StorageZones Controller 2.0

2014-12-07 04:29:31 UTC

Contents

StorageZones Controller 2.0

ShareFile StorageZones Controller extends the ShareFile Software as a Service (SaaS) cloud storage by providing your ShareFile account with on-premises private storage, referred to as StorageZones for ShareFile Data. StorageZones Controller also provides users with secure access to SharePoint document libraries and network file shares through StorageZones Connectors.

StorageZones for ShareFile Data

ShareFile stores data in the secure ShareFile-managed cloud storage or, with StorageZones for ShareFile Data, enables you to configure private, on-premises cloud storage for your account. ShareFile storage options differ as follows:

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

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

StorageZones Connectors

Note: StorageZones Connectors are available for ShareFile Enterprise. StorageZones Connectors are also provided with the XenMobile Enterprise, MDM, and App Editions.

StorageZones Connectors provide users with secure access to documents and folders in SharePoint document libraries and to data stored in network file shares. A StorageZones Connector is installed on a StorageZones Controller and integrates with ShareFile Enterprise subdomains and on-premises StorageZones.

ShareFile displays connected SharePoint document libraries and network files shares in supported ShareFile clients under Folders > SharePoint and Folders > File Shares. The credentials used to log on a user to ShareFile are also used to authenticate with SharePoint libraries and network file shares. If a user needs to use different credentials to access a connected library or share, the user must log out of ShareFile and then log on using the alternate credentials.

- Install
- Manage
- Monitor

About StorageZones Controller 2.0

What's new

StorageZones Controller 2.0 provides the following new features and enhancements:

Integrated administration of StorageZones Connectors – StorageZones Controller is now used to install and manage both StorageZones for ShareFile Data and StorageZones Connectors. The StorageZones Controller installer detects your ShareFile plan and presents the appropriate options.

Support for SharePoint document libraries –

- Easily create secure connections from ShareFile mobile clients to existing network drives and SharePoint document libraries:
    - Administrators use the ShareFile administrator console to pre-populate the SharePoint document libraries presented to users and configure user permissions.
    - Mobile device users simply type the SharePoint URL to create a new connection to a ShareFile document library. Administrators can configure whitelists of allowed sites.
    - No VPN connection is needed to access SharePoint from outside of the corporate network.
- Securely edit content on mobile devices, even when off-line, with an editor built-in to ShareFile that supports SharePoint functionality.
    - Download, check out, edit, and check in Microsoft Office documents. While editing, track changes, spell check, highlight, print, and insert and present in slide show mode.
    - Annotate Adobe PDF documents.
    - Mark entire folders or individual files for off-line access.
    - Add a document or folder created on a mobile device to an existing SharePoint library.

Expanded support for network file shares – In addition to browsing documents on file shares and downloading documents to supported devices, users can now upload documents to file shares. Connected file shares can include the same network "home" drives used in XenDesktop or XenApp environments.

Known issues

- By design, configuration changes to a StorageZones Controller are not propagated to other Controllers in the same StorageZone. Be sure to restart the IIS server after any configuration change.
- When a user navigates to a folder on a network file share, and that folder includes a file with a tilde (~) character in its name, the download might not complete. [#13357]
- In some situations, the Save button is labeled Register.

About StorageZones Controller 2.0

What's new

StorageZones Controller 2.0 provides the following new features and enhancements:

Integrated administration of StorageZones Connectors – StorageZones Controller is now used to install and manage both StorageZones for ShareFile Data and StorageZones Connectors. The StorageZones Controller installer detects your ShareFile plan and presents the appropriate options.

Support for SharePoint document libraries –

- Easily create secure connections from ShareFile mobile clients to existing network drives and SharePoint document libraries:
    - Administrators use the ShareFile administrator console to pre-populate the SharePoint document libraries presented to users and configure user permissions.
    - Mobile device users simply type the SharePoint URL to create a new connection to a ShareFile document library. Administrators can configure whitelists of allowed sites.
    - No VPN connection is needed to access SharePoint from outside of the corporate network.
- Securely edit content on mobile devices, even when off-line, with an editor built-in to ShareFile that supports SharePoint functionality.
    - Download, check out, edit, and check in Microsoft Office documents. While editing, track changes, spell check, highlight, print, and insert and present in slide show mode.
    - Annotate Adobe PDF documents.
    - Mark entire folders or individual files for off-line access.
    - Add a document or folder created on a mobile device to an existing SharePoint library.

Expanded support for network file shares – In addition to browsing documents on file shares and downloading documents to supported devices, users can now upload documents to file shares. Connected file shares can include the same network "home" drives used in XenDesktop or XenApp environments.

Known issues

- By design, configuration changes to a StorageZones Controller are not propagated to other Controllers in the same StorageZone. Be sure to restart the IIS server after any configuration change.
- When a user navigates to a folder on a network file share, and that folder includes a file with a tilde (~) character in its name, the download might not complete. [#13357]
- In some situations, the Save button is labeled Register.

StorageZones Controller system requirements

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

StorageZones for ShareFile Data

- 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 R2, 64-bit edition, SP1 (Enterprise, Datacenter, or Standard)
  - Install on a dedicated server or virtual machine. A high availability production environment requires a minimum of two servers with StorageZones installed.
  - Use a publicly-resolvable Internet hostname (not an IP address).
  - Enable the Web Server (IIS) role.
  - Install ASP.NET 4.5.
  - In the IIS Manager ISAPI and CGI Restrictions, verify that the ASP.NET 4.5 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 commercially trusted Certificate Authority. ShareFile does not support self-signed or unsigned certificates.
  - Recommended as a best practice: Remove or disable the HTTP binding to the StorageZone controller.
  - 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:
  - One or more DMZ proxy servers, such as 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 StorageZone controller 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 on the StorageZones Controller if it is trusted by the DMZ proxy. The external address exposed by the DMZ proxy must use a commercially trusted certificate.

StorageZones Connector for SharePoint

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

  The server where you configure StorageZones Connectors has the same physical or virtual machine system requirements as noted above for StorageZones for ShareFile Data, with this exception: Connectors do not require port 80.
- Microsoft SharePoint Server 2010
- SharePoint policy interactions with StorageZones Connector for SharePoint:
  - The default maximum upload file size for a Web application in SharePoint 2010 is 50 MB. To change the default: In SharePoint Central Administration, go to the Web Application General Settings page and change the Maximum Upload Size. The upload file size limit for SharePoint is 2 GB.
  - ShareFile clients always attempt to check in a major version (publish) of a file. However, SharePoint policies determine whether a file is checked in as a major or minor version.
  - The SharePoint View-Only permission does not enable a user to download files. To read a file from a ShareFile client, a SharePoint user must have Read permission.
- For the latest information about user device support for StorageZones Connectors, refer to the ShareFile Knowledge Base.

Connector for SharePoint authentication

After authenticating the user, the StorageZones Controller server makes connections to the SharePoint server on the authenticated user's behalf and responds to authentication challenges presented by the SharePoint server. Connector for SharePoint supports the following authentication methods on the SharePoint server.

- Basic

  Requires that you add `<add key="CacheCredentials" value="1" />` to C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config.
- Negotiate (Kerberos)
- Windows Challenge/Response (NTLM)

ShareFile mobile clients use Basic authentication over HTTPS to authenticate to the StorageZone Controller or DMZ proxy. Single sign-on to SharePoint is governed by the authentication requirements set on the SharePoint server. To use Kerberos or NTLM authentication on the SharePoint server: Configure the domain controller to trust the StorageZones Controller for delegation.

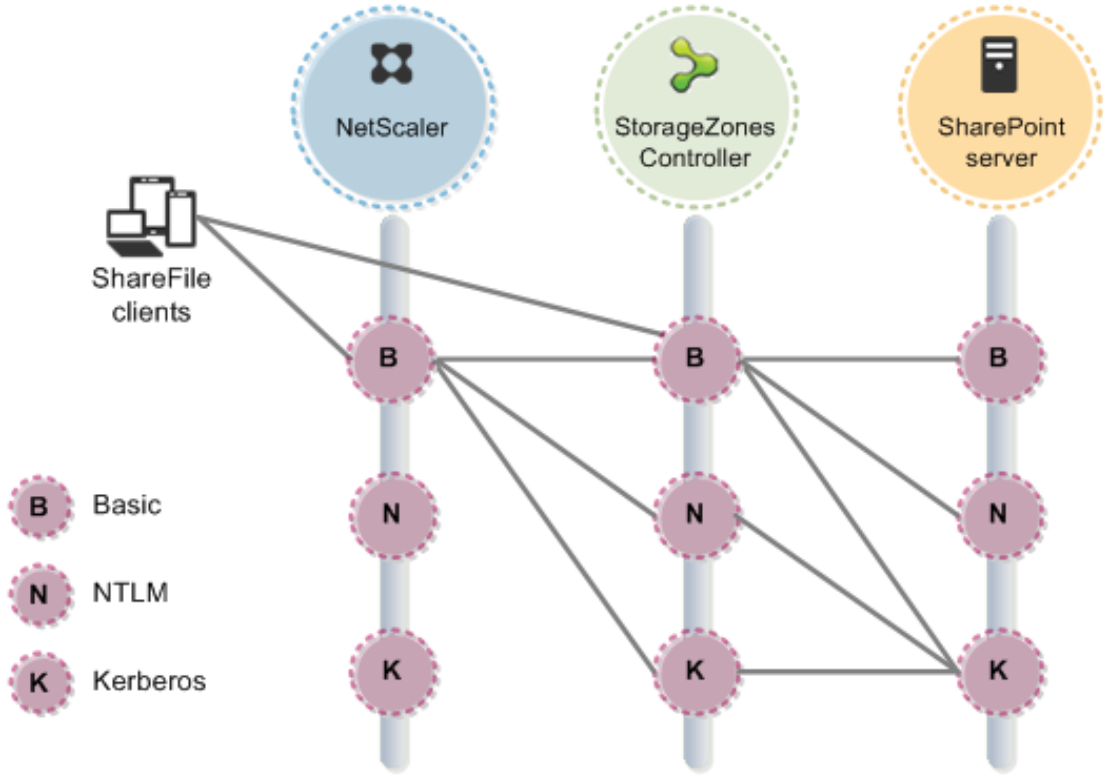
If your SharePoint server is configured for Kerberos authentication: Configure a service principal name (SPN) for the named user service accounts for the SharePoint server application pool. For more information, refer to "Configure trust for delegation for Web parts" in http://support.microsoft.com/kb/832769.

For deployments with NetScaler, it is possible to terminate Basic authentication at the NetScaler and then perform other types of authentication to the StorageZone Controller.

The following table indicates the supported scenarios when NetScaler is configured for Basic authentication.

Authentication method on StorageZones Controller	Authentication method on SharePoint server		
	Basic	Negotiate (Kerberos)	NTLM
Basic	Yes (1)	Yes	Yes
Negotiate (Kerberos)	No	Yes (2)	No
NTLM	No	Yes	No
(1) Requires that you add `<add key="CacheCredentials" value="1" />` to C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config. (2) To provide users with a single sign-on experience, configure the Connector for NTLM authentication.			

The following diagram summarizes the supported combinations of authentication types based on whether the user authenticates at NetScaler.



StorageZones Connector for Network File Shares

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

  The server where you configure StorageZones Connectors has the same physical or virtual machine system requirements as noted above for StorageZones for ShareFile Data, except Connectors do not require port 80.
- For the latest information about user device support for StorageZones Connectors, refer to the ShareFile Knowledge Base.

Connector for Network File Shares authentication

After authenticating the user, the StorageZones Controller server makes connections to the network file server on the authenticated user's behalf and responds to authentication challenges presented by the file server. Connector for Network File Shares supports the following authentication methods on the file server.

- Negotiate (Kerberos)
- Windows Challenge/Response (NTLM)

To use Kerberos or NTLM authentication on the StorageZones Controller: Configure the domain controller to trust the StorageZones Controller for delegation.

For deployments with NetScaler, perform the following configuration to provide users with a single sign-on experience when NetScaler is configured for Basic authentication:

- Configure the Connector for both Negotiate (Kerberos) and NTLM authentication.
- Add `<add key="CacheCredentials" value="1" />` to C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config.

Deploy StorageZones

StorageZones 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 StorageZones health checks and prevents off-line servers from sending requests. The ShareFile control subsystem is maintained in Citrix Online data centers.

Installation of StorageZones creates a private ShareFile storage subsystem for your data on a StorageZones Controller. The ShareFile storage subsystem handles operations related to file contents such as uploads, downloads, and antivirus verification.

For a production deployment of ShareFile with high-availability, the recommended best practice is to install at least two StorageZone Controllers. When you install the first controller, you create a StorageZone. When you install the second controller, you join it to the same StorageZone. StorageZone Controllers that belong to the same StorageZone must use the same file share for storage.

Data storage considerations for StorageZones

- In an enterprise environment where the CIFS share for a StorageZone is 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.
- Place the StorageZones Controllers inside the network, with DMZ tools protecting them.
- For maximum security, use Citrix NetScaler or NetScaler VPX.
- Use SSL-encrypted connections to ensure the security of information transmitted between your users and StorageZones. If you are not using DMZ proxy servers, install a public SSL certificate on the IIS service of all StorageZones Controllers. For a DMZ proxy server that terminates the client connection and uses HTTP, install a public SSL certificate on the proxy server.
- To control connections to ShareFile, IP whitelisting is not a recommended security practice because connections originate from a number of servers in the ShareFile-managed cloud storage, as well as from each individual user device. IP blacklisting, however, is an effective network-level control if your site needs additional security.

Deploy StorageZone Connectors

StorageZone Connectors provide a secure connection to the following data sources:

- SharePoint document libraries. Mobile users can check out, edit, and check in Microsoft Office documents and can annotate Adobe PDF documents. The mobile content editor integrated with ShareFile provides mobile users with a secure, rich editing experience, even when working offline.

- Network file shares. Mobile users can browse, upload, or download documents. StorageZone Controllers store file share names only, not file share data or credentials.

  Note: For sites with XenMobile MDM Edition or XenMobile App Edition, mobile users are limited to read access to SharePoint document libraries and network file shares.

While StorageZone Connectors can integrate with your on-premises StorageZones, StorageZones are not required to use StorageZone Connectors in sites with Citrix XenMobile deployed.

Deploy StorageZones for a proof of concept evaluation

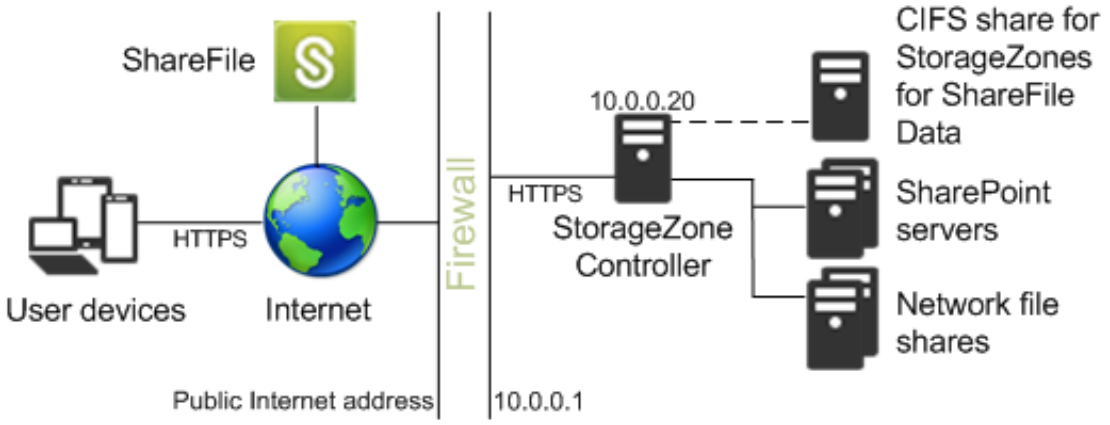


Figure 1. Proof of concept deployment of StorageZones

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 StorageZone Controller, you can use a separate CIFS share or a folder (such as C:*ZoneFiles*) on the hard drive of the StorageZone Controller. All other system requirements apply to an evaluation deployment.

In this scenario, one firewall stands between the Internet and the secure network. The StorageZone Controller 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 StorageZone Controllers.

To evaluate a deployment with multiple StorageZone Controllers, follow the guidelines for a high availability deployment.

Deploy StorageZones for high availability

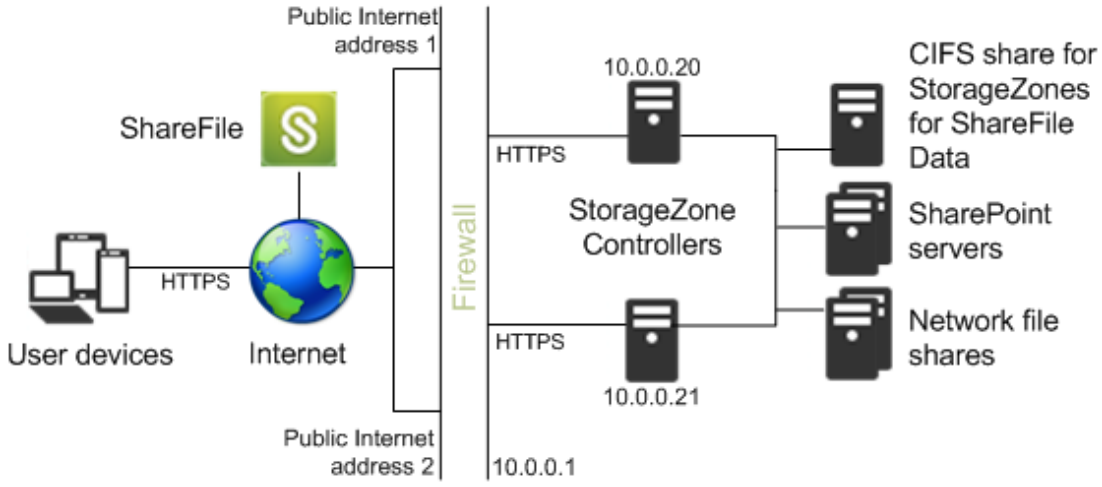


Figure 1. High availability deployment of StorageZones

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

In this scenario, one firewall stands between the Internet and the secure network. StorageZone Controllers reside 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 StorageZone Controllers.

Shared storage configuration

StorageZone Controllers that belong to the same StorageZone must use the same file share for storage. StorageZone Controllers 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. A StorageZone Controller 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 StorageZones console Configuration page. You can continue to run the IIS application pool and the Citrix ShareFile Services using the Network Service account.

Deploy StorageZones behind a DMZ

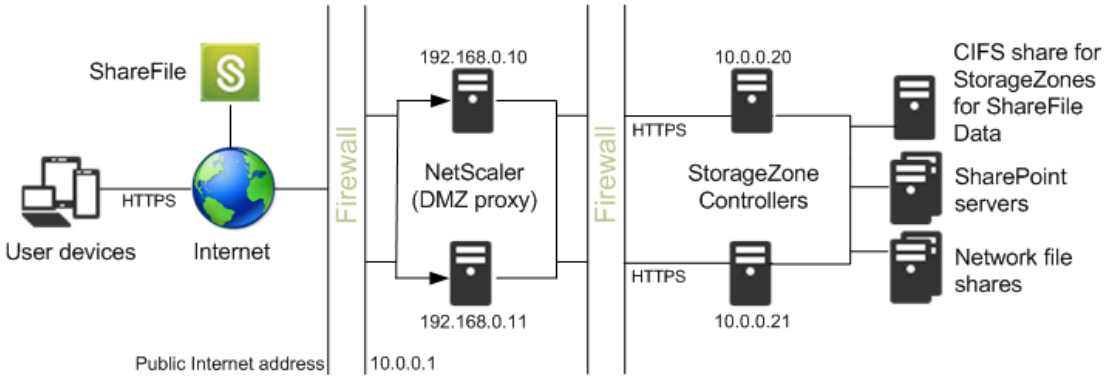


Figure 1. DMZ proxy deployment of StorageZones

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 to a StorageZones originate from sharefile.com, so that only approved traffic reaches the StorageZone Controllers.

  StorageZones has 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 StorageZone Controllers using real-time status indicators.

  Operations can be load-balanced to StorageZone Controllers if all StorageZone Controllers can access the same files.

- Offload SSL from StorageZone Controllers.

- Ensure requests for files on SharePoint or network drives are authenticated before passing through the DMZ.

In this scenario, two firewalls stand between the Internet and the secure network. StorageZone Controllers reside 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).

Configure NetScaler

The steps in this section describe the NetScaler settings needed for StorageZones Controller. All links are for the NetScaler 10.1 documentation. Similar topics are available for earlier versions of NetScaler.

To check for valid URI signatures on all incoming messages and to load balance

1. Create an HTTP callout named `sf_callout`:

   a. In the Configure HTTP Callout dialog box, 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 StorageZone Controllers.

   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 dialog box.

   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.

   For more information, refer to HTTP Callouts in the NetScaler documentation.

2. Follow the preceding steps to configure an HTTP callout named `sf_callout_y`. Use the same settings except for the expression:

   · In URL Stem Expression enter:

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

3. Configure a responder policy:

   a. In the Configure Responder Policy dialog box: 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)
   ```

For more information, refer to Responder in the NetScaler documentation.

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

5. Configure token-based load balancing.

   Use the rule expression: “`http.REQ.URL.QUERY.VALUE("uploadid")`”

6. Configure NetScaler to terminate SSL connections.

   For information, refer to Configuring SSL Offloading and its subtopics in the NetScaler documentation.

To configure content switching and authentication for Connectors

1. Enable content switching, as described in Enabling Content Switching in the NetScaler documentation.

2. Create a content switching policy for user requests for ShareFile data from your on-premises StorageZone:

   a. In the Configure Content Switching Policy dialog box: Enter a Name for the content switching policy. These steps use the name Data_Requests.

   b. Enter the Expression:

   ```
   HTTP.REQ.HOSTNAME.CONTAINS("StorageZonesControllerHostName") &&
   HTTP.REQ.URL.CONTAINS("/cifs/").NOT &&
   HTTP.REQ.URL.CONTAINS("/sp/").NOT
   ```

   c. Click OK.

   For more information, refer to Content Switching in the NetScaler documentation.

3. Create a content switching policy for user requests for data accessed from a StorageZones Connector.

   a. In the Configure Content Switching Policy dialog box: Specify a Name for the content switching policy. These steps use the name Connector_Requests.

   b. Enter the Expression:

   ```
   HTTP.REQ.HOSTNAME.CONTAINS("StorageZonesControllerHostName") &&
   (HTTP.REQ.URL.CONTAINS("/cifs/") ||
   HTTP.REQ.URL.CONTAINS("/sp/"))
   ```

   c. Click OK.

4. Create a content switching virtual server.

5. Set the content switching policy targets:

   - In the Configure Virtual Server (Content Switching) dialog box: For the Data_Requests policy, specify the load balancer virtual server for StorageZones for ShareFile data.

     This load balancer virtual server is the one to which you bound the responder policy in Step 4 of *To check for valid URI signatures on all incoming messages and to load balance*.

   - For the Connector_Requests policy, specify the load balancer virtual server for StorageZones Connector.

6. Configure the authentication virtual server for StorageZones Connector:

   Although authentication to NetScaler is optional, it is a recommended best practice.

   a. In the navigation pane, expand Load Balancing, select the name of the load balancer virtual server for StorageZones Connector, and then click Open.

b. In the Configure Virtual Server (Load Balancing) dialog box, click the Advanced tab and then expand Authentication Settings.

c. Select the check box for 401 Based Authentication and then choose the Authentication VServer.

d. Click the Method and Persistence tab.

e. For Persistence, choose COOKIEINSERT.

f. For Time-out (min), enter 240.

A time-out value of 240 minutes is recommended. The minimum value should be greater than 10 minutes.

For more information, refer to Configuring the Authentication Virtual Server in the NetScaler documentation.

7. Use the Configure Authentication Server dialog box to create and configure an authentication server.

In SSO Name Attribute, enter userPrincipalName.

For more information about other settings, refer to Authentication Policies in the NetScaler documentation.

8. Configure an authentication policy for the authentication server just created:

a. In the Configure Authentication Policy dialog box: Enter a Name for the policy and then select the authentication Server configured in the previous step.

b. Enter the Expression:

```
ns_true
```

For more information, refer to Configure an authentication policy in the NetScaler documentation.

9. Configure a session profile for single sign-on:

a. In the Configure Session Profile dialog box, enter a Name for the profile.

b. Select the check box for Single Sign-on to Web Applications.

c. For Credential Index, select PRIMARY.

d. In Single Sign-on Domain, enter the domain name for your StorageZones Controller.

e. Select the Override Global check boxes for each of the preceding three items.

For more information, refer to Session Profiles in the NetScaler documentation.

10. Configure a session policy for single sign-on:

a. In the Configure Session Policy dialog box, enter a Name for the policy.

b. For Request Profile, select the name of the session profile configured in the previous step.

c. Enter the Expression:

```
ns_true
```

For more information, refer to Session Policies in the NetScaler documentation.

11. Create an authentication virtual server:

a. In the Configure Virtual Server (Authentication) dialog box, enter a Name and the IP Address for the server.

b. Click the Authentication tab and for Protocol, select SSL.

c. Select the check box for Authenticate Users.

d. Under Authentication Policies, click Primary and then choose the authentication policy you configured in Step 7.

e. Click the Policies tab, click Session, and then choose the session policy you configured in Step 9.

For more information, refer to Configuring the Authentication Virtual Server in the NetScaler documentation.

Upgrade Storage Center and StorageZones Connectors

Before you upgrade a StorageZones implementation, familiarize yourself with these new terms and features:

- **StorageZones Controller** – The product name and the name of the server component.
- **StorageZones for ShareFile Data** – Your on-premises private storage, managed by StorageZones Controller. Previously referred to as Storage Center.
- **StorageZones Connectors** – A feature that provides users with secure access to documents and folders in SharePoint document libraries and to data stored in network file shares. StorageZones Connectors are now installed on the StorageZones Controller.

To upgrade to StorageZones Controller 2.0

1. **If StorageZone Connectors 1.0 is installed:** StorageZone Connectors 1.0 cannot be upgraded to StorageZones Controller 2.0. Uninstall StorageZone Connectors 1.0 before proceeding.

2. **If Storage Center 1.0 is installed:** Storage Center 1.0 cannot be directly upgraded to StorageZones Controller 2.0. Upgrade Storage Center 1.0 to Storage Center 1.1 before proceeding. For help with installation, refer to Install Storage Center and configure your first zone.

   Important: Verify that Storage Center 1.1 is configured correctly and working before you upgrade to StorageZones Controller 2.0.

3. **If Storage Center 1.1 is installed:** Upgrade Storage Center 1.1 to StorageZones Controller 2.0.

   a. From the ShareFile download page at http://www.citrix.com/downloads/sharefile.html, log on and download the latest StorageZones Controller 2.0 installer.

      Note: Installing StorageZones Controller changes the Default Web Site on the server to the installation path of the controller.

   b. On the server where you want to upgrade the primary StorageZones Controller, run StorageCenter.msi. The ShareFile StorageZones Controller Setup wizard starts.

   c. Respond to the prompts and then click Finish. The StorageZones Controller console opens.

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

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

      After you click Finish or return to the StorageZones Controller console, the Logon page opens.

   d. Log on. With the Make this Primary Zone Controller tab selected, click Next. The server is now the primary StorageZones Controller.

   e. To change any of the displayed information, click Modify, make your changes, and then click Save.

      Note: To use StorageZones Connectors you must click Modify, configure the connectors, and then click Save. For information about configuring the connectors, refer to Install StorageZones Controller.

   f. On a server you want to join to the zone as a secondary StorageZones Controller, run StorageCenter.msi.

   g. Respond to the prompts and then click Finish. The StorageZones Controller console Logon page opens.

h. Log on, click Join Zone, enter the Primary Zone Controller host name or IP address, and then click Next. The server is now a secondary StorageZones Controller. To change any of the displayed information, click Modify, make your changes, and then click Save.

i. Restart the IIS server of all zone members.

Install StorageZones Controller

When you install a StorageZones Controller, you either create a zone and configure a primary StorageZones Controller or you join secondary StorageZones Controllers to a zone.

While configuring a primary StorageZones Controller, you can choose to:

- **Enable StorageZones for ShareFile Data** and either create a StorageZone or join a StorageZones Controller to an existing zone.

  StorageZones are available only to sites using ShareFile Enterprise.

  A production deployment of ShareFile StorageZones requires at least two servers with StorageZones Controller installed.

- **Enable StorageZones Connectors**.

  StorageZones Connectors are available to sites using ShareFile Enterprise or Citrix XenMobile.

  Use of StorageZones for ShareFile Data is not required for StorageZones Connectors. However, to use StorageZones Connectors with on-premises StorageZones, be sure to create the zones before creating a connector.

Complete the following tasks, in the order presented, to install and set up StorageZones for ShareFile Data or StorageZones Connectors.

To install StorageZones Controller

Important: Verify that your environment meets the system requirements before you start the installation.

1. Download and install the StorageZones Controller software:

   a. From the ShareFile download page at http://www.citrix.com/downloads/sharefile.html, log on and download the latest StorageZones Controller 2.0 installer.

      Note: Installing StorageZones Controller changes the Default Web Site on the server to the installation path of the controller.

   b. On the server where you want to install StorageZones Controller, run StorageCenter.msi. The ShareFile StorageZones Controller Setup wizard starts.

   c. Respond to the prompts and then click Finish. The StorageZones Controller console opens.

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

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

After you click Finish or return to the StorageZones Controller console, the Logon page appears.

2. In the Logon page, enter the email address, password, and subdomain (*mysubdomain*.sharefile.com or, in Europe, *mysubdomain*.sharefile.eu) for your ShareFile account and then click Log On.

3. To set up your primary StorageZones Controller:

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

   b. Primary Zone Controller defaults to `http://localhost/ConfigService`.

      - If you use SSL, change `http` to `https`. Keep in mind that ShareFile supports only valid, trusted public SSL certificates. If you have problems configuring a secondary StorageZone host, ensure that you can resolve the ConfigService URL in a local browser on that server, with no SSL errors.

      - *`localhost`* resolves to the server IP address. You can specify a host name instead. It must be resolvable by a secondary StorageZones Controller server.

   c. In Hostname, enter a unique identifier for your StorageZones Controller.

      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.

   d. In External Address, enter the FQDN for this StorageZones Controller, in the form *externalFQDN*.

      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.

   If you are not using StorageZones for ShareFile Data and want to enable StorageZones Connectors, skip to step 5.

   To also configure secondary StorageZones Controllers, complete this procedure and then refer to Manage StorageZones Controllers.

4. To enable a StorageZone for ShareFile Data and specify settings for persistent storage:

   a. Select the check box for Enable StorageZones for ShareFile Data.

      This option is not available for XenMobile MDM Edition and XenMobile App Edition.

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

      Caution: StorageZones Controller 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 StorageZones for ShareFile Data 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.

StorageZones Controllers belonging to the same StorageZone must use the same file share for storage.

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

d. 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.

e. 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 StorageZones Controller 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 StorageZones, join additional StorageZones Controllers 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, CKeys.txt, immediately breaks access to all StorageZone files. Be sure to back up the encryption key file as part of your normal datacenter procedures.

5. To enable StorageZones Connectors:

a. Select the check boxes for the type of connectors you want to enable: Enable StorageZone Connector for Network File Shares and Enable StorageZone Connector for SharePoint. Enabling the Connectors creates the IIS apps sp and cifs.

b. Optional: To prevent administrators or users from creating connections to particular network file shares or SharePoint document libraries, specify a comma-separated Whitelist of the allowed UNC paths for network file shares and the URL (not including path terminators) for SharePoint document libraries.

Example: \\myserver\homedirs,
https://server/sharepoint.net/Shared%20Documents/,
https://server/sharepoint.net/Shared%20Documents/TeamSite/

Note: Paths to SharePoint document libraries must not include path terminators such as *file*.aspx or /Forms.

All connections are allowed by default, indicated by a Whitelist value of *.

6. Click Register. Your StorageZones Controller information appears.

7. If you specified a WhiteList, restart the IIS server.

To verify that your StorageZone Controller registered with ShareFile

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

1. In the StorageZones Controller console, 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 StorageZones Controller to www.sharefile.com and from an outside PC to the URL of your StorageZones Controller. The StorageZones Controller 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 StorageZones Controller, including SCKeys.txt, which must reside in the root folder of the shared storage.

   SCKeys.txt is created when StorageZones Controller 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 StorageZones Controller.

To change the default zone for user accounts

By default, 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 in the ShareFile administrator console 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 provide access to StorageZones through a proxy server

1. In the StorageZones Controller console (http://*localhost*/configservice/login.aspx), click the Networking tab.
2. Select the Enable Proxy check box.
3. Select an Authentication Mode and enter the proxy server Address and Port.
4. Restart the IIS server of all zone members.

For information about managing StorageZones Controller, StorageZones for ShareFile Data, and StorageZones Connectors, see Manage StorageZones Controller.

Configure the domain controller to trust the StorageZones Controller for delegation

Note: This section applies only to StorageZones Connectors.

To use Kerberos or NTLM authentication on the StorageZones Controller, you must configure the domain controller to trust the StorageZones Controller for delegation, as follows.

1. On the domain controller for the StorageZones domain, click Start > Administrative Tools > Active Directory Users and Computers.
2. Expand domain, and expand the Computers folder.
3. In the right pane, right-click the StorageZone Controller name, select Properties, and then click the Delegation tab.
4. For Kerberos, select Trust this computer for delegation to any service (Kerberos only).
5. For NTLM:
    a. Select Trust this computer for delegation to specified services only and Use any authentication protocol. Click OK.
    b. Click the Add button. In the Add Services dialog box, click Users or Computers and then browse to or type the host name for the CIFS share or SharePoint server. Click OK.

       If you have multiple file servers or SharePoint servers, add a service for each.
    c. In the Available Services list, select the services used: cifs (for Connector for Network File Shares) and http (for Connector for SharePoint). Click OK.

Prepare StorageZones Controller for file recovery

You are responsible for backing up your StorageZones Controller 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 a 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 ShareFile Data backup.

Prerequisites

- The StorageZones for ShareFile Data file backup should follow the same layout as the StorageZones Controller 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* \SZ-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 StorageZones Controller 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 StorageZones Controller.
- 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 StorageZones Controller installation folder.

1. On the StorageZones Controller, open a PowerShell command prompt.

2. Navigate to the Disaster Recovery tools folder in the StorageZones Controller 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 StorageZones Controller, 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 `$storageRoot` parameter to point to your StorageZones Controller persistent storage. For example: `$storageRoot = "\\10.10.10.10\StorageLocation\persistentstorage"`

Configure antivirus scans of uploaded files

StorageZones Controller 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 StorageZones Controller 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 StorageZones Controller, make sure encryption is disabled on the controller: On the StorageZones 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 StorageZones Controller:

   a. Copy the folder C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus to the other server.

   b. On the StorageZones Controller, open C:\inetpub\wwwroot\Citrix\StorageCenter\sp\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 StorageZones Controller configuration:

   a. For `QueueSdkUrl`: If you will run virus scans on a server other than the StorageZones Controller, 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.

Manage StorageZones Controller

This section provides information about managing these ShareFile StorageZones features:

- **StorageZones Controller**

  Join a StorageZones Controller to a StorageZone, disable or redeploy a controller, transfer files to different shared storage.

- **StorageZones for ShareFile Data**

  Move home folders and File Boxes between zones, create a folder in a zone, rename or delete a zone.

- **StorageZones Connectors**

  Grant permissions to create Connectors, create a StorageZones Connector for SharePoint or a StorageZones Connector for network file shares, change user permissions, rename or delete a Connector.

Manage StorageZones Controllers

A StorageZones Controller hosts the storage subsystem for your private StorageZones for ShareFile Data.

To join a secondary StorageZones Controller to a StorageZone

To configure a StorageZone for high availability, connect at least two StorageZones Controllers to it: After you install a primary StorageZones Controller and create a zone (as described in Install StorageZones Controller), install StorageZones Controller on a second server and join that controller to the same zone. StorageZones Controllers belonging to the same zone must use the same file share for storage.

1. Open a Web browser on the server to be a secondary StorageZones Controller, open http://*localhost*/configservice/login.aspx and log on.

2. Click Join existing Zone and select the StorageZone.

3. Enter the requested information and then click Register.

   For Primary Zone Controller, you can enter just the host name or IP address, and ShareFile will fill in the full URL. To test a URL, enter it into the browser's address field. If the URL is correct, a ShareFile banner page appears. If the URL is incorrect and you specified https, verify that you are using valid, trusted public SSL certificates.

4. Restart the IIS server of all zone members.

   A secondary StorageZones Controller inherits the configuration of the primary controller during startup.

To specify a different external or local address for a primary StorageZones Controller

You can change the external address of a primary StorageZones Controller by using this procedure or other server management tools.

1. In the ShareFile web interface, click Admin and then click StorageZones.

2. Click the zone name and then click the primary StorageZones Controller hostname.

3. Specify the new External Address or Local Address and then click Save Changes.

4. Restart the IIS server of all zone members.

To change the passphrase of a primary StorageZones Controller

1. Open the StorageZones Configuration page: http://*localhost*/configservice/login.aspx.
2. Click Modify.
3. 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.

   The passphrase is not the same as your account password and cannot be recovered if lost. If you lose the passphrase, you cannot reinstall StorageZones, join additional StorageZones Controllers 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.
4. If you changed the passphrase on the primary server: Log on to the StorageZones Configuration page for each of the other members and enter the passphrase when prompted.

   You must use the same passphrase for each StorageZones Controller in a zone.
5. Restart the IIS server of all zone members.

To demote and promote StorageZones Controllers

When you need to maintain or replace a primary StorageZones Controller, you must demote it first and then promote a secondary controller.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. To demote a primary StorageZones Controller:
   a. Locate the Registry key:
      `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b. Set isPrimaryConfigServer to false.
   c. Set PrimaryConfigServiceUrl to the URL of the server that will be the new primary StorageZones Controller, using the form http://*ipAddress_or_hostname*/ConfigService/.
   d. Restart the IIS server of all zone members.
2. To promote a secondary StorageZones Controller:
   a. Locate the Registry key:
      `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`

b. Set isPrimaryConfigServer to true.

c. Set PrimaryConfigServiceUrl to http://localhost/ConfigService/.

d. Restart the IIS server of all zone members.

To disable a StorageZones Controller

Note: Use this procedure if each StorageZones Controller has a different external address. Disable a controller from the NetScaler interface if you use the same external address for all StorageZones Controllers.

Disable a StorageZones Controller before taking the server off-line for maintenance.

1. In the ShareFile web interface, click Admin and then click StorageZones.
2. Click the zone name and then click the StorageZones Controller hostname.
3. Clear the Enabled check box and then click Save Changes.
4. Restart the IIS server of all zone members.

To transfer all files to a different server

1. Copy the entire directory structure including SCkeys.txt to the new server.
2. Open the StorageZones Configuration page: http://*localhost*/configservice/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 the IIS server of all zone members.

To delete a StorageZones Controller

Deleting a StorageZones Controller does not delete the data or SCKeys.txt. If you are deleting a primary StorageZones Controller, demote it before continuing.

1. In the ShareFile web interface, click Admin and then click StorageZones.
2. Click the zone name and then click the StorageZones Controller hostname.
3. Click Delete.
4. Restart the IIS server of all zone members.

To redeploy a StorageZones Controller

No information is lost when you redeploy a StorageZones Controller.

1. Uninstall StorageZones from the server.
2. In the ShareFile web interface, click Admin > StorageZones, and then select your zone. Do not delete the zone.
3. Select the StorageZones Controller and delete it.
4. Install StorageZones. Do not register it yet.
5. Run the StorageZones Controller configuration wizard to join the StorageZones Controller to a zone and complete the registration.
6. Restart the IIS server of all zone members.

To recover files and folders from your ShareFile Data backup

The ShareFile Administrator console enables you to browse your StorageZones for ShareFile Data 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 StorageZones Controller for file recovery.
- To use 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 StorageZone 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 the StorageZone are not encrypted, run the DoRecovery.ps1 script directly.
   - If the files in the StorageZone are encrypted, 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 StorageZone 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.

Manage StorageZones for ShareFile Data

A StorageZone is a private, on-premises cloud storage. You can use StorageZones for ShareFile Data with or instead of the ShareFile-managed cloud.

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.
4. Restart the IIS server of all zone members.

To create a folder in a 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. When you create a folder, you can choose whether to use the ShareFile-managed cloud storage or your local StorageZone.
5. Restart the IIS server of all zone members.

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.
4. Restart the IIS server of all zone members.

To delete a StorageZone

1. Click Admin and then click StorageZones.
2. Click the zone name and then click Delete Zone.
3. Restart the IIS server of all zone members.

Create and manage StorageZones Connectors

StorageZones Connectors provide access to documents and folders in:

- SharePoint document libraries
- Network file shares

A connected SharePoint library or network file share appears in the ShareFile client interface under Folders > SharePoint or Folders > Network Shares for users with permission to view the connected resource.

StorageZones Connectors do not support document sharing or sync across devices.

To grant permissions to create StorageZones Connectors

Use the Manage Users page to set permissions that enable Administrators and employee users to create Connectors, as follows:

- Administrators: Allow this user to create and manage Connectors. Enables administrators to use the ShareFile administrator console to create and manage Connectors and to use a supported ShareFile client to create Connectors.
- Employee users: Allow employee to create SharePoint Connectors; Allow employee to create Network Share Connectors. Enables users of supported ShareFile clients to enter the URL of a SharePoint library or network file share and create a Connector to it.

To create a StorageZones Connector for SharePoint

Pre-requisite

- If you are using StorageZones for ShareFile Data, create the zone to be used for the Connector.

The following steps describe how to create a StorageZones Connector from the ShareFile web interface. ShareFile users can also create a Connector from supported devices by typing the URL of the SharePoint site.

1. Click Home, click the Connectors tab, and then click Create Connector.
2. From the Type menu, choose SharePoint.
3. If you are using StorageZones for ShareFile Data, choose a Zone for the Connector.

The zone for a Connector must either be in the same domain as the SharePoint server or must have a trust relationship with it. If you have SharePoint servers in multiple domains and cannot configure trusts between the domains, create a StorageZone Controller for each domain.

4. For Site, type the URL of a SharePoint document library.

   Examples:

   https://mycompany.com/sharepoint/sales-team/Shared Documents/

   https://mycompany.com/sharepoint/sales-team/Shared Documents/Forms/AllItems.aspx

   Note: URLs that do not point to a SharePoint document library, such as https://mycompany.com/sharepoint/ or https://mycompany.com/sharepoint/SitePages/Home.aspx, are invalid.

5. Type a user-friendly Name for the Connector.

   The name is used to identify the SharePoint site to users. The name should be brief so it displays well on mobile devices with small screens.

6. Click Add Connector. The View/Edit Folder Access dialog box appears.

7. Set the access permissions for the Connector: In View/Edit Folder Access, add users and distribution groups, select a check box to grant permission, and then click Save Changes.

   Read/write access is determined by the ShareFile plan: XenMobile MDM Edition and XenMobile App Edition support read access only. XenMobile Enterprise Edition and ShareFile Enterprise Edition support read/write access.

8. Restart the IIS server of all zone members.

To create a StorageZones Connector for network file shares

Pre-requisite

- If you are using StorageZones for ShareFile Data, create the zone to be used for the Connector.

The following steps describe how to create a Connector from the ShareFile Web interface. ShareFile users can also create a Connector from supported devices by typing the path of a file share.

1. Click Home, click the Connectors tab, and then click Create Connector.

2. From the Type menu, choose File Share.

3. If you are using StorageZones for ShareFile Data, choose a Zone for the Connector.

The zone for a Connector must either be in the same domain as the file share or must have a trust relationship with it. If you have SharePoint servers in multiple domains and cannot configure trusts between the domains, create a StorageZone Controller for each domain.

4. For Path, type the UNC path.

   Example that redirects to a user's home directory: \\myserver\homedirs\%username%

   Example with FQDN: \\fileserver.acme.com\shared

5. Type a user-friendly Name for the Connector.

   The name is used to identify the file share to users. The name should be brief so it displays well on mobile devices with small screens.

6. Click Add Connector. The View/Edit Folder Access dialog box appears.

7. Set the access permissions for the Connector: In View/Edit Folder Access, add users and distribution groups, select a check box to grant permission, and then click Save Changes.

   Read/write access is determined by the ShareFile plan: XenMobile MDM Edition and XenMobile App Edition support read access only. XenMobile Enterprise Edition and ShareFile Enterprise Edition support read/write access.

8. Restart the IIS server of all zone members.

To change user access to a Connector

When you create a Connector, you choose whether a user can access it. Use the following steps to change that setting.

To perform the following steps, you must have all rights listed in View/Edit Folder Access.

1. Click Home and then click the Connectors tab.

2. Click Edit/View Access for the Connector you want to update.

3. Select a check box to grant access or clear a check box to deny access and then click Save Changes.

   Read/write access is determined by the ShareFile plan: XenMobile MDM Edition and XenMobile App Edition support read access only. XenMobile Enterprise Edition and ShareFile Enterprise Edition support read/write access.

4. Restart the IIS server of all zone members.

To change a Connector name

A Connector name is used to identify a SharePoint site or network file share to users.

1. Click Home and then click the Connectors tab.
2. In the Title column, click the Connector name.
3. Type a user-friendly Name for the Connector and then click Save.
4. Restart the IIS server of all zone members.

To delete a Connector

Deleting a Connector does not remove data from SharePoint or a network file share.

1. Click Home and then click the Connectors tab.
2. Select the check box for the Connector and then click Delete and OK.
3. Restart the IIS server of all zone members.

Monitor StorageZones Controller

The Monitoring tab on the StorageZones Controller console provides component status to help you troubleshoot configuration issues. Status is provided for items such as access permissions, service status, and ShareFile connectivity.

StorageZones Controller and zone 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 StorageZones Controllers joined to the zone.

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

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