



Technical Report

Citrix ShareFile StorageZones on NetApp Solution Guide

Cedric Courteix, NetApp
February 2013 | TR-4124

“Follow-Me” Data with Citrix and NetApp

IT is struggling to reconcile new user requirements in the workplace, such as the need to securely store, share, and sync data on any device, anywhere, with the need to protect and store sensitive corporate data within their data centers, often to meet compliance requirements. Citrix ShareFile® addresses the needs of both users and IT by delivering a secure yet user-friendly follow-me data solution. NetApp® extends the solution by providing the capability to host more users and boost overall performance by using storage efficiency.

This solution guide highlights the architecture developed jointly by Citrix® and NetApp for running Citrix ShareFile with customer-managed StorageZones on NetApp storage that allows IT to store mission-critical data on the premises.

TABLE OF CONTENTS

1	Introduction	4
1.1	Scope	4
1.2	Key Terminology	4
1.3	Citrix ShareFile and NetApp Solution Highlights	5
2	Solution Design	8
2.1	High-Level Architecture	8
2.2	Detailed Solution Architecture	9
2.3	Solution Technology Components	11
2.4	ShareFile Encryption	12
2.5	Clustered Data ONTAP Storage Architecture	13
2.6	Network Access	14
2.7	Backup and File Restore	16
2.8	Check That the Data Remains On the Premises	21
2.9	StorageZone CIFS Connector for Existing Network Shares	23
3	Solution Validation	26
4	Summary	27
5	Acknowledgements	28
6	Feedback	28
	Resource Links	28
6.1	Citrix ShareFile	28
6.2	NetApp Data ONTAP	28
	Version History	29

LIST OF TABLES

Table 1)	Solution components	12
Table 2)	Hardware components.	12
Table 3)	Tests results.	26
Table 4)	Five key takeaways.	27

LIST OF FIGURES

Figure 1)	ShareFile storage efficiency with NetApp	6
Figure 2)	Consolidate with secure multi-tenancy	7

Figure 3) Citrix-managed versus customer-managed StorageZones.	8
Figure 4) Overall architecture.	9
Figure 5) Supported mobile and desktop applications (graphic provided by Citrix).	10
Figure 6) Control Plane architecture.	10
Figure 7) Customer-managed StorageZones architecture.	11
Figure 8) ShareFile encryption architecture.	13
Figure 9) CIFS share repository.	14
Figure 10) High availability StorageZone.	15
Figure 11) POC network access.	15
Figure 12) Secure DMZ network access.	16
Figure 13) Configure volume Snapshot copies using System Manager.	17
Figure 14) Creating a recovery queue.	18
Figure 15) New recovery queue folder location.	18
Figure 16) Edit recovery script parameters.	18
Figure 17) Process to restore files from NetApp Snapshot copies.	19
Figure 18) List of the UUIDs to be restored.	20
Figure 19) Select an account in the employee directory.	21
Figure 20) Verify user account default StorageZone.	22
Figure 21) Check folder options.	23
Figure 22) ShareFile private cloud with CIFS connector.	24
Figure 23) Storage efficiency savings.	27

1 Introduction

The consumerization of IT is bringing a paradigm shift in IT in many aspects. More and more users are embracing mobile work styles and the concept of bringing their own device to work. In order to be productive when using these devices from any location, the users require access to corporate resources, including applications and data. Over the years, enterprises have accelerated the adoption of desktop virtualization solutions to deliver corporate desktops and applications to users on any device, anywhere. However, they were not able to provide a solution for users to securely access and share data easily. In the absence of an IT-managed solution, users have started to use unsecured, consumer-style file sharing products such as Dropbox and iCloud that may place an organization's sensitive data and intellectual property at significant risk.

IT must deliver a managed service to users that allows them to access their data in sync across all devices and share it with people within and outside their organization. Although the service must deliver on the user's need for a simple yet rich experience, it should also provide IT with the ability to control how data can be stored, accessed, and shared.

Citrix ShareFile Enterprise is a follow-me data solution that meets the mobility and collaboration needs of all users while allowing IT to manage and store data wherever they want. With the ShareFile StorageZones feature, organizations have the flexibility to manage their data on the premises in customer-managed StorageZones or use Citrix-managed StorageZones (secure cloud options available in eight locations around the world) or have a mix of both. With customer-managed StorageZones, IT can place data in their organization's own data center to help meet unique data sovereignty and compliance requirements while optimizing performance by storing data in close proximity to the user. By defining where data should be stored, IT will be able to build the most cost-effective and customized solution for their organization. Customer-managed StorageZones can easily be integrated with an organization's existing infrastructure. With customer-managed StorageZones, IT can leverage highly efficient and scalable NetApp storage to store sensitive data on the premises while delivering the powerful service that users expect.

Through this joint reference architecture, Citrix and NetApp demonstrate the ability to deliver a scalable and unique solution with a secure infrastructure.

1.1 Scope

The solution described in this document is applicable for customers who want to build a file synchronization solution [on premises](#) with Citrix ShareFile Enterprise edition and NetApp unified storage.

This solution guide focuses primarily on the key values and the design elements of this joint architecture. Detailed step-by-step instructions on how to install and administer the solution are outside the scope of this guide.

For an overview of the key highlights of this solution, refer to the [Solution Brief: NetApp Storage Solution for Citrix ShareFile Enterprise](#).

1.2 Key Terminology

This section describes the **NetApp Data ONTAP®** and **Citrix ShareFile** terminology used throughout this document.

- [NetApp Data ONTAP](#). Storage operating system (OS) that manages the NetApp storage array.
- [Clustered Data ONTAP](#). Virtualize storage across various HA pairs, manage it as a single logical pool, and scale out your data. The [Data ONTAP 8](#) operating system offers a unified scale-out storage solution for an adaptable, always-on storage infrastructure to accommodate today's virtualized infrastructure.

- **Vserver** (virtual server). Clustered Data ONTAP includes a logical entity named Vserver. Each Vserver is viewed as an individual storage subsystem inside the cluster.
- **Deduplication and Compression**. These are fundamental components of the core Data ONTAP architecture. Both technologies provide a significant increase in storage capacity.
- **Nondisruptive Operations** (NDO). Eliminates downtime and is embedded in the clustered Data ONTAP scale-out architecture. NDO enables the storage infrastructure to remain up and serve data through the execution of hardware and software maintenance operations, as well as during IT lifecycle operations.
- **Citrix StorageZones**. A feature that enables administrators to choose where data is stored. It allows organizations to manage their data on the premises of the customer's data center or off the premises in secure cloud options or both.
 - **Customer-managed StorageZones**. Relies on the customer data center infrastructure; each zone is designed to support any CIFS-based network share.
 - **Citrix-managed StorageZones**. Secure cloud locations where customer data can be stored. Citrix manages all software/hardware updates, file versioning updates, as well as antivirus software and backup.
- **Control Plane**. Also called the control subsystem. It handles folder permissions, authentication, brokering, and reporting. Citrix hosts it in its data centers in the United States and the European Union.
- **Storage Center**. A Web service that handles all communication from end users and the ShareFile Control Plane. It is the ShareFile storage subsystem and handles operations related to file storage.
- **On-Demand Sync**. This capability is optimized for use with virtual desktops and applications, including those powered by Citrix XenDesktop® and Citrix XenApp®. This capability is built into the ShareFile Sync tool for Windows®. Users can view a list of all files but the download and synchronization occur only when users want to access or edit a file.
- **StorageZones Connectors**. Works in conjunction with StorageZones. It enables instant mobile access to users, to retrieve data on existing network file shares through ShareFile iOS applications. This option does not require a traditional VPN tunnel to be established.

1.3 Citrix ShareFile and NetApp Solution Highlights

Citrix ShareFile StorageZones and NetApp offer a cost-effective and scalable file sharing solution with the following key benefits.

- Storage efficiency
- On-demand flexibility
- Nondisruptive operations
- Unified storage architecture
- Data protection

Storage Efficiency

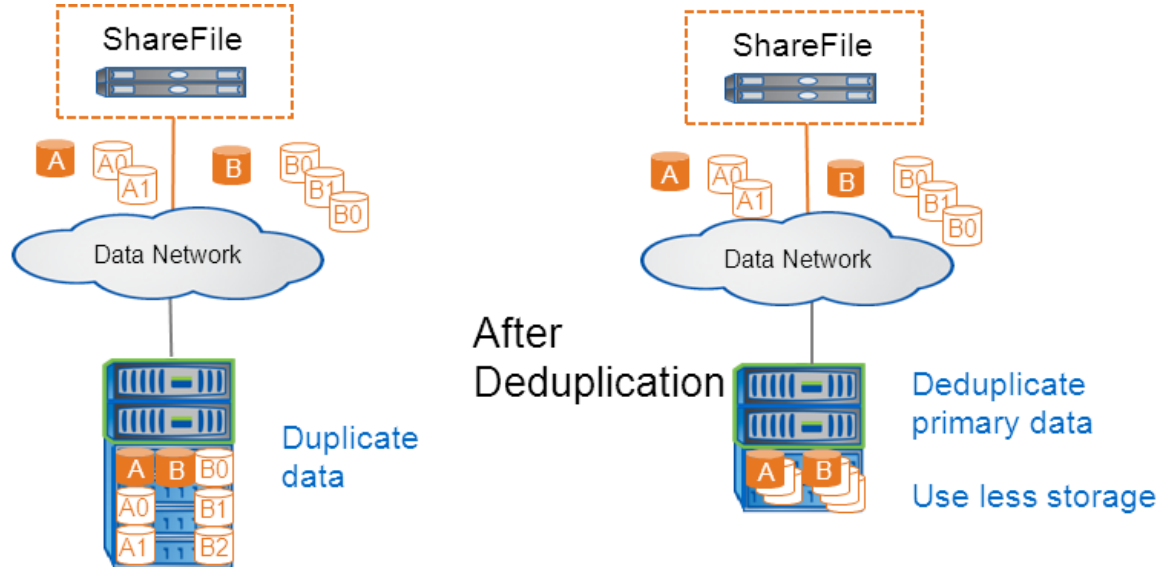
NetApp has several levels of storage efficiency that help customers deploy ShareFile using less storage than what was traditionally required for a storage architecture like ShareFile. For details on NetApp capabilities, refer to [WP-7022: The NetApp Storage Efficiency Guide](#).

- **Deduplication**. NetApp deduplication provides block-level deduplication within the entire flexible volume. Essentially, deduplication removes duplicated blocks, stores only unique blocks in the flexible volume, and creates a small amount of additional metadata in the process.
- **Data Compression**. Compression helps reduce the physical capacity required to store data on storage systems by compressing data within a FlexVol® volume.

- **Thin Provisioning.** NetApp Data ONTAP does not allocate storage to a specific volume until data is written to the physical storage.
- **Autogrow.** Autogrow allows automatic expansion of NetApp volumes to meet the growing needs of the hosted data.

With the ShareFile object storage–based architecture, every update to the user’s files results in the creation of a new file on the back-end storage. Therefore, NetApp storage efficiency technologies help deduplicate the storage required for this highly duplicated data, thereby allowing storage cost savings. Additional savings are also obtained with the use of cross-file deduplication. Customers simultaneously achieve mobility and transparent data access with Citrix ShareFile.

Figure 1) ShareFile storage efficiency with NetApp.



As illustrated in Figure 1, NetApp provides the capability to use deduplication on the primary storage at the block level so that a pair of files that are nearly identical can be reduced to use slightly more capacity than the original file. In this example, files A and B have been updated numerous times, resulting in different versions. Since several iterations of the same file have a high percentage of similar content, NetApp deduplication reduces the footprint of those files in the CIFS share. Additionally, files A and B (and others) may also share identical information, resulting in more savings. Deduplication is one of several NetApp storage efficiency technologies that can help customers to significantly cut costs by using fewer disk drives.

On-Demand Flexibility

With NetApp storage, customers can transparently [scale out](#) their platforms.

Both the Citrix and NetApp components of the solution can be easily scaled out to seamlessly add more users to the environment.

- **Citrix ShareFile Storage Center (IIS Server).** NetApp recommends starting with a zone that contains a minimum of two Web servers for redundancy; more servers can be added later to increase capacity. Each midrange Web server pair can accommodate 5,000 users. For detailed guidance, contact the Citrix account team.
- **NetApp Storage.** Up to 24 nodes can be nondisruptively added to a clustered Data ONTAP deployment. A single CIFS share can span [multiple nodes](#). As a result, customers can scale out transparently without downtime.

Nondisruptive Operations

NetApp nondisruptive operations (NDO) allow seamless storage operations without downtime. Storage upgrades and maintenance can easily be achieved without interrupting the user's access to files.

File sharing is critical to business users; any downtime results in loss of productivity. More importantly, it can result in poor customer satisfaction. NDO in Data ONTAP provides the following benefits.

- Refresh hardware and software transparently without losing access to the customer's data. When it is time for an update, administrators can simply move the CIFS volume to another node within the cluster nondisruptively to retire the old hardware from the cluster.
- Move data to a different node to redistribute the workload across a cluster. This task can be accomplished during normal business hours, allowing for a more dynamic platform, without waiting for the next maintenance window.
- Maintenance operations on specific hardware or software components can also be accomplished transparently. For example, adding a [Flash Cache™](#) acceleration card or redistributing data across controllers can be done nondisruptively.

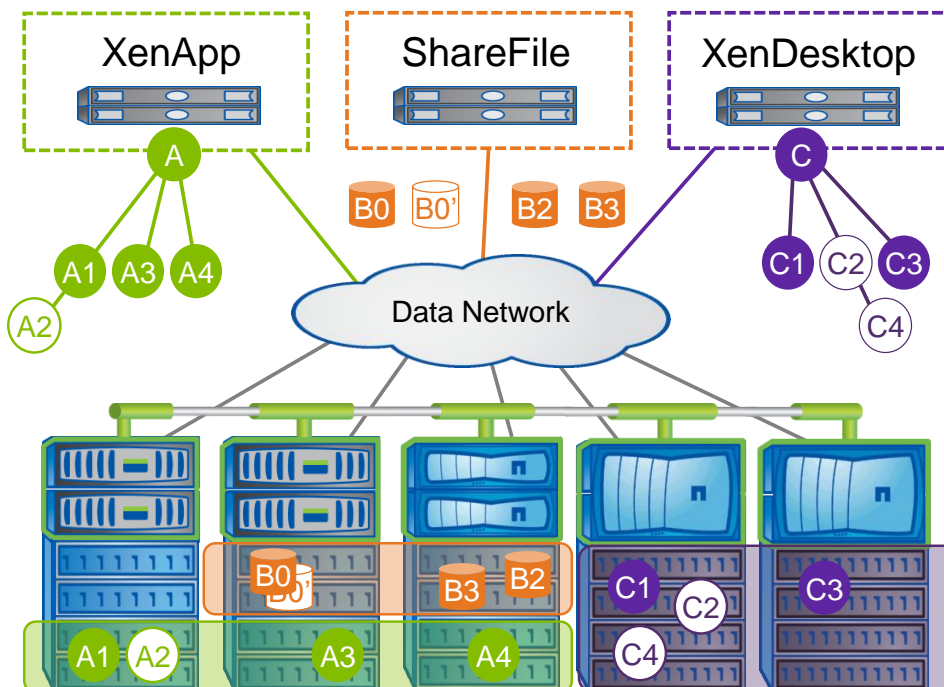
Unified Storage Architecture

The NetApp storage array can be shared between Citrix ShareFile, Citrix XenApp, and Citrix XenDesktop deployments.

It is possible to consolidate and yet use different protocols for the components hosted on NetApp storage. Several protocols can be leveraged on the same physical array. For example, numerous volumes are required when building a XenDesktop environment with Citrix Provisioning Server (PVS). It is possible to host the write-back cache files on an NFS volume where the desktop images (vDisk) will be set up on an iSCSI LUN or CIFS share. Additionally, the user profiles and ShareFile folders will remain on two separate CIFS shares.

Furthermore, this approach can benefit multi-tenant architectures in which different companies or departments requiring isolation leverage the same storage.

Figure 2) Consolidate with secure multi-tenancy.



Data Protection

NetApp Snapshot Based Backups

NetApp [Snapshot](#)™ technology provides great value when backing up the CIFS share object repository for ShareFile StorageZones since it does not require plenty of storage. By implementing Snapshot, administrators can benefit from a quick backup, flexible schedule, and custom retention policies. Remote replication of the backups can be achieved by leveraging NetApp [SnapMirror](#)® technology.

NetApp System Manager should be leveraged to configure backup and replication policies for the CIFS share.

For details, see section “Enabling NetApp Snapshot Based Backups.”

File Restore

Out of the box, Citrix provides a seven-day backup “recycle bin” capability inside the ShareFile user interface. For restores older than seven days, NetApp Snapshot technology can be leveraged.

For details, see section “File Restore from NetApp Snapshot Copies.”

2 Solution Design

This section highlights the joint architecture for deploying Citrix ShareFile with StorageZones on NetApp clustered Data ONTAP.

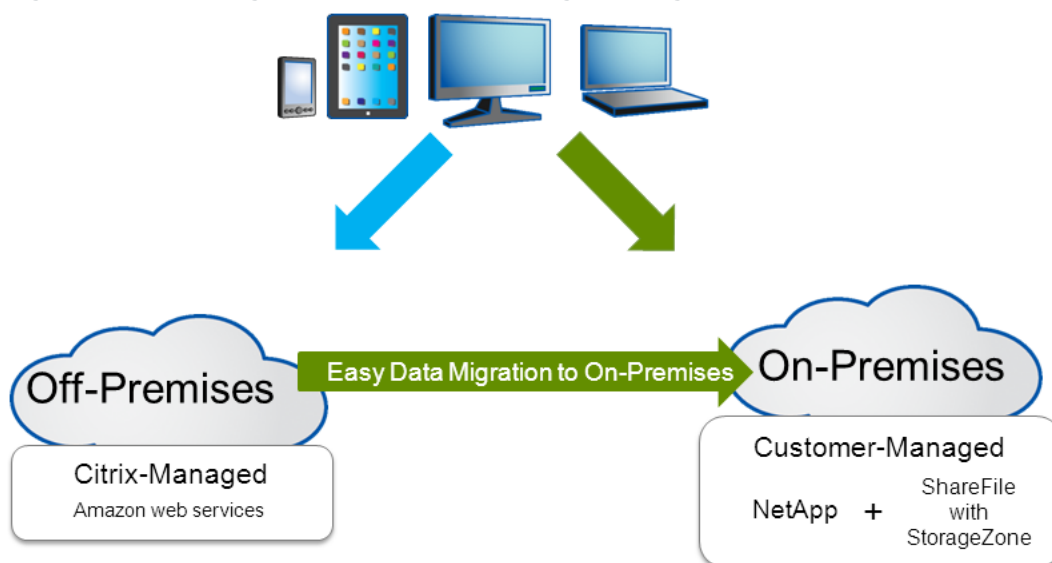
2.1 High-Level Architecture

Citrix ShareFile StorageZones allows customers to manage their data on the premises or in the cloud.

Previously, with a similar architecture, Citrix ShareFile supported only Citrix-managed StorageZones, providing a pure cloud offering hosted on Amazon EC2 and S3. This cloud offering can be combined with customer-managed StorageZones to provide a hybrid architecture.

This hybrid model illustrated in Figure 3 provides customers with the flexibility to leverage cloud or on-premises deployments depending on their compliance and performance requirements.

Figure 3) Citrix-managed versus customer-managed StorageZones.



This solution guide focuses on the on-premises architecture.

2.2 Detailed Solution Architecture

This section focuses on the details of the joint architecture. Figure 4 illustrates the overall architecture. Each component of the ShareFile on-premises infrastructure is described in the sections that follow.

Figure 4) Overall architecture.

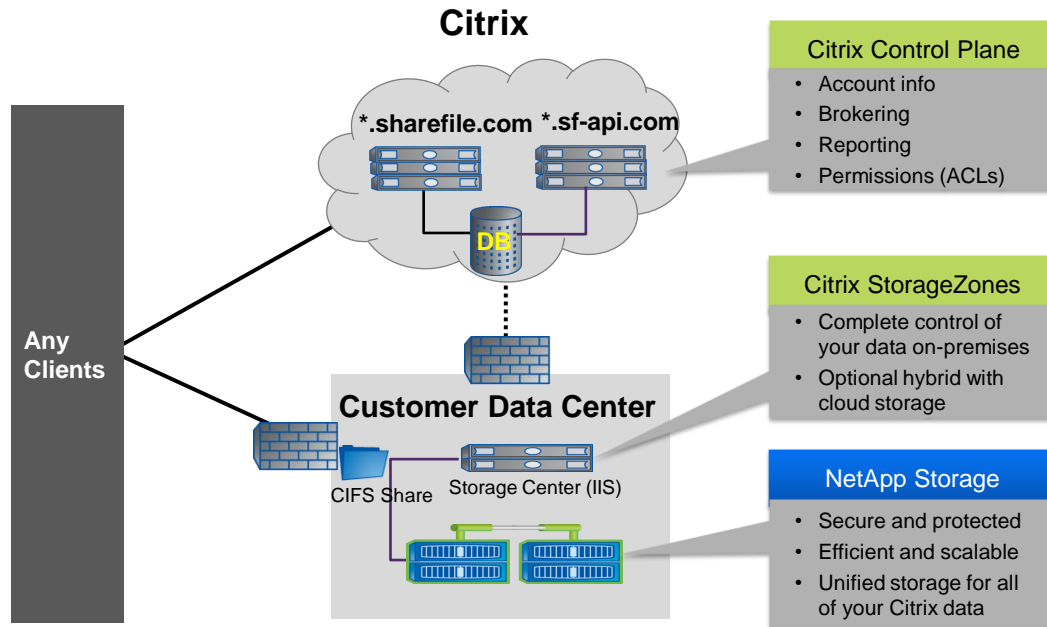


Figure 4 presents the following entities.

- **Client.** There are several **ShareFile clients** that allow end users to access the ShareFile application through browsers, desktop clients, and native mobile applications. In this design, client devices (indicated in left pane in Figure 4) will communicate with the following two subsystems.
 - **Citrix online data center.** The **Control Plane** is hosted in the Citrix data center and is responsible for validating the authentication, brokering to the customer environment, generating reports, and managing file permissions.
 - **Customer data center.** The **Storage Subsystem** in this model is hosted in the customer data center. Citrix refers to this component as a customer-managed StorageZone. NetApp provides a CIFS share with the benefit of native functionality such as storage efficiency, on-demand flexibility, data protection, nondisruptive operations, and unified storage.

Client connectivity and communication begin with the Control Plane. When authorized by the Control Plane, the client devices upload or download files directly from the NetApp storage subsystem.

Note: No customer files go through the Control Plane in the Citrix Online Data Center. All the users' data resides on the premises in the NetApp storage subsystem.

ShareFile Client

Figure 5 highlights the list of supported devices for this solution. For the most up-to-date list, go [here](#).

Figure 5) Supported mobile and desktop applications (graphic provided by Citrix).

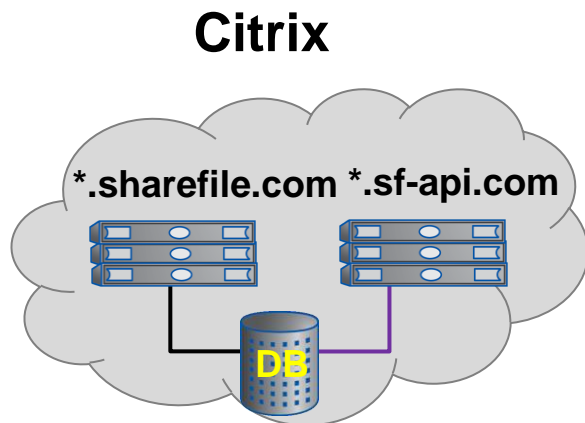


Control Plane

When a user establishes a session from any client device, he or she accesses a secure site through an SSL connection. The URL required to access the environment is specific to the customer. For example: <https://netapp.sharefile.com>.

The **Control Plane** is the component managed by Citrix in its data center. It contains the sharefile.com and sharefile.eu Web sites as well as the ShareFile business logic.

Figure 6) Control Plane architecture.



Storage Subsystem

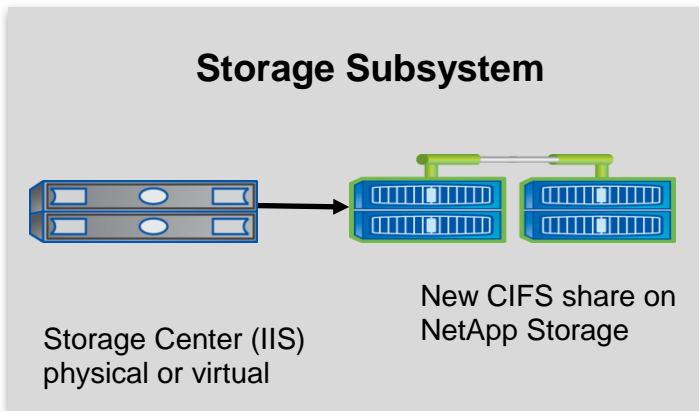
This component is also described as customer-managed StorageZones. NetApp is hosted in the customer's data center along with Storage Center servers that serve as brokering mechanisms to access data. The CIFS share is attached to the Storage Center servers as the content repository.

The **Storage Subsystem** component is described in Figure 7 and includes two elements.

- **ShareFile Storage Center.** One or several Web sites that reside on Microsoft® IIS are configured with ShareFile Storage Center software, which is a lightweight Web service that communicates with ShareFile clients and the on-premises storage.
- **NetApp Storage.** When installing Storage Center, the administrator creates a StorageZone. A single CIFS share hosted on NetApp is required for each zone. After the first Storage Center is added to a zone, NetApp recommends adding another StorageZone server and joining it to the same zone for redundancy. All server members of a StorageZone access the same CIFS repository.

Figure 7) Customer-managed StorageZones architecture.

Customer Data Center



The StorageZone components run inside the customer's data center and require a new CIFS share to be created. Each StorageZone has one or more Storage Center's software installed on Microsoft® Windows Server® 2008 R2 with the Microsoft IIS 7 release. ShareFile relies on an object-oriented file structure and predefined folders are added to the CIFS share when the zone is initialized.

A permanent map to the NetApp CIFS share needs to be mounted on each Microsoft IIS server. The following command can be run either on the Storage Center server or, more easily, through the Windows Explorer user interface.

```
Net use * \\<vServer>\<CIFS share> /persistent:yes
Net use /show map
```

To configure ShareFile for on-premises shared storage, follow the procedure described here: <http://support.citrix.com/proddocs/topic/sharefile-enterprise/sf-deploy-high-availability.html>

2.3 Solution Technology Components

This section describes each of the physical and virtual building blocks included in this solution.

Table 1 lists the software components used in this solution.

Table 1) Solution components.

Solution Component
Hypervisor Foundation of the underlying resources. This includes the following. <ul style="list-style-type: none"> • Citrix XenServer 6.0.2 hosts were used in this solution to run the following virtual machines (VMs). Note that any hypervisor can be used to run these virtual machines. <ul style="list-style-type: none"> – Two VMs: Windows Server 2008 R2 with IIS and Citrix Storage Center software. – Two VMs: Windows Server 2008 R2 with Active Directory® and Domain Name Service (DNS) functions. NetApp recommends using the existing AD and DNS infrastructure. <p>Note that physical servers can also be used to run the above-mentioned server roles.</p>
NetApp <ul style="list-style-type: none"> • Version: clustered Data ONTAP 8.1 • Licenses: CIFS protocol and deduplication • Management software: OnCommand System Manager 2.0 and Virtual Storage Console (VSC) 1.0 for Citrix XenServer

Table 2 lists the hardware components used in this solution.

Table 2) Hardware components.

Solution Components
<ul style="list-style-type: none"> • Two servers with 48GB RAM and two quad-core CPUs per host • Two 10Gb Ethernet ports
Two NetApp FAS2240 4U controllers with eight 2TB 7.2K SAS drives
Two Cisco® Nexus® 5020 switches with several 10GbE Ethernet ports

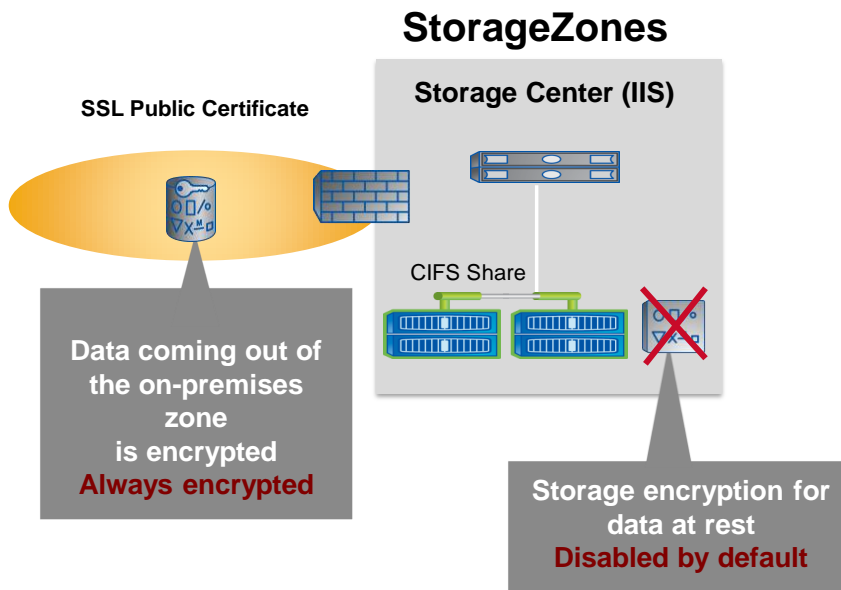
2.4 ShareFile Encryption

Best Practice
Citrix ShareFile will always encrypt data in transit. Citrix and NetApp recommend leaving data unencrypted at rest, since all the data remains secure in the customer data center.

For on-premises deployment, data encryption is not required since the data is stored in the secure on-premises data center. By disabling encryption of data at rest on the premises, customers can also obtain storage savings from NetApp storage efficiency technologies.

Figure 8 shows the encryption architecture, including NetApp and Citrix recommendations on where to enable and disable encryption.

Figure 8) ShareFile encryption architecture.



2.5 Clustered Data ONTAP Storage Architecture

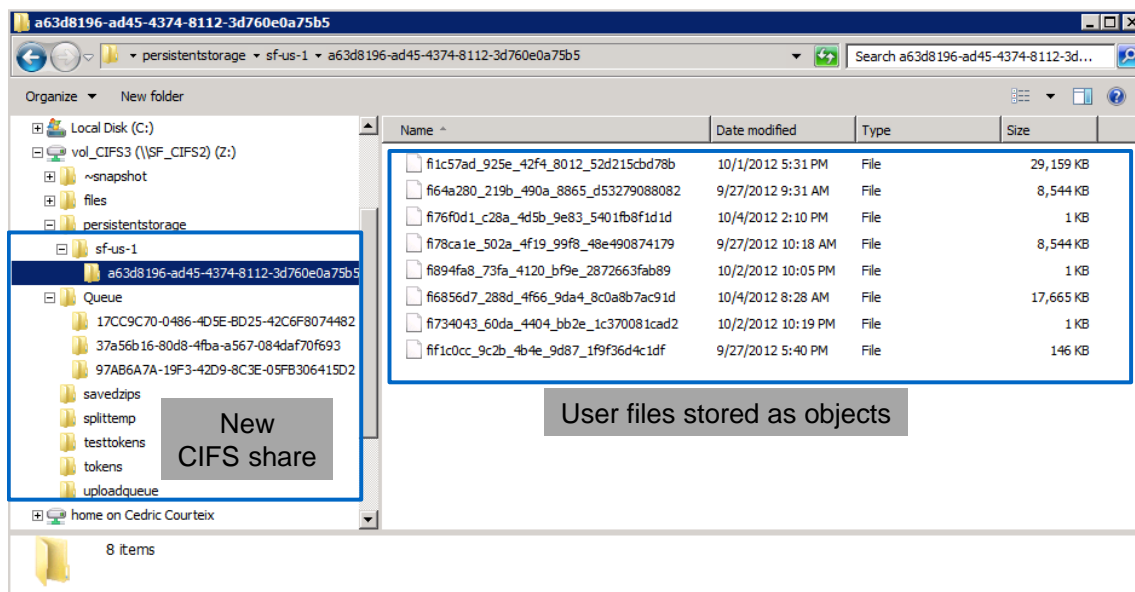
To benefit from the key NetApp capabilities highlighted in [section 1.3](#), the following technology components need to be implemented.

- **A New CIFS Share.** Citrix ShareFile requires a CIFS share with no data in it since the system will create its own folder structure. The object files created by users are stored in a folder called `persistentstorage` (see Figure 9). Follow the [NetApp best practices](#) to set up a Vserver with a dedicated CIFS share using SMB 2.0.
- **CIFS Share Permissions.** Once the setup is completed, configure the new CIFS share using System Manager. It is important to remove the default account permissions (everyone) and enter a dedicated administrative account for the Storage Center to access the CIFS share through SMB. Specifying an administrative account to access the users' files will prevent untrusted users from accessing this [UNC path](#).

For detailed information about clustered Data ONTAP, refer to [TR-3982](#) and [TR-3967](#).

Figure 9 illustrates the file structure that Citrix ShareFile leverages for on-premises release. It is an object-oriented architecture and users' files are stored as objects.

Figure 9) CIFS share repository.



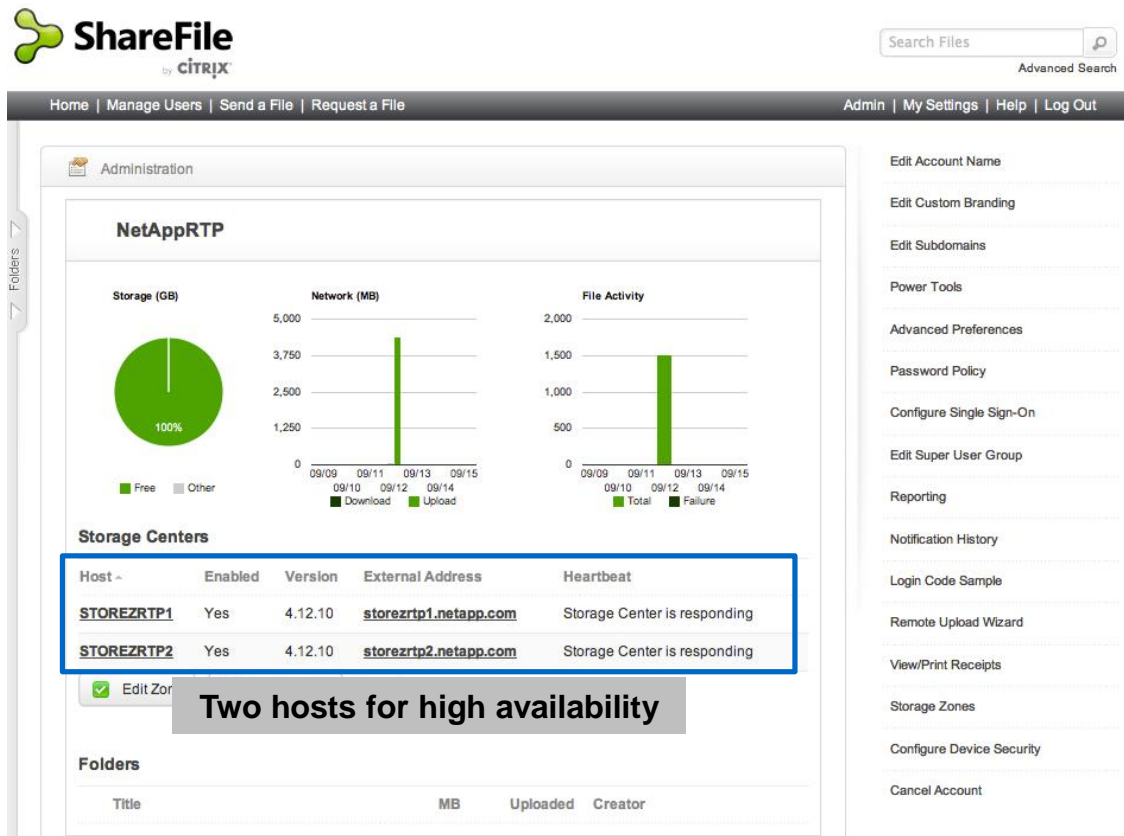
Note that if the administrator renames any of the objects in the preceding figure with its actual file name and extension, the file will become accessible.

2.6 Network Access

Although NetApp recommends creating a redundant infrastructure for the platform depending on the customer's infrastructure, different approaches are available to configure redundant network access. Figure 10 represents a zone configured with two Storage Center servers in load balancing mode.

To access the summary of the StorageZone configuration, open the ShareFile Web user interface with an administrator account. Select the Admin tab and go to StorageZones on the left pane.

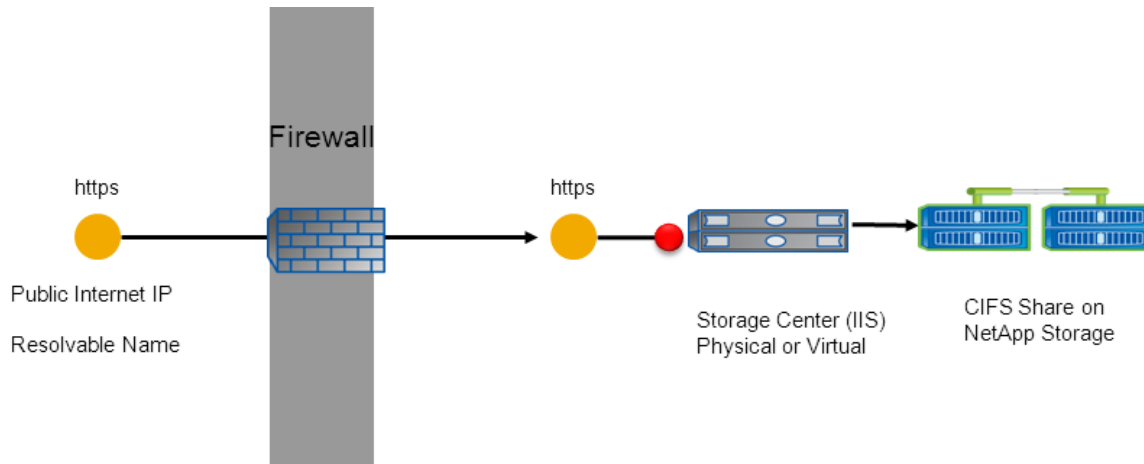
Figure 10) High availability StorageZone.



StorageZones Proof of Concept

Figure 11 illustrates a typical proof-of-concept (POC) architecture. The setup requires at least one external SSL certificate associated to a public IP address to be mapped to the Storage Center server. For details on the required components, refer to the [Citrix POC reference documentation](#).

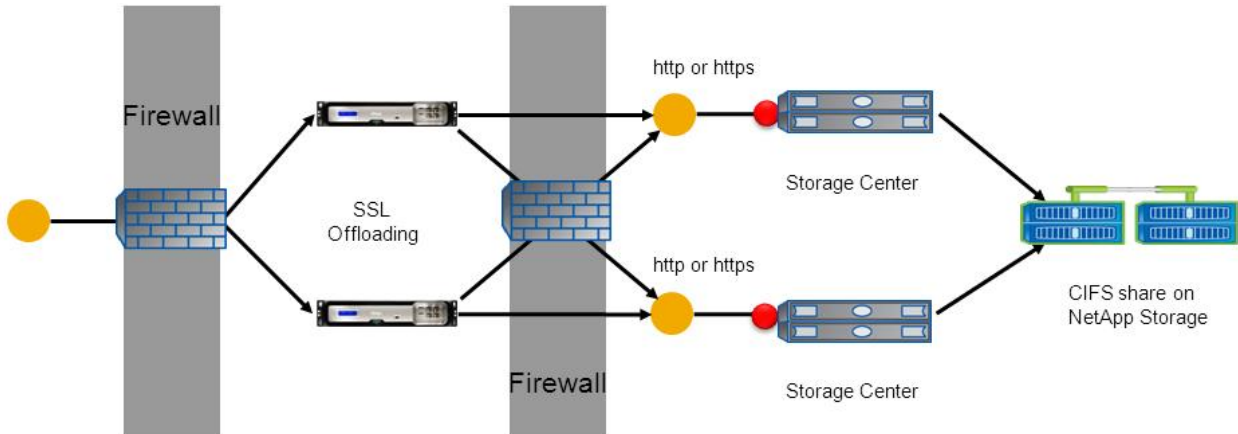
Figure 11) POC network access.



StorageZones Enterprise Deployment

For an enterprise deployment, NetApp recommends leveraging a proxy server for security and load-balancing capabilities. For example, Citrix NetScaler can be used to proxy the communication internally. The goal is to terminate the SSL communication at the proxy entrance and to reestablish a secure link to the Storage Center on the internal network. For details on the required components, go to <http://support.citrix.com/proddocs/topic/sharefile-enterprise/sf-deploy-in-dmz.html>.

Figure 12) Secure DMZ network access.



2.7 Backup and File Restore

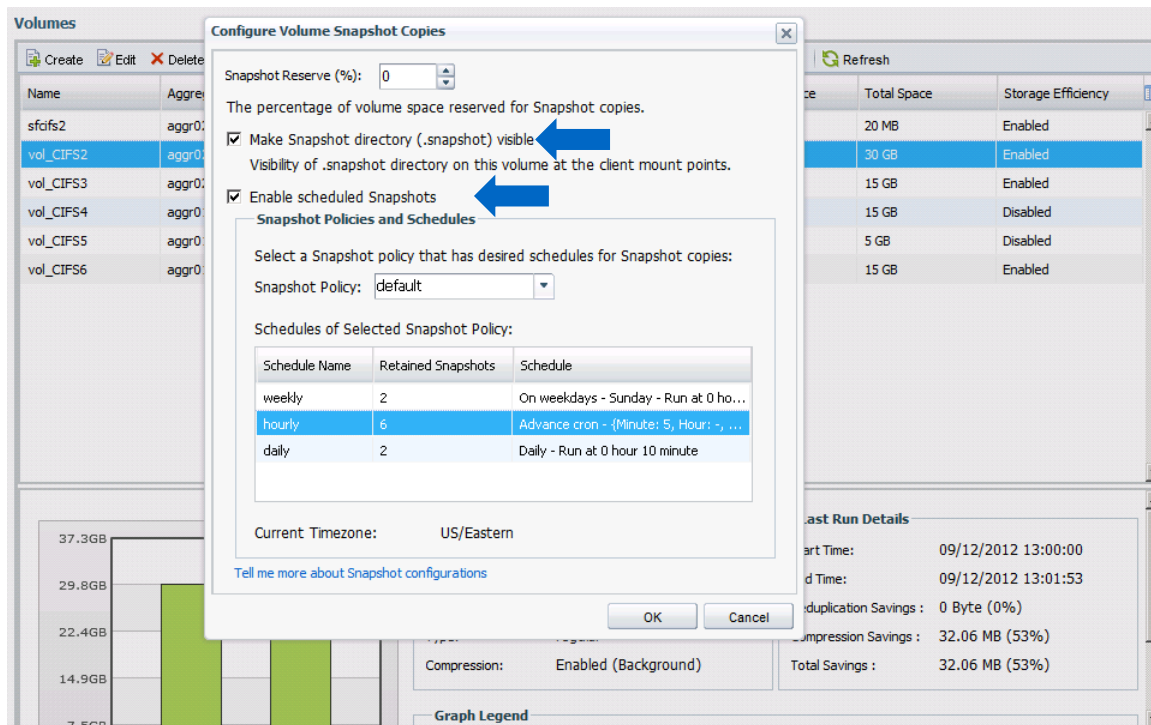
By default, Citrix ShareFile provides the option to restore files that are up to seven days old. This section describes how to set up NetApp Snapshot-based storage-efficient backups and file restore from NetApp Snapshot copies for files that were deleted more than seven days ago.

Enabling NetApp Snapshot Based Backups

To enable Snapshot based backups, perform the following steps.

1. Leverage NetApp System Manager to configure the Snapshot copy schedule and retention policy and optionally SnapMirror remote replication. A Snapshot copy is a read-only image of a volume that captures the state of the file system at a point in time.

Figure 13) Configure volume Snapshot copies using System Manager.



Make sure that the NetApp based Snapshot directory is visible to the administrators at the root of the CIFS share by selecting the Make Snapshot directory (.snapshot) visible checkbox in the Configure Volume Snapshot Copies page (Figure 13).

2. Create and configure a `recovery` queue (a list of files to be recovered) on Storage Center.

This step is required to capture the restoration notification for new files. Without this information it is impossible to associate the file to be restored with the object file stored in the NetApp CIFS share.

- a. Launch a PowerShell™ window on one of the Storage Center servers.
- b. Create a new `recovery` queue using the following commands provided by Citrix in the “C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery” folder.

```
> Import-Module .\recovery.psml
> New-SCQueue -name recovery -operation recovery
```

Note: If you are unable to import the recovery module, launch the following command change permissions¹:

```
> Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
```

- c. By default, only the `copy` and `delete` queues are created. To verify that the `recovery` queue is created, launch the following command:

```
> Get-SCQueue
```

¹ <http://technet.microsoft.com/library/hh847748.aspx>)

Figure 14) Creating a recovery queue.

```

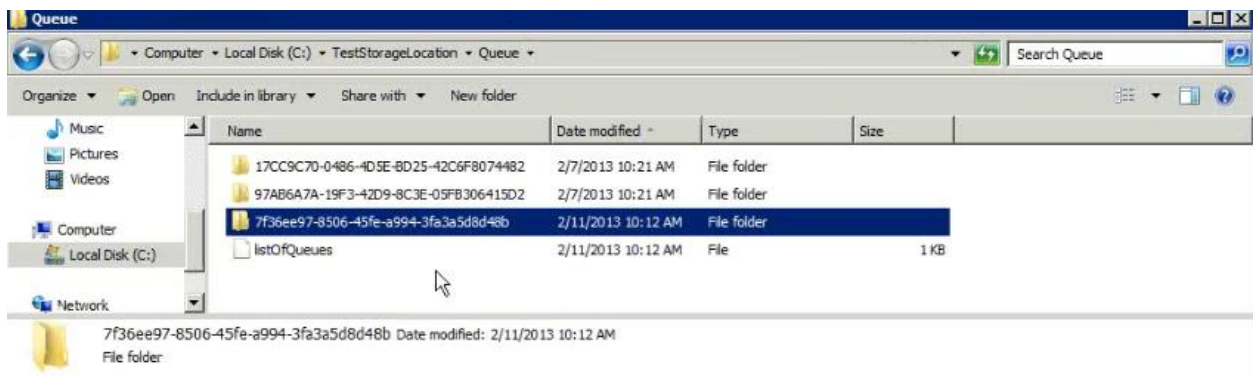
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery"
PS C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery> Import-Module .\Recovery.psm1
PS C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery> Get-SCQueue

id                                     name                                     operation
--                                     -
17CC9C70-0486-4D5E-BD25-42C6F8074482  copy                                     copy
97AB6A7A-19F3-42D9-8C3E-05FB306415D2  delete                                 delete

PS C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery> New-SCQueue -name recovery -operation recovery
Queue 7f36ee97-8506-45fe-a994-3fa3a5d8d48b created
PS C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery>
  
```

Figure 15) New recovery queue folder location.



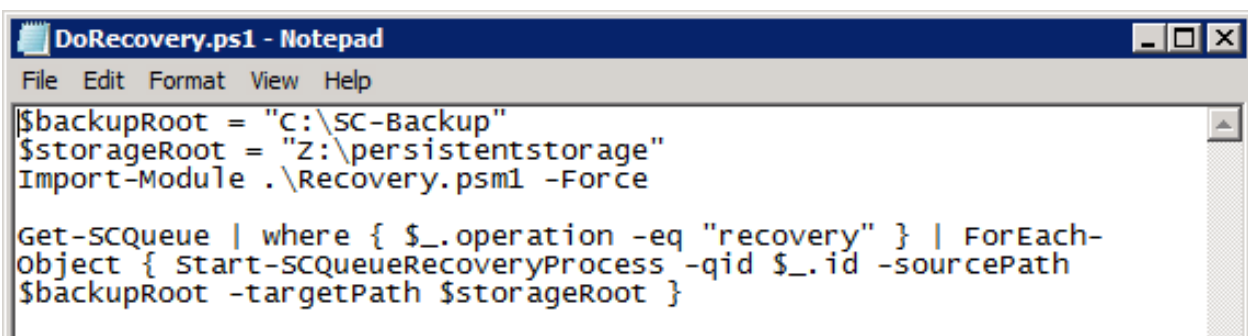
- d. To edit the configuration file, edit the following PowerShell script located in the folder defined in step c.

Figure 16 shows the default values for the DoRecovery.ps1 file. Add the appropriate values for the backup source (\$backupRoot) and file destination (\$storageRoot).

To edit the file, run the following command:

```
> Notepad "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery\DoRecovery.ps1"
```

Figure 16) Edit recovery script parameters.



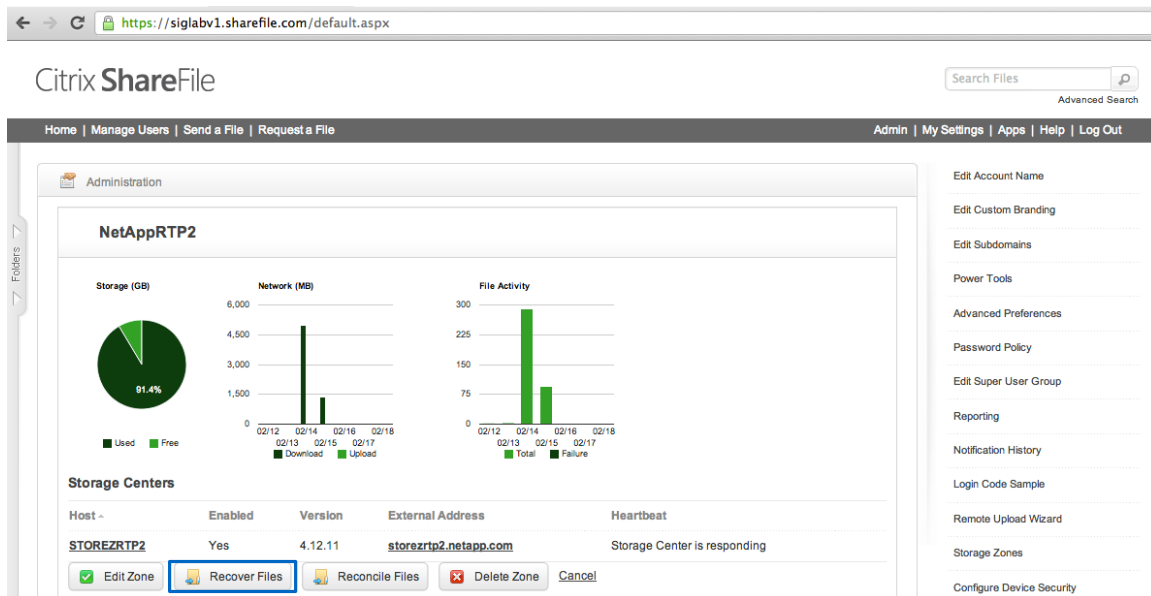
File Restore from NetApp Snapshot Copies

Since the ShareFile metadata for a file deleted by the user will be removed automatically by ShareFile after seven days, NetApp Snapshot technology can be leveraged to restore the files that were deleted more than seven days ago. Figure 17 shows the high-level process for restoring a file from a NetApp Snapshot copy.

Figure 17) Process to restore files from NetApp Snapshot copies.

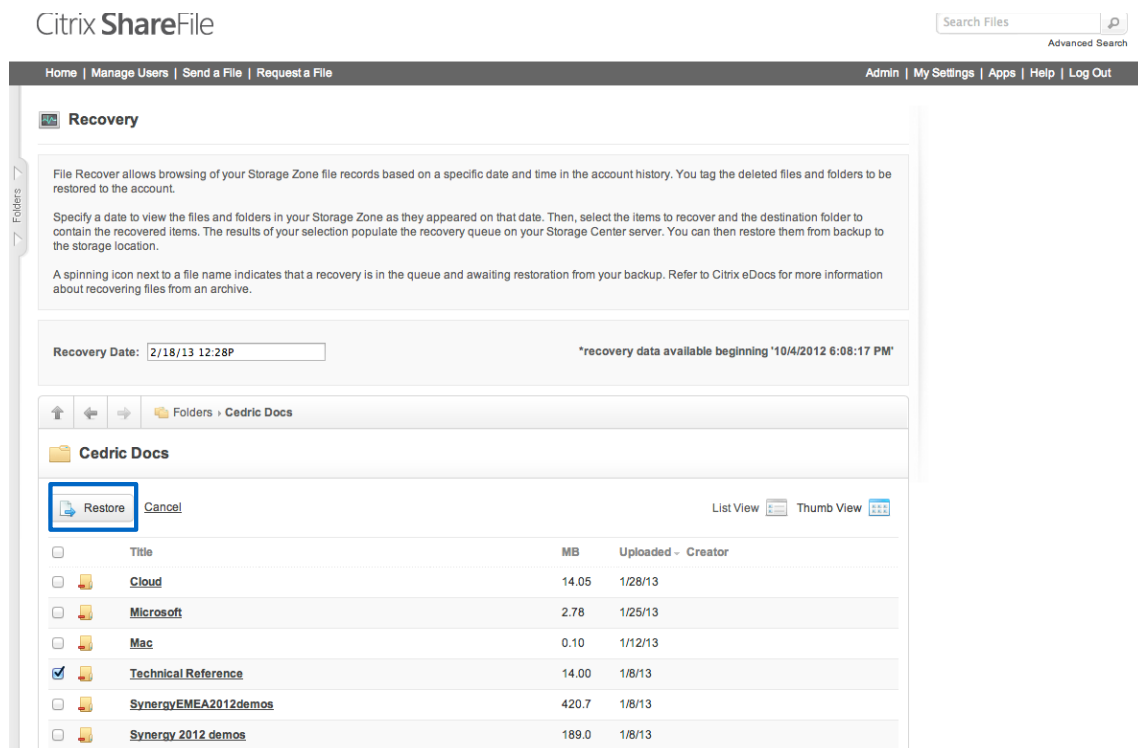


1. As an administrator, launch ShareFile Web interface to select files to be restored.
 - a. Go to the Admin tab and select StorageZones. The StorageZone used in this example is NetAppRTP2. After selecting the zone, click Recover Files to restore from the user interface.



- b. From the Recovery menu, select the files or folders to be restored, and then click Restore.

Note: Using this method, several files and folders can be restored at the same time.



2. Obtain the list of IDs that need to be restored. Launch the following PowerShell command to consult the `recovery` queue previously created:

```
> Get-RecoveryPendingFilesIDs
```

Figure 18) List of the UUIDs to be restored.

```
PS C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery> Get-RecoveryPendingFileIDs
fi6cd7e4_920f_425b_bdac_049ae0235aef
fibf1734_9428_4d10_881a_68578358530d
fi2c5f56_21ee_467e_bc67_889218d028f8
fi2cc740_2337_4e24_be21_ddde64d7cf90
fi71b6cd_c135_46dc_bc8e_420cf3069feb
fi1219cd_4418_44c4_aa16_228e10c94974
fie64013_d0e7_493b_b72c_d03c86f583a3
fie17da3_60bd_4751_bbd3_e2f2c820dbf8
fi2b19d4_eccc_40ea_8de9_a2a260169808
fie61f8c_9d27_446b_9983_27b36a5c23e0
PS C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery>
```

3. Find the files listed in Figure 18 in the Snapshot directory and copy them to the `$backuproot` location previously defined in the `DoRecovery.ps1` configuration file.
 - a. After obtaining the list of UUIDs of the files to be restored, the next step is to search for the object file in the `NetApp ~snapshot` folder under the specific date (identified by the user) corresponding to the UUIDs referenced in the `upload` queue. If the user is unable to provide a date, the administrator will have to search for the most recent version of this file in all the Snapshot directories.
 - b. In this example, the file was located under the daily backup from October 28, 2012. The next step is to save this file to a temporary directory. The following command can be run either on the Storage Center server or, more easily, through the Windows Explorer user interface.

```
Copy ~snapshot\daily.2012-10-28_0010\persistentstorage\sف-us-1\fa63d8196-ad45-4374-8112-3d760e0a75b5\fi6f1576-e7b9-4703-b7b0-094c6f4dcf6d C:\SC-Backup\fi6f1576-e7b9-4703-b7b0-094c6f4dcf6d
```

4. Restore the files and notify the users that the process is complete.
 - a. Run the `DoRecovery.ps1` script that will copy the files in your backup directory to the `storageroot` directory. This process will assign a new UUID to each file and notify the Control Planes that the files were successfully recovered.

```
> .\DoRecovery.ps1
```

- b. Notify the users that the file restore is complete. A best practice is for the ShareFile administrator to provide the URL of the restored file to the users.
- c. Run the `Get-RecoveryPendingFileIDs` script to verify that all files were restored. The list returned should be blank indicating that all objects were found and successfully recovered.

```
> Get-RecoveryPendingFileIDs
```

2.8 Check That the Data Remains On the Premises

For performance and compliance reasons, it is important to verify that the user folders are configured to store data on the premises. If they are not configured, users might store their files in the ShareFile public cloud. To verify user folder configuration, launch the ShareFile Web interface as an administrator.

Figure 19) Select an account in the employee directory.

The screenshot shows the Citrix ShareFile web interface. The top navigation bar includes links for Home, Manage Users, Send a File, Request a File, Admin, My Settings, Apps, Help, and Log Out. The 'Manage Users' section is active, displaying a 'Browse Employees' table. The table has columns for Name, Email, Last Login, and Manage. Two users are listed: 'Adolphus, Corey' and 'Courteix, Cedric'. The 'Courteix, Cedric' row is highlighted with a blue box. A blue arrow points to the 'Manage Users' link in the top navigation bar, and another blue arrow points to the 'Browse Employees' link in the right sidebar. Below the table, a grey box contains the text 'Select a user account to be verified'.

Name	Email	Last Login	Manage
Adolphus, Corey	Corey.Adolphus@netapp.com	12/15/12 1:09A	[Icon]
Courteix, Cedric	cedric.courteix@netapp.com	1/13/13 8:31P	[Icon]

Select a user account to be verified


In the next page, verify that the field containing the default zone for the user account corresponds to the on-premises zone and not to the ShareFile public cloud.

Figure 20) Verify the default StorageZone name.

Citrix ShareFile Search

Home | Manage Users | Send a File | Request a File Admin | My Settings


Cedric Courteix

 View this user's

For security and privacy reasons, some operations and editing capabilities may vary by user. [More Info.](#)

Basic Information

Created: 10/9/12 by Cedric Courteix

Email Address: 

First Name:

Last Name:

Company:

Notifications:

Admin Privileges

- ☒ Grant this user all admin permissions
- ☒ Allow this user to modify account-wide policies
- ☒ Allow this user to edit custom branding
- ☒ Allow this user to access other users' File Boxes
- ☒ Allow this user to view all emails
- ☒ Allow this user to manage employee users
- ☒ Allow this user to manage remote upload forms
- ☒ Allow this user to access account-wide reporting
- ☒ Allow this user to edit shared distribution groups
- ☒ Allow this user to view receipts/invoices
- ☒ Allow this user to edit billing information
- ☒ Allow this user to request plan changes

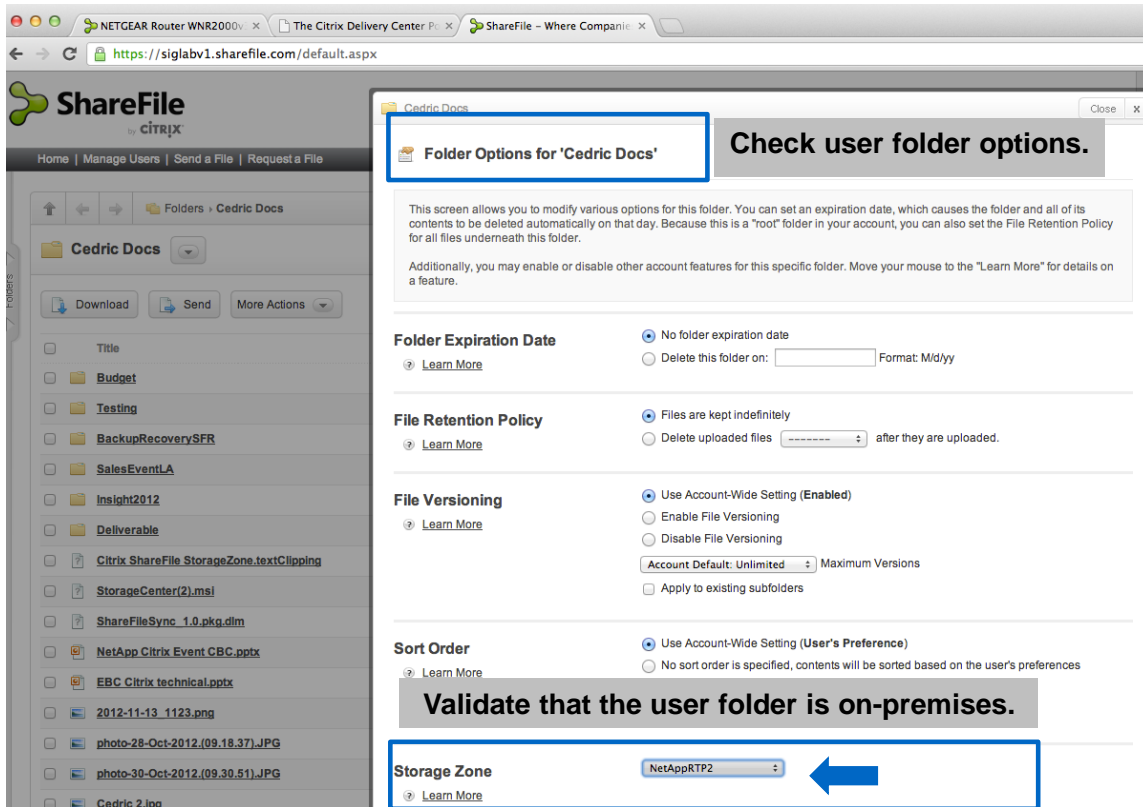
Validate that StorageZone name is correct

Default Storage Zone:

☒ Allow employee to create root-level folders

Users and administrators can verify the configuration of a specific folder by viewing the folder options for that directory.

Figure 21) Check folder options.



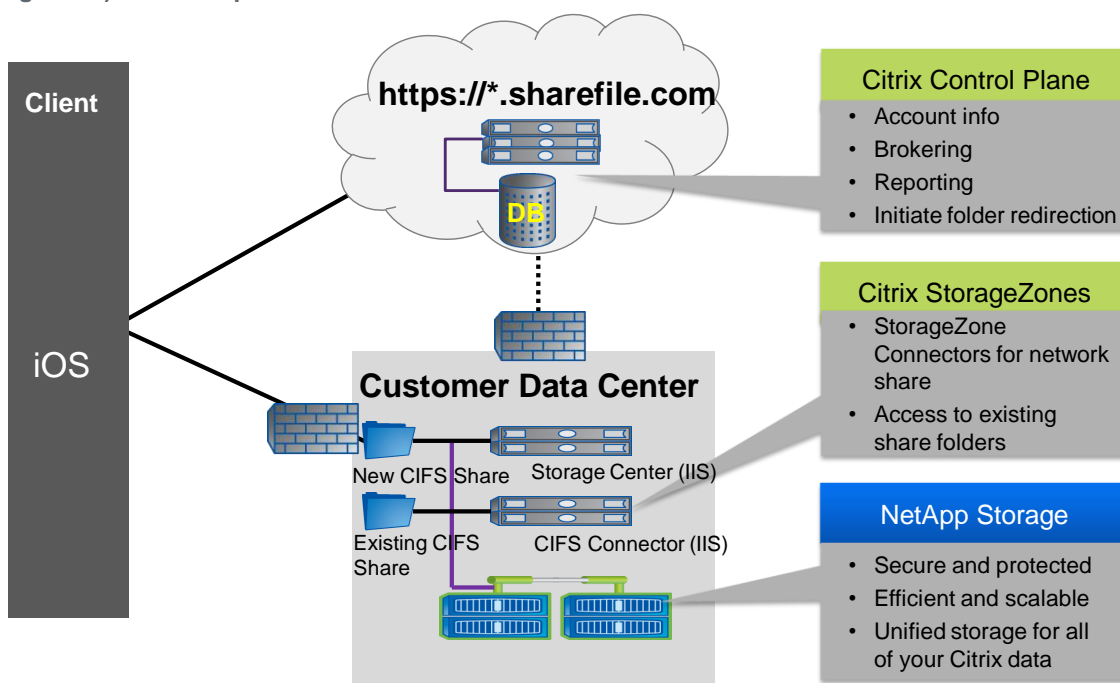
2.9 StorageZone CIFS Connector for Existing Network Shares

The CIFS connector provides the ability to instantly share entire NetApp CIFS directories without having to individually upload each file. This feature is extremely useful for existing shares or for providing read-only access to files to coworkers who are on the road.

Note: An existing CIFS share will maintain its current file structure and permissions. As opposed to Storage Center, in CIFS connector, the files will not be transformed into objects. Administrators can add as many universal naming convention (UNC) paths as needed to StorageZone.

Figure 22 is an example of ShareFile private cloud implementation with the CIFS connector added.

Figure 22) ShareFile private cloud with CIFS connector.



The StorageZone CIFS Connector is a separate feature and must be installed on a dedicated IIS server. In StorageZone version 1.1, this server should be separated from the Storage Center that runs the local ShareFile zone. It is important to note that the CIFS connector cannot run without the use of the Storage Center.

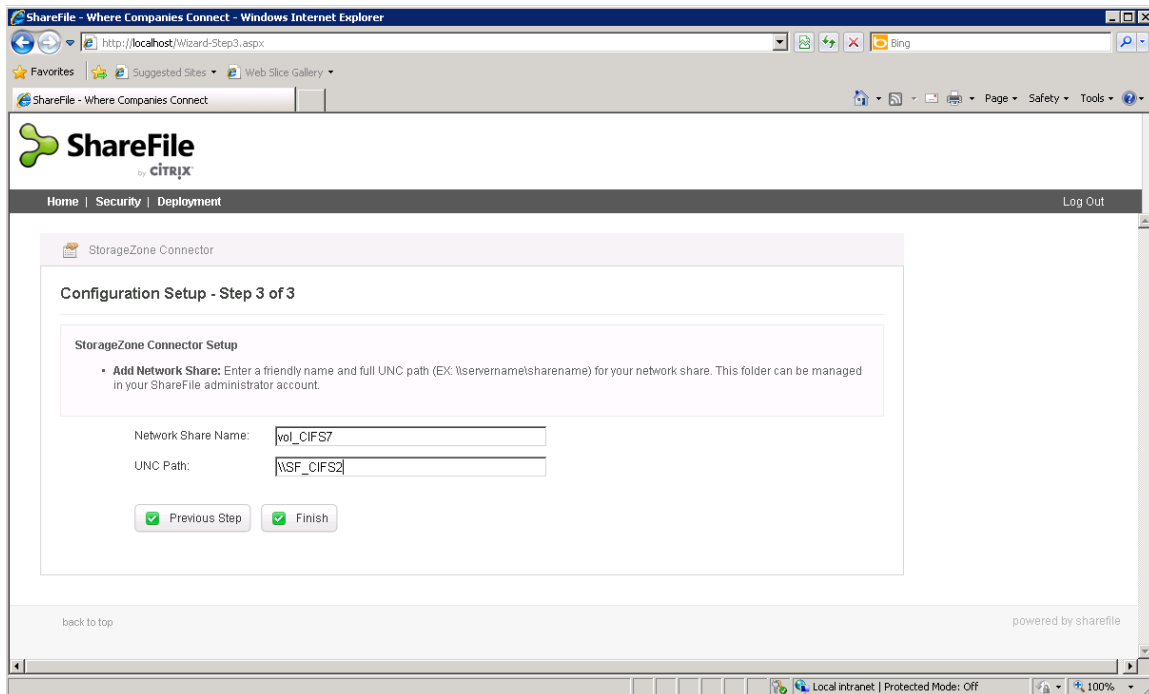
To install and configure this component on NetApp storage, refer to the installation procedure provided in the [Citrix eDocs](#) site.

Add an Existing CIFS Share

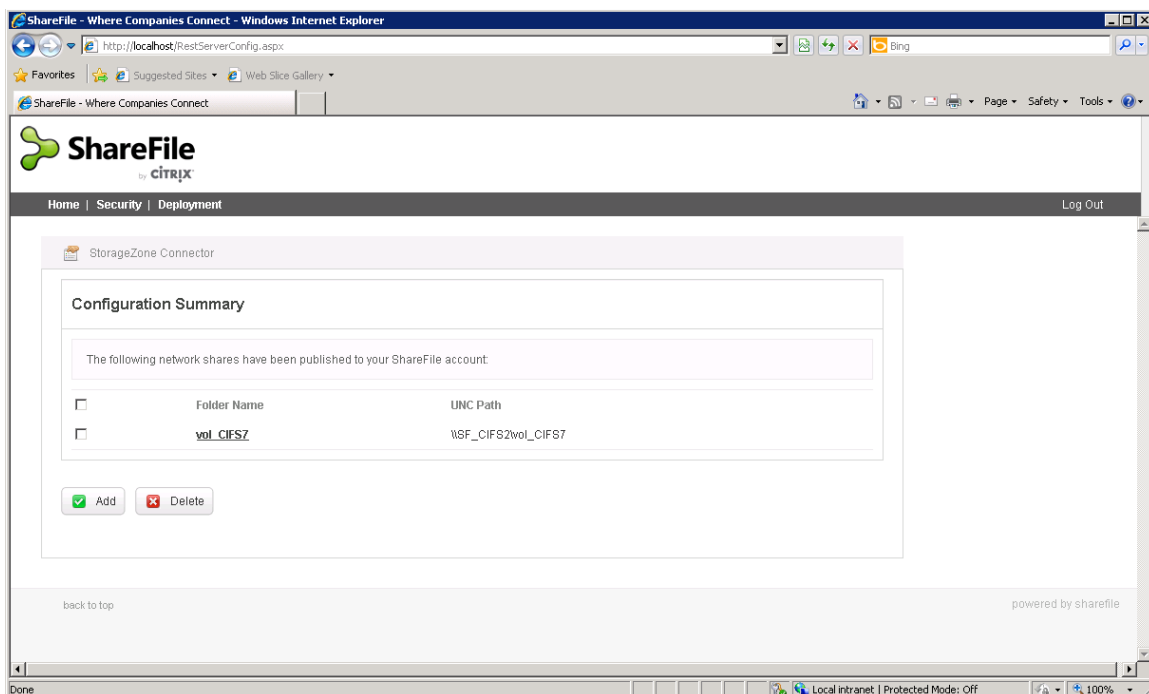
To add a new share to the CIFS connector, complete the following steps.

1. Launch the ShareFile configuration page and log in to the site.
2. Click Add, to add a new share to the CIFS connector library.
3. Enter a folder name and a UNC path and click Publish Share.

In this example, the folder name is `vol_CIFS7` and the UNC path is `\\SF_CIFS2\\vol_CIFS7`. The UNC folder was previously created on NetApp clustered Data ONTAP and populated with three files to demonstrate file access.



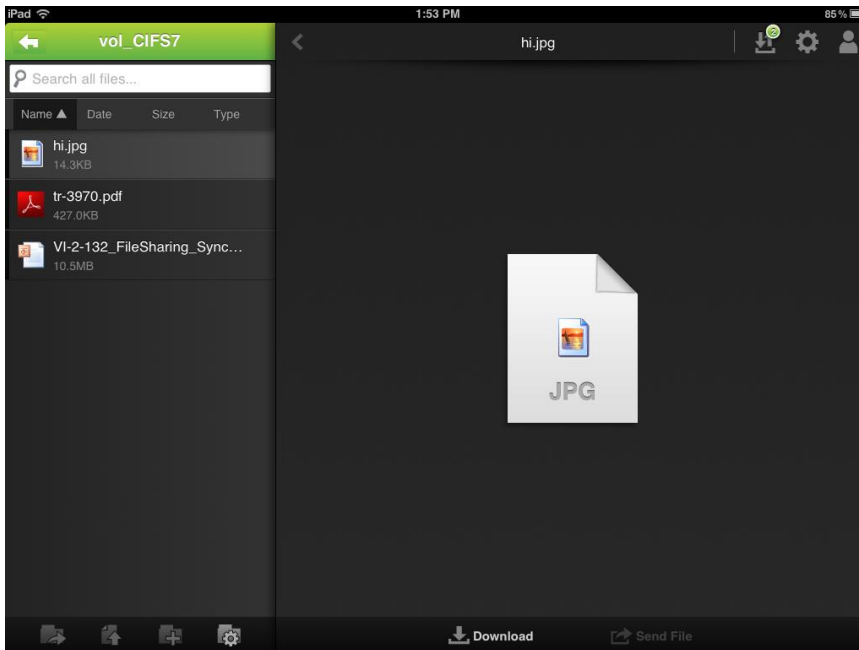
4. The newly created share is displayed on the configuration page. Additional folders can be created using the Add button. To remove a folder, select the checkbox corresponding to the folder name and click Delete.



Download Existing Files For Offline Access

1. Launch the ShareFile application from an iOS device and select the folder previously created. This example uses a folder named vol_CIFS7.

2. Users will be prompted to enter their Windows credentials to securely access this folder. Only those users who have NTFS permissions on the folder will be granted access.
3. Verify that the files placed in the existing NetApp CIFS share are displayed. Click Download to validate that the file is available offline from an iPad or iPhone.



3 Solution Validation

As part of the solution validation, the key capabilities listed in Table 3 were validated.

Table 3) Tests results.

Solution Test	Results
Storage efficiency	<ul style="list-style-type: none"> • Deduplication and compression. Plenty of savings are expected when a file is modified numerous times. Each time an existing file is modified, ShareFile generates a new object file. In our validation, approximately 38% savings were obtained by using deduplication and compression. Note that storage efficiency savings may be higher depending on how many times the files are saved, since object storage creates a new object for each modification of the file. • Thin provisioning and autogrow. These two features were tested for the ability to provide flexibility and storage space savings. <p>Note: Data-at-rest encryption must be disabled to obtain the benefits of deduplication and compression.</p>
File restore	<p>The CIFS share was configured with NetApp Snapshot. The read-only Snapshot copies were available to the administrator at the root of the volume hosting the CIFS share.</p> <p>The four-step process as described in section “File Restore from NetApp Snapshot Copies” was validated to recover missing files.</p>

Solution Test	Results
Nondisruptive operations	<p>This function allows maintenance on the system without disruption to the users. In production, this can provide administrators with the ability to transparently redistribute the workload. It is particularly important for upgrading a specific controller without any interruption.</p> <p>Several tests were performed using this function while users were transferring files. The volume hosting the user data was moved from node 1 to node 2 and it did not interrupt or slow down the users' activity.</p>
Accessing existing CIFS shares	<p>The CIFS connector allowed iOS users to access files hosted on NetApp storage. The existing CIFS shares were not modified.</p> <p>In addition to the ShareFile credentials, the users have to provide their Active Directory credentials to access their files.</p>

4 Summary

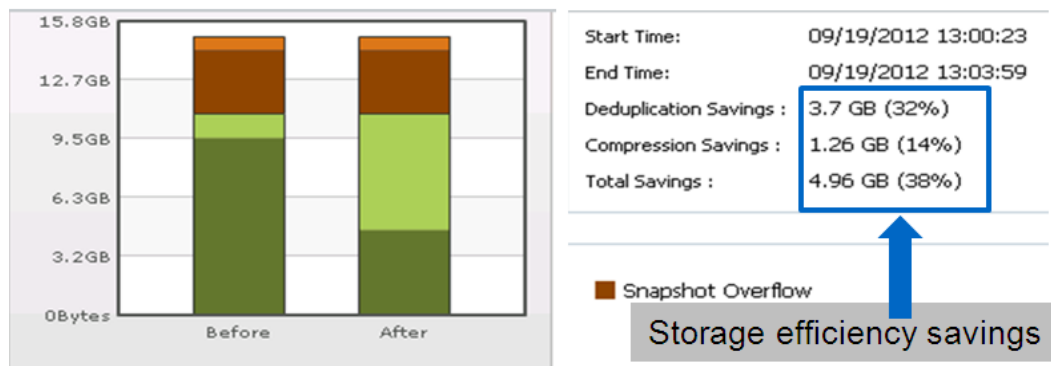
Citrix ShareFile StorageZones and NetApp offer a cost-effective and scalable file sharing solution with the features described in Table 4.

Table 4) Five key takeaways.

NetApp Features	Key Takeaways
Storage efficiency	Leverage storage efficiency features to consume less storage and accommodate more users.
Scalability	Scale up or out as needed with clustered Data ONTAP.
Nondisruptive operations	Take advantage of the NDO capabilities in NetApp to deliver an always-on platform.
Unified storage	Leverage the same storage infrastructure for all your Citrix needs such as server virtualization, application virtualization, desktop virtualization, and file sharing strategy.
Data protection	Keep your data on the premises for enhanced security. Protect your platform with NetApp Snapshot based backups.

The major benefit is the savings obtained by deduplication and compression. In this proof of concept executed in our solutions lab, an average saving of close to 40% was observed.

Figure 23) Storage efficiency savings.



Acknowledgements

The author thanks the following peers for their contribution to the design, creation, and validation of this guide.

Citrix: Adam Lotz, Juliano Maldaner, Joel Stocker, Astha Malik, and Chris Leithe

NetApp: Abhinav Joshi, Troy Mangum, Neil Glick, and Mark Woods

Feedback

If you have questions or comments about this solution guide, contact dl-citrix-core@netapp.com.

Resource Links

Citrix ShareFile

[Citrix StorageZones](#)

[On-Premises Solution](#)

[ShareFile on Citrix eDocs](#)

[Deploy Storage Center for a Proof-of-Concept Evaluation](#)

[Deploy Storage Center for High Availability](#)

[Deploy Storage Center in a DMZ](#)

[ShareFile APIs](#)

[Power Tools](#)

<https://netapp.sharefile.com>

[NetApp Storage Solution for Citrix ShareFile Enterprise Solution Brief](#)

[ShareFile StorageZones Video](#)

[ShareFile Launch Event with Citrix and NetApp](#)

NetApp Data ONTAP

[Clustered Data ONTAP](#)

[Data ONTAP 8 Operating System](#)

[Deduplication and Compression](#)

[Deduplication](#)

[WP-7022: The NetApp Storage Efficiency Guide](#)

[CIFS Share on Clustered Data ONTAP](#)

[Scale Up with Clustered Data ONTAP](#)

[NetApp Best Practices for CIFS Share on Clustered Data ONTAP](#)

[TR-3982: Data ONTAP 8.1 and 8.1.1 Operating in Cluster-Mode: An Introduction](#)

[TR-3967: Deployment and Best Practices Guide for Data ONTAP 8.1 Cluster-Mode Windows File Services](#)

[FAS2240](#)

[Vserver](#)

[Snapshot](#)

[SnapMirror](#)

[UNC Path](#)

[Flash Cache](#)

[OnCommand System Manager](#)

[Virtual Storage Console for XenServer \(VSC\)](#)

Version History

Version	Date	Document Version History
Version 1.0	February 2013	Initial release.

Refer to the [Interoperability Matrix Tool](#) (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

[Go further, faster®](#)



www.netapp.com

© 2013 NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, Data ONTAP, Flash Cache, FlexVol, OnCommand, SnapMirror, and Snapshot are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Cisco and Cisco Nexus are registered trademarks of Cisco Systems. Microsoft, Active Directory, Windows, and Windows Server are registered trademarks and PowerShell is a trademark of Microsoft Corporation. iPhone, iPad, and Mac are registered trademarks of Apple Inc. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. TR-4124-0213