run the cms deregister EXEC command.
- If there is no connectivity between the devices anymore, run the **cms deregister force** EXEC command and manually delete the former Cisco WAAS Central Manager in the new Cisco WAAS Central Manager GUI.

```
wae# cms deregister force
Deregistering WAE device from Central Manager will result in loss of data on encrypted
file systems, imported certificate/private keys for SSL service and wafs preposition
credentials. If secure store is initialized and open, clear secure store and wait for
one datafeed poll rate to retain wafs preposition credentails.
Do you really want to continue (yes|no) [no]?yes Disabling management service.
management services stopped
Sending de-registration request to CM
Failed to contact CM(Unmarshaled: 9001). Please check connectivity with CM device and
status of management service on CM.
Device de-registration failed, removing device registration information.
Please delete the device record on the Central Manager.
Removing cms database tables.
Re-initializing SSL managed store and restarting SSL accelerator.Deregistration
complete. Save current cli configuration using 'copy running-config startup-config'
command because CMS service has been disabled.
#
```

Step 4 After the former Cisco WAAS Central Manager has been deregistered, perform the following tasks:

- Rename the former Cisco WAAS Central Manager.
- Change the IP address of the former Cisco WAAS Central Manager.

- To change the device mode, run the **device mode** global configuration command.
- To reload the device, run the **reload** EXEC command.

```
wae# configure
wae(config)# device mode application-accelerator
The new configuration will take effect after reload.
wae# reload
```

Step 5 After the device has been reloaded, perform the following tasks:

- Rename the new Primary Cisco WAAS Central Manager.
- Change the IP address to fully replace the former one. Otherwise, you will need to update the configuration of your devices to point to the new address of the Cisco WAAS Central Manager.
- Contact a Cisco TAC member for scripts.

```
wae(config)# hostname old primary central-manager name
wae(config-if)# ip address ipaddress netmask
```

Deleting a Software File

Before you begin

After you have successfully upgraded your Cisco WAAS devices, you can remove the software file from your Cisco WAAS system.

Note You may want to wait a few days before removing a software file in the event that you may have to downgrade your system for any reason.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin > Version Management > Software Update**.

Step 2 Click the **Edit** icon next to the software file that you want to delete.

The **Modifying Software File** window appears.

Step 3 Click the **Trash** icon in the taskbar.

You are prompted to confirm your decision to delete the software file.

Step 4 Click **OK**.

The selected software file is removed from your Cisco WAAS network.

Backing Up and Restoring Your Cisco WAAS System

This section contains the following topics:

Backing Up and Restoring the Cisco WAAS Central Manager Database

Before you begin

Consider the following guidelines before you back up or restore the Cisco WAAS Central Manager database:

- If you have already performed a backup when the secure store was in **user-passphrase** mode and you restored it to a system where the secure store is in **auto-passphrase** mode, you must enter the user passphrase to proceed with the restore. After the restore, the system is in **user-passphrase** mode.

  If you already performed a backup when the secure store was in **auto-passphrase** mode and you restored it to a system where the secure store is in **user-passphrase** mode, you do not have to enter a password. After the restore, the system is in **auto-passphrase** mode.

- The Cisco WAAS Central Manager device stores Cisco WAAS network-wide device configuration information in its Centralized Management System (CMS) database. You can manually back up the CMS database contents for greater system reliability.

- The CMS database backup is in a proprietary format that contains an archive database dump, Cisco WAAS Central Manager registration information, and device information that the Cisco WAAS Central Manager uses to communicate with other Cisco WAAS devices. CMS database backup files are not interchangeable between primary and standby Cisco WAAS Central Manager devices. This means that you cannot use the backup file from a primary Cisco WAAS Central Manager to restore a standby Cisco WAAS Central Manager.

- To back up the CMS database for the Cisco WAAS Central Manager, run the **cms database backup** EXEC command. For database backups, specify the location, password, and user ID of the remote server that you want to store the backup file in. If you want to back up only the configuration information, run the **cms database backup config** EXEC command.

Procedure

Step 1 To back up the CMS database to a file, on the Cisco WAAS Central Manager GUI, run the **cms database backup** global configuration command, as shown in the following example:

```
CM# cms database backup
Creating database backup file backup/cms-db-11-05-2010-15-22_4.3.1.0.1.dump
Backup file backup/cms-db-11-05-2010-15-22_4.3.1.0.1 is ready.
Please use 'copy' commands to move the backup file to a remote host.
```

Note The backup file is automatically given a name in the format cms-db-*date-timestamp_version*.dump, for example, **cms-db-7-22-2010-17-36_4.3.1.0.1.dump**. Note that the timestamp is in a 24-hour format (HH:MM) that does not show seconds. It is stored in **/local1/backup**.

Step 2 Save the file to a remote server by using the **copy disk ftp** command. This command copies the file from a local disk to a remote FTP server.

Step 3 Restore the CMS database as follows:

a) Disable the CMS service:

```
CM# configure
CM(config)# no cms enable
CM(config)# exit
```

Note Stopping the CMS service disables the Cisco WAAS Central Manager GUI. All the users who are currently logged in to this GUI are automatically logged out after the CMS service is disabled.

b) To delete the existing CMS database, run the **cms database delete** EXEC command.

c) To initialize the CMS database, run the **cms database create** EXEC command.

d) Restore the CMS database contents from the backup file:

```
CM# cms database restore backup/cms-db-7-22-2008-17-36_4.1.3.0.1.dump
```

Note After the restore, any WAEs that were registered with the Cisco WAAS Central Manager during the time since the backup was created will be disconnected from the Cisco WAAS Central Manager because there is no information about them in the backup file. To bring these WAEs online, you must deregister and reregister them with the Cisco WAAS Central Manager. On each WAE that was disconnected, use the following commands:

```
WAE# cms deregister force
WAE# configure
WAE(config)# cms enable
```

e) To enable the CMS service on the Cisco WAAS Central Manager, run the **cms enable** global configuration command.

Step 4 (Optional) If you want to upgrade the Cisco WAAS Central Manager to a newer model, backing up the former Cisco WAAS Central Manager's database and restoring it on the new device prevents it from being used as a WAE later. For more information, see Upgrading Cisco WAAS Central Manager to New Hardware and Converting an Existing Cisco WAAS Central Manager to a Cisco WAE.

Backing Up and Restoring a Cisco WAE Device

You should back up the database of each Cisco WAAS device on a regular basis in case a system failure occurs.

Note The backup and restore methods described in this section apply only to a Cisco WAE device that is not configured as a Cisco WAAS Central Manager. For information on backing up the Cisco WAAS Central Manager device, see Backing Up and Restoring the Cisco WAAS Central Manager Database, on page 12.

To back up and restore a device's configuration, run the **copy running-config** EXEC command. This command saves the currently running configuration.

Additionally, you can restore a Cisco WAE to the default configuration that it was manufactured with at any time by removing the user data from the disk and Flash memory, and erasing all the existing files cached on the appliance. Basic configuration information, such as network settings, can be preserved. The appliance is accessible through Telnet and Secure Shell (SSH) after it reboots.

Note If software upgrades have been applied, the restoration process returns to the defaults of the currently installed version and not the factory defaults.

To restore a Cisco WAE to its factory defaults or the defaults of the current configuration from the CLI, run the **restore factory-default [preserve basic-config]** EXEC command.

For more information about the CLI commands, see the *Cisco Wide Area Application Services Command Reference Guide* .

Reinstalling the System Software

This section contains the following topics:

About Reinstalling the System Software

The Cisco WAAS software consists of three basic components:

- Disk-based software
- Flash-based software
- Hardware platform cookie (stored in flash memory)

All of these components must be correctly installed for Cisco WAAS software to work properly.

The software is contained in two types of software images provided by Cisco Systems:

- A **.bin** image that contains disk and flash memory components (the Universal version of the WAAS software)
- A **.sysimg** image that contains a flash memory component only

A software recovery CD-ROM ships with some WAE and WAVE hardware devices. Some WAVE devices use a USB flash drive for recovery.

Caution If you upgraded your software after you received your software recovery CD-ROM or image files, using the recovery software images may downgrade your system. Ensure that you are using the desired software recovery version.

An installation that contains only the Cisco WAAS flash memory-based software, without the corresponding disk-based software, boots and operates in a limited mode, allowing for further disk configuration before completing a full installation.

The **.sysimg** component is provided for recovery purposes and allows for repair of flash memory only without modifying the disk contents.

Note The system image that is used depends on your device. For all WAVE devices (64-bit platforms), use the 64-bit system image (with **x86_64** in its name). For all other devices, use the 32-bit system image named without this designator. A Network Processing Engine (NPE) image that has the disk encryption feature disabled for use in countries where disk encryption is not permitted, is provided.

If you have a Cisco WAVE appliance that requires a USB flash drive for software recovery, your USB flash drive must contain both of the needed software images in the form of an ISO archive file that you copy to the flash drive. (See Preparing the USB Flash Drive, on page 16).

These options are available from the software recovery installer menu:

- **Option 1, Configure Network**: If the **.bin** image you need to install is located on the network instead of the CD-ROM or USB flash drive (which may be the case when an older CD-ROM or USB image is used to install new software), then you must choose this option to configure the network before attempting to install the .bin image.

  This option is performed automatically if you install a .sysimg file from the network.

- **Option 2, Manufacture Flash**: This option verifies the flash memory and, if invalid, automatically reformats it to contain a Cisco standard layout. If reformatting is required, a new cookie is installed automatically.

  This option is performed automatically as part of a .bin or .sysimg installation.

- **Option 3, Install Flash Cookie**: This option generates a hardware-specific platform cookie and installs it in flash memory. Use this option only if there has been a change in the hardware components, such as replacing the motherboard, or if you moved a flash memory card between systems.

  This option is performed automatically during the flash manufacturing process, if needed, as part of a **.bin** or **.sysimg** installation.

- **Option 4, Install Flash Image from Network** and **Option 5, Install Flash Image from USB/CD-ROM**: These options allow installation of only the flash memory .sysimg and do not modify disk contents. They can be used when a new chassis has been provided and populated with a customer's old disks that need to be preserved.

  These options automatically perform flash verification and hardware cookie installation, if required. When installing from the network, you are prompted to configure the network if you have not already done so.

- **Option 6, Install Flash Image from Disk**: This option is reserved for future expansion and is not available.

- **Option 7, Re-create RAID device**: This option applies only to WAVE-7541, WAVE-7571, and WAVE-8541 devices and re-creates the RAID array.

- **Option 8, Wipe Out Disks and Install .bin Image**: This option provides the preferred procedure for installing the Cisco WAAS software.

  Caution Option 8 erases the content from the all disk drives in your device.

  This option performs the following steps:

1. Checks that flash memory is formatted to Cisco specifications. If yes, the system continues to Step 2. If no, the system reformats the flash memory, which installs the Cisco file system, and generates and installs a platform-specific cookie for the hardware.
2. Erases data from all drives.
3. Re-manufactures the default Cisco file system layout on the disk.
4. Installs the flash memory component from the **.bin** image.
5. Installs the disk component from the **.bin** image.

Preparing the USB Flash Drive

Before you begin

If you have a Cisco WAVE appliance that requires a USB flash drive for software recovery, you must prepare the USB flash drive with the appropriate files before you can start the software recovery process. You will need the following:

- Windows PC (Windows XP or 7) or Mac computer
- USB flash drive that is 1 GB or larger in size
- The following software recovery files:
  - Cisco WAAS Rescue CD ISO image file, which is available on the Cisco WAAS Software Download page. The filename is similar to **waas-rescue-cdrom-x.x.x.x-k9.iso**, where the x's denote the software version number. Alternatively, the ISO image file is available on the Cisco WAAS release DVD, or you can make an ISO image file from a Cisco WAAS recovery CD.
  - The **syslinux.cfg** file, which is also available on the Cisco WAAS Software Download page and on the Cisco WAAS release DVD.
  - **Unetbootin** utility for Microsoft Windows or Apple Mac, which is available from the Unetbootin Sourceforge website.

Procedure

Step 1 Transfer the software recovery files on to the computer, noting the directory in which they are stored.

Step 2 Insert the USB flash drive into a USB port on the computer.

Step 3 Open **My Computer** (Microsoft Windows) or **Disk Utility** (Apple MAC).

Step 4 Format the USB flash drive:

- For Microsoft Windows, right-click the **Removable Disk** (drive letter will vary with system) and select **Format**.
  - In the formatting tool, from the **File System** drop-down list, select **FAT32**.
  - In the **Format Options** sections, check the **Quick Format** check box, and then click **Start**.
  - After formatting is complete, close the formatting tool.

- For Apple MAC, select the USB drive on the left side of window, and use the **Erase** tab to format for use with **MS-DOS (FAT)**.

Step 5 Launch the **Unetbootin** utility.

Step 6 Select the **Diskimage** option and click the corresponding browse button (...) to select the **waas-rescue-cdrom-***x.x.x.x***-k9.iso** image file.

Step 7 Ensure that USB Drive is selected in the **Type** drop-down list and that the correct drive letter is selected for **Drive**.

Step 8 To install the bootable imate in the USB flash drive, click **OK**. After the installation has completed, click **Exit**.

Step 9 Drag a copy of the **syslinux.cfg** file into the USB flash drive and click **Yes** to confirm the replacement. This file replaces the existing file on the USB flash drive with the one customized for your Cisco WAAS system.

Step 10 Remove the USB flash drive from the computer.

Step 11 To continue reinstalling the system software from the prepared USB flash drive, follow the instructions described in Reinstalling the System Software on a Cisco WAE or Reinstalling the System Software on a Cisco NME-WAE.

Reinstalling the System Software on a Cisco WAE

Procedure

Step 1 Connect a serial console to the Cisco WAE and use the console for the following steps.

Step 2 Insert the software recovery CD-ROM in the CD drive of the Cisco WAEor, if the WAE uses a USB flash drive for recovery, insert a bootable USB flash drive with the software recovery files into the USB port of the device (see Preparing the USB Flash Drive, on page 16). WAE-294, WAE-594, WAE-694, WAVE-7541, WAVE-7571, and WAVE-8541 devices do not have CD drives; they use a USB flash drive for software recovery.

Step 3 Reboot the Cisco WAE. During the boot process, the boot loader pauses for 30 seconds and you must choose the VGA console if you are using Cisco vWAAS. The prompt is displayed as follows:

```
Type "serial" for WAE/WAVE appliance.
Type "vga" for vWAAS.
boot:
```

At the prompt, enter the **vga** commandto continue the boot process for the VGA console on Cisco vWAAS. After 30 seconds with no input, the boot process continues with the standard serial console for Cisco WAAS appliances.

After the WAE boots, you will see the following:

```
Installer Main Menu:
1. Configure Network
2. Manufacture flash
3. Install flash cookie
4. Install flash image from network
5. Install flash image from usb/cdrom
6. Install flash image from disk
7. Recreate RAID device (WAE-7541/7571/8541 only)
8. Wipe out disks and install .bin image
9. Exit (reboot)
Choice [0]:
```

Note The option numbers in the installer main menu may vary, depending on the WAAS software release being installed.

Step 4 Choose **Option 2, Manufacture flash** to prepare the flash memory.

This step prepares a cookie for the device and also retrieves the network configuration that was being used by the Cisco WAAS software. This network configuration is stored in the flash memory and is used to configure the network when the Cisco WAAS software boots up after installation.

Step 5 Choose **Option 3, Install flash cookie** to install the flash cookie that you prepared in the previous step.

Step 6 Choose **Option 5, Install flash image from usb/cdrom** to install the flash image from a CD-ROM or USB flash drive.

Step 7 (Optional) If you are working with a WAVE-7541, WAVE-7571, or WAVE-8541 device, choose **Option 7** to recreate the RAID array.

Step 8 Choose **Option 8, Wipe out disks and install .bin image** to wipe the disks and install the binary image.

This step prepares the disks by erasing them. The Cisco WAAS software image is installed.

Step 9 If you are using a USB flash drive to install the software, remove it from the device.

Step 10 Choose **Option 9, Exit (reboot)** to reboot the WAE.

After the Cisco WAE reboots, it runs the newly installed Cisco WAAS software. The Cisco WAE has a minimal network configuration and is accessible via the terminal console for further configuration.

Reinstalling the System Software on a Cisco NME-WAE

Procedure

Step 1 Log in to the Cisco router in which the Cisco NME-WAE module is installed, and reload the Cisco NME-WAE module:

```
router-2851> enable
router-2851# service-module integrated-Service-Engine 1/0 reload
```

Step 2 Immediately open a session in the module:

```
router-2851# service-module integrated-Service-Engine 1/0 session
```

Step 3 While the module is loading, you will see the following option during boot phase 3. Enter ******* as instructed:

```
[BOOT-PHASE3]: enter `***' for rescue image: ***
```

Step 4 The **Rescue Image** dialog box is displayed. The following example shows how to interact with the **Rescue Image** dialog box (user input is denoted by entries in bold typeface):

```
This is the rescue image. The purpose of this software is to let
you install a new system image onto your system's boot flash
device. This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.
To download an image from network, this software will request
the following information from you:
- which network interface to use
```

```
- IP address and netmask for the selected interface
- default gateway IP address
- FTP server IP address
- username and password on FTP server
- path to system image on server
Please enter an interface from the following list:
0: GigabitEthernet 1/0
1: GigabitEthernet 2/0
enter choice: 0
Using interface GigabitEthernet 1/0
Please enter the local IP address to use for this interface:
[Enter IP Address]: 10.1.13.2
Please enter the netmask for this interface:
[Enter Netmask]: 255.255.255.240
Please enter the IP address for the default gateway:
[Enter Gateway IP Address]: 10.1.13.1
Please enter the IP address for the FTP server where you wish
to obtain the new system image:
[Enter Server IP Address]: 10.107.193.240
Please enter your username on the FTP server (or 'anonymous'):
[Enter Username on server (e.g. anonymous)]: username
Please enter the password for username 'username' on FTP server:
Please enter the directory containing the image file on the FTP server:
[Enter Directory on server (e.g. /)]: /
Please enter the file name of the system image file on the FTP server:
[Enter Filename on server]: WAAS-6.4.3.10-K9.sysimg
Here is the configuration you have entered:
Current config:
IP Address: 10.1.13.2
Netmask: 255.255.255.240
Gateway Address: 10.1.13.1
Server Address: 10.107.193.240
Username: username
Password: *********
Image directory: /
Image filename: WAAS-5.1.1.10-K9.sysimg
Attempting download...
Downloaded 15821824 byte image file
A new system image has been downloaded.
You should write it to flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no')]: yes
Ok, writing new image to flash
.......................................................................... done.
Finished writing image to flash.
Enter 'reboot' to reboot, or 'again' to download and install a new image:
[Enter reboot confirmation ('reboot' or 'again')]: reboot
Restarting system. After the module reboots, install the .bin image from an HTTP server:
NM-WAE-1# copy http install 10.77.156.3 /waas WAAS-6.4.3.10-k9.bin
 Reload the module:
NM-WAE-1# reload
```

Step 5 After the module reboots, it runs the newly installed Cisco WAAS software.

```
NM-WAE-1# copy http install 10.77.156.3 /waas WAAS-6.4.3.10-k9.bin
```

Step 6 Reload the module.

```
NM-WAE-1# reload
```

Ensuring that RAID Pairs Rebuild Successfully

RAID pairs will rebuild on the next reboot after you run the **restore factory-default** EXEC command, replace or add a hard disk drive, delete disk partitions, or reinstall Cisco WAAS from the booted recovery CD-ROM or USB flash drive.

Note You must ensure that all the RAID pairs have completed rebuilding *before* you reboot your Cisco WAE device. If you reboot while the device is still rebuilding, you risk corrupting the file system.

To view the status of the drives and check if the RAID pairs are in **Normal Operation** or in **Rebuilding** status, run the show disk details EXEC command. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process can take several hours.

If you do not wait for the RAID pairs to complete the rebuild process before you reboot the device, you may see the following symptoms, indicating a problem:

- The device is offline in the Cisco WAAS Central Manager GUI.
- CMS cannot be loaded.
- Error message stating that the file system is read-only is displayed.
- The syslog contains errors such as:
  - **Aborting journal on device md2**
  - **Journal commit I/O error**
  - **Journal has aborted**
  - **ext3_readdir: bad entry in directory**
- Other unusual behaviors related to disk operations or the inability to perform them are visible.

If you encounter any of these symptoms, reboot the Cisco WAE and wait until the RAID rebuild finishes normally.

Recovering the System Software

Before you begin

Cisco WAAS devices have a resident rescue system image that is invoked if the image in flash memory is corrupted. A corrupted system image can result from a power failure that occurs while a system image is being written to flash memory. The rescue image can help you download a system image to the main memory of the device and write it to flash memory.

Note The system image used depends on your device. For all Cisco WAVE and Cisco WAE devices (64-bit platforms), use the 64-bit system image (with **x86_64** in its name). For all other devices, use the 32-bit system image named without this designator. An NPE image that has the disk encryption feature disabled for use in countries where disk encryption is not permitted is provided.

Procedure

Step 1 Download the system image file (***.sysimg**) to a host that is running an FTP server.

Step 2 Establish a console connection to the Cisco WAAS device and open a terminal session.

Step 3 To reboot the device, toggle the **power on/off switch**.

After a few seconds, the bootloader pauses and prompts you to enter **1** to boot Cisco WAAS, **r** to boot the rescue image, **x** to reboot, or **9** to escape to the loader prompt. You have 10 seconds to respond before the normal boot process continues.

Step 4 To boot the rescue image, enter **r**.

The **Rescue Image** dialog box is displayed and differs depending on whether your Cisco WAAS device was initially manufactured with Cisco WAAS Version 4.x or 5.x. **Step 5** describes the rescue image on a device that was initially manufactured with Cisco WAAS Version 5.x. **Step 6** describes the rescue image on a device that was initially manufactured with Cisco WAAS Version 4.x.

Step 5 If you see the following output (from a device that was initially manufactured with Cisco WAAS Version 5.x), log in and run the **copy install** EXEC command to install the Cisco WAAS system software image (**.bin** file), as shown in the following example (user input is denoted by entries in bold typeface):

```
The device is running WAAS rescue image. WAAS functionality is unavailable
in a rescue image. If the rescue image was loaded by accident, please reload
the device. If the rescue image was loaded intentionally to reinstall WAAS software
please use the following command:
copy [ftp|http|usb] install ...
SW up-to-date
...
Cisco Wide Area Virtualization Engine Console
Username: admin
Password:
System Initialization Finished.
WAVE# copy ftp install 172.16.10.10 / waas-universal-5.1.1.12-k9.bin
...
Installing system image to flash... Creating backup of database content before database
upgrade.
The new software will run after you reload.
WAVE# reload
Proceed with reload?[confirm]yes
Shutting down all services, will timeout in 15 minutes.
reload in progress ..Restarting system.
```

Step 6 If you see the following output (from a device that was initially manufactured with Cisco WAAS Version 4.x), log in and install the Cisco WAAS system image (**.sysimg** file), as shown in the following example (user input is denoted by entries in bold typeface):

```
This is the rescue image. The purpose of this software is to let
you download and install a new system image onto your system's
boot flash device. This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.
To download an image, this software will request the following
information from you:
- which network interface to use
- IP address and netmask for the selected interface
- default gateway IP address
- server IP address
- which protocol to use to connect to server
```

```
- username/password (if applicable)
- path to system image on server
Please enter an interface from the following list:
0: GigabitEthernet 0/0
1: GigabitEthernet 0/1
enter choice: 0
Using interface GigabitEthernet 0/0
Please enter the local IP address to use for this interface:
[Enter IP Address]: 172.16.22.22
Please enter the netmask for this interface:
[Enter Netmask]: 255.255.255.224
Please enter the IP address for the default gateway:
[Enter Gateway IP Address]: 172.16.22.1
Please enter the IP address for the FTP server where you wish
to obtain the new system image:
[Enter Server IP Address]: 172.16.10.10
Please enter your username on the FTP server (or 'anonymous'):
[Enter Username on server (e.g. anonymous)]: anonymous
Please enter the password for username 'anonymous' on FTP server:
Please enter the directory containing the image file on the FTP server:
[Enter Directory on server (e.g. /)]: /
Please enter the file name of the system image file on the FTP server:
[Enter Filename on server (e.g. WAAS-x86_64-4.x.x-K9.sysimg)]:
waas-x86_64-5.1.1.12-k9.sysimg
Here is the configuration you have entered:
Current config:
IP Address: 172.16.22.22
Netmask: 255.255.255.224
Gateway Address: 172.16.22.1
Server Address: 172.16.10.10
Username: anonymous
Password:
Image directory: /
Image filename: waas-x86_64-5.1.1.12-k9.sysimg
Attempting download...
Downloaded 31899648 byte image file
A new system image has been downloaded.
You should write it to flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no')]: yes
Ok, writing new image to flash
Finished writing image to flash.
Enter 'reboot' to reboot, or 'again' to download and install a new image:
[Enter reboot confirmation ('reboot' or 'again')]: reboot
Restarting system.
Booting system, please wait.........
```

Step 7 Log in to the device with the username **admin**. To verify that you are running the correct version, run the **show version** EXEC command:

```
Username: admin
Password:
Console# show version
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2020 by Cisco Systems, Inc.
Cisco Wide Area Application Services (universal-k9) Software Release 6.4.3 (build b49 Jan
14 2020)
Version: oe294-5.1.1.12
Compiled 12:23:45 Jan 14 2020 by dsmith
Device Id: 50:3d:e5:9c:8f:a5
System was restarted on Tue Jan 14 16:35:50 2020.
```

```
System restart reason: called via cli.
The system has been up for 8 hours, 10 minutes, 19 seconds.
```

Resetting a Lost Administrator Password

Before you begin

If an administrator password is forgotten, lost, or misconfigured, you will have to reset the password on the device.

Note You cannot restore a lost administrator password. You must reset the password, as described in this procedure.

Procedure

Step 1 Establish a console connection to the device and open a terminal session.

Step 2 Reboot the device.

While the device is rebooting, watch for the following prompt, and press **Enter** when you see it:

```
Cisco WAAS boot:hit RETURN to set boot flags:0009
```

Step 3 When prompted to enter bootflags, enter the value **0x8000**.

```
Available boot flags (enter the sum of the desired flags):
0x4000 - bypass nvram config
0x8000 - disable login security
[CE boot - enter bootflags]:0x8000
You have entered boot flags = 0x8000
Boot with these flags? [yes]:yes
[Display output omitted]
Setting the configuration flags to 0x8000 lets you into the system, bypassing all
security. Setting the configuration flags field to 0x4000 lets you bypass the NVRAM
configuration.
```

Step 4 When the device completes the boot sequence, you are prompted to enter the username to access the CLI. Enter the default administrator username (**admin**).

```
Cisco WAE Console
Username: admin
```

Step 5 When you see the CLI prompt, set the password for the user using the username passwd command in global configuration mode:

```
WAE# configure
WAE(config)# username admin passwd
```

This command invokes interactive password configuration. Follow the CLI prompts.

Step 6 Save the configuration change:

```
WAE(config)# exit
WAE# write memory
```

Step 7 (Optional) Reboot your device:

```
WAE# reload
```

Rebooting is optional. However, we recommend that you reboot to ensure that the boot flags are reset, and to ensure that subsequent console administrator logins do not bypass the password check.

Note In the Cisco WAAS software, the bootflags are reset to **0x0** on every reboot.

Recovering from Missing Disk-Based Software

Before you begin

This task describes how to recover from the following types of disk drive issues:

- Your Cisco WAAS device contains a single disk drive that needs to be replaced due to a disk failure.
- Your Cisco WAAS device contains two disk drives and you intentionally deleted the disk partitions on both drives (**disk00** and **disk01**).

  Systems with two or more disk drives are normally protected automatically by RAID-1 on critical system partitions. Therefore, the procedures in this section do not have to be followed when replacing a disk drive in a multidrive system.

Procedure

Step 1 Deactivate the device by completing the following steps:

a) From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.

b) Choose *device-name* > **Activation**.

The **Device Activation** window appears.

c) Uncheck the Activate check box, and then click Submit.

The device is deactivated.

Step 2 Power down the device and replace the failed hard drive.

Step 3 Power on the device.

Install the Cisco WAAS software. For more information on initial configuration, see the Cisco Wide Area Application Services Quick Configuration Guide .

Step 4 Use the CMS identity recovery procedure to recover the device CMS identity and associate this device with the existing device record on the Cisco WAAS Central Manager. For more information, see Recovering Cisco WAAS Device Registration Information.

Recovering Cisco WAAS Device Registration Information

Before you begin

Device registration information is stored both on the device itself and on the Cisco WAAS Central Manager. If a device loses its registration identity or needs to be replaced because of a hardware failure, the Cisco WAAS network administrator can issue a CLI command to recover the lost information, or in the case of adding a new device, assume the identity of the failed device.

Procedure

Step 1 To mark the failed device as **Inactive** and Replaceable by completing the following steps:

a) From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.
b) Choose *device-name* > **Activation**.
c) Uncheck the **Activate** check box. The window refreshes, displaying a check box for marking the device as replaceable.
d) Check the **Replaceable** check box, and click **Submit**.

Note This check box appears in the Cisco WAAS Central Manager GUI only when the device is inactive.

Step 2 If the failed device is configured as a nonoptimizing peer with another device, disable the peer settings on the other device.

A message is displayed if the failed device is a nonoptimizing peer, indicating that the device is a nonoptimizing peer. When a device is replaced, its device ID changes and therefore, the nonoptimizing peer configuration must be updated.

a) From the Cisco WAAS Central Manager menu, choose **Configure** > **Global** > **Peer Settings**.

The **Peer Settings** window for all the devices appears.

b) Click the **Edit** icon next to the nonoptimizing device identified in the message, which will appear in red because its peer is unknown.

The **Peer Settings** window for that device appears.

c) Click the **Remove Device Settings** icon in the taskbar.
d) Click **Submit**.

Step 3 Configure a system device recovery key as follows:

a) From the Cisco WAAS Central Manager menu, choose **Configure** > **Global** > **System Properties**.
b) Click the **Edit** icon next to the **System.device.recovery.key** property.

The **Modifying Config Property** window appears.

c) Enter the password in the **Value** field, and click **Submit**.

The default password is **default**.

Step 4 Configure the basic network settings for the new device.

Step 5 Open a Telnet session to the device CLI and enter the **cms recover identity** *keyword* EXEC command. Here, *keyword* is the device recovery key that you configured in the Cisco WAAS Central Manager GUI.

When the Cisco WAAS Central Manager receives the recovery request from the Cisco WAAS device, it searches its database for the device record that meets the following criteria:

- The record is inactive and replaceable.
- The record has the same hostname or primary IP address, as given in the recovery request.

If the recovery request matches the device record, then the Cisco WAAS Central Manager updates the existing record and sends the requesting device a registration response. The replaceable state is cleared so that no other device can assume the same identity. When the Cisco WAAS device receives its recovered registration information, it writes it to file, initializes its database tables, and starts.

Step 6 To enable the CMS service on the device, run the following commands:

```
WAE# config
WAE(config)# cms enable
WAE(config)# exit
```

Step 7 Activate the device:

a) From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.
b) Choose *Device Name* > **Activation**. The Cisco WAAS device status should be Online.
c) Check the **Activate** check box, and click **Submit**.

Step 8 (Optional) Reconfigure the device peer settings, if the device was configured as a nonoptimizing peer with another device. For more information, see the chapter "Configuring Traffic Interception."

Step 9 Save the device configuration settings by entering the **copy running-config startup-config** EXEC command.

Disk Maintenance for RAID Systems

This section contains the following topics:

About Disk Maintenance for RAID-1 Systems

Cisco WAAS supports hot-swap functionality for both failed disk replacement and scheduled disk maintenance. When a disk fails, Cisco WAAS automatically detects the disk failure, marks the disk as bad, and removes the disk from the RAID-1 volume. To schedule disk maintenance, you must manually shut down the disk.

You must wait for the disk to be completely shut down before you physically remove the disk from the Cisco WAE. When the RAID removal process is complete, Cisco WAAS generates a disk failure alarm and trap. In addition, a syslog error message is logged.

Note If the removal event (such as, a disk failure or software shutdown) occurs while the RAID array is in the rebuild process, the RAID removal process may take up to 1 minute to complete. The duration of this process depends on the size of the disk.

If the Cisco WAAS software removes a failed disk during the RAID rebuild process, a RAID rebuild failure alarm is generated. If you administratively shut down the disk during the RAID rebuild process, a RAID rebuild cancel alarm is generated instead.

When you install a replacement disk, the Cisco WAAS software detects the replacement disk and performs compatibility checks on the disk, initializes the disk by creating partitions, and adds the disk to the software RAID to start the RAID rebuild process.

If the newly inserted disk has the same disk ID as a disk that was previously marked bad in the same physical slot, then the disk will not be mounted, and the post-replacement checks, initialization, and RAID rebuilding will not occur.

A newly installed disk must be of the same type and speed as the old disk and it must meet the following compatibility requirements:

- If the replacement disk is for **disk00**, **disk02**, or **disk04** of a RAID pair, the replacement disk must be the same size as the running disk in the array.
- If the replacement disk is for **disk01**, **disk03**, or **disk05** of a RAID pair, then the replacement disk must have the same or greater RAID capacity as the running disk in the array.

Compatibility checks, which are a part of the hot-swap process, check for capacity compatibility. Incompatibility generates an alarm and cancels the hot-swap process.

Performing Disk Maintenance for RAID-1 Systems

Procedure

Step 1 Manually shut down the disk.

a) Enter global configuration mode and then enter the **disk disk-name** *diskxx* **shutdown** global configuration command:

```
WAE# configure
WAE(config)# disk disk-name diskxx shutdown
```

b) Wait for the disk to be completely shut down before you physically remove the disk from the WAE. When the RAID removal process is complete, Cisco WAAS generates a disk failure alarm and trap. In addition, a syslog error message is logged.

Note We recommend that you disable the **disk error-handling reload** option if it is enabled because it is not necessary to power down the system to remove a disk.

Step 2 Insert a replacement disk into the slot in the WAE. The replacement disk must have a disk ID number that is different from the disk that it is replacing.

Step 3 To re-enable the disk, run the **no disk disk-name** *diskxx* **shutdown** global configuration command.

Removing and Replacing Disks in RAID-5 Systems

Procedure

Step 1 Enter the **disk disk-name** *diskxx* **replace** command in EXEC mode from the Cisco WAAS CLI on the Cisco WAE.

Step 2 Verify that the disk drive *diskxx* is in **Defunct** state by entering the **show disks details** command in EXEC mode. The RAID logical drive is in **Critical** state at this point.

Step 3 Move the handle on the drive to the open position (perpendicular to the drive).

Step 4 Pull the hot-swap drive assembly from the bay.

Step 5 Wait for one minute and then insert the new drive into the same slot by aligning the replacement drive assembly with guide rails in the bay and sliding the drive assembly into the bay until it stops. Make sure that the drive is properly seated in the bay.

Step 6 Close the drive handle.

Step 7 Check the hard disk drive status LED to verify that the hard disk drive is operating correctly. If the amber hard disk drive status LED for a drive is lit continuously, that drive is faulty and must be replaced. If the green hard disk drive activity LED is flashing, it means the drive is being accessed.

Note If a disk is shut down using the **disk disk-name** *diskxx* **replace** EXEC command and the same disk is removed and reinserted, it can be re-enabled by using the **disk disk-name** *diskxx* **enable force** EXEC command. This process is applicable even if the disk is not removed and needs to be re-enabled. This command is not applicable if a new disk is inserted.

Step 8 Wait for 1 minute. To verify that the replaced disk drive is in the **Rebuilding** state, run the **show disk details** command in EXEC mode.

Note The **ServeRAID** controller automatically starts the rebuild operation when it detects the removal and reinsertion of a drive that is a part of the logical RAID drive.

Step 9 Wait until the rebuild operation is complete. To check if the rebuild operation is complete, run the **show disk details** command in EXEC mode. The physical drive state will be **Online** and the RAID logical drive state will be **Okay** after the rebuild operation is completed.

Step 10 Reinstall the software on the device. For more information, see Upgrading the Cisco WAAS Central Manager, on page 7

Step 11 Add the license. For more information, see Managing Cisco WAAS Software Licenses in the chapter "Configuring Other System Settings."

Step 12 Register the Cisco WAE to the Cisco WAAS Central Manager.

A 300-GB SAS drive may take up to 5 hours to finish rebuilding.

Recreating the RAID-5 Array in RAID-5 Systems

Before you begin

If you have multiple disk failures and your RAID-5 logical status is **Offline**, you must recreate the RAID-5 array.

Procedure

Step 1 From the global configuration mode, run the **disk logical shutdown** command to disable the RAID-5 array.

Step 2 To save the running configuration to NV-RAM, run the **write** command in EXEC mode.

Step 3 To reload the system, run the **reload** command in EXEC mode.

Step 4 To check the system configuration after the system is reloaded, run the **show disks details** command in EXEC mode. At this point, the disks are not mounted and the logical RAID drive should be in the **Shutdown** state.

Step 5 To recreate the RAID-5 array, run the **disk recreate-raid** command in EXEC mode.

Step 6 To disable the logical disk shutdown configuration: After successful execution of the **disk recreate-raid** command, enter global configuration mode and run the **no disk logical shutdown** command.

Step 7 To save the configuration to NV-RAM, run the **write** command in EXEC mode.

Step 8 To reload the system, run the **reload** command in EXEC mode.

Step 9 To check the system configuration after the system is reloaded, run the **show disks details** command in EXEC mode.

At this point, the disks should be mounted and the logical RAID drive should not be in the **Shutdown** state.

Step 10 Wait until the rebuild operation is complete. To check if the rebuild operation is complete, run the **show disks details** command in EXEC mode. The physical drive state will be **Online** and the RAID logical drive state will be **Okay** after the rebuild operation is completed.

It takes several hours to finish rebuilding the RAID-5 array.

Step 11 After a multiple disk failure or RAID controller failure, and after the drives are replaced and the RAID disk is rebuilt, the logical disk may remain in the error state. To re-enable the disk, run the **no disk logical shutdown force** command, and then reload the WAE.

Configuring the Cisco WAAS Central Manager Role

This section contains the following topics:

Primary and Standby Cisco WAAS Central Managers

The Cisco WAAS software implements a Standby Cisco WAAS Central Manager. This process allows you to maintain a copy of the Cisco WAAS network configuration on a second Cisco WAAS Central Manager device. If the Primary Cisco WAAS Central Manager fails, the Standby can be used to replace the Primary.

For interoperability, when a Standby Cisco WAAS Central Manager is used, it must be at the same software version as the Primary Cisco WAAS Central Manager to maintain the full Cisco WAAS Central Manager configuration. Otherwise, the Standby Cisco WAAS Central Manager detects this status and does not process any configuration updates that it receives from the Primary Cisco WAAS Central Manager until the problem is corrected.

There is no specified number of Standby Central Managers for meeting redundancy purposes. Regular backup of CMS database content provides better reliability.

Note Primary and Standby Central Managers communicate on TCP ports 443 and 8443. If your network includes a firewall between primary and standby Central Managers, you must configure the firewall to allow traffic on TCP ports 443 and 8443 so that the Central Managers can communicate and stay synchronized.

Converting a Cisco WAE to a Standby Cisco WAAS Central Manager

Before you begin

There are two types of Cisco WAAS software files:

- **Universal**: Includes Central Manager, Application Accelerator, and AppNav Controller functionality.
- **Accelerator only**: Includes Application Accelerator and AppNav Controller functionality only. If you want to change an Application Accelerator or AppNav Controller to a Central Manager, you must use the Universal software file.

If the Cisco WAE is operating with an **Accelerator** only image, you cannot convert it to a Central Manager until after you update it with the Universal software file, reload the device, change the device mode to **central-manager**, and then reload the device again. For information on updating a Cisco WAE, see Upgrading the Cisco WAAS Software.

To check if the WAE is running an Accelerator only image, run the **show version** EXEC command. To display the image type, run the **show running-config** EXEC command.

Procedure

Step 1 To deregister the Cisco WAE from the Cisco WAAS Central Manager, run the **cms deregister force** EXEC command.

This command cleans up any previous association to any other Cisco WAAS Central Manager.

Step 2 To configure the device mode as **central-manager**, run the **device mode central-manager** global configuration command:

```
WAE# configure
WAE(config)# device mode central-manager
```

Step 3 You must reload the device to apply the changes. For more information, see see Rebooting a Device, on page 39.

Step 4 To configure the Cisco WAAS Central Manager role as Standby, run the **central-manager role standby** command.

Step 5 To configure the address of the Primary Cisco WAAS Central Manager, run the **central-manager address** *cm-primary-address* command:

Step 6 To enable the CMS service, run the **cms enable** command.

Converting a Primary Cisco WAAS Central Manager to a Standby Cisco WAAS Central Manager

Procedure

Step 1 To deregister the Cisco WAAS Central Manager, run the **cms deregister** EXEC command:

This command cleans up any previous association to any other Cisco WAAS Central Manager.

Step 2 To configure the Cisco WAAS Central Manager role as Standby, run the **central-manager role standby** global configuration command.

Step 3 To configure the address of the Primary Central Manager, run the **central-manager address** *cm-primary-address* global configuration command.

Step 4 To enable the CMS service, run the **cms enable** global configuration command.

Converting a Standby Cisco WAAS Central Manager to a Primary Cisco WAAS Central Manager

If your Primary Cisco WAAS Central Manager becomes inoperable, you can manually reconfigure one of your warm Standby Cisco WAAS Central Managers to be the Primary Cisco WAAS Central Manager. To configure the new role, run the **central-manager role primary** global configuration command as follows:

```
WAE# configure
WAE(config)# central-manager role primary
```

This command changes the role from Standby to Primary and restarts the management service to recognize the change.

If a previous failed Primary Central Manager becomes available again, you can recover it to make it the Primary Cisco WAAS Central Manager again. For more information, see Cisco WAAS Central Manager Failover and Recovery, on page 33.

If you switch a warm Standby Cisco WAAS Central Manager to Primary while your Primary Cisco WAAS Central Manager is still online and active, both Cisco WAAS Central Managers detect each other, automatically shut themselves down, and disable management services. The Cisco WAAS Central Managers are switched to halted, which is automatically saved in flash memory.

To return halted Cisco WAAS Central Managers to an **online** status, decide which Cisco WAAS Central Manager should be the Primary and which should be the Standby. On the Primary, run the following CLI commands:

```
WAE# configure
WAE(config)# central-manager role primary
WAE(config)# cms enable
```

On the Standby, run the following CLI commands:

```
WAE# configure
WAE(config)# central-manager role standby
WAE(config)# central-manager address cm-primary-address
WAE(config)# cms enable
```

Switching Both the Cisco WAAS Central Manager Roles

Before you begin

Caution When you switch a Cisco WAAS Central Manager from Primary to Standby, the configuration on the Cisco WAAS Central Manager is erased. The Cisco WAAS Central Manager, after becoming a Standby, will begin replicating its configuration information from the current Primary Cisco WAAS Central Manager. If Standby and Primary units are not synchronized before switching roles, important configuration information can be lost.

Procedure

Step 1 Ensure that your Cisco WAAS Central Manager devices are running the same version of Cisco WAAS software.

Step 2 Synchronize the physical clocks on both devices so that both the Cisco WAAS Central Managers have the same Coordinated Universal Time (UTC) configured.

Step 3 To ensure that the Standby is synchronized with the Primary, check the status of the following items:

a) Check the online status of your devices.

The original Standby Cisco WAAS Central Manager and all currently active devices should be showing as **online** in the Cisco WAAS Central Manager GUI. This step ensures that all other devices know about both Cisco WAAS Central Managers.

b) Check the status of recent updates from the Primary WAAS Central Manager.

To check the time of the last update, run the **show cms info** EXEC command. To be current, the value of the **Time of last config-sync** field should be between **1** and **5 minutes** old. This time range verifies that the Standby Cisco WAAS Central Manager has fully replicated the Primary Cisco WAAS Central Manager configuration.

If the update time is not current, determine whether or not there is a connectivity problem or if the Primary Cisco WAAS Central Manager is down. Fix the problem, if necessary, and wait until the configuration has replicated, as indicated by the time of the last update.

Step 4 Switch roles in the following order:

a) Disable the original **Primary** Cisco WAAS Central Manager.

```
WAE2(config)# no cms enable
```

b) Switch the original **Standby** Cisco WAAS Central Manager to **primary mode**:

```
WAE2# configure
WAE2(config)# central-manager role primary

WAE1-CM3(config)# central-manager role standby
Switching CM to standby will cause all configuration settings made on this CM to be
lost.
Please confirm you want to continue (yes|no) [no]?yes
Restarting CMS services
```

c) Wait until the original **Standby** Cisco WAAS Central Manager is completely up and that you have verified that it is now working as the **Primary** Cisco WAAS Central Manager.

d) Switch the original **primary** Cisco WAAS Central Manager to **standby mode**:

```
WAE1# configure
WAE1(config)# central-manager role standby
WAE1(config)# cms enable
```

The CMS service is restarted automatically after you configure a role change.

Cisco WAAS Central Manager Failover and Recovery

Before you begin

If your Primary Cisco WAAS Central Manager becomes inoperable, you can reconfigure one of your Standby Central Managers to be the Primary Central Manager, and later, when the failed Cisco WAAS Central Manager becomes available, you can reconfigure it to be the Primary again.

For Cisco Central Manager integrated with Cisco vManage for Cisco WAAS Version 6.4.5 and later:

- If your Primary Cisco WAAS Central Manager becomes inoperable, a Standby Central Manager automatically continues connectivity with Cisco vManage.
- Upgrade guidelines: If the Cisco WAAS Central Manager is registered as a partner with Cisco vManage, during the upgrade from Cisco WAAS Version 6.4.5 to 6.4.5a, the **vManage.cer** file is automatically moved from **/state/cm/vManage/vManage.cer** to **/state/cm/pki/certificates/vManage/vManage.cer**.
- Downgrade guidelines: If the Cisco WAAS Central Manager is registered as a partner with Cisco vManage, during the downgrade from Cisco WAAS Version 6.4.5a to 645, the **vManage.cer** file is automatically moved from **/state/cm/pki/certificates/vManage/vManage.cer** to **/state/cm/vManage/vManage.cer**.
- For more information on Cisco vManage, see Integrating Cisco vManage with Cisco WAAS Central Manager in the chapter "Configuring Cisco AppNav."

Procedure

Step 1 Convert a Standby Cisco WAAS Central Manager to be the Primary Cisco WAAS Central Manager, as described in Converting a Standby Cisco WAAS Central Manager to a Primary Cisco WAAS Central Manager, on page 31.

Step 2 When the failed Cisco WAAS Central Manager becomes available again, configure it as a Standby Central Manager, as described in Converting a Primary Cisco WAAS Central Manager to a Standby Cisco WAAS Central Manager, on page 30, beginning with **Step 2**. Skip **Step 1** and do not use the **cms deregister** EXEC command.

Step 3 Switch both the Cisco WAAS Central Manager roles, as described in Switching Both the Cisco WAAS Central Manager Roles, on page 32.

Note In some scenarios, when a Standby Cisco WAAS Central Manager is registered newly with a Cisco WAAS Central Manager that is already managing more than 1000 Cisco WAEs, the devices may go off line. To avoid this, in case of large deployments, we recommend that you register the Standby Cisco WAAS Central Manager to the Primary Cisco WAAS Central ManagerCentral Manager at the beginning of the deployment, so that in case of an unexpected fail over the Standby takes up the Primary role.

Note When a backup operation is in progress on a Standby Cisco WAAS Central Manager that is supporting a Primary Cisco WAAS Central Manager managing more than 1000 Cisco WAEs: the Standby Cisco WAAS Central Manager goes off line if the backup operation takes more than 10 minutes. Additionally, you will not be able to login to the Primary Cisco WAAS Central Manager GUI when a backup operation is in progress.

Enabling Disk Encryption

Disk encryption addresses the need to securely protect sensitive information that flows through deployed Cisco WAAS systems and that is stored in Cisco WAAS persistent storage. The disk encryption feature includes two aspects: the actual data encryption on the Cisco WAE disk and the encryption key storage and management.

When you enable disk encryption, all the data in Cisco WAAS persistent storage will be encrypted. The encryption key for unlocking the encrypted data is stored in the Cisco WAAS Central Manager, and key management is handled by the Cisco WAAS Central Manager. When you reboot the Cisco WAE after configuring disk encryption, the Cisco WAE retrieves the key from the Cisco WAAS Central Manager automatically, allowing normal access to the data that is stored in Cisco WAAS persistent storage.

Note If a Cisco WAE is unable to reach the Cisco WAAS Central Manager during a reboot, it will do everything except mount the encrypted partitions. In this state, all traffic will be handled as pass-through. After communication with the Cisco WAAS Central Manager is restored (and the encryption key is obtained), the encrypted partitions are mounted. There is no loss of cache content.

Before you begin

Disk encryption requirements are as follows:

- You must have a Cisco WAAS Central Manager configured for use in your network.
- Your Cisco WAE devices must be registered with the Central Manager.
- Your Cisco WAE devices must be online (have an active connection) with the Cisco WAAS Central Manager. This requirement applies only if you are enabling disk encryption.
- You must reboot your Cisco WAE for the disk encryption configuration to take effect.

After you reboot your Cisco WAE, the encryption partitions are created using the new key, and any previously existing data is removed from the partition.

Any change to the disk encryption configuration, whether to enable or disable encryption, causes the disk to clear its cache. This feature protects sensitive customer data from being decrypted and accessed should the WAE ever be stolen.

If you enable disk encryption and then downgrade to a software version that does not support this feature, you will not be able to use the data partitions. In such cases, you must delete the disk partitions after you downgrade.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices >** *device-name* or **Device Groups >** *device-group-name*.

Step 2 Choose **Configure > Storage > Disk Encryption** and check the **Enable** check box to enable disk encryption. The **Enable** check box is unchecked by default.

Step 3 Select from the below options to ensure that the data is completely erased

- **Skip disk sanitization**: Existing data will be erased during reload after disk encryption disable/enable action. No additional disk sanitization will be performed.
- **Single pass disk sanitization**: Entire data partition will be sanitized by overwriting all addressable disk location using binary zeros upon next reload. This action takes six to eight hours to complete.
- **Three pass disk sanitization**: Entire data partition will be sanitized by overwriting all addressable disk location using binary zeros, binary ones and with random pattern upon next reload. This action takes upto 48 hours to complete.

When you enable or disable disk encryption, the file system is reinitialized during the first subsequent reboot. Reinitialization may take from ten minutes to several hours, depending on the size of the disk partitions. During this time, the Cisco WAE will be accessible, but it will not provide any service.

If you change the Cisco WAAS Central Manager IP address, or if you relocate the Cisco WAAS Central Manager, or replace one Cisco WAAS Central Manager with another Cisco WAAS Central Manager that has not copied over all of the information from the original Cisco WAAS Central Manager, and you reload the Cisco WAE when disk encryption is enabled, the Cisco WAE file system will not be able to complete the reinitialization process or obtain the encryption key from the Cisco WAAS Central Manager.

Step 4 Click **Submit** to save the settings. To disable disk encryption, uncheck the **Enable** check box and click **Submit**.

To enable and disable disk encryption from the Cisco WAE CLI, run the **disk encrypt** global configuration command.

Note If you are using an NPE image, note that the disk encryption feature is disabled in countries where disk encryption is not permitted.

Note When a Standby Cisco WAAS Central Manager has been in service for at least two times, the datafeed poll rate time interval (approximately 10 minutes), and has received management updates from the Primary Cisco WAAS Central Manager, the updates will include the latest version of the encryption key. Failover to the standby in this situation occurs transparently to the Cisco WAE. The datefeed poll rate defines the interval for the Cisco WAE to poll the Cisco WAAS Central Manager for configuration changes. This interval is **300 seconds** by default.

If the Cisco WAE fails to obtain the encryption key, disable disk encryption by running the **no disk encrypt enable** global configuration command from the CLI, and reload the Cisco WAE. Ensure connectivity to the

Cisco WAAS Central Manager before you enable disk encryption and reload the Cisco WAE. This process will clear the disk cache.

To view the encryption status details, run the **show disks details** EXEC command. While the file system is initializing, the **show disks details** command displays the message: **System initialization is not finished, please wait...**. You can also view the disk encryption status, whether it is enabled or disabled, in the Cisco WAAS Central Manager GUI's **Device Dashboard** window.

Configuring a Disk Error-Handling Method

Before you begin

Note Configuring and enabling disk error handling is no longer necessary for devices that support disk hot-swap. In Cisco WAAS Version 4.0.13 and later, the software automatically removes from service any disk with a critical error.

If the bad disk drive is a critical disk drive, and the automatic reload feature is enabled, then the Cisco WAAS software marks the disk drive bad and the Cisco WAAS device is automatically reloaded. After the Cisco WAAS device is reloaded, a syslog message and an SNMP trap are generated.

Note The automatic reload feature is automatically enabled, but is not configurable on devices running Cisco WAAS Version 4.1.3 and later.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 2 Choose **Configure** > **Storage** > **Disk Error Handling**.

The **Disk Error Handling Current Settings** window appears.

Step 3 The **Disk Error Handling Current Settings** window has two check boxes:

- To enable the window for configuration, check the **Enable** check box.
- Check the **Enable Disk Error Handling Remap**. This forces the disks to attempt to remap disk errors automatically. This is checked (enabled) by default.

Step 4 To save the settings, click **Submit**.

Enabling Data Cache Management

Before you begin

The Cisco WAAS Central Manager allows you to configure existing Akamai Cache and Object Cache data partitions by increasing or decreasing the cache sizes whenever needed on the existing Cisco WAE system. Note the following scenarios with respect to Cisco WAAS devices, software version and new or subsequent Data Cache Management configuration.

Upgrading Cisco WAE-294, WAE-594, or WAE-694 with Cisco WAAS Software Version 6.1.1 and later:

- When you upgrade to Cisco WAAS Software Version 6.1.1 and later and configure the device(s) for data cache management for the first time and perform a reload.
- All the data-cache is lost on reload.

Upgrading Cisco vWAAS or Cisco ISR-WAAS for Cisco WAAS Software Version 6.x:

- When you upgrade to Cisco WAAS Software Version 6.1.1 and later, and configure the device/s for data cache management for the first time and perform a reload, both data and system partitions are re-created.
- Logs and Data Cache are cleaned up, but software version and Cisco WAAS Central Manager registration information is preserved.

Fresh deployment in all models:

- When you do a fresh deployment of Cisco WAAS Software Version 6.1.1 and later, and configure the device/s for data cache management for the first time and perform a reload, only Akamai and object-cache data is lost.

Second or subsequent configuration in all models:

- Configuring Data Cache Management for second or subsequent times cleans only the Akamai and Object cache partitions. All other partitions are retained.

Limitations for Data Cache Management

- If you want to configure data cache management from the Cisco WAAS Central Manager GUI, both the Cisco WAAS Central Manager and the devices registered with it need to be running Cisco WAAS Version 6.1.1 or later.
- The device needs to be in **Application Accelerator** mode to configure Akamai and Object Cache capability.
- The Cisco WAAS Central Manager supports mixed mode of devices in different versions. When you configure Data Cache Management at the **Device** level, the configurations apply only to the devices running Cisco WAAS Version 6.1.1 and later and not to those earlier than Cisco WAAS Version 6.1.1.
- Data Cache Management is not supported on the following hardware platforms: Cisco WAVE-7541, WAVE-7571 and WAVE-8541, Cisco vWAAS-12000 and vWAAS-50000.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 2 Choose **Configure** > **Storage** > **Cache Size Management**.

The **Cache Size Management** window appears.

Step 3 Select from the available options.

- **Default**: Sets the available partition size for Akamai cache and Object cache according to predefined values.
- **Akamai-Object Cache-Equal**: Sets the available partition size to 50% each, for both Akamai cache and Object cache.
- **Akamai-weight1**: Sets the partition size to 60% for Akamai cache and 40% for Object cache.
- **Akamai-weight2**: Sets the partition size to 80% for Akamai cache and 20% for Object cache.
- **ObjectCache-weight1**: Sets the partition size to 60% for Object cache and 40% for Akamai cache.
- **ObjectCache-weight2**: Sets the partition size to80% for Object cache and 20% for Akamai cache.

Step 4 To save the settings, click **Submit**.

Consider the following:

- The data partition is effective only after the device is reloaded.
- To enable data cache management the CLI, run the **disk cache enable** global configuration command.
- To view the data cache details, choose choose **Devices** > *device-name* or **Device Groups** > *device-group-name* > **Monitor** > **CLI Commands** > **Show Commands** and select the **show disk cache-details** command. The cache details are displayed for devices that are running Cisco WAAS Version 6.1.1.

Note When you downgrade a device from Cisco WAAS Version 6.1.1 to any 5.x.x version, object-cache is no longer valid. As a result the associated CLIs are also not visible on the devices.

Activating All Inactive Cisco WAAS Devices

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > **All Devices**.

The **All Devices** window appears.

Step 2 Click the **Activate All Inactive WAEs** icon in the taskbar.

The **Activate All Inactive WAEs** window appears.

Step 3 To choose existing location for all the inactivated Cisco WAAS devices, click the **Select an existing location for all inactive WAEs** radio button, and then choose a location from the corresponding drop-down list.

Alternatively, choose to create a new location for each inactive device by clicking the **Create a new location for each inactive WAE** radio button. Specify a parent location for all newly created locations by choosing a location from the Select a parent location for all newly created locations drop-down list.

Step 4 Click **Submit**.

The inactive Cisco WAEs are reactivated and placed in the specified location.

Rebooting a Device or Device Group

This sectontion contains the following topics:

Rebooting a Device

Before you begin

Using the Cisco WAAS Central Manager GUI, you can reboot a device or device group remotely. For how to reboot a device group, see Rebooting a Device Group, on page 40.

Note If you reboot a Cisco WAAS Central Manager that has Secure Store enabled with **user-provided passphrase** mode, you must reopen Secure Store after the reboot by running the **cms secure-store open** EXEC command.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.

The device **Dashboard** window appears.

Step 2 In the **Device Info** pane, click the **Reload** icon.

You are prompted to confirm your decision.

Step 3 To confirm that you want to reboot the device, click **OK**.

Step 4 To reboot a device from the CLI, run the **reload** EXEC command.

Rebooting a Device Group

Before you begin

Using the Cisco WAAS Central Manager GUI, you can reboot a device or device group remotely. For how to reboot an individual device, see Rebooting a Device, on page 39.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** > *device-group-name*.

The **Modifying Device Group** window appears.

Step 2 In the taskbar, click the **Reboot All Devices in Device Group** icon.

You are prompted to confirm your decision.

Step 3 To confirm that you want to reboot the device group, click **OK**.

Performing a Controlled Shutdown

A controlled shutdown refers to the process of properly shutting down a Cisco WAAS device without turning off the power on the device (the fans continue to run and the power LED remains on). With a controlled shutdown, all of the application activities and the operating system are properly stopped on the appliance, but the power remains on. Controlled shutdowns can help you minimize the downtime when the appliance is being serviced.

Caution If a controlled shutdown is not performed, the Cisco WAAS file system can be corrupted. It also takes longer to reboot the appliance if it was not properly shut down.

You can perform a controlled shutdown from the CLI by running the **shutdown** EXEC command. For more details, see the *Cisco Wide Area Application Services Command Reference Guide* .

If you are running Cisco WAAS on a network module that is installed in a Cisco access router, perform a controlled shutdown from the router CLI by running the **service-module integrated-service-engine** *slot/unit* **shutdown** EXEC command. For more details, see *Configuring Cisco WAAS Network Modules for Cisco Access Routers*.