Storage Center 1.1

2014-12-07 04:29:32 UTC

Contents

Storage Center 1.1

ShareFile Storage Center extends the ShareFile Software as a Service (SaaS) cloud storage by providing your ShareFile account with on-premises private storage, referred to as StorageZones. The ShareFile cloud storage differs from on-premises storage as follows:

- ShareFile-managed cloud storage is a public multi-tenant storage system maintained by Citrix.
- A ShareFile Storage Center is a private single-tenant storage system maintained by you and can be used only by your account.

You can use StorageZones with or instead of the ShareFile-managed cloud storage.

To provide iOS users secure read-only access to data stored in legacy network shares, use StorageZone Connectors. A StorageZone Connector integrates with your ShareFile subdomain and on-premises StorageZones. ShareFile displays network shares as root level folders along with other ShareFile content. Users must enter credentials to access a network share.

Storage Center system requirements

Note: The following ShareFile features are not compatible with Storage Center: ShareFile Desktop Widget and access to a ShareFile account from an FTP client.

- ShareFile Enterprise account
- A CIFS share for private data storage
- A physical or virtual machine with 2 CPUs and 4 GB RAM
  - Windows Server 2008 Datacenter R2, 64-bit edition, SP1

    Windows Server 2008 Standard R2, 64-bit edition, SP1
  - Install on a dedicated server or virtual machine. A high availability production environment requires a minimum of two servers with Storage Center installed.
  - Use a publicly-resolvable Internet hostname (not an IP address).
  - Enable the Web Server (IIS) role.
  - Install ASP.NET 4.0.
  - In the IIS Manager ISAPI and CGI Restrictions, verify that the ASP.NET 4.0 Restrictions value is Allow.
  - Enable SSL for communications with ShareFile.

    If you use SSL directly with IIS, refer to http://support.microsoft.com/kb/298805 for information about configuring SSL.
  - If you are not using DMZ proxy servers, install a public SSL certificate on the IIS service.

    Use an SSL certificate that is from a Windows-accepted Certificate Authority. ShareFile does not support self-signed or unsigned certificates.
  - Recommended as a best practice: Remove or disable the HTTP binding to the Storage Center server.
  - Allow inbound TCP requests on port 443 through the Windows firewall.
  - Open port 80 on localhost (for the server health check).
- For a DMZ proxy deployment:
  - Two DMZ proxy servers, such as two Citrix NetScaler VPX instances
  - For a DMZ proxy server that terminates the client connection and uses HTTP, install a public SSL certificate on the proxy server.

If communications between the DMZ proxy server and the Storage Center server are secure, you can use HTTP. However, HTTPS is recommended as a best practice. If you use HTTPS, you can use a private (Enterprise) certificate that is trusted in the DMZ proxy.

StorageZone Connectors

- ShareFile Enterprise account
- A physical or virtual machine with 2 CPUs and 4 GB RAM

  Note: You must install StorageZone Connectors on a separate server from Storage Center.

  - Windows Server 2008 Datacenter R2, 64-bit edition, SP1

    Windows Server 2008 Standard R2, 64-bit edition, SP1

  - Install on a dedicated server or virtual machine. A high availability production environment requires a minimum of two servers with Storage Center installed.
  - Use a publicly-resolvable Internet hostname (not an IP address).
  - Enable the Web Server (IIS) role.
  - Install ASP.NET 4.0.
  - In the IIS Manager ISAPI and CGI Restrictions, verify that the ASP.NET 4.0 Restrictions value is Allow.
  - Enable SSL for communications with ShareFile.

    If you use SSL directly with IIS, refer to http://support.microsoft.com/kb/298805 for information about configuring SSL.

  - If you are not using DMZ proxy servers, install a public SSL certificate on the IIS service.

    Use an SSL certificate that is from a Windows-accepted Certificate Authority. ShareFile does not support self-signed or unsigned certificates.

  - Recommended as a best practice: Remove or disable the HTTP binding to the Storage Center server.
  - Allow inbound TCP requests on port 443 through the Windows firewall.
- Users can access network shares on these devices:

  - iPhone and iPad: iOS 5.x or 6.x

Storage Center system requirements

Note: The following ShareFile features are not compatible with Storage Center: ShareFile Desktop Widget and access to a ShareFile account from an FTP client.

- ShareFile Enterprise account
- A CIFS share for private data storage
- A physical or virtual machine with 2 CPUs and 4 GB RAM
  - Windows Server 2008 Datacenter R2, 64-bit edition, SP1

    Windows Server 2008 Standard R2, 64-bit edition, SP1
  - Install on a dedicated server or virtual machine. A high availability production environment requires a minimum of two servers with Storage Center installed.
  - Use a publicly-resolvable Internet hostname (not an IP address).
  - Enable the Web Server (IIS) role.
  - Install ASP.NET 4.0.
  - In the IIS Manager ISAPI and CGI Restrictions, verify that the ASP.NET 4.0 Restrictions value is Allow.
  - Enable SSL for communications with ShareFile.

    If you use SSL directly with IIS, refer to http://support.microsoft.com/kb/298805 for information about configuring SSL.
  - If you are not using DMZ proxy servers, install a public SSL certificate on the IIS service.

    Use an SSL certificate that is from a Windows-accepted Certificate Authority. ShareFile does not support self-signed or unsigned certificates.
  - Recommended as a best practice: Remove or disable the HTTP binding to the Storage Center server.
  - Allow inbound TCP requests on port 443 through the Windows firewall.
  - Open port 80 on localhost (for the server health check).
- For a DMZ proxy deployment:
  - Two DMZ proxy servers, such as two Citrix NetScaler VPX instances
  - For a DMZ proxy server that terminates the client connection and uses HTTP, install a public SSL certificate on the proxy server.

If communications between the DMZ proxy server and the Storage Center server are secure, you can use HTTP. However, HTTPS is recommended as a best practice. If you use HTTPS, you can use a private (Enterprise) certificate that is trusted in the DMZ proxy.

StorageZone Connectors

- ShareFile Enterprise account
- A physical or virtual machine with 2 CPUs and 4 GB RAM

  Note: You must install StorageZone Connectors on a separate server from Storage Center.

  - Windows Server 2008 Datacenter R2, 64-bit edition, SP1

    Windows Server 2008 Standard R2, 64-bit edition, SP1

  - Install on a dedicated server or virtual machine. A high availability production environment requires a minimum of two servers with Storage Center installed.
  - Use a publicly-resolvable Internet hostname (not an IP address).
  - Enable the Web Server (IIS) role.
  - Install ASP.NET 4.0.
  - In the IIS Manager ISAPI and CGI Restrictions, verify that the ASP.NET 4.0 Restrictions value is Allow.
  - Enable SSL for communications with ShareFile.

    If you use SSL directly with IIS, refer to http://support.microsoft.com/kb/298805 for information about configuring SSL.

  - If you are not using DMZ proxy servers, install a public SSL certificate on the IIS service.

    Use an SSL certificate that is from a Windows-accepted Certificate Authority. ShareFile does not support self-signed or unsigned certificates.

  - Recommended as a best practice: Remove or disable the HTTP binding to the Storage Center server.
  - Allow inbound TCP requests on port 443 through the Windows firewall.
- Users can access network shares on these devices:

  - iPhone and iPad: iOS 5.x or 6.x

Deploy Storage Center

Storage Center is a Web service that handles all HTTPS operations from end users and the ShareFile control subsystem. The ShareFile control subsystem handles all operations not related to file contents, such as authentication, authorization, file browsing, configuration, metadata, sending and requesting files, and load balancing. The control subsystem also performs Storage Center health checks and prevents off-line servers from sending requests. The ShareFile control subsystem is maintained in Citrix Online data centers.

The ShareFile storage subsystem handles operations related to file contents such as uploads, downloads, and antivirus verification. When you create a StorageZone, you are creating a private storage subsystem for your ShareFile data.

For a production deployment of ShareFile, the recommended best practice is to use at least two servers with Storage Center installed, for high availability. When you install Storage Center, you create a StorageZone. You can then install Storage Center on another server and join it to the same StorageZone. Storage Centers that belong to the same StorageZone must use the same file share for storage.

Deploy StorageZone Connectors

StorageZone Connectors provide a secure connection to user data stored in legacy network shares. A StorageZone Connector integrates with your ShareFile subdomain and on-premises StorageZones to enable authenticated users to browse network shares along with other ShareFile content. ShareFile servers store network share names only; network share data and credentials are not stored.

You can configure StorageZone Connector servers for high availability.

You can also deploy a StorageZone Connector that is not integrated with your ShareFile account to provide mobile device users access to network shares. This option requires administrators to distribute a configuration file to mobile users.

Deploy Storage Center for a proof of concept evaluation

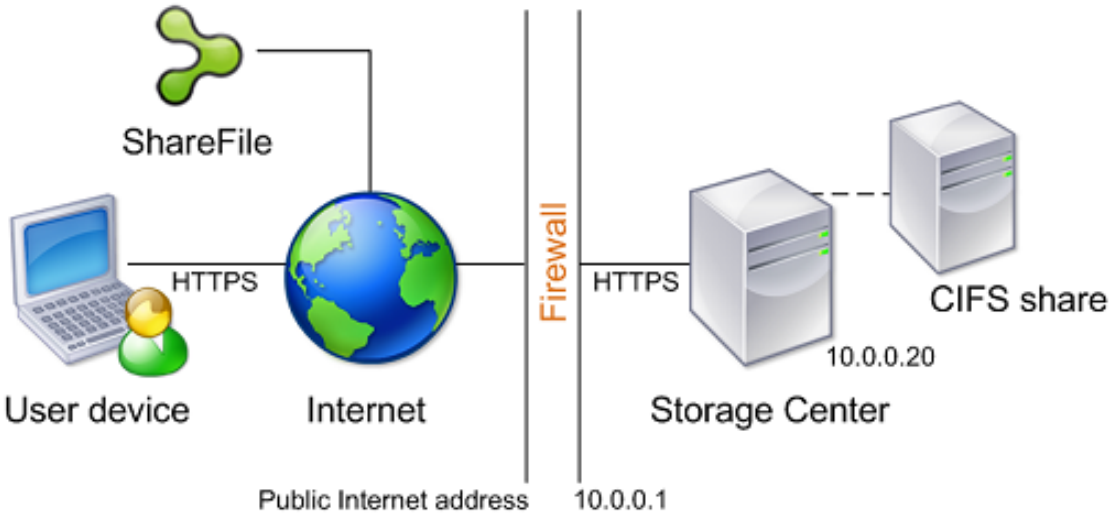

Figure 1. Proof of concept deployment of Storage Center

Caution: A proof of concept deployment is intended for evaluation purposes only and should not be used for critical data storage.

To evaluate a single Storage Center instance, you can use a separate CIFS share or use a folder (such as C:*ZoneFiles*) on the Storage Center hard drive instead of a CIFS share. All other system requirements apply to an evaluation deployment.

In this scenario, one firewall stands between the Internet and the secure network. Storage Center resides inside the firewall to control access. User connections to ShareFile must traverse the firewall and use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall and install a public SSL certificate on the IIS service of all Storage Center servers.

To evaluate multiple Storage Center instances, use a high availability deployment.

Deploy Storage Center for high availability

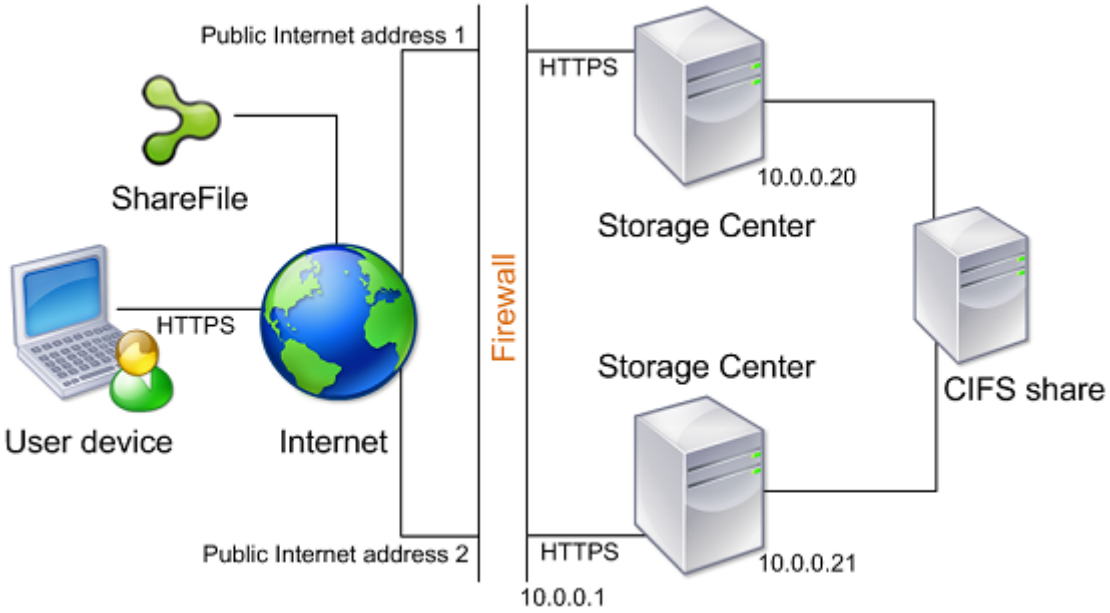

Figure 1. High availability deployment of Storage Center

The recommended best practice for the simplest production deployment is to use a high availability configuration, which requires a second Storage Center and shared storage. You can configure multiple external public addresses, each associated with a different Storage Center. The Storage Center control subsystem randomly chooses a Storage Center for operations.

In this scenario, one firewall stands between the Internet and the secure network. Storage Center resides inside the firewall to control access. User connections to ShareFile must traverse the firewall and use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall and install a public SSL certificate on the IIS service of all Storage Center servers.

Shared storage configuration

You must configure multiple Storage Centers in the same StorageZone to use the same shared storage. Storage Centers access the share using the IIS Account Pool user. By default, application pools operate under the Network Service user account, which has low-level user rights. Storage Center uses the Network Service account by default.

You can use a named user account instead of the Network Service account to access the share. To use a named user account, just specify the user name and password in the Storage Center console Configuration page. You can continue to run the IIS application pool and the Citrix ShareFile Services using the Network Service account.

Deploy Storage Center in a DMZ

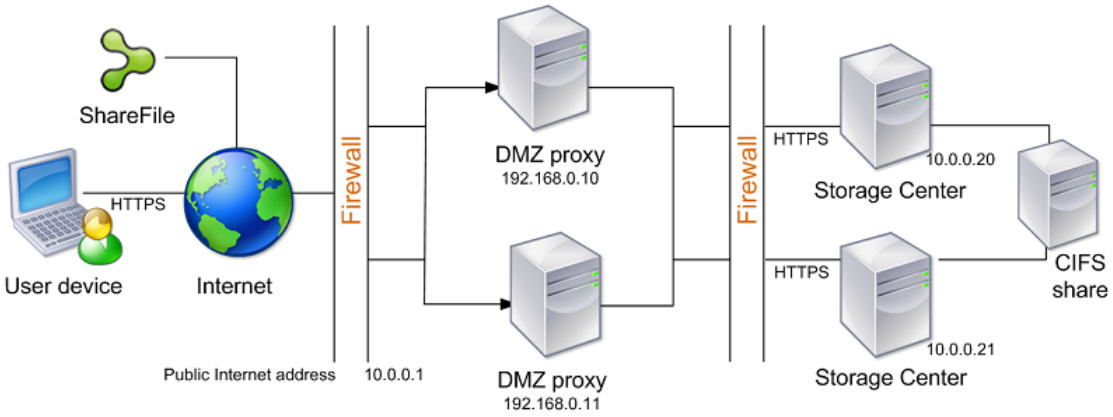

Figure 1. DMZ proxy deployment of Storage Center

A demilitarized zone (DMZ) provides an extra layer of security for the internal network. A DMZ proxy, such as Citrix NetScaler VPX, is an optional component used to:

- Ensure all requests that reach the Storage Center originate from sharefile.com, so that only approved traffic reaches the Storage Centers.

  Storage Centers have a validate operation that checks for valid URI signatures for all incoming messages. The DMZ component is responsible for validating signatures before forwarding messages.

- Load balance requests to Storage Center using real-time status indicators.

  Operations can be load-balanced to the Storage Centers in a StorageZone, provided that all Storage Centers can access the same files.

- Offload SSL from Storage Centers.

In this scenario, two firewalls stand between the Internet and the secure network. Storage Center resides in the internal network. User connections to ShareFile must traverse the first firewall and use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall and install a public SSL certificate on the IIS service of the DMZ proxy servers (if they terminate the user connection).

To configure NetScaler

To use Citrix NetScaler to check for valid URI signatures on all incoming messages and to load balance, configure NetScaler as follows. For more information, refer to the "HTTP Callouts" and "Responder" topics in the NetScaler documentation in Citrix eDocs.

1. In the Configure HTTP Callout window, create an HTTP callout named `sf_callout`:
   a. Click Virtual Server or IP Address and specify the address.
   b. Under Request to send to the server, click Attribute-based and then click Configure Request Attributes.
   c. Select Get Method.
   d. In Host Expression enter the virtual server IP address or the host IP address for any of the Storage Centers.
   e. In URL Stem Expression enter: `"/validate.ashx?RequestURI=" + HTTP.REQ.URL.BEFORE_STR("&h").HTTP_URL_SAFE.B64ENCODE + "&h="+ HTTP.REQ.URL.QUERY.VALUE("h")`
   f. Click OK and then return to the Configure HTTP Callout window.
   g. Under Server Response, choose a Return Type of Bool.
   h. In Expression to extract data from the response enter: `HTTP.RES.STATUS.EQ(200).NOT`
   i. Click Create.
2. Follow the preceding steps to configure an HTTP callout named `sf_callout_y`:
   - In URL Stem Expression enter:

     ```
     "/validate.ashx?RequestURI=" +
     HTTP.REQ.URL.HTTP_URL_SAFE.B64ENCODE + "&h="
     ```

   - All other settings are the same.
3. Configure a responder policy:
   a. For Action, choose Drop.
   b. In Expression, enter:

     ```
     http.REQ.URL.CONTAINS("&h=") &&
     http.req.url.contains("/crossdomain.xml").not &&
     http.req.url.contains("/validate.ashx?requri").not &&
     SYS.HTTP_CALLOUT(sf_callout) ||
     http.REQ.URL.CONTAINS("&h=").NOT &&
     http.req.url.contains("/crossdomain.xml").not &&
     http.req.url.contains("/validate.ashx?requri").not &&
     SYS.HTTP_CALLOUT(sf_callout_y)
     ```

4. Bind the responder policy to the load balancer virtual server and configure SSL session-based persistence.

5. Configure token-based load balancing as described in the NetScaler documentation. Use the rule expression: “`http.REQ.URL.QUERY.VALUE("uploadid")`”

6. Configure NetScaler to terminate SSL connections as described in the NetScaler documentation.

Install Storage Center and configure your first zone

A production deployment of ShareFile requires at least two servers with Storage Center installed. When you install Storage Center, you create a StorageZone. You can then install Storage Center on another server and join it to the same zone. Storage Centers belonging to the same StorageZone must use the same file share for storage.

Complete the following tasks, in the order presented, to install and set up Storage Center.

To install Storage Center

You must be in the Administrators group to install the Storage Center software. (Elevating your privilege to local administrator through User Account Control is not a substitute for Administrators group membership.)

Important: Verify that your environment meets the system requirements before you install Storage Center.

1. From the ShareFile download page at http://www.citrix.com/downloads/sharefile.html, log on and download the Storage Center installer.

   Note: Installing Storage Center changes the Default Web Site on the server to the installation path of the Storage Center.

2. On the server where you want to install Storage Center, run StorageCenter.msi. The ShareFile Storage Center Setup wizard starts.

3. Respond to the prompts and then click Finish. The Storage Center console opens.

   Important: If you plan to clone the Storage Center computer, do not proceed with configuration. Capture the disk image and then configure each Storage Center.

   To return to the Storage Center console at any time, open http://*localhost*/login.aspx or start the configuration tool from the Start menu.

   After you click Finish or return to the Storage Center console, the Logon page appears.

4. In the Logon page, enter the email address, password, and subdomain (*mysubdomain*.sharefile.com or, in Europe, *mysubdomain*.sharefile.eu) for the ShareFile account you are setting up a StorageZone and then click Log On.

5. Click Create new Zone and enter a name for the zone.

6. In Hostname, enter a unique identifier for your Storage Center server. ShareFile recommends that you use the server hostname as the identifier. This should be a friendly name and not the FQDN. This name appears in the ShareFile Administrator console.

7. In External Address, enter a URL for this Storage Center server, in the form http://*externalFQDN* or https://*externalFQDN*:*port*. The URL must be accessible from the Internet. If you are using a load balancer, enter its address. When you submit the page, ShareFile validates this address.

8. In Storage Location, enter the UNC path to your CIFS share, in the form *server**share*.

   Caution: ShareFile Storage Center will overwrite any data in this path with a proprietary storage format. Never specify a path to a location with file data. Reserve this storage location for ShareFile storage only.

   The Network Service account (or the account the Citrix ShareFile Management Service is configured to run as) must have full access to this storage location. Alternatively, you can configure full anonymous/guest access for the share.

9. Specify the Storage Logon and Storage Password for the UNC path of your storage location.

10. To encrypt the files stored on your file share, select the Enable Encryption check box. In an enterprise environment where the CIFS share is inside your network and already secured by third-party tools, we recommend that you do not encrypt the files on the share. Although this additional security is offered as an option for maximum security when required, encrypting files on the share will make the disk unreadable by third-party tools such as antivirus scanners and filer tools, including data deduplication tools. ShareFile uses a file encryption key to confirm the validity of download requests and encrypt the storage. In the next step, you specify a passphrase to protect the file encryption key.

11. Specify a Passphrase to be used to protect your file encryption key. Be sure to archive the passphrase and encryption key in a secure location. You must use the same passphrase for each ShareFile Storage Center in a zone. The passphrase is not the same as your account password and cannot be recovered if lost. If you lose the passphrase, you cannot reinstall Storage Center, join additional Storage Centers to the StorageZone, or recover the StorageZone if the server fails.

    Note: The encryption key appears in the root of the shared storage path. Losing the encryption key file immediately breaks access to all StorageZone files.

12. Click Register. Your Storage Center information appears.

To verify that your StorageZone registered with ShareFile

Verify that a StorageZone registered with ShareFile and then check for other configuration issues.

1. Click the Monitoring tab.

2. Verify that Heartbeat Status has a green checkmark. A red icon indicates that sharefile.com is not receiving the heartbeat messages. In that case, verify network connectivity from your Storage Center server to www.sharefile.com and from an outside PC to the URL of your Storage Center server. The Storage Center server must be accessible on port 443 with a valid, trusted public SSL certificate.

3. Verify that the shared storage has a folder structure and a few files created by Storage Center, including SCKeys.txt, which must reside in the root folder of the shared storage. SCKeys.txt is created when Storage Center is installed, provided there are no credential or access rights issues. If SCKeys.txt is not present, verify the access control lists on your file share and then reinstall Storage Center.

To change the default storage zone for user accounts

After you install Storage Center, existing and newly provisioned user accounts use the ShareFile-managed cloud storage as the default zone.

To specify the default zone for user accounts provisioned from AD, open the User Management Tool and click the options icon.

Members of the super user group can change the default zone for an individual user through Manage Users. That page also enables you to change the Allow employee to select storage zone for root-level folders and Allow this user to create and manage Zones settings.

To move home folders and File Boxes between zones

Use these steps to move home folders and File Boxes from the ShareFile-managed cloud storage to a private zone or between private zones.

1. Click Home and then navigate to the folder.

2. In the right navigation pane, click Edit Folder Options.

3. From the StorageZone menu, select a zone and then click Save.

To create a folder in your StorageZone

1. Click Home and then click Folders.

2. On the Folder tab, click Add Folder.

3. Specify folder information as usual and, for Storage Site, select the StorageZone where you want this folder and its contents to be stored. Click Create Folder.

4. Configure the folder as usual. Your StorageZone configuration is complete. When you create a folder, you can choose whether to use the ShareFile-managed cloud storage or your local StorageZone.

To provide access to Storage Center through a proxy server

1. Log on to the Storage Center console and then click the Networking tab.
2. Select the Enable Proxy check box.
3. Choose an Authentication Mode and enter the proxy server Address and Port.

Prepare Storage Center for file recovery

You are responsible for backing up your StorageZones local file storage. ShareFile archives the corresponding file metadata that resides in the ShareFile cloud for 3 years. Because the file storage and metadata are in two locations, ShareFile provides features that enable you to:

- Recover a file from your local file storage backup when, for example, a user needs access to a file that was deleted more than 7 days ago. The ShareFile recovery feature provides a script that copies files from your backup.
- Reconcile the metadata stored on the ShareFile cloud with your on-premises storage when a failure of your storage results in unrecoverable data. In a disaster recovery scenario, use the ShareFile reconcile feature so that files no longer in your StorageZone on a specified date and time are permanently removed from the ShareFile cloud.

After you complete the set up described in this section, you can then use the ShareFile administrator console To recover files and folders from your StorageZone backup.

Prerequisites

- The Storage Center file backup should follow the same layout as the Storage Center persistent storage.

Storage layout	Backup layout
PrimaryStorageIP \StorageLocation \persistentstorage \sf-us-1 \a024f83e-b147-437e-9f28-e7d03634af42 \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5 \fi7d5cbb_93c8_43f0_a664_74f27e72bc83 \fi47cd7e_64c4_47be_beb7_1207c93c1270	*BackupStorageIP* \SC-Backup \sf-us-1 \a024f83e-b147-437e-9f28-e7d03634af42 \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5 \fi7d5cbb_93c8_43f0_a664_74f27e72bc83 \fi47cd7e_64c4_47be_beb7_1207c93c1270

  If your backup location does not follow the same layout as the Storage Center persistent storage, you must perform an additional step during the recovery process to copy files from the backup location to the location that you specify in the Recovery PowerShell script.
- Enable the execution of Windows PowerShell scripts (32-bit and 64-bit versions) on the Storage Center server.
- Windows PowerShell (32-bit and 64-bit versions) must support .NET 4 runtime assemblies.

To create a disaster recovery queue

This one-time setup is required. The following command examples use the default Storage Center installation folder.

1. On the Storage Center server, open a PowerShell command prompt.

2. Navigate to the Disaster Recovery tools folder in the Storage Center installation folder: `PS C:\> cd 'C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery'`

3. Import the Recovery.psm1 module: `PS C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery> Import-Module .\Recovery.psm1`

4. Create the recovery queue: `PS C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery> New-SCQueue -name recovery -operation recovery` The output of that command indicates the queue was created. For example: `Queue 92736b5d-1cff-4760-92c8-d8b04dc92cb2 created`

To customize the recovery PowerShell script for your location

The DoRecovery.ps1 PowerShell script is executed by the task scheduler to handle the recovery process. This file includes the file backup and storage locations which you must specify for your site.

1. On the Storage Center server, navigate to the recovery PowerShell script: `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery\DoRecovery.ps1`

2. Edit that script as follows:

   a. Set the `$backupRoot` parameter to point to your backup location. For example: `$backupRoot = "\\10.10.10.11\SC-Backup"`

   b. Set the `$storageRoot` parameter to point to your Storage Center location. For example: `$storageRoot = "\\10.10.10.10\StorageLocation\persistentstorage"`

Configure antivirus scans of uploaded files

Storage Center installation includes several files that support antivirus scans. The files are installed by default in C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus.

After you customize the configuration file and use Windows Task Scheduler to schedule the scans, as described in the following steps, each file upload request causes Storage Center to queue the file for an antivirus scan. If issues are reported for a scanned file, the Folders view includes a warning icon for the file.

Prerequisite

- If you will run virus scans (SFAntiVirus.exe) on the Storage Center server, make sure encryption is disabled on that server: On the Storage Center console Configuration page, verify that the Enable Encryption check box is cleared.

To prepare the configuration for your location

1. To run virus scans on a server other than the Storage Center server:
   a. Copy the folder C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus to the other server.
   b. On the Storage Center server, open C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.config and set `QueueSDKRestricted` to `0`: `<add key="QueueSDKRestricted" value="0" />`
2. On the server where you will run virus scans, edit SFAntiVirus.exe.config with the values for your Storage Center configuration:
   a. For `QueueSdkUrl`: If you will run virus scans on a server other than the Storage Center server, replace `localhost` with the server DNS name.
   b. For `CommandFile`: Specify the full path to the anti-virus software. That software must reside on the same server as the ShareFile antivirus folder.
   c. For `CommandOptions` and return codes: The command line settings provided in the configuration file are an example. Provide the appropriate settings for your anti-virus software and environment.
   d. For `ScanFileTimeout`: Larger files can take longer to scan. Tune this setting according to the file sizes expected in your storage.
   e. For `EnableLogging`: By default, the ShareFile antivirus log file is created where virus scans are run.
3. In a command line window, run the following command to set up virus scans: `SFAntiVirus.exe -register` *`SFusername SFpassword`*

To create and schedule a task for virus scans

1. Start Windows Task Scheduler and in the Actions pane click Create Task.
2. On the General tab:
    a. Provide a meaningful Name for the task.
    b. Under Security options, click Change User or Group, and specify a Windows user to run the task. The user must have full access permission on the storage location.
    c. Select Run whether user is logged on or not. Leave the Do not store password check box cleared.
    d. Select Run with highest privileges.
    e. From the Configure for menu, select the operating system of the server where the task will be run.
3. To create a trigger: On the Triggers tab, click New. Then, for Begin the task, choose On a schedule and specify a schedule.
4. To create an action: On the Actions tab, click New.
    a. For Action, choose Start a program and specify the full path to the program. For example: `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus\SFAntiVirus.exe`
    b. For Start in, specify the location of SFAntiVirus.exe: `c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus`
5. On the Settings tab, for If the task is already running, then the following rule applies, choose Do not start a new instance.

Install StorageZone Connectors

Use of StorageZone Connectors with your ShareFile subdomain does not require Storage Center. To use StorageZone Connectors with on-premises StorageZones, complete Storage Center setup before configuring the connectors.

You must be in the Administrators group to install the StorageZone Connector software. (Elevating your privilege to local administrator through User Account Control is not a substitute for Administrators group membership.)

Important: Verify that your environment meets the system requirements before you install a StorageZone Connector.

1. From the ShareFile download page at http://www.citrix.com/downloads/sharefile.html, log on and download the StorageZone Connector for Network Shares installer.

2. On the server where you want to install StorageZone Connectors, run StorageZoneConnectorNS_*version*.msi. The StorageZone Connector wizard starts.

3. Respond to the prompts and then click Finish.

4. Configure the connector and join it to your ShareFile subdomain or StorageZone:

    a. Log on to the server where you installed the StorageZone Connector: http://*localhost*/login.aspx. Use your ShareFile account administrator credentials. After you complete configuration, use that same URL to manage the connector.

    b. In External Address, enter a URL for this StorageZone Connector server, in the form http://*externalFQDN* or https://*externalFQDN* where *externalFQDN* is the fully qualified domain name of the server. The URL must be accessible from the Internet. If you are using a load balancer, enter its address. When you submit the page, ShareFile validates this address.

    c. Specify a Passphrase to be used to encrypt the network share metadata. Be sure to archive the passphrase and encryption key in a secure location. The passphrase is not the same as your account password and cannot be recovered if lost.

    d. Specify a network share using the on-screen instructions. You can add more network shares after you complete initial configuration.

    e. Choose a deployment option, using the on-screen instructions as a guide. Integrated Mode, the default option, enables users to view network shares along with their other ShareFile data.

    f. If you chose the Standalone Mode deployment option: Open the saved configuration file in a text editor, customize the text that is in the `description` tag, and then email the file to your users. The text in the `description` tag appears on the mobile device when a user is prompted to accept the connection. In the email, be sure to instruct users to click the link to install an app on their mobile device so they can view network shares. Installation requires the user to accept a security certificate and provide credentials.

g. Click Finish. A Configuration Summary appears.

h. Optional: Add more network shares to this connection.

5. Grant users access to the network share folders: This step applies to the Integrated Mode only.

   a. Log in to your ShareFile subdomain.

   b. Click Home, click the name of the network share, and then click View/Edit Folder Access.

   c. Assign users only the download permission on the share.
6. Repeat all steps in this procedure to set up additional connectors. You can add StorageZone Connectors to your ShareFile subdomain and to on-premises StorageZones.

To configure StorageZone Connectors for high availability

1. After you configure a StorageZone Connector, copy the following files from the installation directory of the connector (by default, C:\inetpub\wwwroot\Citrix\StorageZoneConnector) to one or more servers to be used as additional servers: AppSettingsRelease.config

   NSShares.config

2. On each additional connector server, log on to the Storage Center configuration page and when prompted for the passphrase, enter the passphrase specified for the configured StorageZone Connector server. The Storage Center console Configuration page displays the settings of the configured StorageZone Connector.

Manage Storage Center

To join a Storage Center to a StorageZone

When you install Storage Center, you create a StorageZone. You can then install Storage Center on another server and join it to the same zone. Storage Centers belonging to the same zone must use the same file share for storage.

1. In a Web browser, open http://*localhost*/login.aspx and log on.
2. Click Join existing Zone, select the StorageZone, and then click Register.

To specify a different external or local address for a Storage Center

You can change the external address of a Storage Center by using this procedure or other server management tools.

1. Click Admin and then click StorageZones.
2. Click the zone name and then click the Storage Center hostname.
3. Specify the new External Address or Local Address and then click Save Changes.

To disable a Storage Center

Disable a Storage Center before taking the server off-line for maintenance. If you use a different external address for each Storage Center, use this procedure. If you use the same external address for all Storage Centers, disable a Storage Center from the NetScaler interface.

1. Click Admin and then click StorageZones.
2. Click the zone name and then click the Storage Center hostname.
3. Clear the Enabled check box and then click Save Changes.

To transfer all files to a different server

1. Copy the entire directory structure including SCkeys.txt to the new server.
2. Open the Storage Center Configuration page: http://*localhost*/login.aspx.
3. Click Modify.
4. In Storage Location, enter the UNC path to your CIFS share, in the form *server**share* and then click Save.
5. Restart IIS.

To delete a Storage Center

Deleting a Storage Center does not delete the data or SCKeys.txt.

1. Click Admin and then click StorageZones.
2. Click the zone name and then click the Storage Center hostname.
3. Click Delete.

To rename a StorageZone

1. Click Admin and then click StorageZones.
2. Click the zone name and then click Edit Zone.
3. Type a new name and then click Save Changes.

To delete a StorageZone

1. Click Admin and then click StorageZones.
2. Click the zone name and then click Delete Zone.

To redeploy Storage Center

No information is lost when you redeploy Storage Center.

1. Uninstall Storage Center.
2. Login to sharefile.com, click Admin > StorageZones, and then select your zone. Do not delete the zone.
3. Select the Storage Center and delete it.

4. Install Storage Center. Do not register it yet.

5. Run the Storage Center configuration wizard to join the Storage Center to a zone and complete the registration.

To recover files and folders from your StorageZone backup

The ShareFile Administrator console enables you to browse your StorageZone file records for a particular date and time and tag any files and folders that you want to restore. ShareFile adds the tagged items to a recovery queue. You can then run the provided script to restore the files from a backup to the storage location.

Prerequisites

- Complete the setup described in Prepare Storage Center for file recovery.
- If you want a new folder to contain the recovered files, create a folder before starting the file restore.

1. Click Admin and then click StorageZones.
2. Click the zone name and then click Recover Files.
3. Click in the Recovery Date text box and select a date and time. The file list for the StorageZone on the specified date and time appears.
4. Select the check box for each file to restore and then click Restore.
5. Select the folder to contain the restored files and then click Restore. The Folder list shows a spinning icon to indicate that the recovery is in process.
6. If your backup location does not follow the same layout as the Storage Center persistent storage, copy the files from the backup location to the location you specified when editing DoRecovery.ps1. For help with this manual process, refer to the help file provided in the Disaster Recovery folder.
7. Complete the recovery:
   - If the files in Storage Center are not encrypted, run the DoRecovery.ps1 script directly.
   - If the files in Storage Center are encrypted, you must run the recovery script under Network Service or Named User privilege. In that case, it is easiest to schedule a task under one of those privileges, as described in the following task.

   The recovery script copies the files from the backup to the storage location. After you refresh the console, the spinning icons disappear for files successfully recovered. If you cannot recover a file, refer to the help file provided in the Disaster Recovery folder for information about changing a file's recovery queue status to failed.

To create and schedule a task for the recovery script

1. Start Windows Task Scheduler and in the Actions pane click Create Task.

2. On the General tab:

   a. Provide a meaningful Name for the task.

   b. Under Security options, click Change User or Group and enter the object name Network Service.

   c. From the Configure for menu, select the operating system of the server where the task will be run.

3. To create a trigger: On the Triggers tab, click New. Then, for Begin the task, choose On a schedule and specify a schedule.

4. To create an action: On the Actions tab, click New.

   a. For Action, choose Start a program and enter the Program/script:
   `C:\Windows\System32\cmd.exe`

   b. For Add arguments, enter: `/c`
   ```
   "c:\windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
   -File .\DoRecovery.ps1" >> .\recovery.log
   2>>.\recoveryerror.log
   ```

   c. For Start in, specify the Storage Center installation location, such as:
   `c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

To reconcile the ShareFile cloud with a StorageZone

A problem, such as a disk failure, that causes data loss in your local storage results in an inconsistent state between your local storage and the metadata stored in the ShareFile cloud. You can automatically reconcile those differences so that metadata for files no longer in your StorageZone on a specified date and time are permanently removed from the ShareFile cloud.

Caution: Perform a reconcile only if you have irrecoverable data loss in your local file storage. A reconcile permanently erases the metadata from the ShareFile cloud for any files that are not found in your local file storage as of the date and time that you specify.

1. Click Admin and then click StorageZones.
2. Click the zone name and then click Reconcile Files.
3. Click in the Reconcile Date text box and select a date and time.
4. Click Reconcile. A confirmation dialog box appears.

Monitor Storage Center

The Monitoring tab on the Storage Center console provides status of Storage Center components to help with troubleshooting configuration issues. Status is provided for items such as access permissions, service status, and ShareFile connectivity.

StorageZone and Storage Center host information is available from the ShareFile Administrator console, as follows.

1. Click Admin and then click StorageZones. A list of StorageZones appears. The Health status indicates whether sharefile.com is receiving heartbeat messages from Storage Center for the zone.

2. Click a zone name. Information about the storage use, network use, and file activity for the zone appears.

3. Click a Storage Center hostname. Information about the storage use, network use, and file activity of the server appears.