Cisco Wide Area Application Services Upgrade Guide

January 30, 2018

Software Versions 6.1.x, 6.2.x, or 6.4.x

This document describes how to upgrade Cisco Wide Area Application Services (WAAS) to software version 6.1.x, 6.2.x, or 6.4.x.

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:

Information About Upgrading to Version 6.1.x, 6.2.x, or 6.4.x

This section provides general information about upgrading your WAAS software to version 6.1.x, 6.2.x, or 6.4.x and contains these topics:

Cisco Systems, Inc.
www.cisco.com

Upgrade Paths

Upgrading to version 6.1.x, 6.2.x, or 6.4.x is supported from certain older versions only. If you have a WAAS device that is running a version from which upgrading directly to version 6.1.x, 6.2.x, or 6.4.x is not supported, first upgrade the device to the next highest supported intermediate version and then upgrade to the desired 6.1.x, 6.2.x, or 6.4.x version.

Table 1 specifies which WAAS software versions can be directly upgraded to version 6.1.x, 6.2.x, or 6.4.x and which versions require an intermediate upgrade.

Table 1 WAAS Versions and Upgrade Paths

Current WAAS Software Version	WAAS CM Upgrade Path	WAAS Upgrade Path
5.5.3 and later	• Upgrade directly to 6.1.x, 6.2.x, or 6.4.x	• Upgrade directly to 6.1.x, 6.2.x, or 6.4.x
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 6.1.x, 6.2.x, or 6.4.x	3. Upgrade to 5.5.3, 5.5.5x (5.5.5, 5.5.5a), or 5.5.7x 4. Upgrade to 6.1.x, 6.2.x, or 6.4.x
4.2.x	1. Upgrade to version 4.3.x through 5.4.x 2. Upgrade to 5.5.3, 5.5.5x (5.5.5, 5.5.5a), or 5.5.7x 3. Upgrade to 6.1.x, 6.2.x, or 6.4.x	1. Upgrade to version 4.3.x through 5.4.x 2. Upgrade to 5.5.3, 5.5.5x (5.5.5, 5.5.5a), or 5.5.7x 3. Upgrade to 6.1.x, 6.2.x, or 6.4.x

Upgrade Restrictions and Prerequisites

The following list includes prerequisites and restrictions that you need to know about before upgrading your software:

- You must upgrade the Central Manager software to version 6.1.x, 6.2.x, or 6.4.x prior to upgrading other Wide Area Application Engine (WAE) devices in your network.
- Make sure the Cisco IOS release on the router or switch has been scrubbed for WCCP issues for your specific platform. You must do this action only on routers and switches that participate in transparent redirection and is not applicable to policy-based routing (PBR) or inline deployments. If you do not do this action and there is a current active WAAS network, disable WCCP in the routers and switches in the data center and all branches before the software upgrade to 6.1.x, 6.2.x, or 6.4.x.
- You may need to update firmware or BIOS on some or all of your devices; see the *Release Note for Cisco Wide Area Application Services* for the latest information on firmware requirements and updates.
- The following device platform is no longer supported on WAAS version 5.1 or later: NME-502. WAAS version 5.1 or later does not operate or install on this device.
- The following device platforms are no longer supported on WAAS version 5.0 or later: NME-302, NME-522, WAE-512, and WAE-612 platforms. WAAS version 5.0 or later does not operate or install on these devices. Additionally, the NME-502 platform is not supported in WAAS version 5.1.

- If you are using NTLM Windows domain authentication or are using a nonstandard port (other than port 88) for Kerberos authentication, you must change these configurations and ensure that your domain controller is configured for Kerebos authentication before proceeding with an upgrade to WAAS version 5.1 or later, which does not support NTLM or nonstandard ports. For more details on the procedure, see the WAAS *Release Note for Cisco Wide Area Application Services*.

Note If you upgrade from MCPDEV to Cisco IOS XE Denali 16.3 or later image, you need to reinstall the ISR-WAAS.

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. 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 an 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.

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

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.

If you determine that you need more processing capacity, contact your Cisco representative.

Upgrading Your WAAS Software

This section contains the following topics:

Information About Upgrade Methods

You can use one of the following methods 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 Software Recovery CD or USB method 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 through the command-line interface (CLI).

The remainder of this document assumes that you are using FTP or TFTP and the CLI to upgrade your software.

If you are using one of the other methods, see the "Maintaining Your WAAS System" chapter of the *Cisco Wide Area Application Services Configuration Guide*.

Upgrading Your Firmware

On WAE and WAVE appliances, before proceeding with your software upgrade, we recommend that you update the following three types of system firmware to the latest versions to best support new WAAS features:

- BIOS on the WAVE-594/694/7541/7571/8541 models—The latest BIOS is required for the AppNav operation in WAAS version 5.0 and later.
- BMC firmware on the WAVE-294/594/694/7541/7571/8541 models—The latest BMC firmware is required for the Intelligent Platform Management Interface (IPMI) over LAN feature in WAAS version 5.0 and later.
- RAID controller firmware on the WAE-674/7341/7371 and WAVE-7541/7571/8541—The latest RAID controller firmware is recommended to avoid some rarely encountered RAID controller issues.

See the *Release Note for Cisco Wide Area Application Services* for the latest information on firmware requirements and updates.

Selecting a WAAS Upgrade Software Image

Two different WAAS software images are available. One provides only accelerator and AppNav Controller (ANC) functionality, while the other provides all (universal) functionality, as shown in Table 2.

Table 2 WAAS Software Images

Image Type	Descriptions
Accelerator	Includes Application Accelerator and ANC functionality only. This image is smaller than the Universe image, which makes it the preferred software image to use for upgrading your WAE devices.
Universal	Includes Central Manager, Application Accelerator functionality and ANC functionality. You can use this type of software file to upgrade either a Central Manager or an Application Accelerator device. This image is considerably larger than the Accelerator-only software 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.

Upgrading Sequence

Use this procedure to upgrade your WAAS network to version 6.1.x, 6.2.x, or 6.4.x.

Step 1 Create a backup of the Central Manager database and save it to an external hard drive, as described in the Creating a Backup of the Primary Central Manager.

Step 2 Upgrade the Secondary Central Manager, if present, as described in the Upgrading the Standby Central Manager.

Step 3 Upgrade the primary Central Manager, as described in the Upgrading the Primary Central Manager.

Note You must upgrade your Central Manager(s) before you upgrade the rest of the WAE devices in your WAAS network.

Step 4 Upgrade the other WAE network devices, as described in the Upgrading the Branch WAAS Software and the Upgrading the Data Center WAAS Software.

Note The CIFS application is removed from WAAS Version 6.0 and later. For information about CIFS to SMB migration, please see earlier versions of the *Cisco Wide Area Application Services Upgrade Guide*.

Creating a Backup of the Primary Central Manager

Use this procedure to back up the primary Central Manager (CM) 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

Use this procedure to upgrade the WAAS software on the standby CM.

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 standby CM is online and green.

Upgrading the Primary Central Manager

Use this procedure to upgrade the WAAS software on the primary CM.

Prerequisites

Upgrade the standby CM before you upgrade the primary CM, as described in 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 in the AllWAASGroup.

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

b. Choose **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 6.1.x, 6.2.x, or 6.4.x. The standby CM was upgraded first followed by the primary CM.

Upgrading the Branch WAAS Software

Use this procedure to upgrade each WAAS branch WAE to version 6.1.x, 6.2.x, or 6.4.x.

Prerequisites

- Make sure that you have already upgraded the secondary and primary CM(s)
- Use FTP to copy the WAAS software image to a local server or push the software image to your WAE devices through the CM, as described in the "Maintaining Your WAAS System" chapter of the *Cisco Wide Area Application Services Configuration Guide*.

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.

Step 4 Open a console or Telnet session to the branch WAE.

Step 5 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 6 Reload the WAE.

```
reload
```

Step 7 Verify that the image installed correctly.

```
show version
```

Step 8 Verify that the correct licenses are installed.

```
show license
```

If an Enterprise license has been purchased and not enabled, go to Steps 9 and 10. Otherwise, go to Step 11.

Step 9 (Optional) Clear the Transport license.

```
clear license Transport
```

Step 10 (Optional) Add the Enterprise license.

```
license add Enterprise
```

Step 11 Save the configuration.

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

Step 12 From the WAAS CM GUI, choose **Devices** > *branchWAE* and verify that the WAE is online and has a green device status.

Step 13 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 version 6.1.x, 6.2.x, or 6.4.x.

Upgrading the Data Center WAAS Software

Use this procedure to prepare for and upgrade the data center WAAS Software to version 6.1.x, 6.2.x, or 6.4.x.

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.

Step 4 Follow the procedure in the Upgrading Each Data Center WAE, for each data center device.

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.

Upgrading Each Data Center WAE

Use this procedure to upgrade the data center WAE software.

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
```

```
wccp tcp-promiscuous service-pair x x
no enable
exit
```

b. Wait until the countdown expires or press **Ctrl-C** to skip waiting for a 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 or switch. This step is recommended only if the Cisco IOS release on the router or 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 **Devices** > *dataCenterWAE* and verify that the WAE is online and has a green device status.

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

a. Telnet to each core router or switch.

b. Enable WCCP.

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

See the Enabling WCCP on WAE Devices in a Cluster for an example ACL template.

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 tcp-promiscuous service-pair x x
enable
exit
```

If you are using wccp single service, use these commands instead:

```
config
wccp tcp-promiscuous y
enable
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 clients
```

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

```
show wccp statistics
```

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 version 6.1.x, 6.2.x, or 6.4.x and have WCCP enabled.

Enabling WCCP on WAE Devices in a Cluster

Use this procedure to enable WCCP on WAE devices in a cluster.

Procedure

Step 1 Validate your Cisco IOS release with a bug scrub for WCCP-related issues for your specific platform.

Step 2 Enable WCCP on the WAEs in the cluster

Step 3 Enable WCCP on the intercepting routers or switches; you can use or modify the following router ACL template for running WCCP in your network.

```
!
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
!
```

Validity Testing and Rollbacks

This section describes specific actions that are related to backing up your software, restoring your software from a backup, registering upgrades, and testing different aspects of your network affected by the upgrade.

- Backing Up the Central Manager Database
- Restoring the Central Manager Databases
- Registering an Upgraded WAE with the Central Manager
- Performing a WAE Software Downgrade
- Performing WCCP Validity Testing
- Performing SMB Validity Testing and Performing a Rollback

Backing Up the Central Manager Database

Use this procedure 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 Central Manager 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 Central Manager Database).

Guidelines and Restrictions

Use the following guidelines when restoring the CM databases:

- 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 "Configuring Other System Settings" chapter of the *Cisco Wide Area Application Services Configuration Guide.*

This section contains the following topics:

Restoring the Standby Central Manager Database

Use this procedure to restore the standby CM database.

Procedure

Step 1 From the standby CM, disable the Centralized Management System (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 Central Manager Database

Use this procedure to restore the primary CM database.

Prerequisites

Restore the standby CM database before you restore the primary CM database (see the Restoring the Standby Central Manager Database).

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 the 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.

Registering an Upgraded WAE with the Central Manager

If you cannot set a WAE in the Central Manager after upgrading the device, you must register the upgraded WAE, as shown in the following procedure.

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, choose **Devices** > *branchWAE* > **Activation** to activate the branch WAE.

Performing a WAE Software Downgrade

Use this procedure to install a previous version of software on a branch WAE if 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
```

If you want to downgrade your entire WAAS network software to a previous version, see the *Release Note for Cisco Wide Area Application Services*.

Performing WCCP Validity Testing

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

Enter the commands three to four times in succession to determine if counters are incrementing.

The commands are as follows:

- WAE commands:
  - **show clock detail**
  - **show wccp statistics**
  - s**how wccp routers**
  - **show wccp clients**
  - **show wccp flows tcp-promiscuous detail**
- Router and 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 and 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 and 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 Cisco IOS issues, capture the following debug output to either the console or a Telnet session:

- **debug ip wccp events**

- **debug ip wccp packets**

Performing SMB Validity Testing and Performing a Rollback

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

Guidelines and Restrictions

Use the following guidelines when performing SMB 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 that you test or create 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 contains the following topics:

Preparing the Shared Server and Client for SMB Validity Testing

Use this procedure to prepare the shared server and client for SMB 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.
- A domain user exists for each PC client.
- 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 SMB Performance Test with WAAS

Use this procedure to manually perform a SMB 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 place 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).

Evaluating the Manual Test Results

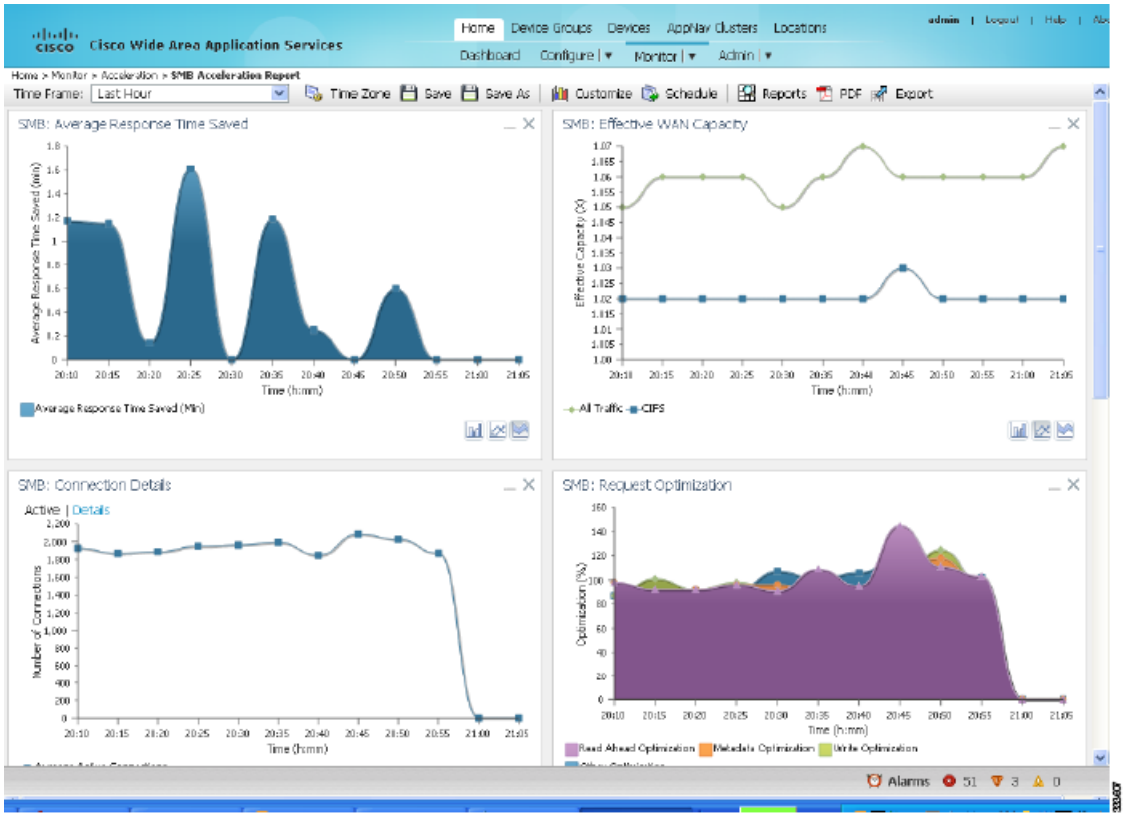
This section describes the expected results of the manual SMB performance test (see the Performing a Manual SMB Performance Test with WAAS).

The test should show significant 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 SMB connections (**Devices** > *branchWAE* > **Monitor** > **Acceleration** > **SMB Acceleration Report**).

Figure 1 shows some of the SMB charts.

Figure 1 SMB 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 SMB connection, enter the **show statistics connection optimized smb detail** command.

To display overall SMB accelerator statistics, enter the **show statistics accelerator smb detail** command as follows:

```
WAE674# show statistics accelerator smb detail

SMB:
   Global Statistics
   -----------------
   Time Accelerator was started:                                    Mon Jan 29
 06:11:00 2018
   Time Statistics were Last Reset/Cleared:                         Mon Jan 29
 06:11:00 2018
   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
. . .
```

Additional Resources

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 Monitoring Guide*
- *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*
- *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*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 294 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 594 and 694 Hardware Installation Guide*

- *Cisco Wide Area Virtualization Engine 7541, 7571, and 8541 Hardware Installation Guide*
- *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*

Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Additional Resources" section.