Configuring File Services

This chapter describes how to configure file services, which allows branch office users to access data stored at centralized data centers more efficiently. The file services feature overcomes the WAN latency and bandwidth limitations by caching data on Edge Wide Area Application Engines (WAEs) near branch office users. Cisco Wide Area Application Services (WAAS) file services use Server Message Block (SMB) application accelerators.

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

This chapter contains the following sections:

- About File Services
- Overview of the File Services Features
- Preparing for File Services
- Configuring File Services

About File Services

Enterprises today have remote offices in different parts of the country and around the world. Typically, these remote offices have their own file servers to store and manage the data needed by their local users.

The problem with this method of operation is that it is costly to purchase, manage, and upgrade file servers at each remote office. A great deal of resources and manpower must be dedicated to maintaining these file servers, especially to protect the data in case of server failure. To achieve the required level of data assurance, the remote office must devote resources to back up the data at the remote site and physically move it to a secure location, often at a considerable distance from the site. If you multiply this scenario by tens, hundreds, and thousands of remote offices, you can see that this approach to enterprise data management not only raises costs exponentially, it also greatly increases risks to critical data.

The logical solution is to move all of the enterprise's important data to a central location containing the facilities, trained personnel, and storage mass required to manage the data properly. By having a data center provide backup and other storage-management facilities, the enterprise can achieve better utilization of both personnel and storage, as well as a higher level of data assurance and security.

The WAN between the enterprise's data center and its remote offices tends to be unreliable and slow, with limited bandwidth and high latency. In addition, the WAN creates other obstacles to the implementation of the data center solution.

One obstacle is created by the file server protocols that operate over the WAN. Every file operation generates several exchanges of protocol messages between the client and the file server. This situation is usually not noticeable on the LAN, but quickly causes high latency over the WAN. Occasionally, this high latency breaks the file server protocol altogether.

Even in cases where the file server protocol is able to function correctly over the WAN, there are typically long delays between each transaction. These delays can often cause timeouts in user applications such as word-processing programs, image-editing programs, and design tools, which stops applications from functioning correctly.

All of these problems—unreliable WANs, file system protocol compatibility, and user application compatibility—contribute to an unfriendly work environment that negatively affects the user experience and diminishes productivity.
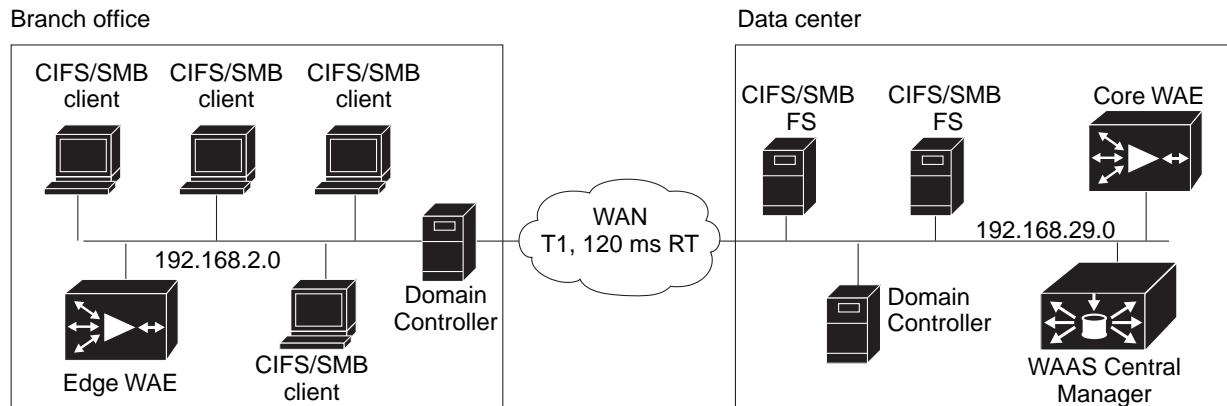
The WAAS File Services feature overcomes WAN latency and bandwidth limitations by caching data on Edge WAEs near the user. This data caching method allows branch office users to access centralized data at LAN-like speeds over the WAN. The solution is based on several key concepts:

- Use the WAN as little as possible—By minimizing the number of operations that need to traverse the WAN, WAAS effectively shields users from many of the obstacles that WANs create.

- Use the WAN optimally—The File Services feature uses sophisticated caching, compression, and network optimization technologies, which enable the system to use the WAN optimally.

- Preserve file system protocol semantics—Although WAAS software uses its own proprietary protocol over the WAN, it leaves the complete semantics of the standard file system protocol commands intact. This is essential to preserve the correctness and coherency of the data in the network.

- Make the solution transparent to users—The best solutions are the ones that do their jobs unnoticed, without interfering with end users' operations or forcing users to change their ways of doing business. The WAAS file services solution does not require any software installations, either on the server side or at the client-side, and does not require a user to learn anything new. Users derive all the benefits of having a secure data center without needing to change any of their work habits.

By using the WAAS File Services feature, enterprises can consolidate their file servers to a data center that provides the facilities, IT personnel, and storage devices required to manage the data properly.

Figure 11-1 shows a typical deployment scenario after WAAS file services have been set up.

Figure 11-1   *WAAS File Services Solution*

Overview of the File Services Features

This section provides an overview of the WAAS File Services features and contains the following topics:

- Automatic Discovery
- Data Coherency
- Microsoft Interoperability

To accelerate SMB traffic, you can use the following accelerator:

- SMB—The SMB accelerator, introduced in WAAS Version 5.0.1, relies on automatic discovery, transparently accelerates traffic, and does not support prepositioning. This accelerator has configuration options that you can fine-tune for specific needs.

  This accelerator supports the SMB 1.0, 2.0, and 2.1 protocols for signed SMB traffic.

Note   Legacy-mode Cisco Wide Area File Services (WAFS) is no longer supported beginning with WAAS Version 4.4.1. Legacy WAFS users must migrate to the SMB accelerator before upgrading.

Automatic Discovery

The automatic discovery feature allows you to enable SMB without having to register individual file servers in the WAAS Central Manager. With the automatic discovery feature, WAAS attempts to automatically discover and connect to a new file server when a SMB request is received.

Data Coherency

WAAS software ensures data integrity across the system by using two interrelated features – *coherency*, which manages the freshness of data, and *concurrency*, which controls the access to data by multiple clients.

Maintaining multiple copies of data files in multiple locations increases the likelihood that one or more of these copies will be changed, causing it to lose consistency or coherency with the others. Coherency semantics are used to provide guarantees of freshness (whether the copy is up-to-date or not) and the propagation of updates to and from the origin file server.

The WAAS software applies the following coherency semantics to its built-in coherency policies:

- Strict SMB behavior for intra-site—Users of the same cache are always guaranteed standard, strict SMB coherency semantics.

- Cache validation on SMB open—In SMB, the File Open operation is passed through to the file server. For coherency purposes, WAAS software validates the freshness of the file on every file that is open, and invalidates the cached file if a new version exists on the file server.

  WAAS software validates data by comparing the time stamp of a file in the cache to the time stamp of the file on the file server. If the time stamps are identical, the cached copy in the Edge WAE is considered valid, and the user is permitted to open the file from the Edge WAE cache.

  If the time stamps are different, the Edge WAE removes the file from its cache and requests a fresh copy from the file server.

- Proactive cache updating—WAAS software supports the use of change notifications in SMB environments as a way to keep cached data on the Edge WAEs up-to-date.

  When a client makes a change to a directory or file, the Edge WAE sends a change notification to the file server. The file server then sends a change notification to all the Edge WAEs, which includes a list of the modified directories and files. Upon receiving the change notification, each Edge WAE checks its cache and invalidates the directories and files listed in the notification, and then updates its cache with the latest versions.

  For example, if a user edits an existing Word document and saves the changes to the Edge WAE cache, the Edge WAE sends a change notification to the file server so that it knows that the file has been modified. The Edge WAE then sends the changed sections to the file server, and the file server proactively sends change notifications to the other Edge WAEs in the network. These Edge WAEs then update their cache so that the file is consistent across all access points.

  This process is also applicable when you rename a directory, add a new subdirectory, rename a file, or create a new file in a cached directory.

- Flush on SMB close—In SMB, the File Close operation forces all the write buffers to be flushed to the file server, and the Close request is only granted after all the updates have been propagated to the file server. From a coherency standpoint, the combination of validate on file open and flush on file close ensures that well-behaved applications, such as Microsoft Office, operate in session semantics. The Open, Lock, Edit, Unlock, and Close commands are guaranteed to work correctly on the WAAS network.

  This authorization process prevents users from accessing directories and files in the cache that they do not have permission to access on the file server.

Microsoft Interoperability

The WAAS file services feature interoperates with these Microsoft SMB features:

- Active Directory for user authentication and authorization

- Microsoft DFS infrastructure

- Windows shadow copy for shared folders, as described in Windows Shadow Copy for Shared Folders)

Windows Shadow Copy for Shared Folders

WAAS file services support the Shadow Copy for Shared Folders feature that is part of the Windows Server 2003 or 2008 operating system. This feature uses the Microsoft Volume Shadow Copy Service to create snapshots of file systems so that users can easily view previous versions of folders and files.

In a WAAS environment, users view shadow copies the same way they would in a native Windows environment by right-clicking a folder or file from the cache and choosing **Properties > Previous Version**.

For more information about Shadow Copy for Shared Folders, including the limitations of the feature, refer to your Microsoft Windows Server 2003 or 2008 documentation.

Users can perform the same tasks when accessing a shadow copy folder on the Edge WAE as they can in the native environment on the file server. These tasks include:

- Browsing the shadow copy folder
- Copying or restoring the contents of the shadow copy folder
- Viewing and copying files in the shadow copy folder

The Shadow Copy for Shared Folders feature does not support the following tasks:

- Renaming or deleting a shadow copy directory
- Renaming, creating, or deleting files in a shadow copy directory

Supported Servers and Clients

WAAS supports Shadow Copy for Shared Folders on the following file servers:

- Windows Server 2008 and Windows Server 2008 R2
- Windows Server 2003 (with and without SP1)
- NetApp Data ONTap versions 6.5.2, 6.5.4, 7.0, and 7.3.3
- EMC Celerra versions 5.3, 5.4, and 5.6

WAAS supports Shadow Copy for Shared Folders for the following clients:

- Windows 7
- Windows Vista
- Windows XP Professional
- Windows 2000 (with SP3 or later)
- Windows 2003

Note   Windows 2000 and Windows XP (without SP2) clients require the Previous Versions Client to be installed to support Shadow Copy for Shared Folders.

Preparing for File Services

Before enabling file services on your WAEs, ensure that you complete the following tasks:

- If you want to configure multiple devices with the same settings, ensure that you have created a device group that contains all the devices you want to enable with file services. For information on creating device groups, see Chapter 3, "Using Device Groups and Device Locations."

Using File Services on the Cisco WAAS Network Module (NME-WAE)

If you are running WAAS on a network module that is installed in a Cisco access router, there are specific memory requirements for supporting file services. The NME-WAE must contain at least 1 GB of RAM to support file services:

If you try to enable file services and the device does not contain enough memory, the WAAS Central Manager will display an error message.

You can check the amount of memory that a device contains in the Device Dashboard window. For details, see Device Dashboard Window of Chapter 15, "Monitoring and Troubleshooting Your WAAS Network."

Configuring File Services

To accelerate SMB traffic, you can enable and configure the SMB accelerators, as described in the following topic:

- Configuring the SMB Accelerator.

Configuring the SMB Accelerator

Table 11-1 provides an overview of the steps that you must complete to configure the SMB accelerator.

Table 11-1   Checklist for Configuring SMB Accelerator

Task	Additional Information and Instructions
1. Prepare for file services.	Provides the tasks that you need to complete before enabling and configuring file services on your WAAS devices. For more information, see Preparing for File Services.
2. Enable SMB acceleration.	Enables and configures the SMB accelerator. For more information, see Enabling and Disabling the Global Optimization Features of Chapter 12, "Configuring Application Acceleration."
3. (Optional) Identify dynamic shares.	Identifies the dynamic shares on an exported file server. If your file server uses Access Based Enumeration (ABE) to give users different views of the share, you must configure the dynamic shares on the WAAS Central Manager. For more information, see Creating Dynamic Shares for the SMB Accelerator.

Creating Dynamic Shares for the SMB Accelerator

Many file servers use dynamic shares, which allow multiple users to access the same share, but be automatically mapped to a different directory based on a user's credentials. Dynamic shares are most commonly used on file servers to set up user home directories. For example, a directory named Home can be set up as a dynamic share on a file server so that users accessing that share are automatically redirected to their own personal directory.

If a file server contains a dynamic share or is using Access Based Enumeration (ABE), you must register that dynamic share with the WAAS Central Manager, as described in this section.

Defining a dynamic share in the WAAS Central Manager allows each user to see a different view of the share and allows the operation of ABE if it is configured on the Windows server.

> **Note**   Dynamic share configuration on the WAAS Central Manager overrides any dynamic share configuration set up directly on the WAE device using the CLI.

Before adding a dynamic share, note the following prerequisites:

- Each dynamic share on a file server must be unique.
- You can use the WAAS Central Manager GUI to define any directory as a dynamic share. However, if a directory is not set up as a dynamic share on the file server, all users will read or write the same content from the same directory and will not be redirected to different directories based on their credentials.

To add a dynamic share for SMB accelerator, follow these steps:

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

Step 2   Choose **Configure > File Services > SMB Dynamic Shares**.

A list of dynamic shares appears. The Dynamic Shares window shows all the dynamic shares configured. From this window, you can perform the following tasks:

- Edit the configuration of an existing dynamic share by selecting it from the Dynamic Share(s) list and clicking the **Edit** taskbar icon.
- Delete the dynamic share by selecting it from the Dynamic Share(s) list and clicking the **Delete** taskbar icon.
- Add a new dynamic share definition, as described in the next steps.

Step 3   Click the **Add Dynamic Share** taskbar icon to add a new dynamic share.

The Dynamic Share window is displayed.

Step 4   In the File Server field, enter a valid FQDN or IP address of the file server with the dynamic share.

If you specify the file server name, the WAE resolves it to an IP address.

Step 5   From the Resolved IP Address(es) drop-down list, which shows the registered file servers, choose a file server.

Step 6   In the Share field, specify the location of the dynamic share by performing one of the following tasks:

- Enter the name of the dynamic share on the file server. The following characters cannot be used in the share name: \, /, :, *, ?, ", <, >, |.
- Click **Browse** next to the Share Name field to navigate to the correct root directory.

> **Note**   The Browse button appears only if you have at least one WAE device with the SMB accelerator enabled and registered to the WAAS Central Manager.

Step 7   Ensure that the status of the share is set to enabled. If you change the status to disabled, the share will not be set up as a dynamic share in your WAAS environment.

Step 8   Click **OK**.

The specified directory now functions as a dynamic share on the WAE.