Cisco Wide Area Application Services Upgrade Guide

Published: May 31, 2011

Software Version 4.4

This document describes how to upgrade Cisco Wide Area Application Services (WAAS) to software release 4.4.x. This document also describes how to migrate an existing WAAS 4.0.x legacy Common Internet File System (CIFS) infrastructure to the CIFS application accelerator introduced in WAAS 4.1.

Note The procedures in this note contain CLI command examples. For more information about the commands used in the procedures, see the *Cisco Wide Area Application Services Command Reference*.

This document contains the following sections.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About Upgrading to Version 4.4

This section provides information for upgrading to the 4.4.x release and includes the following topics:

WAAS Versions and Upgrade Path

Upgrading to release 4.4.x is supported from certain older releases only. If you have a WAAS device that is running a release from which upgrading directly to release 4.4.x is not supported, first upgrade the device to the next highest supported intermediate release, and then upgrade to the desired 4.4.x release.

Table 1-1 shows the upgrade path for upgrading a WAAS device to release 4.4.x.

Table 1-1 WAAS Versions and Upgrade

Current WAAS Software	Intermediate Upgrade Version	Final Upgrade Version
4.0.x	Direct upgrade not supported. Upgrade first to a version listed below, then to version 4.4.x.	4.4.x
4.1.x, 4.2.x, or 4.3.x	4.1.1d, 4.1.3, 4.1.3b, 4.1.5c, 4.1.5f, 4.1.7, 4.1.7b, 4.2.1, 4.2.3, 4.2.3c, 4.3.1, and 4.3.3	4.4.x

Note To upgrade the WAAS network to WAAS 4.4.x, the Central Manager must be at an equal or later software version than the other WAE devices in the network.

Note If you are using legacy mode WAFS, before you can upgrade to WAAS 4.4.x, you must first migrate all devices from legacy mode WAFS to the transparent CIFS accelerator, because legacy mode WAFS is not supported in version 4.4. For information on CIFS migration, see the "Migrating from CIFS Legacy Mode to CIFS Accelerator Mode" section on page 13.

For important upgrade details, consult the WAAS *Release Note for Cisco Wide Area Application Services* for the software version to which you want to upgrade.

Removed Features

With the introduction of release 4.4, the following features have been removed and are no longer supported:

- Legacy mode WAFS—This mode is no longer supported in the Central Manager and WAEs and upgrading is prevented if legacy mode WAFS is enabled on any device in the WAAS network. Legacy WAFS users must migrate to the transparent CIFS accelerator before upgrading. See the "Migrating from CIFS Legacy Mode to CIFS Accelerator Mode" section on page 13.

- Legacy mode print services—This print services mode is no longer supported in WAEs and the Central Manager, which can no longer act as a print repository or distribute print drivers. Legacy print services users must migrate to the Windows Print accelerator or a virtual blade print server solution.

  A version 4.4 Central Manager can continue to manage earlier version WAEs that have legacy print services enabled, but print services can be configured on these WAEs only through the device CLI.
- WAE-511, WAE-611, and WAE-7326 platforms—These WAE models are no longer supported and WAAS version 4.4 does not operate on these appliances. Upgrading is prevented on these platforms and the WAAS 4.4.1 software image is not listed in the Central Manager Software Update window if you attempt to update one of these individual devices.

Upgrade Prerequisites and Guidelines

This section describes the upgrade prerequisites and guidelines. Consult the WAAS *Release Note for Cisco Wide Area Application Services* of the particular WAAS software version for additional requirements and guidelines.

This section includes the following topics:

Cisco RAID Controller Firmware Upgrade and Validation

Before upgrading the software, you must upgrade the WAE firmware to avoid possible firmware related issues on WAE-674, WAE-7341, and WAE-7371 devices. We recommend using Firmware version L4_15427 or later.

The symptoms of firmware issues are as follows:

- Syslog output contains several instances of the following message:

  ```
  WAAS-SYS-3-900000: sd 0:0:0:0: rejecting I/O to offline device."
  ```

- A sysreport and running-config cannot be generated and copied to /local/local1.

  Both of the above symptoms are an indication of the file system becoming read only during traffic flow.

- An increasing number of pending connections appear in the output of the **show statistics tfo** command, indicating that new connections cannot be optimized. You can use this command to proactively check the functionality of the system.

The solution is to upgrade to the 5.2-0 (15427) RAID Controller Firmware, which can be found on Cisco.com at the Cisco Wide Area Application Services (WAAS) Firmware Downloads (registered customers only) page. The firmware binary image is named L4_15427_FIRMWARE.bin.

To determine the RAID controller firmware version on a device, run the **show disks tech-support** EXEC command. Look for the Firmware line, where the version number is shown at the end in parentheses, as follows:

```
Firmware                                  : 5.2-0 (15427)
```

The version number must be 15427 or higher.

Instructions for applying and validating the firmware update are posted on cisco.com together with the firmware and are named L4_15427_FIRMWARE.pdf.

WAAS Software Upgrade Guidelines

Observe the following prerequisites before you upgrade the software:

- Make sure the IOS version on the router/switch has been scrubbed for WCCP issues for your specific platform. This needs to be done only on routers/switches participating in transparent redirection and is not applicable to PBR or inline deployments. If this was not done and there is a current active WAAS network, disable WCCP in the routers/switches in the data center and all branches before the software upgrade to 4.4.x.
- If you are using legacy mode WAFS, you must first migrate all devices from legacy mode WAFS to the transparent CIFS accelerator, because legacy mode WAFS is not supported in version 4.4 and later. For information on CIFS migration, see the "Migrating from CIFS Legacy Mode to CIFS Accelerator Mode" section on page 13. Perform the migration of CIFS legacy mode to CIFS accelerator mode in a separate change window from the WAAS software version upgrade.
- The minimum firmware release required is 15427 for all WAE-7371, WAE-7341, and WAE- 674 devices.
- Consult the WAAS *Release Note for Cisco Wide Area Application Services* of the particular WAAS software version for additional requirements and guidelines.

Note If you are using WCCP, the default value for the WCCP source IP mask changed in version 4.2.1 and later to 0xF00. However, if you are upgrading a WAE that used the previous default WCCP source IP mask of 0x1741 (or any custom mask), its WCCP mask will not be changed. And if you are downgrading a WAE to a version earlier than 4.2.1, its WCCP source IP mask will not be changed. By not changing the mask during upgrade or downgrade, the WAE avoids unexpected mask changes and WCCP farm disruptions. All WAEs in a WCCP farm must have the same mask or they will not participate in the farm.

Capacity Planning

Capacity planning is an ongoing process as branches and applications are added. Check the WAE devices to make sure that they are providing adequate caching and optimization and that connection limits are not exceeded.

Upgrade Methods

The following three methods can be used to perform the WAAS upgrade and transfer the new software image onto the WAE devices in the WAAS network:

- Use the Central Manager Software Update feature to distribute the WAAS software image to WAAS devices.
- Install the software image directly using the Rescue CD to perform a clean install (not an upgrade), which deletes the previous WAAS software image, deletes any cache, and so forth.
- Use FTP or TFTP directly on the WAE via the CLI.

The last method is described in this document. The other methods are described in the *Cisco Wide Area Application Services Configuration Guide* chapter entitled "Maintaining Your WAAS System."

Two different WAAS software images are available, as follows:

- Universal—Includes Central Manager and Application Accelerator functionality. You can use this type of software file to upgrade either a Central Manager or an Application Accelerator device but this software file is significantly larger, so for Application Accelerator devices we recommend using the Accelerator only image.
- Accelerator only—Includes Application Accelerator functionality only. You can use this type of software file to upgrade only an Application Accelerator device.

Be sure to use the correct type of software image for the devices you want to upgrade, either a Universal or Accelerator only image.

Additionally, a separate set of No Payload Encryption (NPE) images are provided that have the disk encryption feature disabled. These images are suitable for use in countries where disk encryption is not permitted. Be sure to use the standard or NPE software images as required. You can recognize the NPE images by the "-npe" designation in the image filenames.

Upgrade Sequence

To upgrade a WAAS network to WAAS 4.4.x, the software version installed on the Central Manager (CM) must be equal to or later than the version installed on the other WAE network devices. For this reason, you must upgrade the Central Managers before you upgrade the rest of the WAE devices.

The upgrade process consists of the following steps:

1. Create a back up of the Central Manager database and save it to an external hard drive (see the "Creating a Backup of the Primary Central Manager" section on page 6).
2. Upgrade the Secondary Central Manager if present (see the "Upgrading the Standby Central Manager" section on page 6).
3. Upgrade the Primary Central Manager (see the "Upgrading the Primary Central Manager" section on page 7).
4. Upgrade the other WAE network devices (see the "Upgrading the Branch WAAS Software" section on page 7).

Upgrading the Central Manager WAAS Software

This section describes how to back up the Primary Central Manager, update the Secondary Central Manager (if present), and update the Primary Central Manager.

This section contains the following topics:

Creating a Backup of the Primary Central Manager

This procedure describes how to back up the Primary Central Manager database and copy the backup file to an FTP server.

Procedure

Step 1 Telnet to the primary CM.

```
telnet cm_ip_address
```

Step 2 Create the database backup.

```
cms database backup
```

Step 3 Copy the backup file to a remote FTP server.

```
copy disk ftp ftpserver / waas-db-filename.dump remote_filename
```

Step 4 Verify that the backup file copied correctly by checking the file for correct size and timestamp.

Upgrading the Standby Central Manager

This procedure describes how to upgrade the WAAS software on the Standby Central Manager.

Procedure

Step 1 Telnet to the Standby CM IP address.

```
telnet standby_cm_ip_address
```

Step 2 Copy the new software image to the Standby CM.

```
copy ftp install ftpserver / waas-image.bin
```

This example assumes that the file is in the root directory of the FTP server. Provide the correct path if needed.

Step 3 Reload the Standby CM.

```
reload
```

Step 4 Verify that the new image loaded correctly.

```
show version
```

Step 5 Ping the Primary CM and branch WAE devices to confirm connectivity.

Step 6 Wait at least 5 minutes and then confirm the database last synchronization time to ensure that the database has been synchronized.

```
show cms info
```

Step 7 From the Primary CM, confirm that the status indicator for the Secondary CM is online and green.

Upgrading the Primary Central Manager

This section describes how to upgrade the WAAS software on the Primary Central Manager.

Prerequisites

Upgrade the secondary Central Manager before you upgrade the Primary Central Manager (see the "Upgrading the Standby Central Manager" section on page 6).

Procedure

Step 1 Telnet to the Primary CM IP address.

```
telnet primary_cm_ip_address
```

Step 2 Copy the new software image to the Primary CM.

```
copy ftp install ftpserver / waas-image.bin
```

This example assumes that the file is in the root directory of the FTP server. Provide the correct path if needed.

Step 3 Reload the Primary CM.

```
reload
```

Step 4 Verify that the new image loaded correctly.

```
show version
```

Step 5 Ping the Standby CM and branch WAE devices to confirm connectivity.

Step 6 Confirm that the CMS services are running.

```
show cms info
```

Step 7 Verify that all the WAE devices are online and are in the AllWAASGroup.

a. Choose **My WAN > Manage Devices** and verify that all the WAE devices are online and have a green device status.

b. Choose **My WAN > Manage Device Groups > AllWAASGroup > Assign Devices** and verify that all WAEs are listed with a green check mark.

Checkpoint

The CMs are updated with the new WAAS software version 4.4.x. The Secondary CM was upgraded first followed by the Primary CM.

Upgrading the Branch WAAS Software

This section describes how to upgrade each WAAS branch WAE to version 4.4.x.

Prerequisites

The prerequisites for upgrading are as follows:

- Upgrade the Secondary and Primary CMs before upgrading the branches (see the "Upgrading the Central Manager WAAS Software" section on page 5).
- Copy the WAAS software image to a local server (using FTP) for use during the upgrade or push the software image to WAE devices through the CM. See the *Cisco Wide Area Application Services Configuration Guide* chapter named "Maintaining Your WAAS System."

This section includes the following topics:

Preparing to Upgrade the Branch WAE

We recommend that you check the health of the WAE devices before upgrading the branch WAE devices.

Procedure

Step 1 Access the CM GUI.

```
https://cm_ip_address:8443
```

Step 2 Verify that all the WAE devices are online (green).

Step 3 Address any alarm conditions that may exist.

Upgrading the Branch WAE Software

This procedure shows how to upgrade the branch WAE software.

Procedure

Step 1 Open a console or telnet session to the branch WAE.

Step 2 Copy the software image to the WAE.

```
copy ftp install ftpserver / waas-image.bin
```

This example assumes that the file is in the root directory of the FTP server. Provide the correct path if needed. You can use either the Universal or Accelerator only images.

Step 3 Reload the WAE.

```
reload
```

Step 4 Verify that the image installed correctly.

```
show version
```

Step 5 Verify that the correct licenses are installed.

```
show license
```

If an Enterprise license has been purchased and not enabled, go to Steps 6 and 7. Otherwise, go to Step 8.

Step 6 (Optional) Clear the Transport license.

```
clear license Transport
```

Step 7 (Optional) Add the Enterprise license.

```
license add Enterprise
```

Step 8 Save the configuration.

```
copy running-config startup-config
```

Step 9 From the WAAS CM GUI, choose **My WAN > Devices >** *branchWAE* and verify that the WAE is online and has a green device status.

Step 10 Verify the WAE device functionality as follows:

a. Assuming that WCCP is used for the traffic interception method, verify the WCCP is functioning properly.

```
show run | include wccp
```

b. (Optional) Confirm that flows are being optimized.

```
show statistics connection
```

c. Confirm that the Enterprise license is enabled.

```
show license
```

If the Enterprise license is not enabled, proceed with Steps d through f.

d. Clear the Transport license.

```
clear license Transport
```

e. Add the Enterprise license.

```
license add Enterprise
```

f. Save the changed configuration.

```
copy running-config startup-config
```

Checkpoint

All the branch WAE devices within the active WAAS network are upgraded to release 4.4.x.

Upgrading the Data Center WAAS Software

This section describes how to prepare for and upgrade the data center WAAS Software. The data center WAE devices will be upgraded to 4.4.x.

This section includes the following topics:

Preparing to Upgrade Data Center WAAS Software

This procedure shows how to prepare for upgrading the data center WAE devices.

Procedure

Step 1 Access the primary Central Manager GUI.

`https://cm_ip_address:8443`

Step 2 Verify that all the WAE devices are online (green).

Step 3 Address any alarm conditions that may exist.

Enabling/Disabling WCCP on WAE Devices in a Cluster

This section describes the recommended practice of enabling or disabling WCCP on WAE devices in a cluster.

When enabling WCCP on WAE devices in a cluster, first enable WCCP on the WAEs in the cluster, followed by enabling WCCP on the intercepting routers/switches, provided that you have validated the IOS version with a bug scrub for WCCP related issues for your specific platform.

To disable WCCP, we recommend that you disable WCCP on the WAE devices first and wait for a graceful shut down to allow existing TCP connections to expire before disabling WCCP on the intercepting routers/switches. If a scrub of IOS has been performed, you can proceed with upgrading the WAE devices without disabling WCCP.

The following ACL template is recommended while running WCCP (IOS version and hardware platform permitting). The template must be altered to suit your environment.

```
!
ip access-list extended WCCPLIST
 remark ** ACL used for WCCP redirect-list **
 remark **WAAS WCCP Mgmt ports **
 deny   tcp any any eq telnet
 deny   tcp any any eq 22
 deny   tcp any any eq 161
 deny   tcp any any eq 162
 deny   tcp any any eq 123
 deny   tcp any any eq bgp
 deny   tcp any any eq tacacs
 deny   tcp any eq telnet any
 deny   tcp any eq 22 any
 deny   tcp any eq 161 any
 deny   tcp any eq 162 any
 deny   tcp any eq 123 any
 deny   tcp any eq bgp any
 deny   tcp any eq tacacs any
 remark ** Allow only explicit traffic **
  permit tcp x.x.x.x 0.0.0.255 y.y.y.y 0.0.0.255
  permit tcp y.y.y.y 0.0.0.255 x.x.x.x 0.0.0.255
 remark **
 remark ** Deny all other traffic
 deny ip any any
!
```

Upgrading the Data Center WAE

This procedure shows how to upgrade the data center WAE software.

Note For a graceful termination of existing TCP flows optimized by WAAS, we recommend that you disable WCCP on the WAE first, as described in Step 1 of this procedure. Then wait until the graceful timer counts down, during which period no new connections are redirected to the WAE and the existing connections are allowed to gracefully terminate. Upon completion of the countdown timer, all existing connections are terminated.

Note This procedure removes the WAE from the interception path while the upgrade is done and applies to deployments that use WCCP for redirection in the data center. If you are not using WCCP interception in the data center, you should use another method to remove the WAE from the interception path. For an inline deployment, use the **interface InlineGroup** *slot/group* **shutdown** global configuration command to bypass the traffic on the active inline groups. In a serial inline cluster, shut down the interfaces on the intermediate WAE first, then on the optimizing WAE in the cluster. For a deployment using Cisco ACE for interception, gracefully shut down the ACE real server by using the **no inservice** command in either real server host or real server redirect configuration mode.

Procedure

Step 1 Disable WCCP on the WAE as follows to allow a graceful termination of existing TCP flows that are optimized by WAAS:

a. Disable WCCP.

```
config
no wccp version 2
exit
```

b. Wait until the countdown expires or press **Ctrl + C** to skip waiting for graceful WCCP shutdown.

c. Verify that WCCP is disabled.

```
show wccp status
```

d. Save the changed configuration.

```
copy running-config startup-config
```

Step 2 (Optional) Disable WCCP on the intercepting router/switch. This step is recommended only if the IOS version on the router/switch has not been scrubbed for WCCP issues for your specific platform.

```
config t
no ip wccp 61
no ip wccp 62
exit
```

Step 3 (Optional) Verify that WCCP is disabled. This step is needed only if you disabled WCCP in Step 2.

```
show ip wccp
```

Step 4 Upgrade the data center WAE software as follows:

a. Open a console or telnet session to the data center WAE.

b. Copy the software image to the WAE.

```
copy ftp install ftpserver / waas-image.bin
```

This example assumes that the file is in the root directory of the FTP server. Provide the correct path if needed. You can use either the Universal or Accelerator only images.

c. Reload the WAE.

```
reload
```

d. Verify that the image installed correctly.

```
show version
```

e. Confirm that WCCP is disabled.

```
show wccp status
```

f. Save the changed configuration.

```
copy running-config startup-config
```

Step 5 From the WAAS CM GUI, choose **My WAN** > **Devices** > *dataCenterWAE* and verify that the WAE is online and has a green device status.

Step 6 (Optional) Enable WCCP on all intercepting routers/switches in the router list as follows:

a. Telnet to each core router/switch.

b. Enable WCCP.

```
config t
ip wccp 61 redirect-list ACL_name
ip wccp 62 redirect-list ACL_name
```

To see an example ACL template, see the "Enabling/Disabling WCCP on WAE Devices in a Cluster" section on page 10.

This step is needed only if you disabled WCCP in Step 2.

Step 7 Verify WAE device functionality as follows:

a. Enable WCCP.

```
config
wccp version 2
exit
```

b. Confirm that redirecting intercepting router IDs are seen.

```
show wccp routers
```

c. Confirm that all WAE devices in the cluster are seen.

```
show wccp wide-area-engine
```

d. Confirm that the packet count to the WAE is increasing and no loops are detected.

```
show wccp gre
```

e. Verify that the buckets assigned for Service Group 61 match those of Service Group 62 and are assigned to the WAE.

```
show wccp flows tcp-promiscuous detail
```

f. Confirm that flows are being optimized.

```
show statistics connection
```

Checkpoint

All WAE devices in the data center are upgraded to release 4.4.x and have WCCP enabled.

Migrating from CIFS Legacy Mode to CIFS Accelerator Mode

This section describes how to migrate from CIFS legacy mode to CIFS accelerator mode, which is required before you can upgrade to WAAS version 4.4.1, which does not support CIFS legacy mode.

If you have previously migrated to CIFS accelerator mode, you can skip this section, unless you receive legacy WAFS error messages when you attempt to upgrade to version 4.4. For more information, see the "Legacy WAFS Bypass Script" section on page 14.

For more detailed information about CIFS migration, see the whitepaper *Cisco WAAS Software 4.1 Common Internet File System Migration*.

The two methods for migrating from CIFS legacy mode to CIFS accelerator mode are as follows:

- Disruptive Migration—Enables the CIFS accelerator at the time of upgrade. CIFS legacy mode must first be disabled, at which time the CIFS accelerator can be enabled. This method is disruptive and affects CIFS optimized traffic between the WAE devices on the branch and data center sides until all the sites have the CIFS accelerator enabled. It can be applied to any existing WAAS 4.0.x deployment. This method requires little preplanning, but end users do experience short WAAS and WAAS files service outages; however, it has the advantage of a relatively quick and straightforward execution.
- Graceful Migration—Allows CIFS legacy mode to continue functioning while migrating to the CIFS accelerator. This method is non-disruptive and allows migration without impacting traffic between the WAE devices on the branch or data center sides as the sites are migrated to the CIFS accelerator. This method requires preplanning and systematic execution over a significant period of time, but it has the advantage of nonstop operation of WAAS and WAAS file services.

Note CIFS legacy mode is not supported in version 4.4 and later. If you are upgrading from version 4.0 to an intermediate version and then to version 4.4, we recommend using the disruptive migration method.

Note The CIFS cache is not lost during migration from CIFS legacy mode to CIFS accelerator mode. Disk allocation for CIFS in all releases is similar.

Note Auto-discovery differs between the CIFS legacy and CIFS accelerator modes. Legacy mode uses CIFS auto-discovery, which is based on selection of the "best" Core device from the configured Cores for each Edge, whereas CIFS accelerator mode uses standard WAAS auto-discovery, which is based on routing and interception. You must verify that the network and the interception are configured properly and an existing stable CIFS environment exists before the migration. The differences between the auto-discovery mechanisms may lead to different Core selections in the accelerator and legacy modes.

This section contains the following topics:

Legacy WAFS Bypass Script

On upgrade to version 4.4, if you receive an alarm or error message that legacy WAFS services are enabled on your WAAS network and you are sure that you have removed all legacy WAFS configurations, it may be because of leftover configurations that were not properly cleaned up.

The alarm is as follows: "Legacy WAFS and Print features are not available in the image being downloaded. Installation can only proceed after WAFS CORE/EDGE services have been disabled via Central Manager GUI on all Devices and Device Groups. Refer syslog.txt further details."

The error message is as follows:

```
WAFS_EDGE_TOTAL_____________________________________1
WAE_________________________________________________1
1. 674-147
ERROR: The image being downloaded does NOT support Legacy WAFS or Legacy Print Services.
Central Manager will not upgrade till WAFS Core and/or WAFS edge services are enabled on
the network.
Please disable them first from the Central Manager GUI before upgrading Central Manager.

If the reported configurations are because of an incomplete migration and
the services are no longer effective, then use the command
<script execute wafs_services_not_in_active_use.pl>, from the Command Line Interface
to bypass the check and retry again.
NOTE: If the WAFS services are active on the network, then upgrade to 4.4.x
will impact the file services.
```

The error message reports the names (up to 10) of devices and device groups that appear to be running WAFS services and the full list is reported in the syslog. Check these devices and device groups for enabled legacy WAFS services and disable any legacy WAFS services that are enabled.

If you continue to receive the alarm or error message on upgrade and you are certain that no WAFS services are enabled on these devices or device groups, then you can run a script to bypass the legacy WAFS check and allow the upgrade to version 4.4. The command syntax and name of the script is reported in the error message and is as follows:

```
centralmanager# script execute wafs_services_not_in_active_use.pl
```

After you run this script, you can retry the upgrade to version 4.4. If any legacy WAFS services are enabled on devices being upgraded, they are discarded and file services are interrupted. You must use the CIFS accelerator for file services acceleration, see the "Performing a Disruptive Migration" section on page 15 for more information.

Migrating Preposition Directives and Dynamic Shares

Regardless of the method that you use to migrate to the CIFS accelerator, you should migrate the preposition directives and dynamic shares from legacy mode to CIFS accelerator mode before upgrading to version 4.4. If you do not migrate legacy preposition directives and dynamic shares before upgrading, they are removed by the upgrade and you must recreate them afterwards in CIFS accelerator mode.

You can migrate preposition directives and dynamic shares to CIFS accelerator mode as follows:

Step 1 Edit each preposition directive to remove the assigned edge devices:

a. From the WAAS Central Manager GUI navigation pane, choose **Configure > File Services > Preposition**. The Preposition Directives window appears.

b. Click the **Edit** icon next to the preposition directive that you want to edit.

c. Click the **Assign Edge Devices** tab to display the assigned edge devices.

d. Click the **Remove all Edge Devices** icon to remove all edge devices.

e. Click the Assign Edge Groups tab to display the assigned edge device groups.

f. Click the **Remove all Edge Groups** icon to remove all edge device groups.

Step 2 Edit each preposition directive to change the mode to transparent CIFS accelerator mode:

a. Uncheck the box **CIFS - Use WAFS transport mode** and enter the file server name in the File Server field.

b. From the Location drop-down list, choose the device location that will provide browsing services for the file server. For the best browsing performance, specify a location that is close to the file server.

c. In the User name, Password, and Confirm fields, enter the username and password credentials for the file server. If the username is in a Windows domain, specify the domain name as part of the User name field, as follows: domain\username. The access credentials that you enter must allow read access to the prepositioned root directories and to their parent directories.

d. Click **Submit**.

Step 3 If there are existing dynamic shares defined, edit each dynamic share to change the mode to transparent CIFS accelerator mode:

a. Uncheck the box **CIFS - Use WAFS transport mode** and enter the file server name in the File Server field.

b. In the User name, Password, and Confirm fields, enter the username and password credentials for the file server. If the username is in a Windows domain, specify the domain name as part of the User name field, as follows: domain\username. These credentials are used only to access the file server when you click the **Browse** button.

c. Click **Submit**.

For additional information about CIFS migration and creating preposition directives, see the whitepaper *Cisco WAAS Software 4.1 Common Internet File System Migration*.

Performing a Disruptive Migration

This procedure shows how to perform a disruptive migration from CIFS legacy mode to CIFS accelerator mode. It is the simplest and easiest method to perform and is recommended if you choose not to use the graceful migration procedure. During the migration, CIFS connections are optimized with TFO/DRE but they are not CIFS accelerated until the WAE devices have been upgraded to a release with the CIFS accelerator enabled. Existing legacy CIFS connections are closed during the upgrade and the migration. Additionally, it requires several reboots on each WAE device.

Procedure

Step 1 Log in to the primary CM GUI.

`https://cm_ip_address:8443`

Step 2 Verify that all the WAE devices are online (green).

Step 3 Address any existing alarm conditions before proceeding.

Step 4 From the CM GUI, disable CIFS legacy mode and enable the CIFS accelerator as follows:

a. Choose **My WAN > Manage Devices >** *EdgeWAE* **> Configure > Legacy Services > WAFS Edge Configuration** and uncheck the Enable Edge Service check box.

Note You can also disable the edge service through device groups depending upon the individual network configurations. By default, all WAE devices should be members of the AllDevicesGroup, which can be used to remove edge services.

b. Choose **My WAN > Manage Device Groups >** *Core_Cluster* **> Delete Cluster** to delete the specified core cluster.

c. Choose **My WAN > Manage Devices >** *CoreWAE* **> Configure > Legacy Services > WAFS Core Configuration** and uncheck the Enable Core Server check box.

d. Choose **My WAN > Manage Devices >** *EdgeWAE* **> Configure > Enabled Features** and check the CIFS Accelerator check box. An alarm is raised informing you that the device roles changed (from legacy WAFS to CIFS accelerator) and a reload is required.

Note Check marks should now be beside TFO, DRE, Persistent Compression, and CIFS Accelerator. The following Accelerator check boxes should be unchecked (unless the appropriate licenses have been installed): Video, MAPI, NFS, HTTP, SSL, and EPM.

Note You can also enable the CIFS accelerator through device groups depending upon the individual network configurations. By default, all WAE devices should be members of the AllDevicesGroup, which can be used to enable CIFS accelerator.

e. Reload each affected WAE.

```
reload
```

Note You can initiate a reload though the CM either individually or through the Device Groups to which the WAE devices belong. If the WAE devices are divided into Device Groups, by default, all the devices are members of the AllDevicesGroup, which you can use to reload all the group devices.

Step 5 Verify proper WAE functionality as follows:

a. Confirm that the redirecting intercepting router IDs are seen.

```
show wccp routers
```

b. Confirm that all WAE devices in the cluster are seen.

```
show wccp wide-area-engine
```

c. Confirm that the packet count to the WAE is increasing and no loops are detected.

```
show wccp gre
```

d. Verify that the buckets assigned for Service Group 61 match those of Service Group 62 and are assigned to the WAE.

```
show wccp flows tcp-promiscuous detail
```

e. Verify that only the CIFS accelerator is enabled.

```
show accelerators
```

f. Confirm that other flows are optimized and you see "C" for CIFS optimizations applied (seen only if CIFS traffic is present).

```
show statistics connection
```

Step 6 Remove any remaining CIFS legacy mode configurations from all devices. See the "Removing Remaining Legacy Mode Configurations" section on page 24.

Performing a Graceful Migration

This section describes how to perform a graceful migration from CIFS legacy mode to CIFS accelerator mode. It requires multiple data center WAE devices where half the devices can handle the full traffic load. This migration method might require adding new WAE devices in the data center.

Note CIFS legacy mode is not supported in version 4.4 and later. If you are upgrading from version 4.0.x to an intermediate version and then to version 4.4, we recommend using the disruptive migration method instead. (See the "Performing a Disruptive Migration" section on page 15.)

The graceful migration method consists of the following steps:

1. Logically split the existing cluster of Core WAE devices running CIFS legacy mode into two groups.
2. Configure half the WAE devices (or add others) with WCCP and the CIFS accelerator, and remove WCCP from the other half of the existing WAE devices that continue to run CIFS legacy mode.

   CIFS traffic is optimized using the CIFS legacy mode data center WAE devices, while all the other TCP connections are optimized using the CIFS accelerator WAE devices.
3. Migrate all the branch sites to the CIFS accelerator over time, gradually moving branch traffic from the legacy CIFS devices to the CIFS accelerator data center devices.
4. Remove CIFS legacy mode configurations from all remaining data center WAE devices and then enable WCCP and the CIFS accelerator on these devices.

   If you added WAE devices for the migration, you can remove them or leave them in place for added capacity.

Data Center Preparation

This section describes how to prepare for the migration in the data center, which can be done without a change window because production traffic is not affected.

This section includes the following topics:

Preparing New WAE Devices

This procedure shows how to prepare the new WAE devices that will be used in the migration and can remain in the network after the migration is completed.

Prerequisites

Confirm that version 15427 or later firmware is running on the WAE devices (see the "Cisco RAID Controller Firmware Upgrade and Validation" section on page 3).

Guidelines and Restrictions

This procedure has the following guidelines and restrictions:

- Do not enable WCCP on the new WAE devices.
- Do not register the new devices with the Central Manager at this time.

Procedure

Step 1 Install the device, burn-in, and specify the basic configuration as follows:

a. Cable, apply power, and burn in for 48 hours.

b. Open a console into the WAE.

c. Configure all network related settings.

d. Test network connectivity.

e. Ping the default gateway.

f. Ping the Primary CM IP address.

g. Ping the Secondary CM IP address (if present).

Step 2 Upgrade the WAAS software as follows:

a. Copy the software image to the device.

```
copy ftp install ftpserver / waas-image.bin
```

This example assumes that the file is in the root directory of the FTP server. Provide the correct path if needed. You can use either the Universal or Accelerator only images.

b. Reload the device.

```
reload
```

c. Verify that the software is installed correctly by checking the version number of the installed software.

```
show version
```

d. Confirm that WCCP is disabled.

```
config
no wccp version 2
exit
```

e. Configure other settings as needed.

f. Save changes to the configuration.

```
copy running-config startup-config
```

Checkpoint

At this point, you should have the new WAE installed with updated firmware and the desired WAAS software release (4.1.x, 4.2.x, or 4.3.x) installed with network connectivity. WCCP is not yet configured and this device is not yet registered with the CM.

Note For information about preposition and dynamic shares, see the Release Note for Cisco Wide Area Application Services (Software Version 4.4.1x).

Enabling/Disabling WCCP on WAE Devices in a Cluster

This section describes the recommended practice of enabling or disabling WCCP on WAE devices in a cluster.

When enabling WCCP on WAE devices in a cluster, first enable WCCP on the WAEs in the cluster, followed by enabling WCCP on the intercepting routers/switches, provided that you have validated the IOS version with a bug scrub for WCCP related issues for your specific platform.

To disable WCCP, we recommend that you disable WCCP on the WAE devices first and wait for a graceful shut down to allow existing TCP connections to expire before disabling WCCP on the intercepting routers/switches. If a scrub of IOS has been performed, you can proceed with upgrading the WAE devices without disabling WCCP.

The following ACL template is recommended while running WCCP (IOS version and hardware platform permitting). The template must be altered to suit your environment.

```
!
ip access-list extended WCCPLIST
 remark ** ACL used for WCCP redirect-list **
 remark **WAAS WCCP Mgmt ports **
 deny   tcp any any eq telnet
 deny   tcp any any eq 22
 deny   tcp any any eq 161
 deny   tcp any any eq 162
 deny   tcp any any eq 123
 deny   tcp any any eq bgp
 deny   tcp any any eq tacacs
 deny   tcp any eq telnet any
 deny   tcp any eq 22 any
 deny   tcp any eq 161 any
 deny   tcp any eq 162 any
 deny   tcp any eq 123 any
 deny   tcp any eq bgp any
 deny   tcp any eq tacacs any
 remark ** Allow only explicit traffic **
  permit tcp x.x.x.x 0.0.0.255 y.y.y.y 0.0.0.255
  permit tcp y.y.y.y 0.0.0.255 x.x.x.x 0.0.0.255
 remark **
 remark ** Deny all other traffic
 deny ip any any
!
```

Disabling WCCP on CIFS Legacy WAE and Activating WCCP on CIFS Accelerator WAE

This procedure shows how to activate WCCP on the CIFS accelerator WAE and disable WCCP on the CIFS legacy WAE.

Guidelines and Restrictions

This procedure has the following guidelines and restrictions:

- When enabling WCCP, we recommend using an ACL to permit interesting traffic to and from sites to be optimized. Otherwise, use a standard ACL template as shown in the "Enabling/Disabling WCCP on WAE Devices in a Cluster" section on page 10.
- For CIFS validation, see the "Additional Information—Performing CIFS Validity Testing and Performing a Rollback" section on page 29.
- Although WCCP has been removed from the WAE devices at the data center with CIFS legacy mode configured, CIFS continues to work. The connection between the Edge WAE devices and the Core WAE devices in CIFS legacy mode is established through a point-to-point connection that does not involve WCCP. This point-to-point connection is set up during the configuration of connectivity directives.

Procedure

Step 1 Disable WCCP on the existing Core WAE running CIFS legacy mode as follows:

a. Telnet to the Core WAE.

b. Disable WCCP.

```
configure
no wccp version 2
exit
```

c. Verify that WCCP is disabled.

```
show wccp status
```

d. Save the configuration change.

```
copy running-config startup-config
```

Step 2 On the CM, activate the new data center WAE that is running the CIFS accelerator as follows:

a. Log in to the CM.

b. Choose **My WAN** > **Devices** > *newWAE* > **Activate**.

Step 3 Enable WCCP on all intercepting routers/switches as follows:

a. Telnet to each router/switch.

b. Enable WCCP.

```
config t
ip wccp 61 redirect-list ACL_name
ip wccp 62 redirect-list ACL_name
exit
```

Step 4 Enable WCCP on the new WAE that is running the CIFS accelerator as follows:

Note When enabling WCCP on WAE devices in a cluster, enable WCCP on the WAE with the lowest IP followed by the WAE with the second lowest and so forth, and then enable WCCP on the intercepting router/switch (see the "Enabling/Disabling WCCP on WAE Devices in a Cluster" section on page 10).

a. Telnet to the WAE.

b. Enable WCCP.

```
configure
wccp version 2
exit
```

Step 5 On the branch WAE devices, check and verify that the CIFS legacy mode is operating and verify that a port 4050 tunnel exists to the Core WAE that is still running CIFS legacy mode.

```
show statistics connection
```

Checkpoint

At this point in the process, you now have two sets of WAE devices in the data center:

- One set is running CIFS legacy mode with WCCP disabled but is still functioning as a Core WAE cluster for CIFS legacy mode.
- The second set has WCCP and the CIFS accelerator enabled and is optimizing all other applications.

CIFS is optimized one way only on connections initiated at the branches to the data center. These connections rely on the configured CIFS connectivity directives. Because WCCP is enabled on the branches only and not at the data center, at the branch site, TCP traffic is redirected to the WAE where the CIFS port 4050 point-to-point tunnel is used to optimize CIFS traffic depending upon the configured connectivity directives.

For connections initiated at the data center, because WCCP is enabled only on the WAE devices running CIFS accelerator mode, CIFS is not optimized unless the paired site is also running the CIFS accelerator.

Migrating Branch WAE Devices from CIFS Legacy Mode to CIFS Accelerator Mode

This procedure shows how to migrate branch WAE devices from CIFS legacy mode to CIFS accelerator mode. Using the Central Manager, you migrate selected sites to the CIFS accelerator by removing the checkmark from the WAFS Edge Configuration page (and also, if configured, from the WAFS Core Configuration page) on the individual branch WAE devices. Then the CIFS accelerator is enabled.

The migration of sites continues until all the branch sites have been successfully migrated to the CIFS accelerator and no branch sites or devices exist with CIFS legacy mode enabled.

Procedure

Step 1 Log in to the primary CM GUI.

`https://cm_ip_address:8443`

Step 2 Verify that all the WAE devices are online (green).

Step 3 Address any alarm conditions before proceeding.

Step 4 From the CM GUI, disable CIFS legacy mode and enable CIFS accelerator mode as follows:

a. Choose **My WAN > Manage Devices >** *EdgeWAE* **> Configure > Legacy Services > WAFS Edge Configuration** and uncheck the Enable Edge Service check box.

Note You can also disable features through device groups depending on how your WAAS network is designed. The ability to disable device features either individually or as a group allows you to migrate certain sites to CIFS accelerator while other sites continue to optimize CIFS using the legacy mode.

b. Choose **My WAN > Manage Device Groups >** C*ore_Cluster* **> Delete Cluster** to delete the selected cluster.

c. Choose **My WAN > Manage Devices >** *EdgeWAE* **> Configure > Legacy Services > WAFS Core Configuration** and uncheck the Enable Core Server check box.

d. Choose **My WAN > Manage Devices >** *EdgeWAE* **> Configure > Enabled Features** and check the CIFS Accelerator check box. An alarm is raised informing you that the device roles changed (from legacy WAFS to CIFS accelerator) and a reload is required.

Note Check marks should now be beside TFO, DRE, Persistent Compression, and CIFS Accelerator. The following Accelerator check boxes should be unchecked (unless the appropriate licenses have been installed): Video, MAPI, NFS, HTTP, SSL, and EPM.

Note You can also enable features through device groups depending on how your WAAS network is designed. The ability to enable device features either individually or as a group allows you to migrate certain sites to CIFS accelerator while other sites continue to optimize CIFS using the legacy mode.

e. Reload the device.

```
reload
```

Caution Reload is a disruptive process. Any existing connections through the WAE are terminated. When the WAE returns to an online state, new connections are optimized but existing connections established during the reload continue unoptimized until the connection is reestablished.

Step 5 Verify device functionality as follows:

a. Verify that only the CIFS accelerator is enabled.

```
show accelerators
```

b. Verify that the connections are being optimized.

```
show statistics connection
```

c. Confirm that the packet count to the WAE is increasing and no loops are detected.

```
show wccp gre
```

d. Confirm that redirecting intercepting router IDs are seen.

```
show wccp routers
```

e. Confirm that all the WAE devices in the cluster are seen.

```
show wccp wide-area-engine
```

f. Verify that the buckets assigned for Service Group 61 match those of Service Group 62 and are assigned to the WAE.

```
show wccp flows tcp-promiscuous detail
```

g. Confirm that the other flows are being optimized.

```
show statistics connection
```

Step 6 Remove any remaining CIFS legacy mode configurations from all branch devices. See the "Removing Remaining Legacy Mode Configurations" section on page 24.

Checkpoint

At this point, you should have all WAE devices running the CIFS accelerator except for half of the data center WAE devices.

Removing CIFS Legacy Configurations from Data Center WAE Devices

This procedure shows how to remove CIFS legacy configurations from data center WAE devices and enable both CIFS accelerator and WCCP so that the devices can rejoin as members of the CIFS accelerator farm.

Prerequisites

Confirm that you have migrated all the branch sites to the CIFS accelerator and that no branch device on the network is running CIFS legacy mode.

Procedure

Step 1 Log in to the primary CM GUI.

`https://`*`cm_ip_address`*`:8443`

Step 2 Verify that all the WAE devices are online (green).

Step 3 Address any alarm conditions before proceeding.

Step 4 From the CM GUI, disable CIFS legacy mode and enable CIFS accelerator mode as follows:

a. Choose **My WAN** > **Manage Devices** > *CoreWAE* > **Configure** > **Legacy Services** > **WAFS Edge Configuration** and uncheck the Enable Edge Server check box.

b. Choose **My WAN** > **Manage Device Groups** > *Core_Cluster* > **Delete Cluster** to delete the selected cluster.

c. Choose **My WAN** > **Manage Devices** > *CoreWAE* > **Configure** > **Legacy Services** > **WAFS Core Configuration** and uncheck the Enable Core Server check box.

d. Choose **My WAN** > **Manage Devices** > *CoreWAE* > **Configure** > **Enabled Features** and check the CIFS Accelerator check box. An alarm is raised informing you that the device roles changed (from legacy WAFS to CIFS accelerator) and a reload is required.

Note Check marks should now be beside TFO, DRE, Persistent Compression, and CIFS Accelerator. The following Accelerator check boxes should be unchecked (unless the appropriate licenses have been installed): Video, MAPI, NFS, HTTP, SSL, and EPM.

e. Reload the device.

```
reload
```

Step 5 Confirm that connections are being optimized.

```
show statistics connection
```

Step 6 Remove any remaining CIFS legacy mode configurations from all data center devices. See the "Removing Remaining Legacy Mode Configurations" section on page 24.

Checkpoint

All WAE devices are running the CIFS accelerator and none are running in CIFS legacy mode.

Removing Remaining Legacy Mode Configurations

After migrating from CIFS legacy mode to CIFS accelerator mode, we recommend removing any remaining CIFS legacy mode configurations from all devices. These configurations could include the following:

- Legacy mode preposition directives
- Legacy mode dynamic shares
- WAFS core cluster configurations
- WAFS file servers
- WAFS connectivity directives
- WAFS adapter policies
- WAFS related SNMP traps and triggers

Additional Information—CM Downgrade and Database Rollback

This section describes how to create a backup of the CM database, which you must do both before and after an upgrade, and how to roll back to a previous version of the database should you encounter a problem during the upgrade.

This section includes the following topics:

Backing Up the CM Database

This procedure shows how to how to back up the databases of the Primary and Standby CMs.

Procedure

Step 1 From the Primary CM, create a backup of the database.

```
cms database backup
```

Step 2 Copy the Primary CM backup file to a remote location.

```
cd /local1
copy disk ftp ftp_ip_address remote_directory remote_file_name local_file_name
```

Step 3 From the Standby CM, create a backup of the database.

```
cms database backup
```

Step 4 Copy the Standby CM backup file to a remote location.

```
cd /local1
copy disk ftp ftp_ip_address remote_directory remote_file-name local_file_name
```

Restoring the CM Databases

This section describes how to restore the databases on the Primary and Standby CMs using their database backup files (see the "Backing Up the CM Database" section on page 25).

Guidelines and Restrictions

Use the following guidelines to restoring the CM databases:

- When restoring the CM database, ensure that the CM is using the same software version as when the database backup file was created.
- Restore the Standby CM first and then restore the Primary CM.
- If you are restoring a backup from a CM where the secure store was in user-provided passphrase mode when the backup was made, you may be asked to provide the secure store password during the restore process. For more information on the secure store, see the *Cisco Wide Area Application Services Configuration Guide* chapter named "Configuring Other System Settings."

This section includes the following topics:

Restoring the Standby CM Database

This procedure shows how to restore the Standby CM database.

Procedure

Step 1 From the Standby CM, disable the CMS service.

```
config
no cms enable
exit
```

Step 2 Delete the existing CMS database.

```
cms database delete
```

Step 3 Initialize the CMS database.

```
cms database create
```

Step 4 Restore the CMS database contents from the backup file.

```
cms database restore bkup_file_name
```

Step 5 Enable the CMS service.

```
config
cms enable
exit
```

Step 6 Verify that the CMS services are running and that the database has synchronized.

```
show cms info
```

Wait at least 5 minutes and then confirm that the database last synchronization time is current. If the time is not current, wait another 5 minutes.

Step 7 Check the current date and time on the Standby CM.

```
show clock
```

Step 8 Verify the CMS status in the running configuration.

```
show running-config | include cms
```

Restoring the Primary CM Database

This procedure shows how to restore the Primary CM Database.

Prerequisites

Restore the Standby CM database before you restore the Primary CM database (see the "Restoring the Standby CM Database" section on page 25).

Procedure

Step 1 From the Primary CM, disable the CMS service.

```
config
no cms enable
exit
```

Note Stopping the CMS service disables the CM GUI. All users logged in to this GUI are logged out when the CMS service is disabled.

Step 2 Delete the existing CMS database.

```
cms database delete
```

Step 3 Initialize the CMS database.

```
cms database create
```

Step 4 Restore the CMS database contents from the backup file.

```
cms database restore bkup_file_name
```

Step 5 Enable the CMS service.

```
config
cms enable
exit
```

Step 6 Verify that the CMS services are running.

```
show cms info
```

Step 7 Check the current date and time on the Standby CM.

```
show clock
```

Step 8 Confirm that you see "Ready to accept incoming RPC requests" in the log file (errorlog/cms_log.current), which indicates that the WAE is ready to establish connections with the Central Manager.

Look for the timestamp from the output and compare it with current time.

Step 9 Verify the CMS status in the running configuration.

```
show running-config | include cms
```

Step 10 Access the CM GUI from a browser.

Downgrading to a Previous Version

For the most current information about how to downgrade to a previous version, see the *Release Note for Cisco Wide Area Application Services*.

Additional Information—Registering an Upgraded WAE with the CM

This procedure shows how to register an upgraded WAE if after the upgrade, you cannot see the WAE from the CM.

Procedure

Step 1 From the CM, delete the branch WAE.

Step 2 From the branch WAE, enter the following commands:

```
cms deregister force
```

```
cms enable
```

Step 3 From the CM, activate the branch WAE. Choose **My WAN** > **Devices** > *branchWAE* > **Activate**.

Additional Information—Performing a Branch WAE Software Downgrade

This procedure describes how to install a previous version of software on a branch WAE should you encounter a problem during the upgrade.

Procedure

Step 1 Determine the previously installed version.

```
show version last
```

Step 2 Install the previous WAAS software version as follows:

a. Telnet to the branch WAE.

b. Install the previous version software image.

```
copy ftp install ftpserver / waas-image.bin
```

Step 3 Reload the branch WAE.

```
reload
```

Step 4 Verify that the software image installed correctly.

```
show version
```

Additional Information—Performing WCCP Validity Testing

This section lists the commands that you can use for WCCP validity testing.

Enter the commands 3 to 4 times in succession to determine if counters are incrementing.

The commands are as follows:

- WAE commands:
  - **show clock detail**
  - **show wccp gre**
  - **show wccp router**
  - **show wccp wide-area-engine**
  - **show wccp flows tcp-promiscuous detail**
- Router/switch commands (for each service group, where applicable):
  - **show ip wccp**

  - **show ip wccp** *service* **service**
  - **show ip wccp** *service* **detail**
  - **show ip wccp** *service* **internal** (available in most recent releases only)
  - **show ip wccp interface detail** (available in most recent releases only)
- Router/switch commands (when hashing is used):
  - **show tcam counts**
  - **show mls stat**
  - **show mls netflow table detail**
  - **show mls netflow ip count**
  - **show mls netflow ip sw-installed count**
  - **show mls netflow ip sw-installed detail**
  - **show fm interface** *interface_name*
- Router/switch commands (when masking is used):
  - **show ip wccp** *service* **mask**
  - **show ip wccp** *service* **merge**
  - **show tcam interface** *interface name* **acl** {**in** | **out**} **ip**
  - **show tcam interface** *interface name* **acl** {**in** | **out**} **ip detail**

For possible IOS issues, capture the following debug output to either the console or a telnet session:

- **debug ip wccp events**
- **debug ip wccp packets**

Additional Information—Performing CIFS Validity Testing and Performing a Rollback

This section describes the methods that you can use for CIFS validity testing, which includes manual procedures and automation tools.

Guidelines and Restrictions

Use the following guidelines when performing CIFS validity testing and performing a rollback:

- Choose a single file or a variety of files for the test. You must use the same file or files for all the tests (base, cold, hot).
- Use an existing share or create a directory structure on the file server. Verify that the share has permissions set for Domain Users. We recommend testing or creating a share that has multiple nested directories (at least 2 to 3 levels deep) that contain files of various types (such as PowerPoint, Excel, or Word) and sizes.

This section includes the following topics:

- Rolling Back from CIFS Accelerator Mode to CIFS Legacy Mode, page 33

Preparing the Shared Server and Client for CIFS Validity Testing

This procedure shows how to prepare the shared server and client for CIFS validity testing.

Procedure

Step 1 On the server, create a share directory that contains several subfolders and files.

Step 2 Verify the following items on the shared server:

- Adequate permissions for Domain Users used in the testing.
- Domain users can access the share before testing WAAS.
- SMB signing (digital signature) is disabled on the server.

Step 3 Verify the following items on the client:

- PC clients are part of the tested Domain environment.
- Domain user exists for each of the PC clients.
- Tested shares do not rely on local user and groups but rather have permissions for Domain Users and groups.
- Microsoft Office (Word, Excel, PowerPoint) is installed.

Performing a Manual CIFS Performance Test with WAAS

This procedure shows how to manually perform a CIFS performance test.

Procedure

Step 1 Verify operation by opening some Microsoft Office documents from the shared server.

Record the filename, size, and open time.

Filename	File Size	Time to Open

Step 2 Modify the files by adding some text and saving.

Record the time it takes to save.

Filename	File Size	Time to Save

Step 3 Open the files again to inspect response time and data integrity.

Record the time it took to open them and get to the spot where your changes were made.

Filename	File Size	Time to Open

Step 4 Evaluate the results of the testing (see the "Evaluating the Manual Test Results" section on page 31).

Evaluating the Manual Test Results

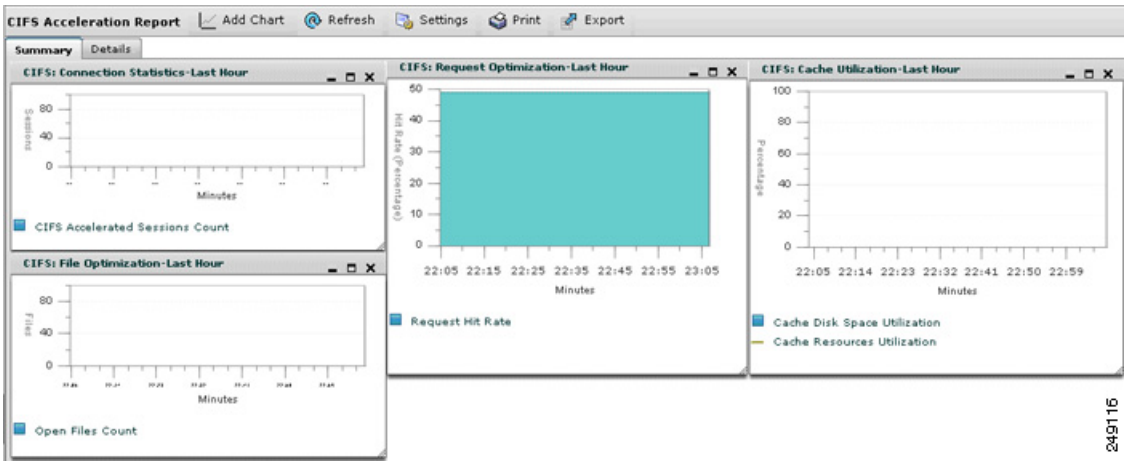
This section describes the expected results of the manual CIFS performance test (see the "Performing a Manual CIFS Performance Test with WAAS" section on page 30).

The test should show tremendous improvement in the time to open and time to save operations. The same behavior should also be observed with the modified file.

The Central Manager provides real time statistics and a summary report for CIFS connections (My WAN > Manage Devices > *branchWAE* > Monitor > Acceleration > CIFS Acceleration Report).

Figure 1 shows some of the CIFS charts.

Figure 1 CIFS Acceleration Report



From the CLI, the following information appears:

```
WAE674# show statistics connection optimized

Current Active Optimized Flows:                       1
   Current Active Optimized TCP Plus Flows:           1
   Current Active Optimized TCP Only Flows:           0
   Current Active Optimized TCP Preposition Flows:    0
Current Active Auto-Discovery Flows:                  0
Current Active Pass-Through Flows:                    0
Historical Flows:                                     100

D:DRE,L:LZ,T:TCP Optimization,
A:AcceleratorIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO
ConnID  Source IP:Port        Dest IP:Port          PeerID             Accel
214682  2.8.35.100:2122       2.8.1.200:445         00:23:7d:06:6e:08  TCDL
```

To display detailed information about any CIFS connection, enter the **show statistics connection optimized cifs detail** command.

To display overall CIFS accelerator statistics, use the **show statistics accelerator cifs detail** command as follows:

```
WAE674# show statistics accelerator cifs detail

CIFS:
   Global Statistics
   -----------------
   Time Accelerator was started:                                    Sun May 17
 06:11:00 2009
   Time Statistics were Last Reset/Cleared:                         Sun May 17
 06:11:00 2009
   Total Handled Connections:                                       10565
   Total Optimized Connections:                                     0
   Total Connections Handed-off with Compression Policies Unchanged:  0
   Total Dropped Connections:                                       0
   Current Active Connections:                                      0
   Current Pending Connections:                                     0
   Maximum Active Connections:                                      5
   Number of local reply generating requests:                       13266
   Number of remote reply generating requests:                      13266
   The Average time to generate a local reply (msec):               0
   Average time to receive remote reply (ms):                       1
```

. . .

Rolling Back from CIFS Accelerator Mode to CIFS Legacy Mode

This procedure shows how to roll back from CIFS accelerator mode to CIFS legacy mode if a failure occurs when upgrading to CIFS accelerator mode or CIFS is not optimized. CIFS accelerator mode can be rolled back to CIFS legacy mode by reenabling the CIFS Edge Services on the WAE devices and recreating the connectivity directive for the particular branch.

Note CIFS legacy mode is not supported on WAAS version 4.4. If you want to roll back to CIFS legacy mode you must be running an earlier WAAS software version or first downgrade to an earlier software version.

Procedure

Step 1 Perform the following tasks on the edge WAE devices:

a. Choose **My WAN** > **Manage Devices** > *EdgeWAE* > **Configure** > **Acceleration** > **Enabled Features** and uncheck the CIFS Accelerator check box.

b. Choose **My WAN** > **Manage Devices** > *EdgeWAE* > **Configure** > **Acceleration** > **Legacy Services** > **WAFS Edge Configuration** > **Enable Edge Services**.

c. Reload the device.

```
reload
```

d. Choose **My WAN** > **Connectivity** > *Select Connectivity Directive* and add the Edge device.

Step 2 Perform the following tasks on the core WAE devices:

a. Choose **My WAN** > **Manage Devices** > *CoreWAE* > **Configure** > **Acceleration** > **Enabled Features** and uncheck the CIFS Accelerator check box.

b. Choose **My WAN** > **Manage Devices** > *CoreWAE* > **Configure** > **Acceleration** > **Legacy Services** > **WAFS Core Configuration**, check the Enable Core Server check box, and either choose an existing core cluster or create a new one.

c. Reload the device.

```
reload
```

Step 3 Recreate connectivity directives as follows:

a. Choose **MY WAN** > **Configure** > **Legacy Services** > **Connectivity**.

b. Create a Connectivity Directive.

c. Add appropriate Edge devices to the selected core cluster.

Related Documentation

For additional information on the Cisco WAAS software, see the following documentation:

- *Release Note for Cisco Wide Area Application Services*

- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services API Reference*
- *Cisco Wide Area Application Services Upgrade Guide* (this manual)
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *Cisco SRE Service Module Configuration and Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *WAAS Enhanced Network Modules*
- *Cisco Wide Area Application Services Online Help*
- *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Installing the Cisco WAE Inline Network Adapter*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.