



Technical Report

## Citrix ShareFile StorageZones on NetApp Solution Guide

Cedric Courteix, Ramesh Kamath, Rachel Zhu, NetApp  
November 2013 | TR-4124

Ver. 2.1

### **“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 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. It also highlights NetApp's integration with file recovery on Citrix ShareFile, that is, the NetApp Recovery Manager for Citrix ShareFile.

## TABLE OF CONTENTS

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Scope	4
1.2	Key Terminology	4
1.3	Citrix ShareFile and NetApp Solution Highlights	5
<b>2</b>	<b>Solution Design</b>	<b>9</b>
2.1	High-Level Architecture	9
2.2	Detailed Solution Architecture	10
2.3	Solution Technology Components	13
2.4	ShareFile Encryption	13
2.5	ShareFile File Versioning	14
2.6	Clustered Data ONTAP Storage Architecture	15
2.7	Storage Efficiency	17
2.8	Network Access	18
2.9	NetApp Recovery Manager for Citrix ShareFile	19
2.10	Check That Data Remains on Premises	35
2.11	StorageZones Connectors	37
<b>3</b>	<b>Solution Validation</b>	<b>41</b>
<b>4</b>	<b>Summary</b>	<b>41</b>
	<b>Appendix</b>	<b>43</b>
	<b>Acknowledgements</b>	<b>46</b>
	<b>Feedback</b>	<b>46</b>
	<b>Resource Links</b>	<b>46</b>
	Citrix ShareFile	46
	NetApp Data ONTAP	46
	<b>Version History</b>	<b>47</b>

## LIST OF TABLES

Table 1)	Solution components	13
Table 2)	Hardware components	13
Table 3)	Test results	41
Table 4)	Key takeaways	41

## LIST OF FIGURES

Figure 1) ShareFile storage efficiency with NetApp.....	6
Figure 2) Consolidate with secure multi-tenancy.....	8
Figure 3) Citrix-managed versus customer-managed StorageZones.....	9
Figure 4) Overall architecture.....	10
Figure 5) Supported mobile and desktop applications (graphic provided by Citrix).....	11
Figure 6) Control plane architecture.....	11
Figure 7) Customer-managed StorageZones architecture.....	12
Figure 8) ShareFile encryption architecture.....	14
Figure 9) ShareFile file versioning.....	15
Figure 10) CIFS share repository.....	15
Figure 11) Enabling deduplication and compression on CIFS share.....	17
Figure 12) Storage efficiency savings.....	17
Figure 13) High-availability StorageZones.....	18
Figure 14) POC network access.....	18
Figure 15) Secure DMZ network access.....	19
Figure 16) ShareFile recovery queue flowchart.....	20
Figure 17) NRM-CS service flowchart.....	21
Figure 18) NetApp data protection options for ShareFile data.....	22
Figure 19) Typical NRM-CS deployment on Citrix ShareFile environment.....	22
Figure 20) ShareFile/NRM-CS restore process.....	34
Figure 21) Select account in employee directory.....	36
Figure 22) Verify default StorageZones name.....	36
Figure 23) Check folder options.....	37
Figure 24) ShareFile private cloud with CIFS connector.....	38
Figure 25) Network file access with ShareFile app on Android.....	40
Figure 26) Storage efficiency savings.....	42

# 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 might 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 it wants. With the ShareFile StorageZones feature, organizations have the flexibility to manage their data on the premises in customer-managed StorageZones, 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 its 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 its 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<sup>®</sup> 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.

- **Storage Virtual Machine, formerly called [Vserver \(virtual server\)](#).** Clustered Data ONTAP includes a logical entity named Storage Virtual Machine. Each Storage Virtual Machine is viewed as an individual storage subsystem inside the cluster.
- **NetApp Recovery Manager for Citrix ShareFile (NRM-CS).** NetApp Recovery Manager for Citrix ShareFile (NRM-CS) provides a file-recovery solution for Citrix ShareFile StorageZones, which uses NetApp FAS controllers as its back-end storage.
- **[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.** Rely 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.
- **[StorageZones Controller](#).** 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.** Work in conjunction with StorageZones. These connectors enable 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

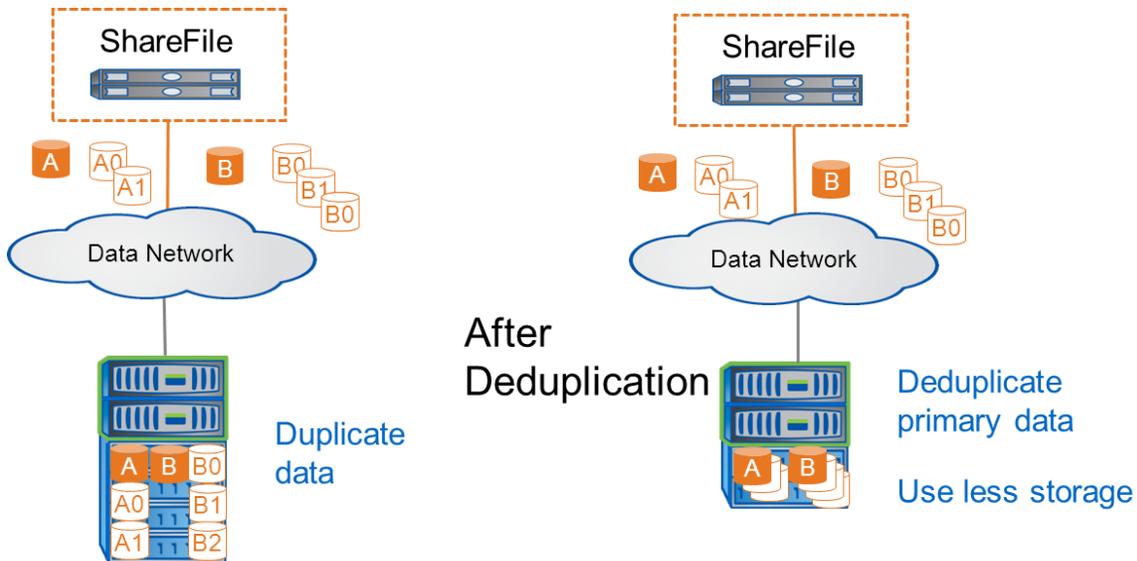
#### Storage Efficiency

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<sup>®</sup> 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. Because 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) might 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 StorageZones Controller (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 important, 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](#)<sup>™</sup> acceleration card or redistributing data across controllers can be done nondisruptively.

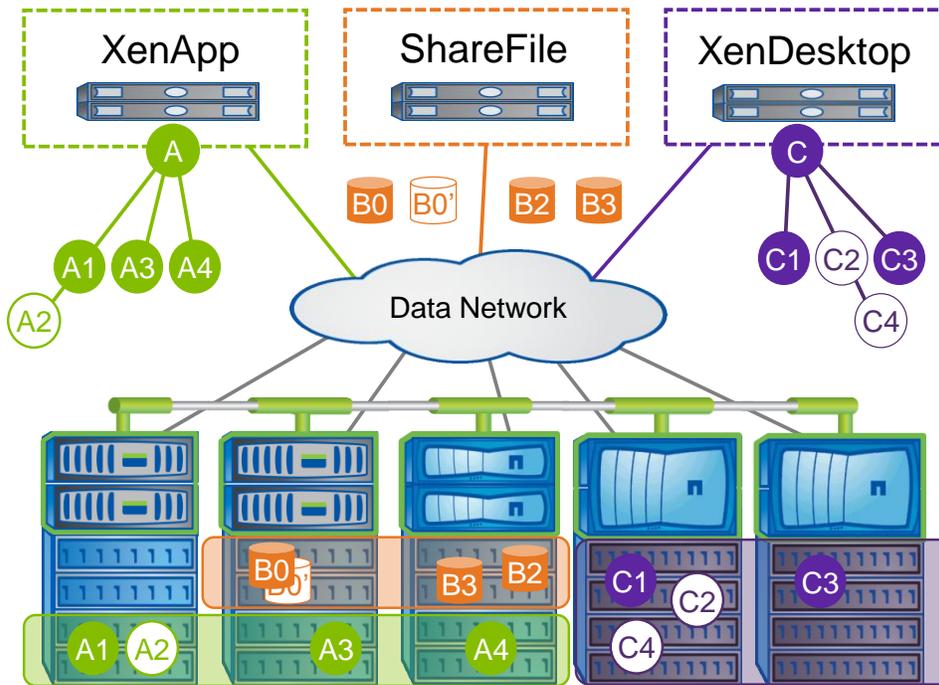
## Unified Storage Architecture

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

### Backups Based on NetApp Snapshot

NetApp [Snapshot](#)™ technology provides great value when backing up the CIFS share object repository for ShareFile StorageZones because 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. Secondary backups can be achieved using NetApp SnapVault® technology.

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

### 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, the NetApp Recovery Manager for Citrix ShareFile can be leveraged.

For details, see section “NetApp Recovery Manager for Citrix ShareFile.”

## 2 Solution Design

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

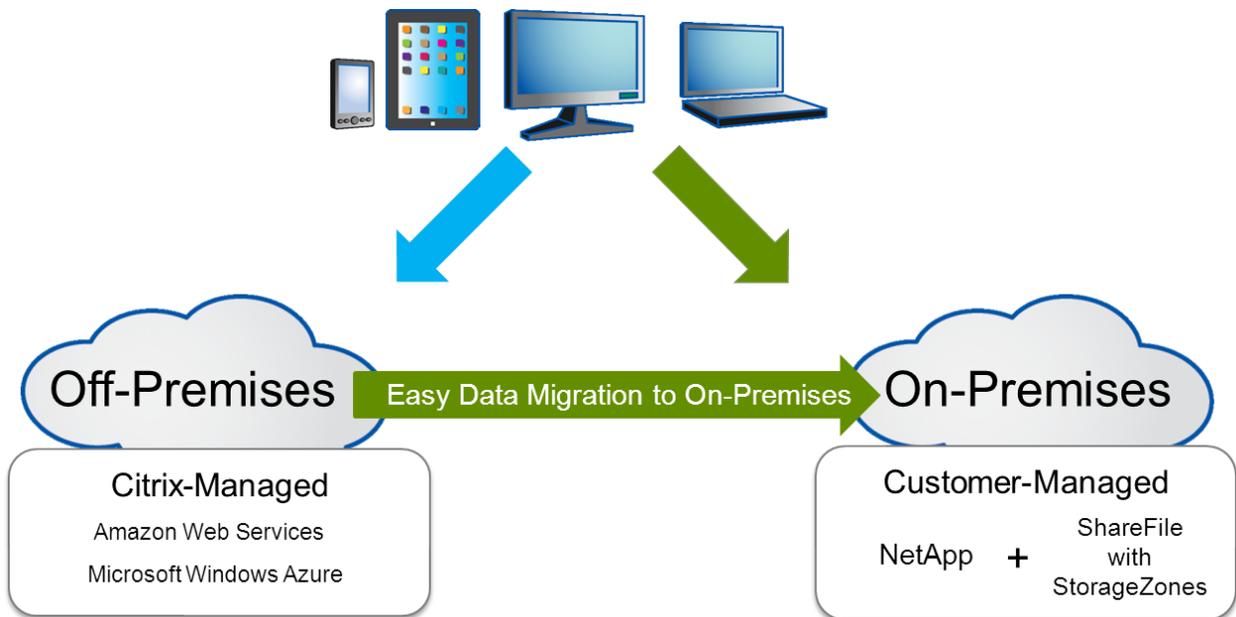
### 2.1 High-Level Architecture

Citrix ShareFile StorageZones allow 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 or Microsoft® Windows Azure. These cloud offerings can also 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.

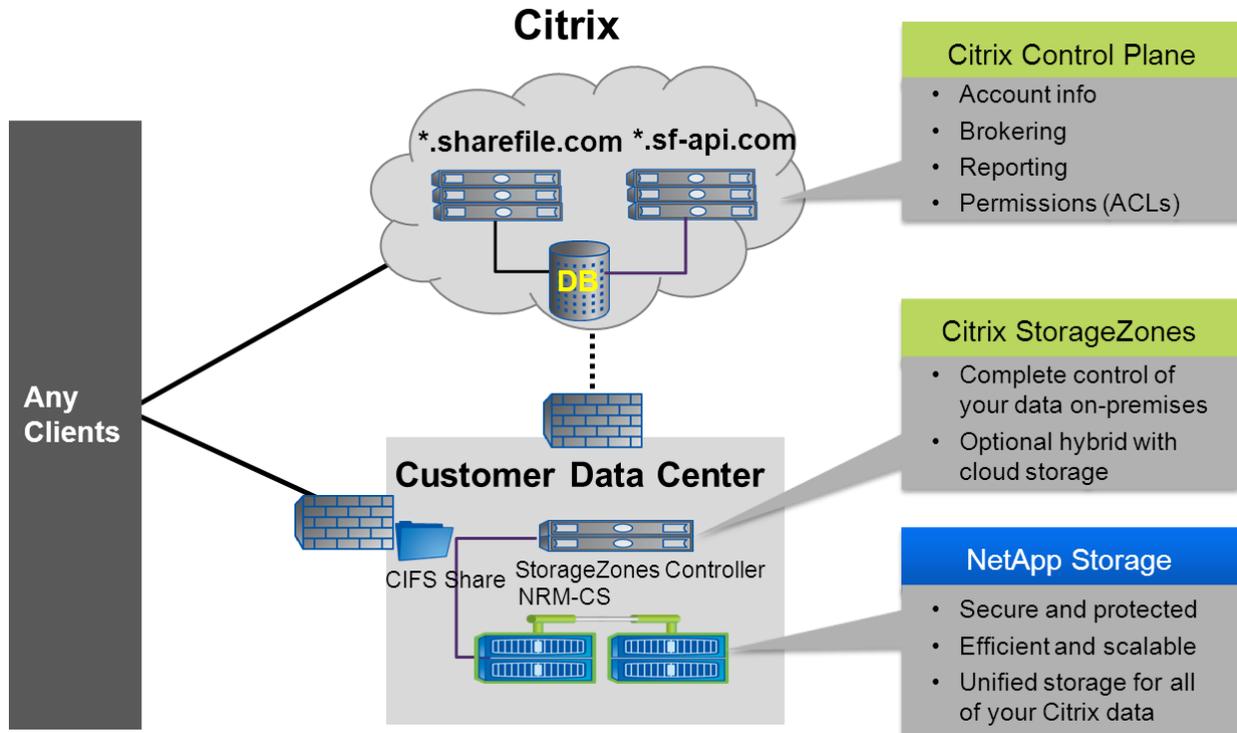


Figure 4 presents the following entities:

- **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 StorageZones. 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).

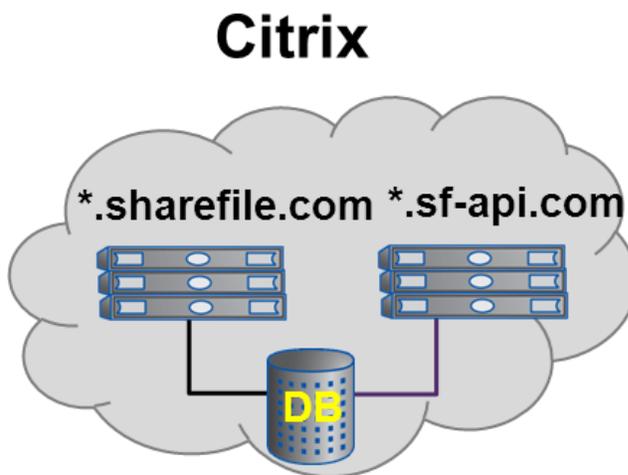


## Control Plane

When a user establishes a session from any client device, that user 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 websites as well as the ShareFile business logic.

Figure 6) Control plane architecture.



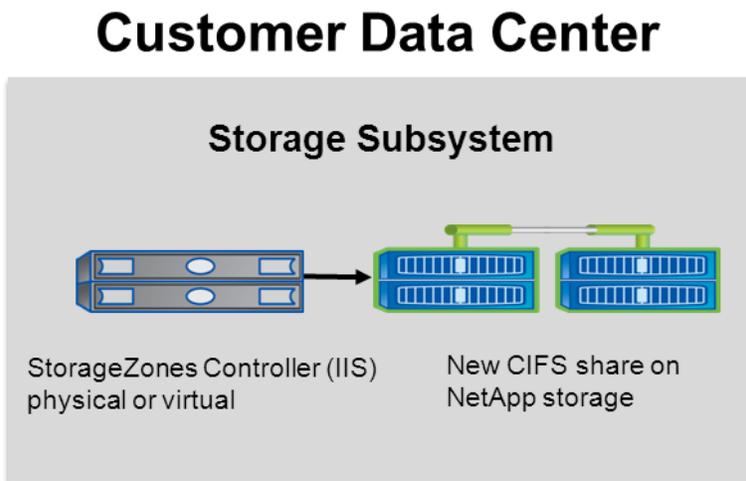
## Storage Subsystem

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

The storage subsystem component is described in Figure 7 and includes two elements:

- **ShareFile StorageZones Controller.** One or several websites that reside on Microsoft IIS are configured with ShareFile StorageZones Controller software, which is a lightweight web service that communicates with ShareFile clients and the on-premises storage.
- **NetApp storage.** When installing StorageZones Controller, the administrator creates a StorageZone. A single CIFS share hosted on NetApp is required for each zone. After the first StorageZones Controller is added to a zone, NetApp recommends adding another StorageZones 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.



To configure ShareFile for on-premises shared storage, follow the procedure listed in the ShareFile StorageZones Controller documentation, available at <http://support.citrix.com/proddocs/topic/sharefile/sf-enterprise-landing-page.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
<p><b>Hypervisor</b></p> <p>Foundation of the underlying resources. This includes the following:</p> <ul style="list-style-type: none"> <li>The servers running ShareFile can either be physical or virtual machines. The virtual machines can reside on any hypervisor. However, Citrix XenServer 6.1 hosts were used in this solution to run the following virtual machines (VMs): <ul style="list-style-type: none"> <li>Two VMs: Windows Server® 2008 R2 with IIS and Citrix StorageZones Controller 2.1 software.</li> <li>Two VMs: Windows Server 2008 R2 with Active Directory® and Domain Name Service (DNS) functions. NetApp recommends using the existing AD and DNS infrastructure.</li> </ul> </li> </ul> <p>Note that physical servers can also be used to run these server roles.</p>
<p><b>NetApp</b></p> <ul style="list-style-type: none"> <li>Version: clustered Data ONTAP 8.1. Also supports Data ONTAP 8.1.2 and 8.2.</li> </ul> <p><b>Note:</b> Data ONTAP systems running 7-Mode are also supported for the ShareFile solution.</p> <ul style="list-style-type: none"> <li>Licenses: CIFS protocol and deduplication</li> <li>Additional Licenses: SnapRestore®, SnapMirror, and SnapVault (based on NRM-CS configuration)</li> <li>Management software: <a href="#">OnCommand System Manager</a> 2.0 and <a href="#">Virtual Storage Console</a> (VSC) 2.0 for Citrix XenServer</li> </ul>

Table 2 lists the hardware components used in this solution.

Table 2) Hardware components.

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

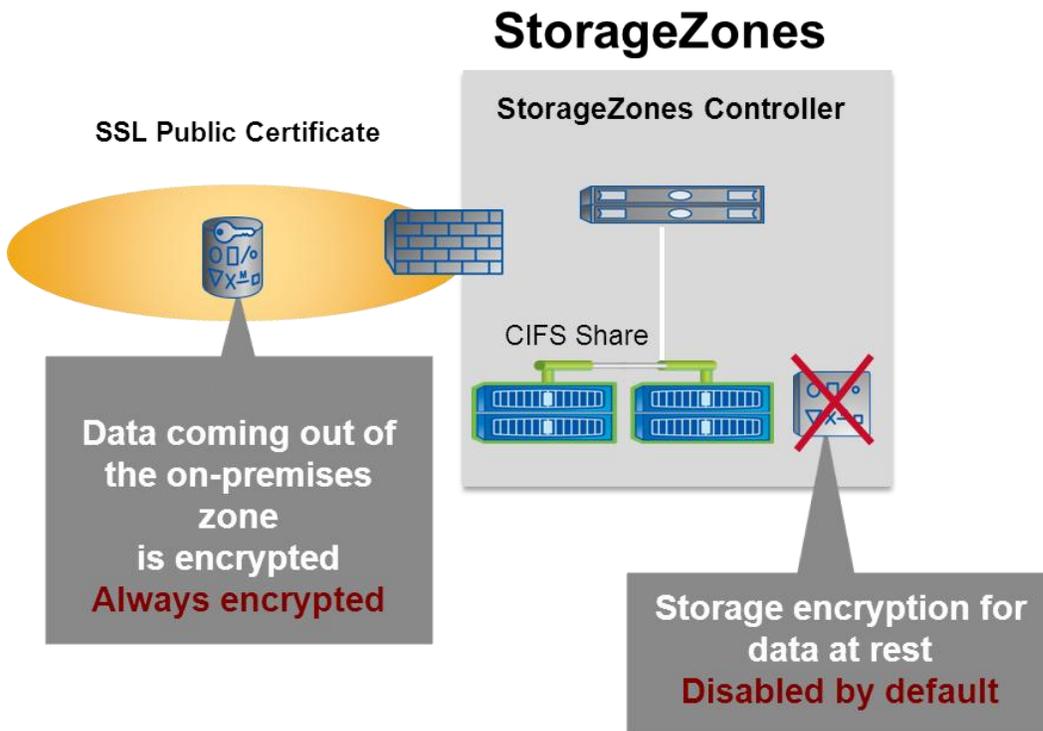
## 2.4 ShareFile Encryption

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

For on-premises deployment, data encryption is not required because 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 ShareFile File Versioning

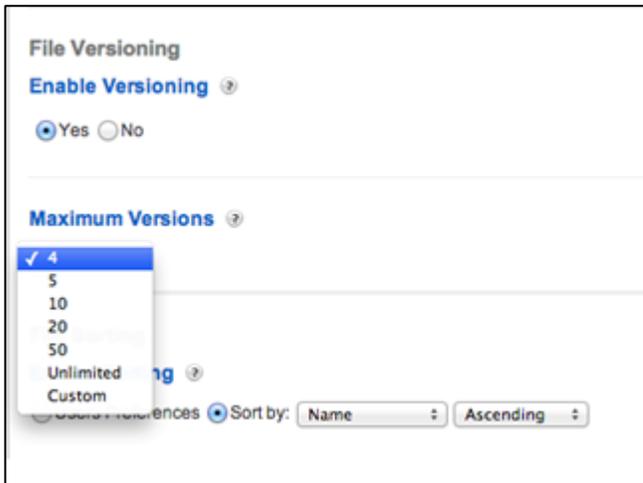
ShareFile's file versioning feature allows you to view different versions of a file uploaded with the same name. Files with the same name will automatically be saved as the latest version, and you can also view the earlier versions. By default, if this feature is enabled, file versioning will save unlimited versions of a given file to allow you to view the entire history of any files on your account. ShareFile Sync for devices will only run if [File Versioning](#) is enabled. This requirement is in place to prevent any loss of data by accidental overwrites.

Because ShareFile writes to one directory and a limited number of files can be stored in one directory, the best practice is **not** to use unlimited file versions to control the total number of files in the ShareFile directory. To enable greater scale, ShareFile expects to modify this architecture in a future release.

### Best Practice

NetApp recommends using four or five as maximum versions to control the number of objectives in the ShareFile CIFS directory.

Figure 9) ShareFile file versioning.



## 2.6 Clustered Data ONTAP Storage Architecture

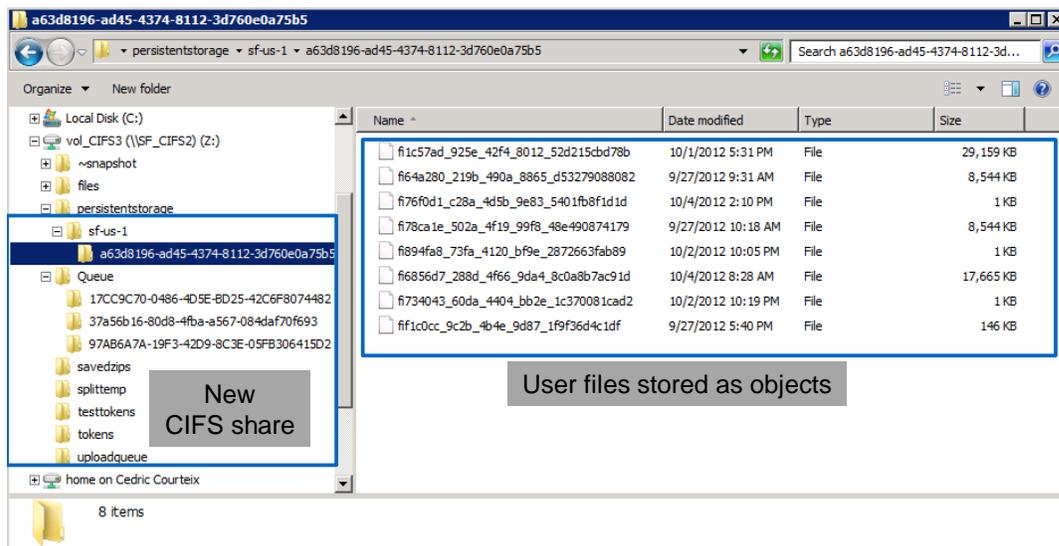
To benefit from the key NetApp capabilities highlighted in [section 1.3](#), the following technology components need to be implemented:

- **A new CIFS share.** Citrix ShareFile requires a CIFS share with no data in it because the system will create its own folder structure. The object files created by users are stored in a folder called `persistentstorage` (see Figure 10). Follow the [NetApp best practices](#) to set up a virtual storage server with a dedicated CIFS share using SMB 2.0.
- **CIFS share permissions.** After 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 StorageZones Controller 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 10 illustrates the file structure that Citrix ShareFile leverages for on-premises release.

Figure 10) 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.

Citrix ShareFile is an object-oriented architecture, and users' files are stored as objects. Each time a user updates a file, the updated file is stored as a new object. This design creates many objects under a single directory called "persistentstorage" in the CIFS share. The number of files in this single directory grows very quickly, and it creates a scalability issue. Citrix is aware of limitations around number of files per folder and is working to address this in its future release.

Meanwhile, NetApp recommends that you:

- Monitor the file count in the "persistentstorage" directory
- Tune `maxdirsize` up to 3% of system memory
- Select systems with a maximum amount of system memory based on the workload being sized
- Create additional StorageZones to spread files into multiple CIFS shares
- Tune Citrix ShareFile version control detail; see section 2.5, "ShareFile File Versioning"

When the max directory size is achieved, you will see the following error message:

```
<date> <storage name> WARNING          wafl.dir.size.max: Directory /vol/<vol name>/<directory name>
reached the maxdirsize limit. Reduce the number of files or use the vol options command to
increase this limit
```

In Data ONTAP 8.1 and higher, there is no explicit limit on the number of subdirectories that a WAFL<sup>®</sup> directory can contain. Users can continue to create files as long as the `maxdirsize` values are not exceeded. Data ONTAP provides a number of adjustable limits that are set to provide a great out-of-the-box experience for most NetApp customers. Certain applications and environments benefit from adjusting these defaults.

The `maxdirsize` parameter represents the largest possible directory (metadata and indirect blocks) in kilobytes. This parameter defaults to 1% of system memory and for newer systems rarely needs to be adjusted. For example, a FAS2240 with 6GB of addressable system memory will support directories that hold over 400,000 CIFS files without changing the default `maxdirsize`. The setting is a per FlexVol volume setting (the global option has been deprecated) and applies to every individual directory in the FlexVol volume. All the file and subdirectory entries in a given directory are accounted for in `maxdirsize`. Files contained within subdirectories do not count against the `maxdirsize` of the directory.

If the parameter needs to be increased, NetApp strongly recommends limiting the size to at most three times the default (3% of system memory). Don't go beyond this number unless you are sure that only a few directories will be that large over the life of the application. For example, in a FAS2240 system with 6GB memory, 458,864 files can be created in one directory as default. After changing `maxdirsize` to 3% memory, which is 184.32MB, 18,887,360 files now can be stored in one directory.

Also, make sure that all related volumes in the ecosystem (for example, the SnapMirror destination) have had the same tuned parameters and that the 3x guideline hasn't been exceeded for the second platform.

Remember that once a directory grows larger, it can never shrink. If you are tuning `maxdirsize` to allow very large directories, be vigilant to recover space from directories that have grown and then shrunk significantly.

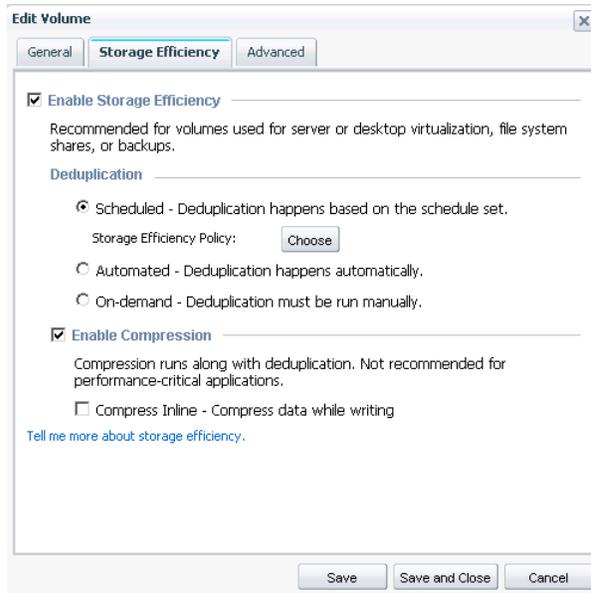
In Data ONTAP 7-Mode, the `maxdirsize` value can be tuned by using `vol options maxdirsize`. In clustered Data ONTAP, you can set the maximum directory size in advanced mode `vol modify vservers <servername> -volume <volname> -maxdir-size <size>`.

## 2.7 Storage Efficiency

ShareFile stores files as objects. For each modification made on a file, a separate object is created on the storage. Thereby, NetApp storage efficiency technologies such as deduplication and compression provide significant storage savings.

To enable deduplication and compression from the OnCommand System Manager, access the Storage Efficiency tab on the Volume properties.

Figure 11) Enabling deduplication and compression on CIFS share.



On an average, with Citrix ShareFile deployments you can obtain approximately 40% storage savings with NetApp deduplication and compression<sup>1</sup>.

**Note:** Storage efficiency savings might be higher depending on how many times the files are saved, because object storage creates a new object for each modification of the file.

Figure 12) Storage efficiency savings.



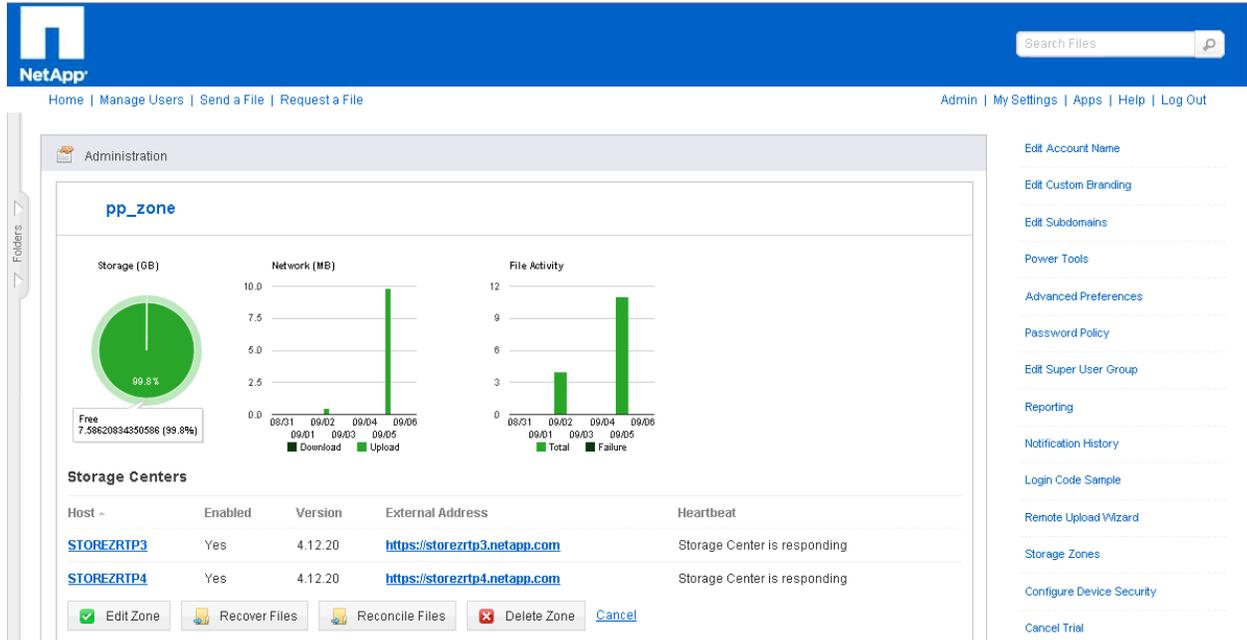
<sup>1</sup> Actual customer results might vary.

## 2.8 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 13 represents a zone configured with two StorageZones Controller servers in load-balancing mode.

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

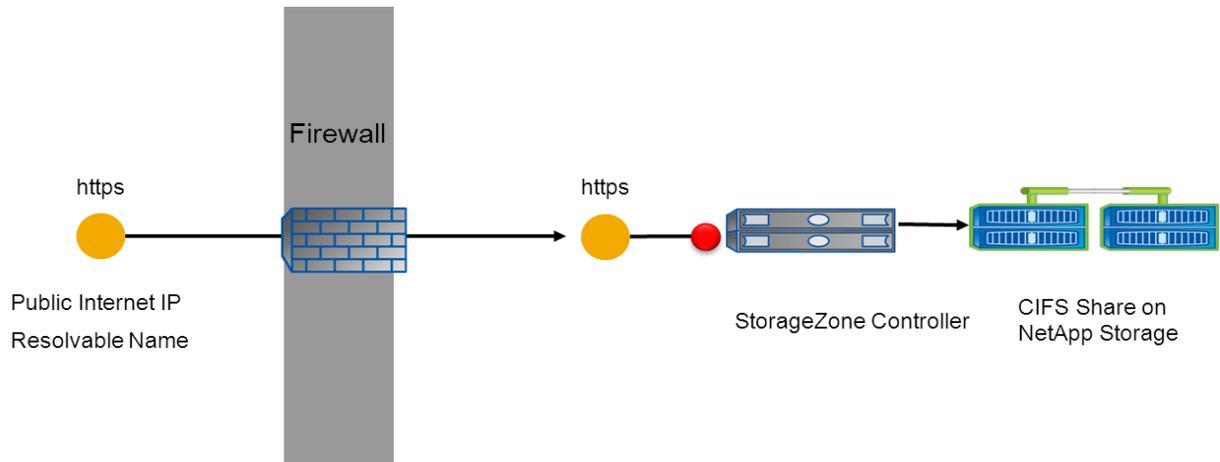
Figure 13) High-availability StorageZones.



## StorageZones Proof of Concept

Figure 14 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 StorageZones Controller server. For details on the required components, refer to <http://support.citrix.com/proddocs/topic/sharefile-storagezones-21/sf-deploy-for-evaluation.html>.

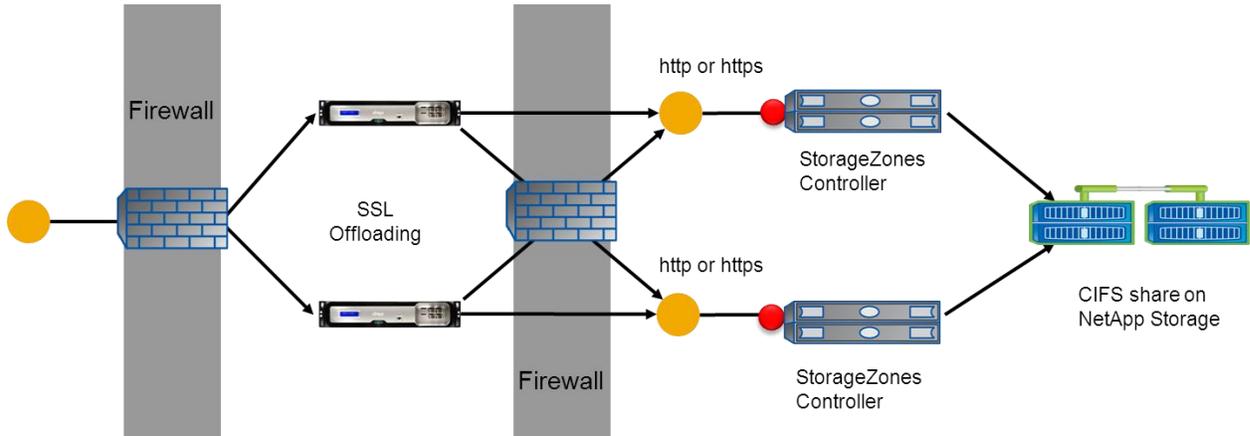
Figure 14) POC network access.



## 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 StorageZones Controller on the internal network. For details on the required components, refer to [Citrix ShareFile DMZ Deployment Guide](#).

Figure 15) Secure DMZ network access.



## 2.9 NetApp Recovery Manager for Citrix ShareFile

NetApp Recovery Manager for Citrix ShareFile (NRM-CS) is a Citrix Ready certified product that provides an administrator-driven user file-recovery solution for Citrix ShareFile StorageZones deployments using on-premises NetApp storage.

Citrix ShareFile by default preserves the user files deleted from the ShareFile Recycle Bin for a period of seven days, after which the files are unavailable for restore from within native ShareFile. In such cases, NRM-CS empowers administrators to restore user files/folders by using either NetApp Snapshot copies on primary storage, NetApp SnapMirror, or NetApp SnapVault, as applicable.

NRM-CS runs as a Windows service that keeps polling the ShareFile recovery queue for restore requests. It then accomplishes the restore by orchestrating the recovery process of finding the requisite user files, recovering the files from the NetApp storage, and placing them in the user's ShareFile StorageZones. Figure 16 and Figure 17 provide the flowchart schematic for the ShareFile recovery queue and the NRM-CS service, respectively.

Figure 16) ShareFile recovery queue flowchart.

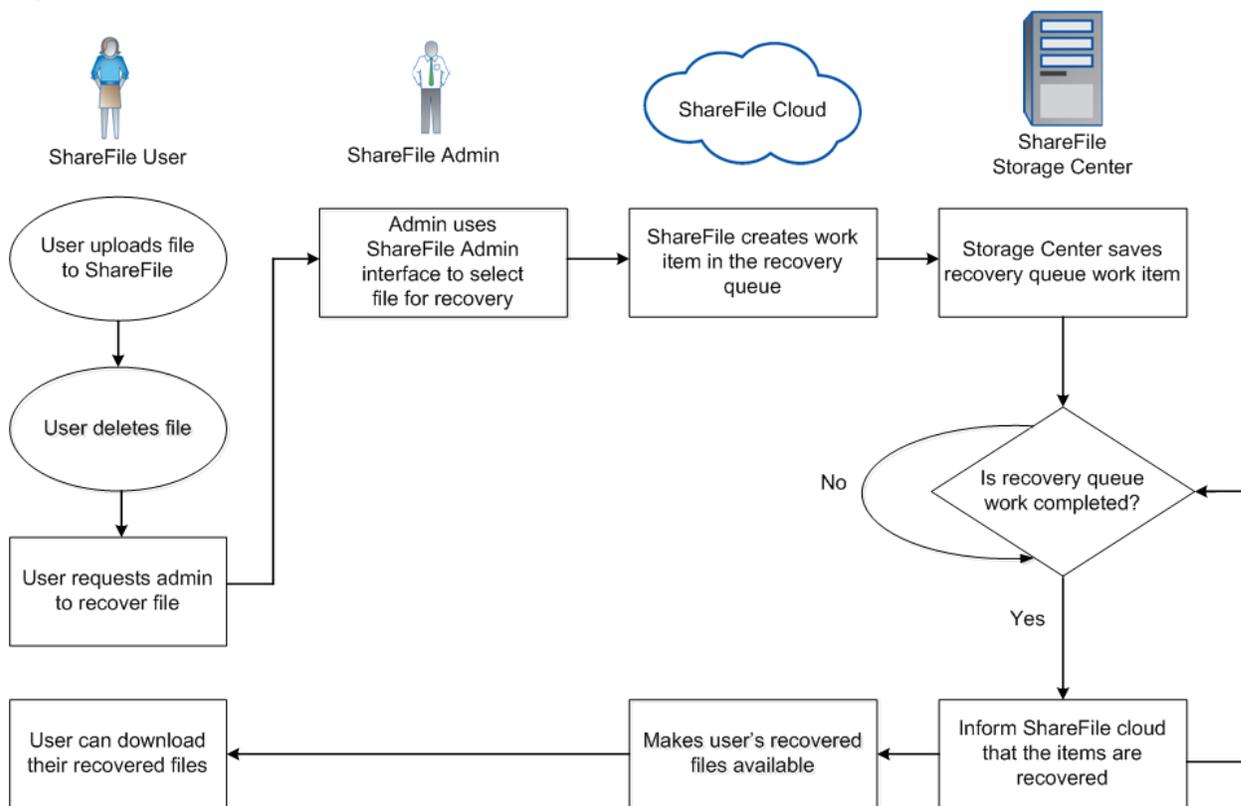


Figure 17) NRM-CS service flowchart.

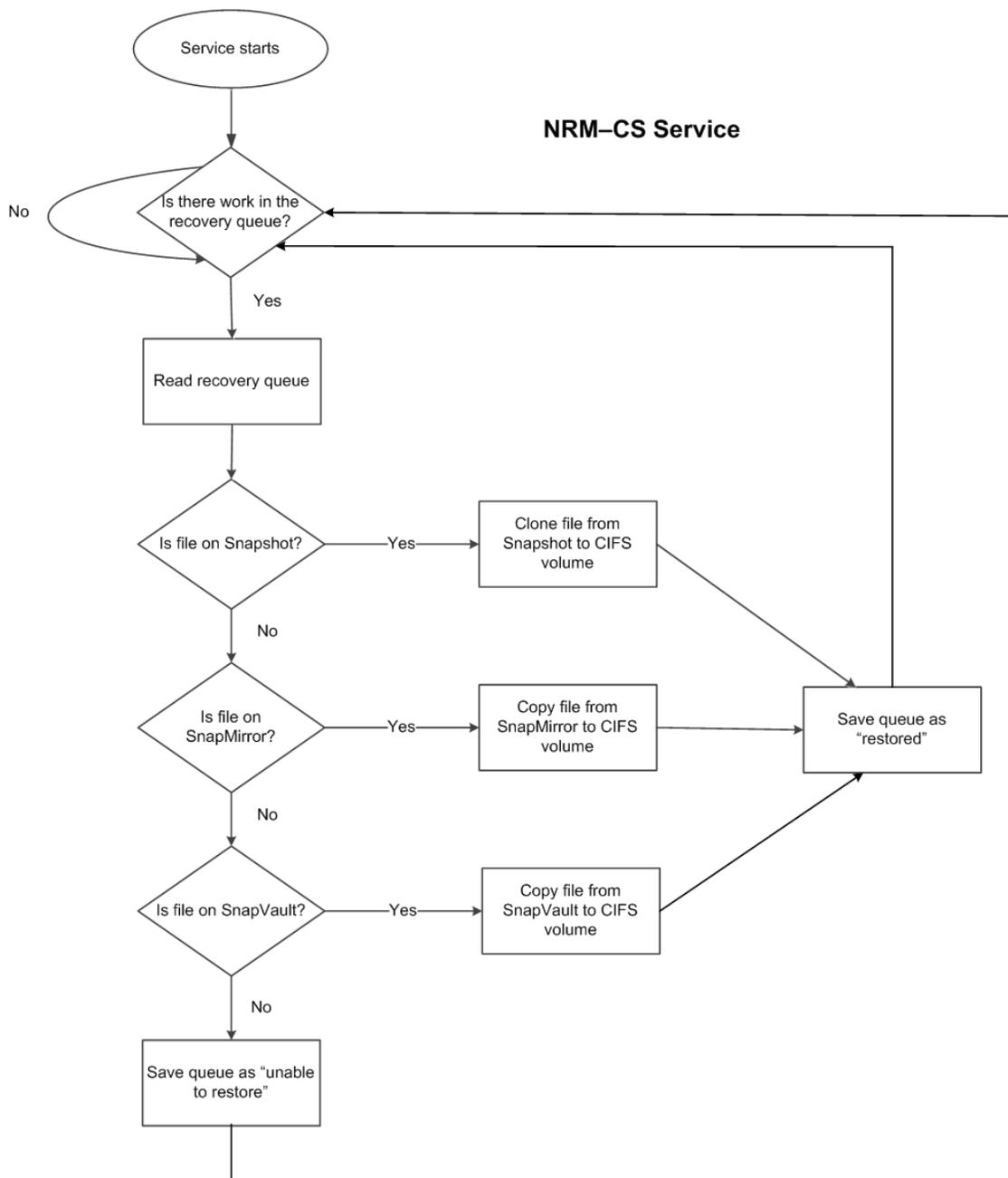


Figure 18 shows the data protection software available for ShareFile data on NetApp.

Figure 18) NetApp data protection options for ShareFile data.

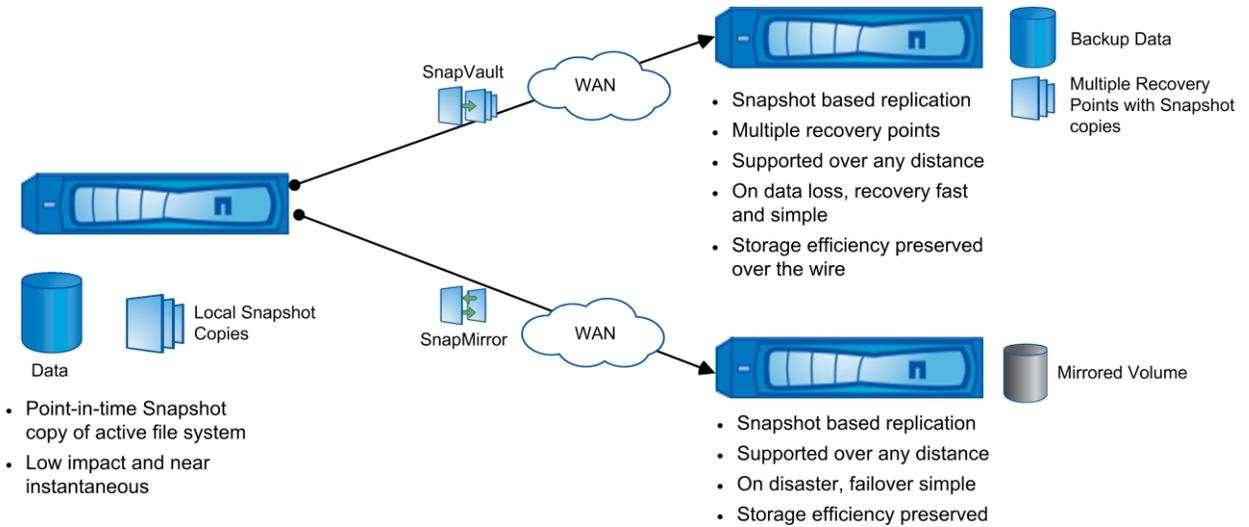
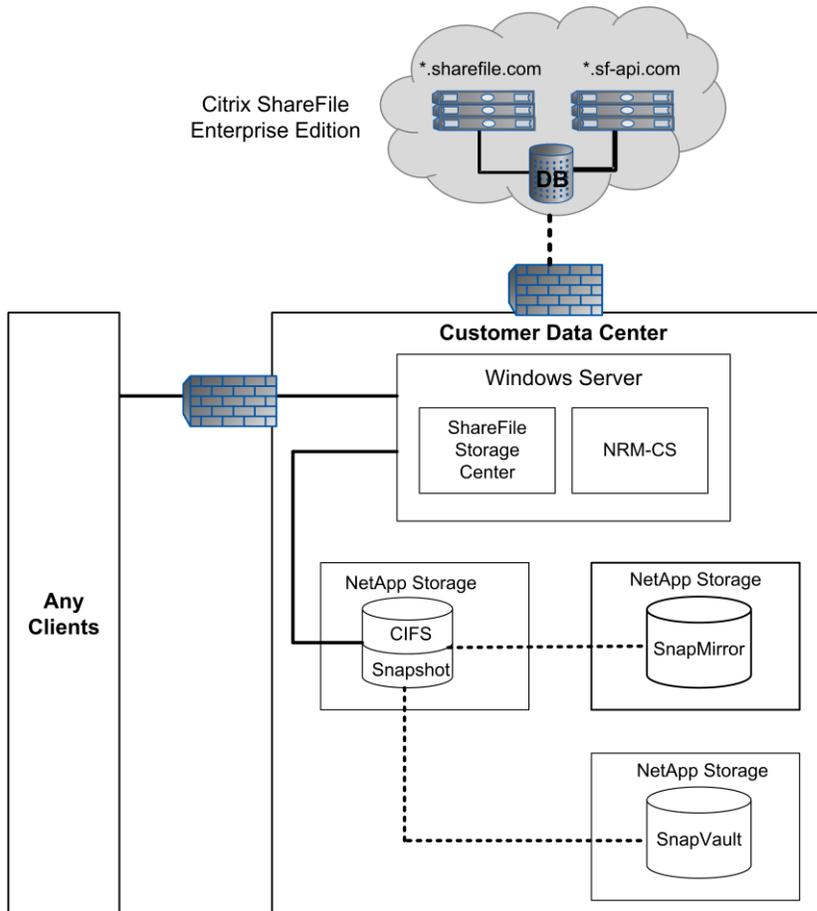


Figure 19) Typical NRM-CS deployment on Citrix ShareFile environment.



## Installing NRM-CS

NRM-CS is available for download from the [NetApp Support site](#). Data ONTAP support compatibility can be determined by using the [NetApp Interoperability Matrix Tool \(IMT\)](#). NRM-CS can be installed on Windows 2008 R2 (or later).

The NRM-CS installer also supports an upgrade from the NRM 1.0 to the NRM 1.1 version. In case of an upgrade, the configuration utility of NRM-CS has to be rerun to add the NDMP credentials and to verify the configuration.

**Note:** NetApp recommends installing NRM-CS on the same server machine as the ShareFile StorageZones Controller for simplicity.

However, NRM-CS can also be installed on a separate standalone Windows Server instance. In such a deployment scenario, the following change must be made on the StorageZones Controller machine prior to NRM-CS installation. This parameter controls the queue API's access to nonlocal URLs.

Edit the config file for the StorageZones Controller at `C:\inetpub\wwwroot\Citrix\StorageZonesController\AppSettingsRelease.config` and change the value of the "QueueSDKRestricted" key from 1 to 0.

```
<add key="NSValidateRequests" value="1"/>
<add key="QueueSDKRestricted" value="0"/>
<add key="AdminPagesRestricted" value="1"/>
```

The software prerequisites for NRM-CS installation are:

- Microsoft .NET Framework v4 Full: <http://www.microsoft.com/en-us/download/details.aspx?id=17851>
- Windows PowerShell® 3 (part of the Windows Management Framework 3.0) <http://www.microsoft.com/en-us/download/details.aspx?id=34595>

For installation steps, refer to the [NetApp Recovery Manager 1.1 for Citrix ShareFile Installation and Administration Guide](#).

**Note:** NRM-CS does not support recovery from qtrees mounted as CIFS share or qtree SnapMirror destinations.

## License Requirements

The following licenses are required for NRM-CS, depending on the environment:

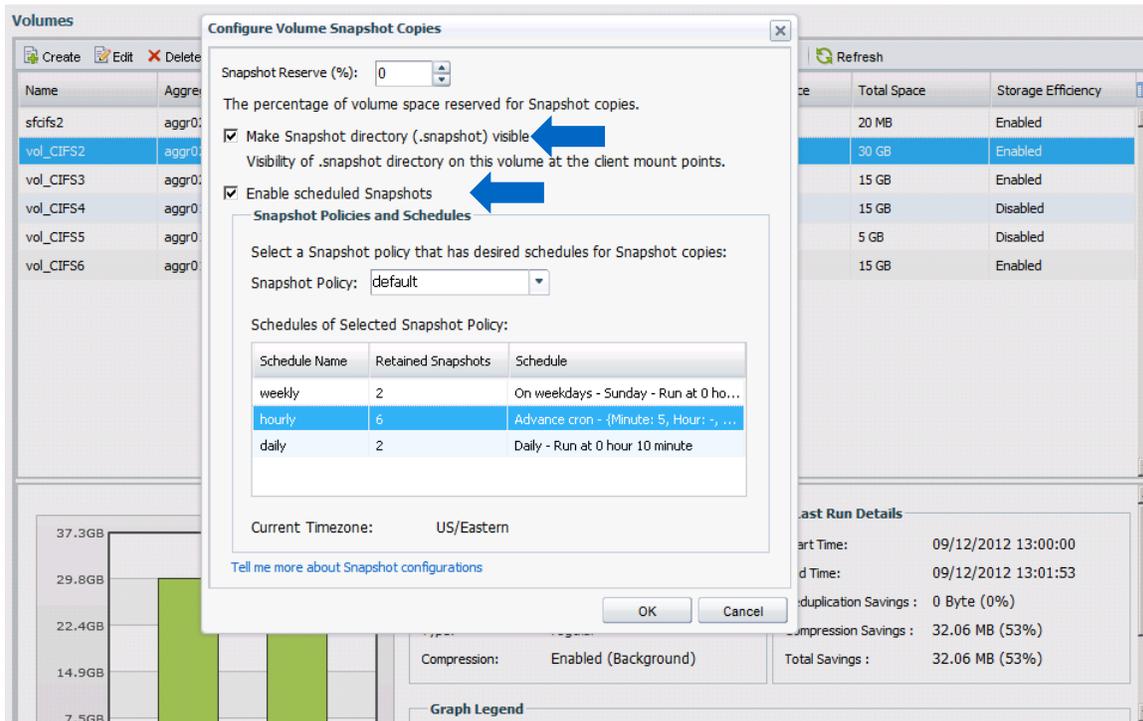
- Data ONTAP 7-Mode system:
  - cifs
  - snaprestore
  - snapmirror
  - sv\_ontap\_sec
- Clustered Data ONTAP system:
  - cifs
  - snaprestore
  - snapmirror
  - snapvault

## Enabling Backups Based on NetApp Snapshot

This section describes how to set up storage-efficient backups based on NetApp Snapshot.

To enable Snapshot backups, perform the following steps.

1. Leverage NetApp OnCommand 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.

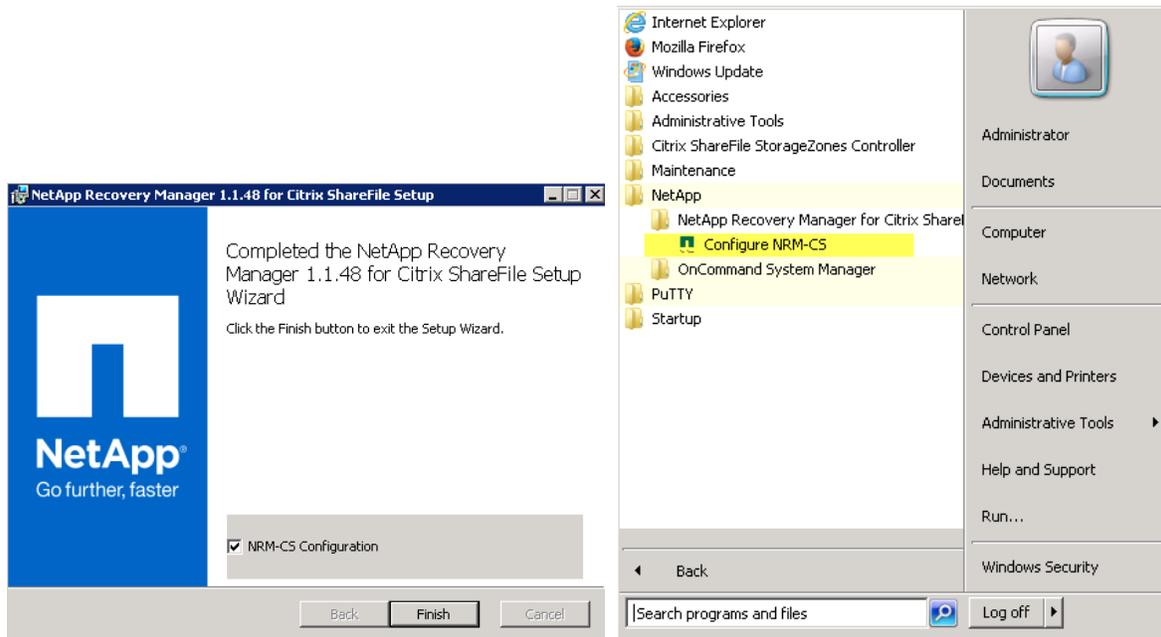


2. Make sure that the NetApp Snapshot directory is visible to the administrators at the root of the CIFS share by selecting the Make Snapshot directory (.snapshot) visible checkbox in the Configure Volume Snapshot Copies page.

## Configuring NRM-CS

NRM-CS supports StorageZones controllers created on both Data ONTAP 7-Mode and clustered Data ONTAP CIFS shares.

The NRM-CS configuration utility can be launched either during the installation or from the Windows Programs menu after installation.



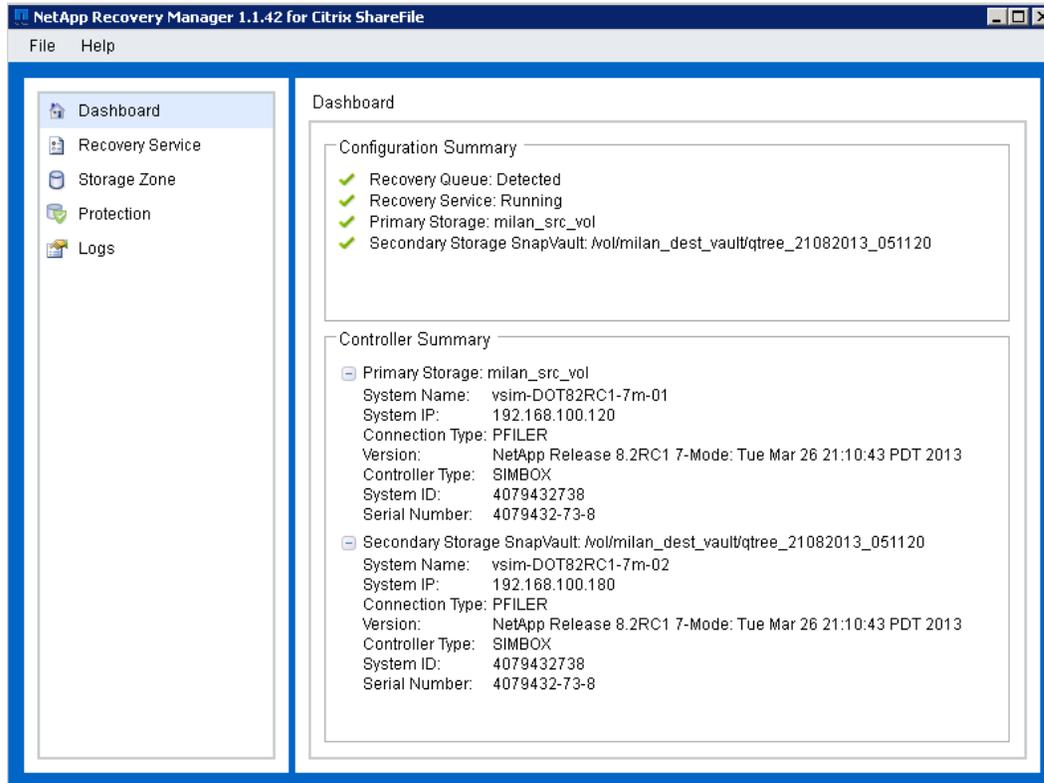
**Note:** NetApp recommends creating the SnapMirror and/or the SnapVault relationships for the CIFS share prior to configuring NRM-CS. For details on configuring SnapMirror and SnapVault, refer to the appendix of this document.

On the NRM-CS configuration screen, the following tabs are available for configuration:

- **Dashboard.** A single-pane view of the NRM-CS configuration details.
- **Recovery Service.** Configuration window to set up the NRM-CS Recovery Service parameters and ShareFile recovery queue.
- **StorageZones.** StorageZones CIFS share configuration.
- **Protection.** Specify available SnapMirror and SnapVault configurations.
- **Logs.** NRM-CS log file entries.

## Dashboard

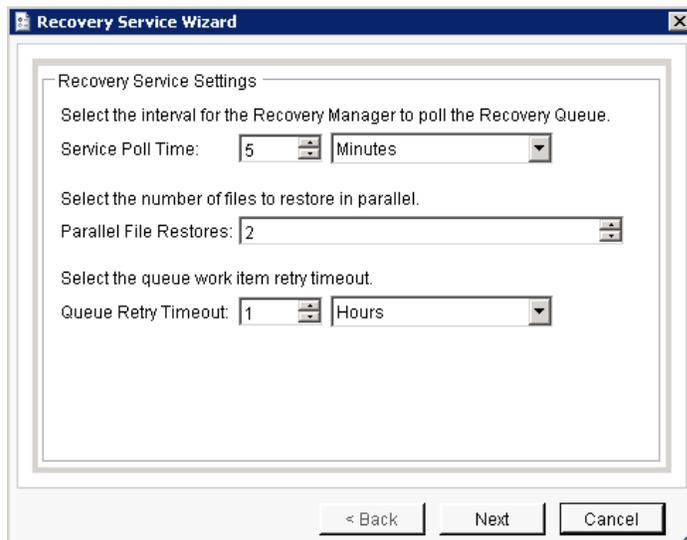
Dashboard provides a single-pane view of the NRM-CS configuration, including NetApp storage controller and ShareFile StorageZones summary.



## Recovery Service

The Recovery Service tab allows the user to configure the NRM-CS recovery service parameters such as poll time, parallel restores, ShareFile StorageZones Controller, and the creation of recovery queue on ShareFile.

1. In the Recovery Service tab, click Edit to open the Recovery Service wizard.



2. In the Recovery Service Wizard dialog box, set the following:

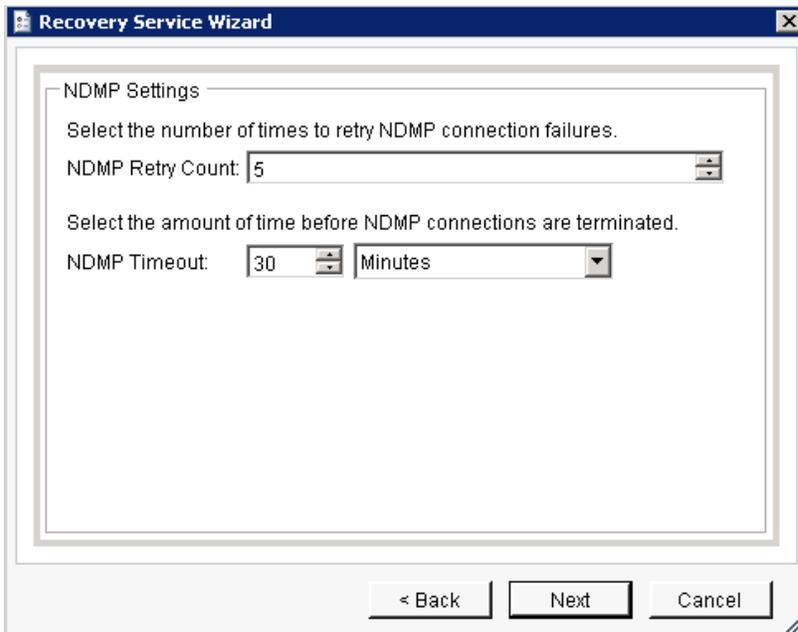
- **Service Poll Time.** The time interval between polling of ShareFile recovery queue by NRM-CS for file recovery requests.

**Note:** NetApp recommends a service poll time of five minutes (default). In addition to expediting the availability of NRM-CS restored files in ShareFile, the value of `Recovery-Interval` has to be changed to match the NRM service poll time.

```
<add key="enable-extended-logging" value="0"/>
<add key="ClientSettingsProvider.ServiceUri" value=""/>
<add key="httpMethod" value="https"/>
<add key="HeartBeat-Interval" value="5"/> <!-- Interval in
minutes-->
<add key="Recovery-Interval" value="300"/> <!-- Interval in
seconds-->
</appsettings>
<system.net>
  <connectionManagement>
    <add address="*" maxconnection="100"/>
  </connectionManagement>
</system.net>
```

- **Parallel File Restore.** Number of parallel threads allowed for restore of user files. Maximum allowed value is eight parallel restores.
- **Queue Retry Timeout.** Maximum interval for NRM-CS to wait for completion of a failed restore.

3. Click Next to proceed to configure the NDMP settings.

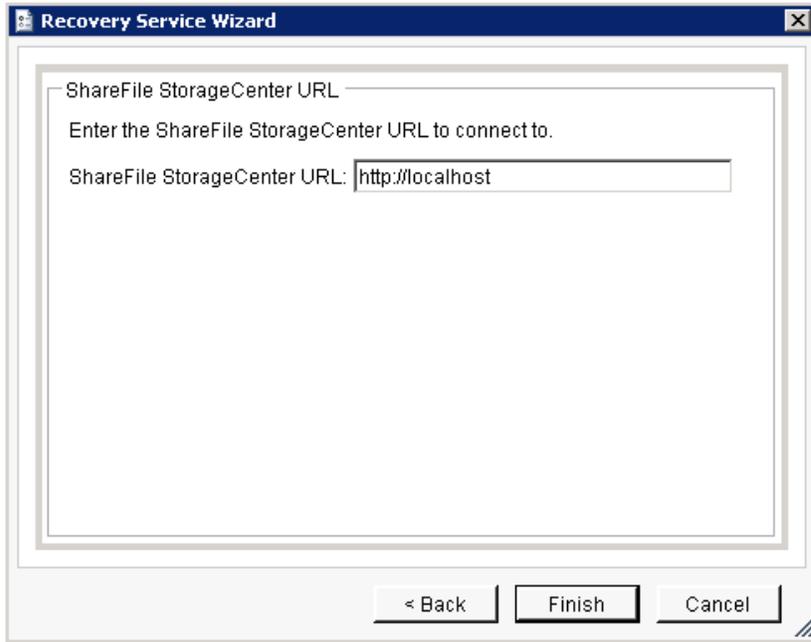


4. Configure the settings as follows:

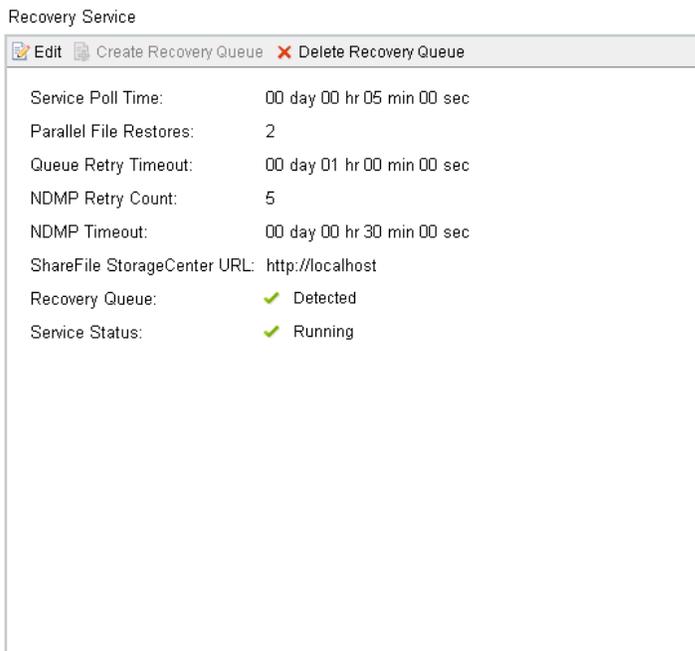
- **NDMP Retry Count.** Number of retries allowed for creating a successful NDMP session.
- **NDMP Timeout.** Maximum wait time for setting up an NDMP session.

5. Click Next to enter the ShareFile StorageZones Controller details.

**Note:** In cases where the NRM-CS is installed on a server other than the ShareFile StorageZones Controller, https might have to be used instead of http.



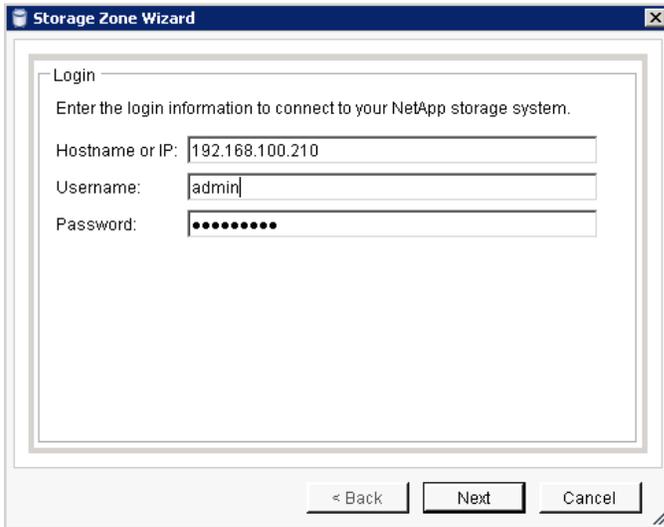
6. Click Create Recovery Queue to complete the configuration of the Recovery Service.



## StorageZones

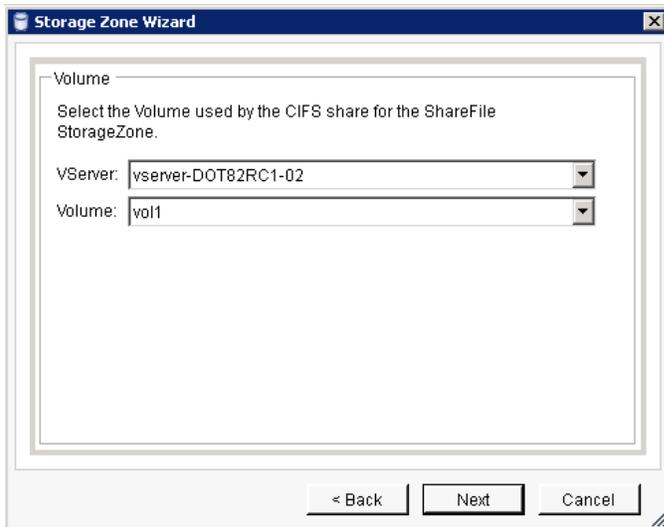
The details of the NetApp storage volume used for the ShareFile storage and NDMP credentials (required for restoring files from SnapMirror and SnapVault) are provided in the StorageZones tab.

1. Enter the NetApp controller host name/IP followed by the login credentials. NRM-CS automatically detects whether controllers are running Data ONTAP 7-Mode or clustered Data ONTAP.



The screenshot shows the 'Storage Zone Wizard' window with the 'Login' step. The instructions are: 'Enter the login information to connect to your NetApp storage system.' The fields are: 'Hostname or IP:' with the value '192.168.100.210', 'Username:' with the value 'admin', and 'Password:' with masked characters. At the bottom, there are three buttons: '< Back', 'Next', and 'Cancel'.

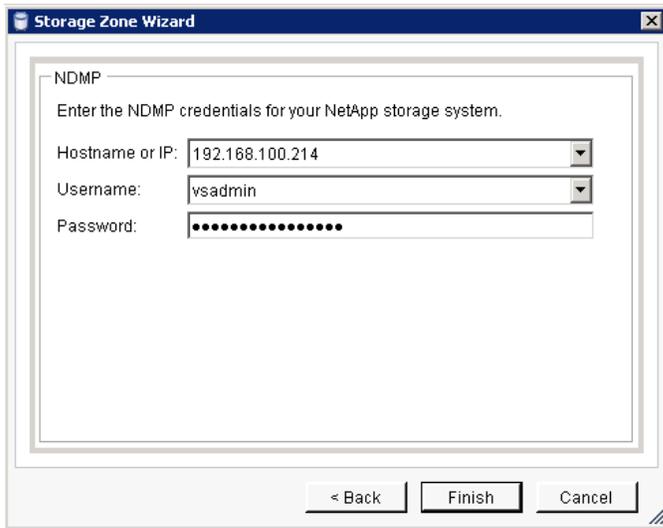
2. For NetApp controllers running clustered Data ONTAP, select the Vserver and the corresponding volume hosting the CIFS share used by ShareFile.



The screenshot shows the 'Storage Zone Wizard' window with the 'Volume' step. The instructions are: 'Select the Volume used by the CIFS share for the ShareFile StorageZone.' The fields are: 'VServer:' with a dropdown menu showing 'vserver-DOT82RC1-02', and 'Volume:' with a dropdown menu showing 'vol1'. At the bottom, there are three buttons: '< Back', 'Next', and 'Cancel'.

In case of a Data ONTAP 7-Mode controller, the available volumes will be listed. NRM-CS does not support vFiler<sup>®</sup> units on Data ONTAP 7-Mode.

3. NRM-CS uses NDMP to restore files from SnapMirror and SnapVault. Enter the NDMP credentials.



The image shows a 'Storage Zone Wizard' dialog box with a title bar containing a close button. The main area is titled 'NDMP' and contains the instruction 'Enter the NDMP credentials for your NetApp storage system.' Below this are three input fields: 'Hostname or IP:' with the value '192.168.100.214', 'Username:' with the value 'vsadmin', and 'Password:' with a masked password represented by a series of dots. At the bottom of the dialog are three buttons: '< Back', 'Finish', and 'Cancel'.

**Note:** In case of a clustered Data ONTAP 8.2 system, disable `node-scope` to use the SVM NDMP.

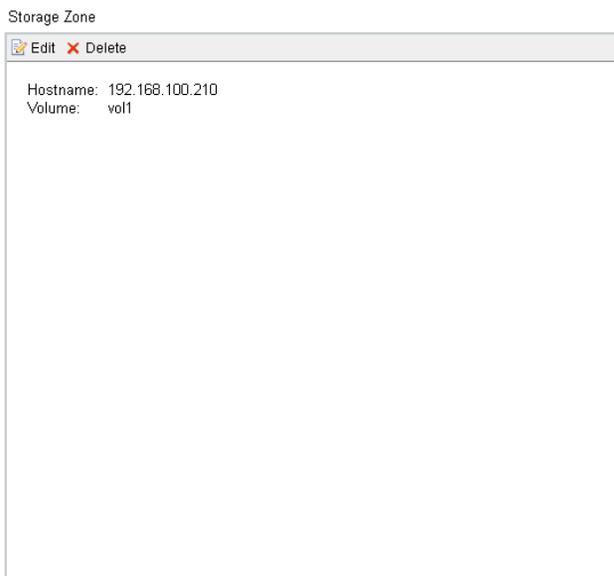
4. The password for the SVM NDMP can be obtained by running the following command on the CLI:

```
services ndmp generate-password -user vsadmin
```

```
vserver-DOT82RC1-02::> services ndmp generate-password -user vsadmin  
  
Vserver: vserver-DOT82RC1-02  
User: vsadmin  
Password: 9RqHHrdK69K2lcDF
```

**Note:** For systems running clustered Data ONTAP 8.1 or 8.1.2, SVM node scope is not available, and the node NDMP credentials are used. NRM-CS automatically detects the node user name in such systems.

The StorageZones details are now successfully entered into the NRM-CS configuration.

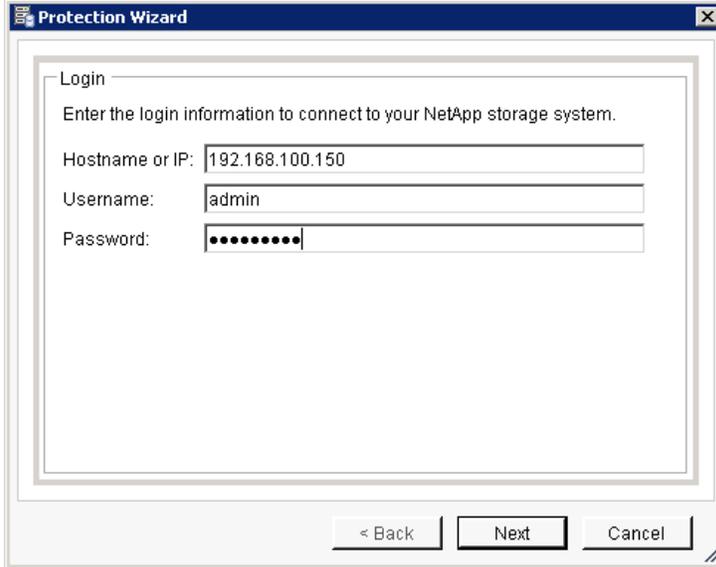


The image shows a 'Storage Zone' configuration window with a title bar containing 'Edit' and 'Delete' buttons. The main area displays the following details: 'Hostname: 192.168.100.210' and 'Volume: vol1'.

## Protection

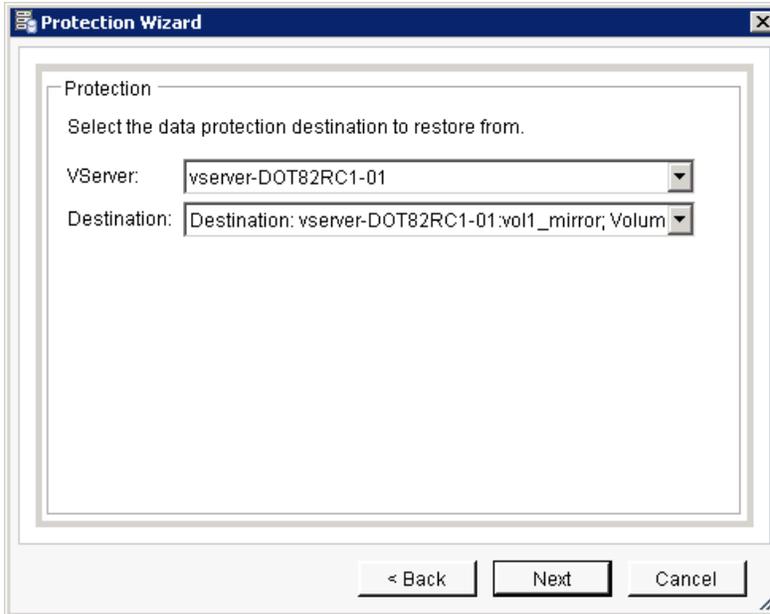
The Protection tab allows you to add the SnapMirror and SnapVault relationships available for the CIFS share and also specify its restore priority.

1. Clicking Add in the Protection tab allows you to enter the SnapMirror or SnapVault relationship, as desired.
2. Enter the destination NetApp controller host name/IP and the login credentials.



The screenshot shows the 'Login' step of the Protection Wizard. The window title is 'Protection Wizard'. The main content area is titled 'Login' and contains the instruction: 'Enter the login information to connect to your NetApp storage system.' Below this are three input fields: 'Hostname or IP:' with the value '192.168.100.150', 'Username:' with the value 'admin', and 'Password:' with a masked password represented by ten dots. At the bottom of the window are three buttons: '< Back', 'Next', and 'Cancel'.

3. Select the corresponding SVM and the destination SnapMirror or SnapVault instance, as applicable.

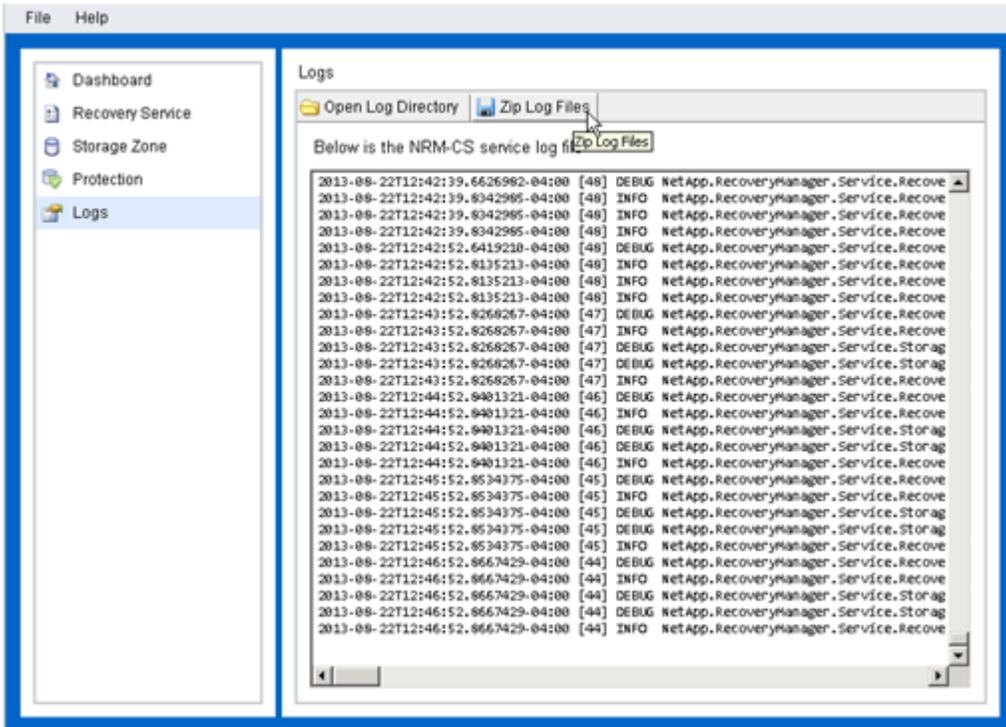


The screenshot shows the 'Protection' step of the Protection Wizard. The window title is 'Protection Wizard'. The main content area is titled 'Protection' and contains the instruction: 'Select the data protection destination to restore from.' Below this are two dropdown menus: 'VServer:' with the value 'vserver-DOT82RC1-01' and 'Destination:' with the value 'Destination: vserver-DOT82RC1-01:vol1\_mirror; Volum'. At the bottom of the window are three buttons: '< Back', 'Next', and 'Cancel'.



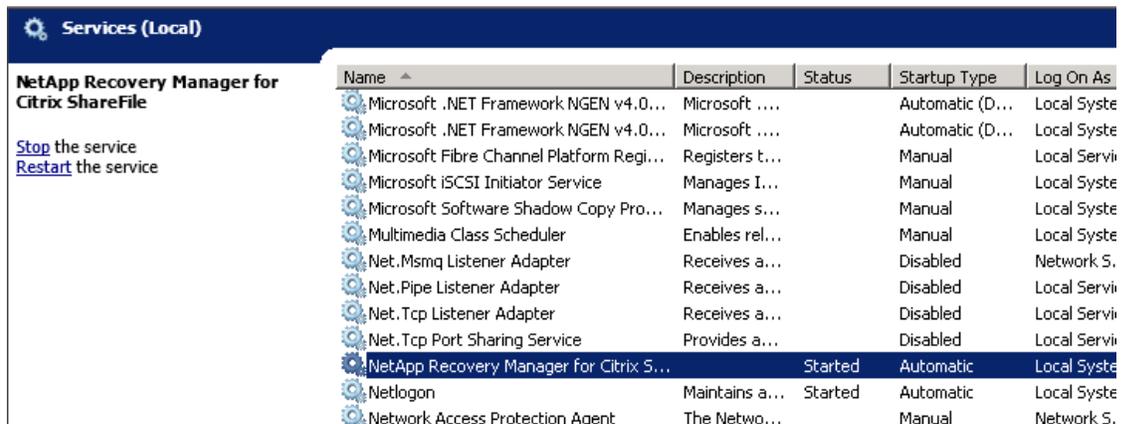
## Logs

The NRM-CS logs are available under the Logs view.



## Windows Service

NRM-CS runs in the background as an automatic Windows service. Therefore, NRM-CS does not have a separate user interface for user file/folder restore.



## File/Folder Restore from ShareFile/NRM-CS

Figure 20 depicts the restore process for files/folders in ShareFile.

Figure 20) ShareFile/NRM-CS restore process.

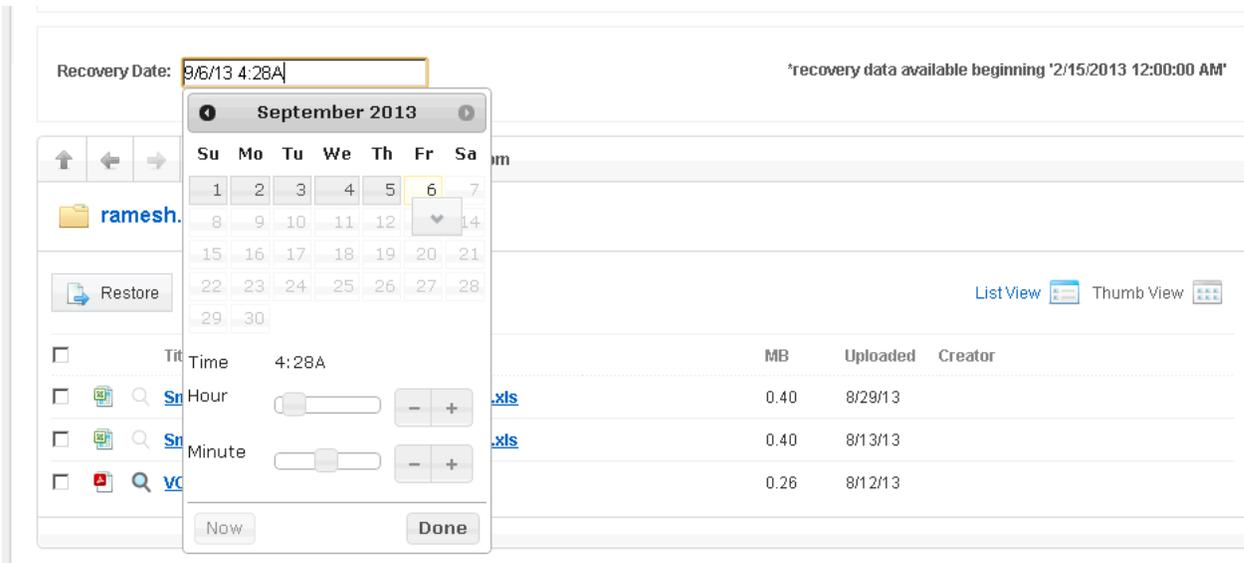


As an administrator, launch ShareFile web interface to select files to be restored.

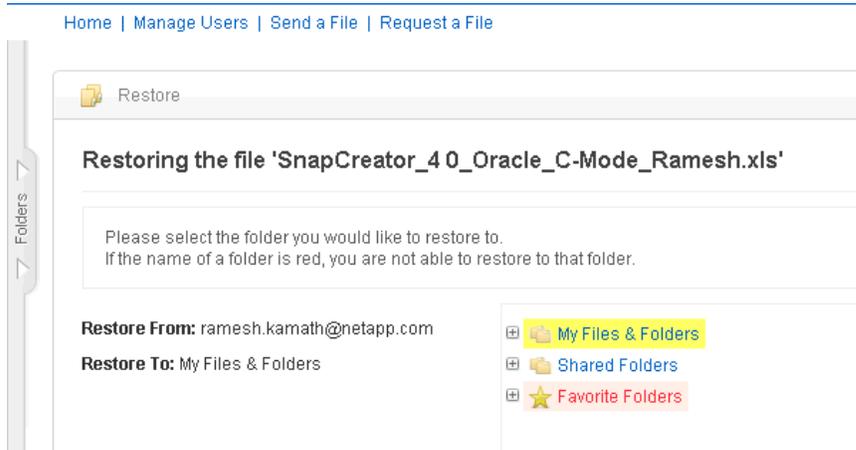
1. In the Admin tab, select StorageZones. The StorageZone used in this example is NetAppRTP2. After selecting the zone, click Recover Files to restore.

Host	Enabled	Version	External Address	Heartbeat
STOREZ RTP2	Yes	4.12.20	storezrtp2.netapp.com	Storage Center is responding

2. From the Recovery menu, select the files or folders to be restored from a specific time and then click Restore.



### 3. Select the restore destination.



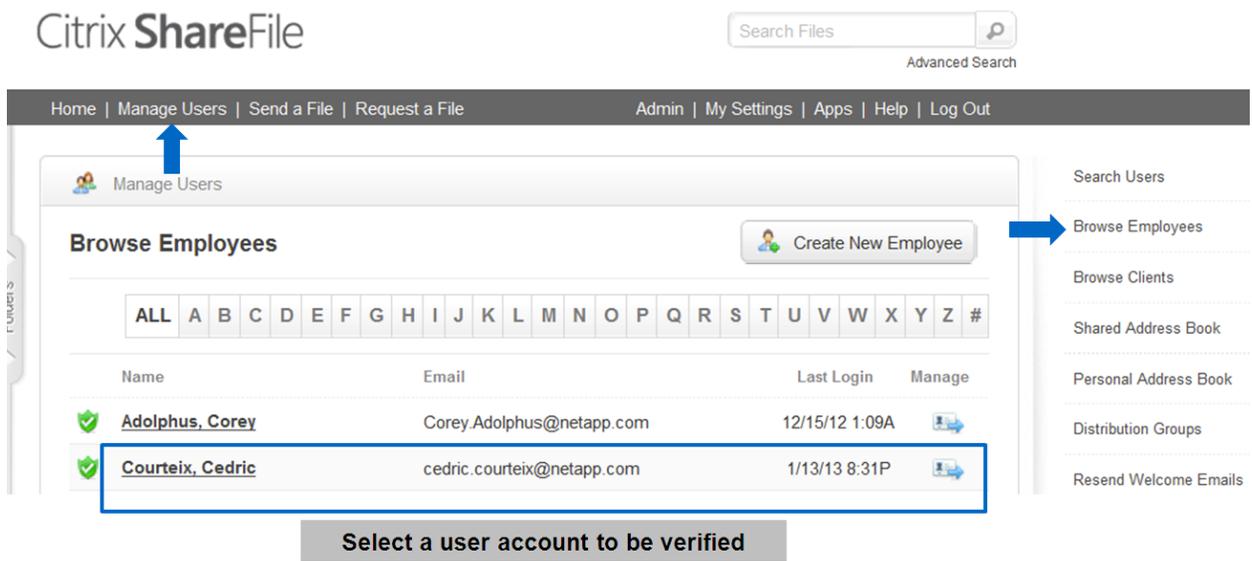
**Note:** Using this method, several files and folders can be restored at the same time.

**Note:** NRM-CS is automatically invoked in the background when the files are not available from within ShareFile.

## 2.10 Check That Data Remains on Premises

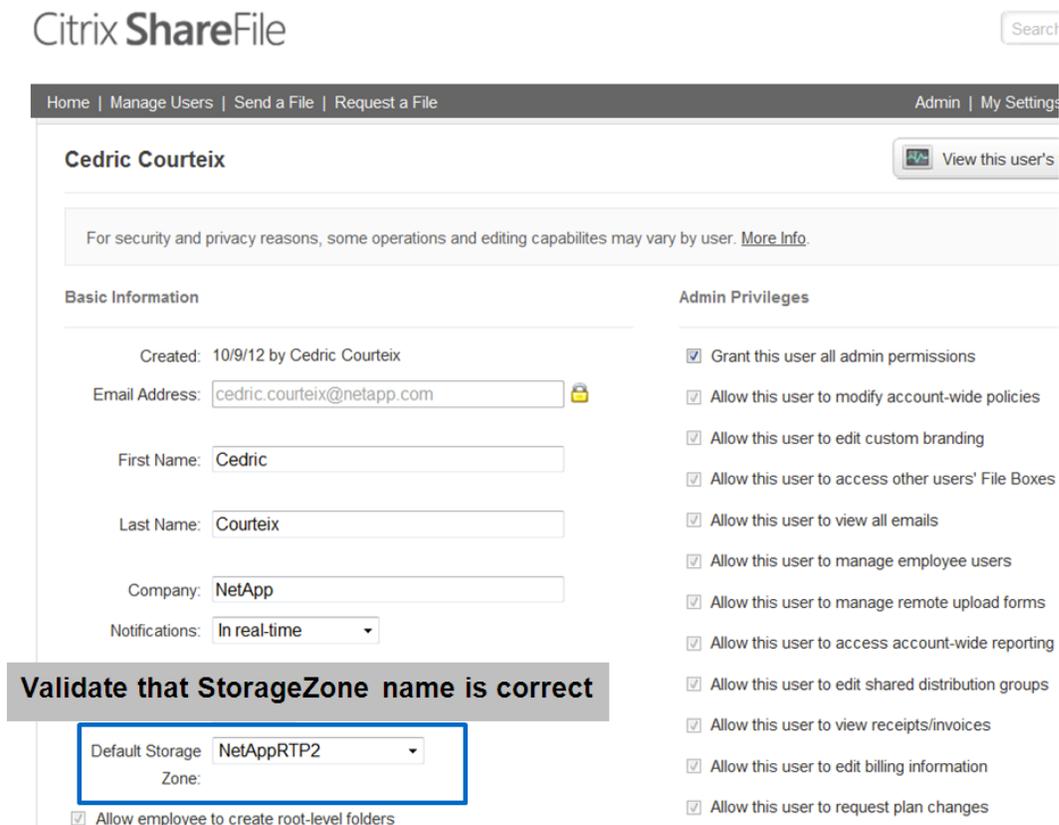
For performance and compliance reasons, it is important to verify that the user folders are configured to store data on the premises. If they are not configured, users might store their files in the ShareFile public cloud. To verify user folder configuration, launch the ShareFile web interface as an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

Figure 21) Select account in employee directory.



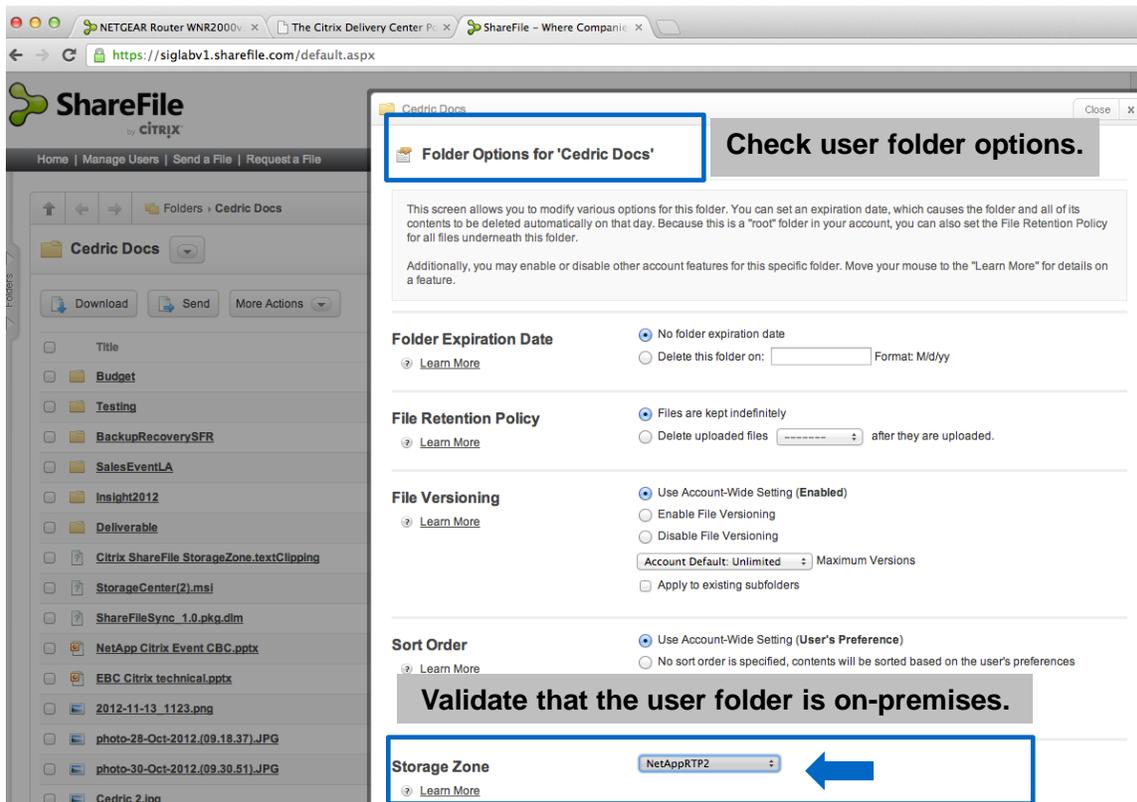
In the next page, verify that the field containing the default zone for the user account corresponds to the on-premises zone and not to the ShareFile public cloud.

Figure 22) Verify default StorageZones name.



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

Figure 23) Check folder options.



## 2.11 StorageZones Connectors

StorageZones Connectors allow ShareFile remote users to securely access documents and folders stored in SharePoint® document libraries and on network file shares. A StorageZones Connector is embedded on a StorageZones Controller and integrates with the on-premises StorageZones.

StorageZones Connectors can be created by selecting Home > Connectors > Create Connectors.

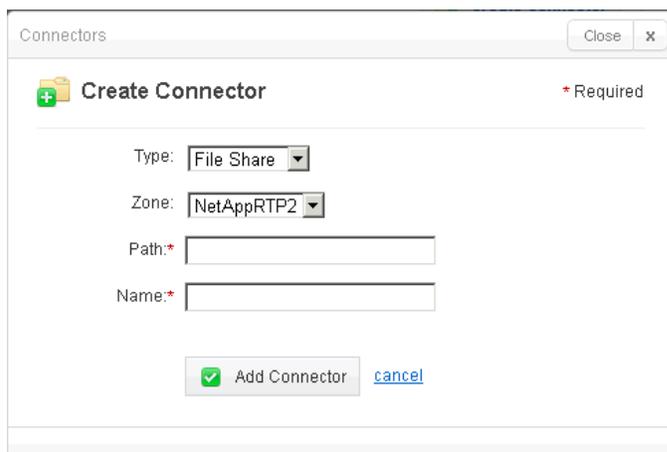
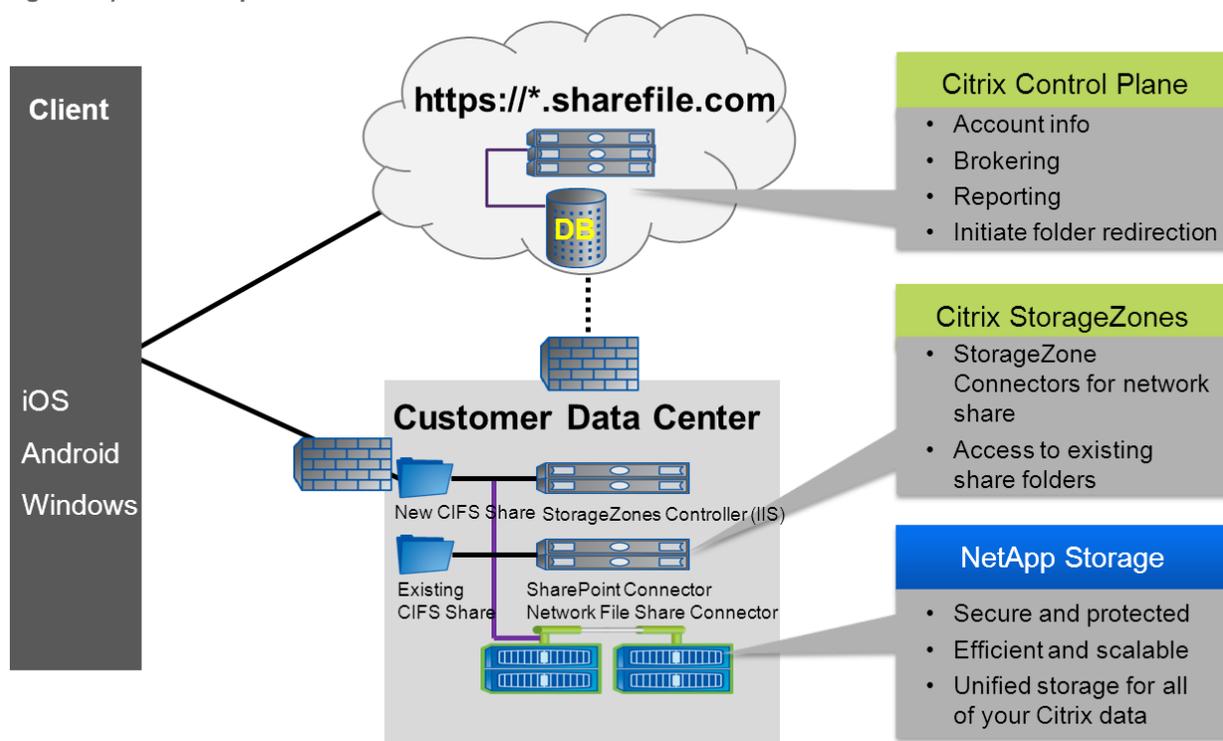


Figure 23 is an example of ShareFile private cloud implementation with the SharePoint and Network File Share Connectors added.

Figure 24) ShareFile private cloud with CIFS connector.



#### Best Practice

NetApp recommends using the existing data protection methods for the SharePoint document library and the network file shares. NRM-CS configuration can be used for data protection of new ShareFile data.

### StorageZones Connector for Network File Shares

The StorageZones connector for Network File Shares 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 because ShareFile will not manage the metadata for these folders. As opposed to StorageZones Controller, the files will not be transformed into objects. Administrators can add as many universal naming convention (UNC) paths as needed to a StorageZone.

The StorageZones CIFS Connector is a separate feature and must be installed on a dedicated IIS server. 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 StorageZones Network File Share connector, complete the following steps:

1. Launch the ShareFile configuration page and log in to the site.
2. Select Home > Connectors > Create Connectors.
3. Select type File Share and the StorageZone. Enter the file share path and a unique name, then click Add Connector.

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 two files to demonstrate file access.

Connectors Close x

**Create Connector** \* Required

Type:

Zone:

Path:\*

Name:\*

Add Connector [cancel](#)

4. The newly created share is displayed on the Connectors page. To remove a folder, select the checkbox corresponding to the folder name and click Delete.

NetApp Search Files

Home | Manage Users | Send a File | Request a File Admin | My Settings | Apps | Help | Log Out

My Files & Folders | Shared Folders | Favorite Folders | **Connectors**

Connectors Create Connector

Delete

<input type="checkbox"/>	Title	Path	Type	
<input type="checkbox"/>	Connector_CIFS	\\SF_CIFS2\vol_CIFS7	File Share	<a href="#">Edit/View Access</a>

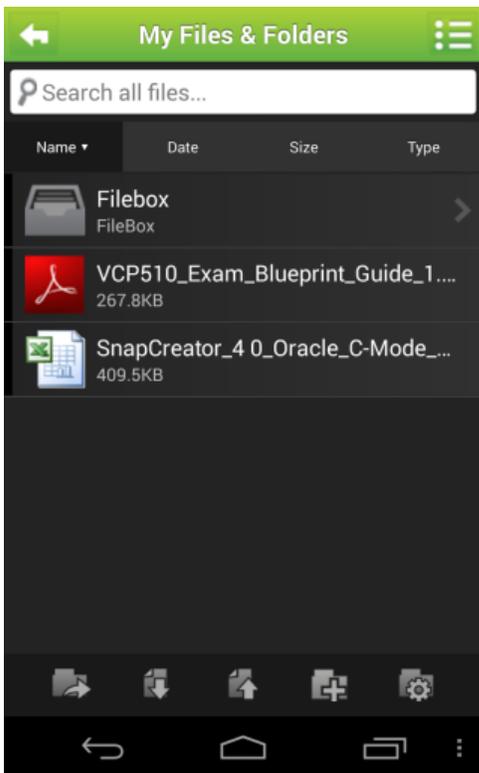
File Box  
Sent Messages  
Recycle Bin

## Download Existing Files for Offline Access

1. Launch the ShareFile application from an iOS/Android 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®, iPhone®, or Android device. Both read and write access can be provided to users to the Network Share with the StorageZones connector.

**Note:** Read/write access is determined by the ShareFile license plan.

Figure 25) Network file access with ShareFile app on Android.



### StorageZones Connector for SharePoint

A StorageZones Connector for SharePoint can be created by adding the SharePoint document library website address in the Create Connector window.

The SharePoint document libraries are displayed on ShareFile under Folders > SharePoint and Folders > File Shares. The credentials used to log on a user to ShareFile are required to access the SharePoint libraries.

**Note:** NetApp recommends using SnapManager for SharePoint for protection of SharePoint deployments on NetApp storage.

#### Best Practice

NetApp recommends using the latest available versions of ShareFile clients and mobile apps.

### 3 Solution Validation

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

Table 3) Test results.

Solution Test	Results
Storage efficiency	<ul style="list-style-type: none"> <li>• <b>Deduplication and compression.</b> 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 40% savings were obtained by using deduplication and compression<sup>2</sup>. Note that storage efficiency savings might be higher depending on how many times the files are saved, because object storage creates a new object for each modification of the file.</li> <li>• <b>Thin provisioning and autogrow.</b> These two features were tested for the ability to provide flexibility and storage space savings.</li> </ul> <p><b>Note:</b> Data-at-rest encryption must be disabled to obtain the benefits of deduplication and compression.</p>
File restore	The CIFS share was configured with NetApp Snapshot and SnapMirror protection. NRM-CS was configured as per the environment. Deleted files were successfully restored using NRM-CS from the ShareFile Administrator Restore user interface.
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 StorageZones 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>
Access existing Microsoft SharePoint document library	The StorageZones connector for SharePoint enables user access to files on the SharePoint document library without making any changes to the existing SharePoint setup.

### 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) Key takeaways.

NetApp Feature	Key Takeaways
Storage efficiency	Leverage storage efficiency features to consume less storage and accommodate more users.

<sup>2</sup> Actual customer results may vary.

NetApp Feature	Key Takeaways
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, SnapMirror, and SnapVault.
NetApp Recovery Manager for Citrix ShareFile	Enable quick administrator-driven recovery of files and folders using NRM-CS.

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 30% was observed. Storage efficiency savings of 30% to 40% can be expected in typical deployments<sup>3</sup>.

Figure 26) Storage efficiency savings.



<sup>3</sup> Actual customer results might vary.

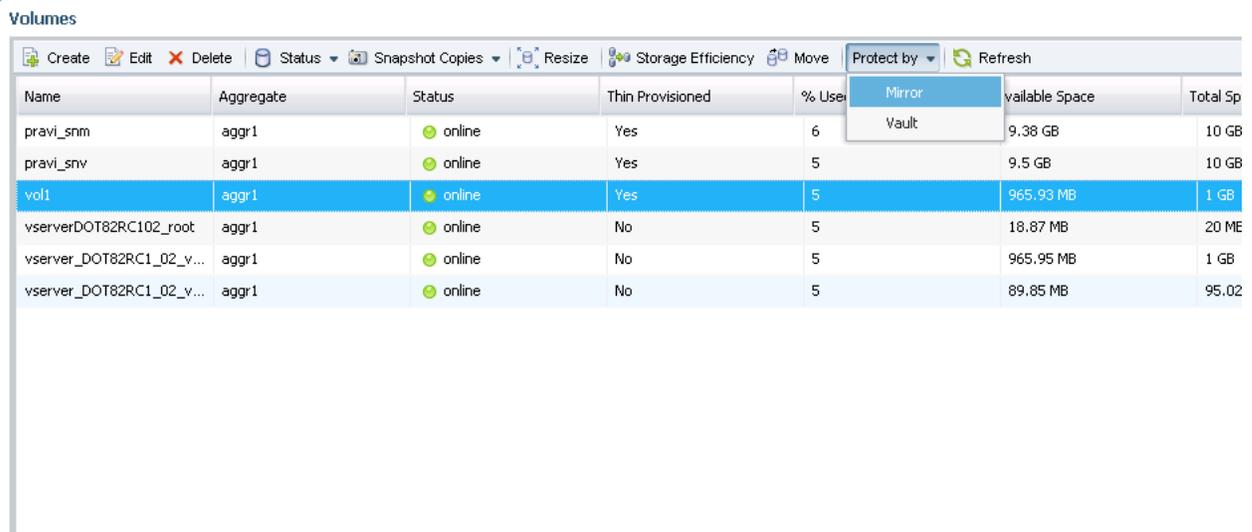
## Appendix

### Configuring SnapMirror and SnapVault

This section covers the typical configuration of SnapMirror and SnapVault for a CIFS share used for ShareFile StorageZones.

1. In OnCommand System Manager, select the volume used for the CIFS share and select SnapMirror protection.

Volumes



Name	Aggregate	Status	Thin Provisioned	% Used	Protect by	available Space	Total Sp
pravi_snm	aggr1	online	Yes	6	Mirror	9,38 GB	10 GB
pravi_snv	aggr1	online	Yes	5	Vault	9,5 GB	10 GB
vol1	aggr1	online	Yes	5		965,93 MB	1 GB
vserverDOT82RC102_root	aggr1	online	No	5		18,87 MB	20 MB
vserver_DOT82RC1_02_y...	aggr1	online	No	5		965,95 MB	1 GB
vserver_DOT82RC1_02_y...	aggr1	online	No	5		89,85 MB	95,02

2. In the SnapMirror configuration window, select the cluster peer and the destination SnapMirror volume. Specify the protection policy and the schedule.

### Create Mirror Relationship ✕

**i** Provide asynchronous disaster recovery. Data protection mirror relationships enable you to periodically create and transfer Snapshot copies of data on the source volume to the destination volume; and retain those Snapshot copies.  
[Tell me more about mirror](#)

---

**Source Volume**

Cluster: cluster-DOT82RC1-02  
Vserver: vserver-DOT82RC1-02  
Volume: vol1 ( Used space 12 MB )

---

**Destination Volume**

**?** Cluster:  [Create Peer](#)

Vserver:

Volume:  New Volume  Select Volume

Volume name:  Aggregate:   
4.53 GB available (of 16.7 GB)

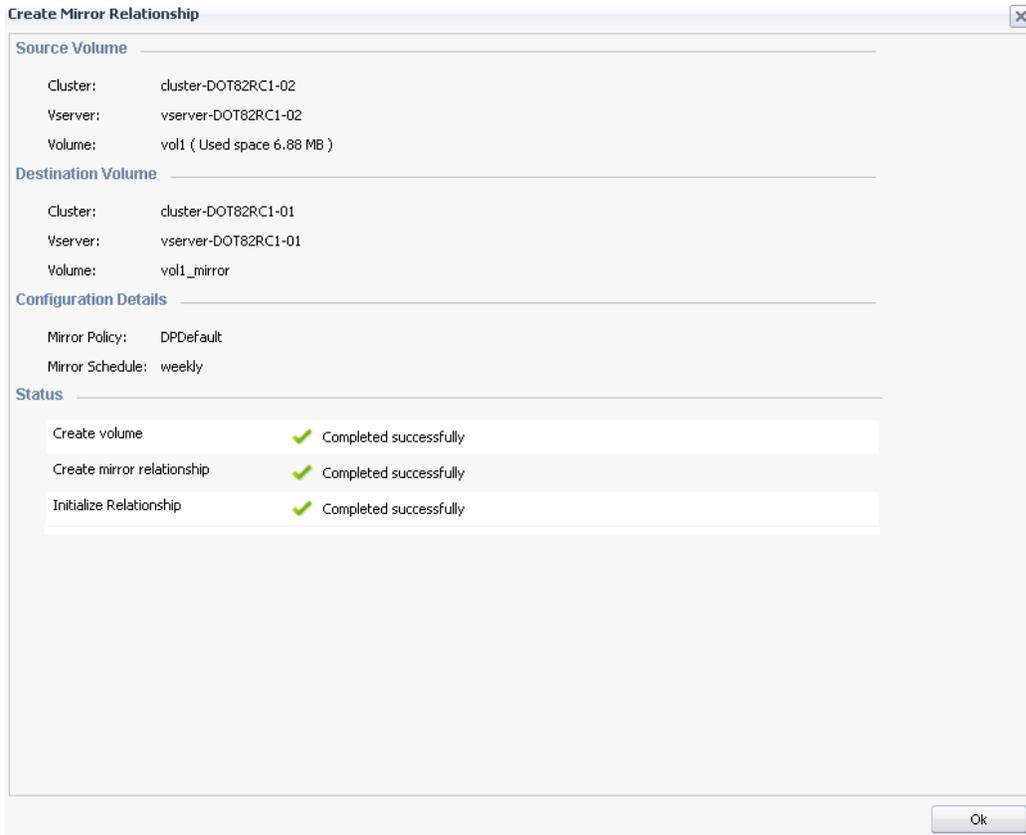
---

**Configuration Details**

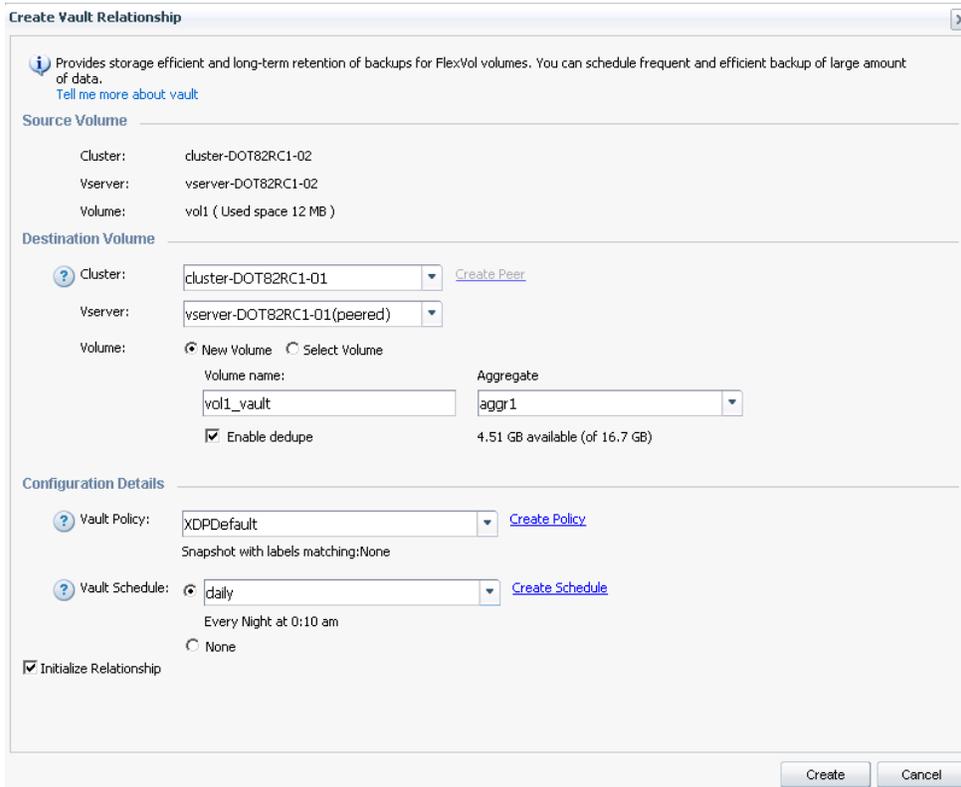
**?** Mirror Policy:  [Create Policy](#)

**?** Mirror Schedule:   [Create Schedule](#)  
 Every Sun at 0:15 am  
 None

Initialize Relationship



3. Similarly, the SnapVault relationship can be created by selecting the Vault option for the volume.



**Note:** NetApp suggests the following schedule for a Snapshot, SnapMirror, and SnapVault configuration:

- Snapshot. Hourly
- SnapVault. Daily
- SnapMirror. Weekly

However, the schedules will differ on a case-by-case basis depending on customer environments and the recovery point objective (RPO) requirements.

## Acknowledgements

The authors would like to thank the following peers for their contribution to the design, creation, and validation of this guide.

- **Citrix:** Chris Leithe, Adam Lotz, Juliano Maldaner, Astha Malik, and Joel Stocker
- **NetApp:** Abhinav Joshi, Bryan Knight, Troy Mangum, and Praveena Palaniswamy

## Feedback

If you have questions or comments about this solution guide, contact [dl-citrix-core@netapp.com](mailto:dl-citrix-core@netapp.com).

## Resource Links

### Citrix ShareFile

[Citrix StorageZones](#)

[On-Premises Solution](#)

[ShareFile on Citrix eDocs](#)

[ShareFile APIs](#)

[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](#)

[Deduplication](#)

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

[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](#)

[Storage Virtual Machine](#)

[Snapshot](#)

[SnapMirror](#)

[SnapVault](#)

[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
Version 2.0	September 2013	Version updated to include NRM-CS
Version 2.1	November 2013	Hyperlinks updated

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®](#)

© 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, SnapRestore, Snapshot, SnapVault, vFiler, and WAFL are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Cisco Nexus is a registered trademark of Cisco Systems. Active Directory, Microsoft, SharePoint, Windows, Windows PowerShell, and Windows Server are registered trademarks of Microsoft Corporation. iPad and iPhone 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-4124-1013

