DELL EMC UNITY: DR ACCESS AND TESTING

Dell EMC Unity OE 4.5

TABLE OF CONTENTS

OVERVIEW

On Dell EMC Unity, there are several methods available to access file system data from the destination system of a replication session. This document describes the available options for DR access and testing for file systems leveraging native synchronous or asynchronous replication. These procedures can be leveraged when running DR test operations to ensure that the replicated data can be read and written to. It also allows applications to be brought online online using the data from the destination system to ensure there are no errors.

You can access both file systems and snapshots on the destination of an asynchronous replication session. However, it is highly recommended to use snapshots since the file system is still actively being replicated. For synchronous replication sessions, only snapshots can be accessed. The following options are available:

NAME	ACCESS TYPE	PROTOCOLS	RESOURCE	INTERFACE
Proxy NAS Servers (OE 4.3+)	Read-Only	SMB NFS	Read-Only File Systems Read-Only Snapshots Read-Write Snapshots	Proxy NAS Server Interface
SMB Proxy NAS Shares (OE 4.5+)	Read-Write	SMB	Read-Only Snapshots Read-Write Snapshots	Proxy NAS Server Interface
NFS	Read-Write	NFS	Read-Write Snapshots	Backup & Test Interface
FTP/SFTP	Read-Write	FTP SFTP	Read-Only File Systems Read-Only Snapshots Read-Write Snapshots	Backup & Test Interface
NDMPCopy	Read-Write	SMB NFS	Read/Write File System (restored from Snapshot)	Backup & Test Interface

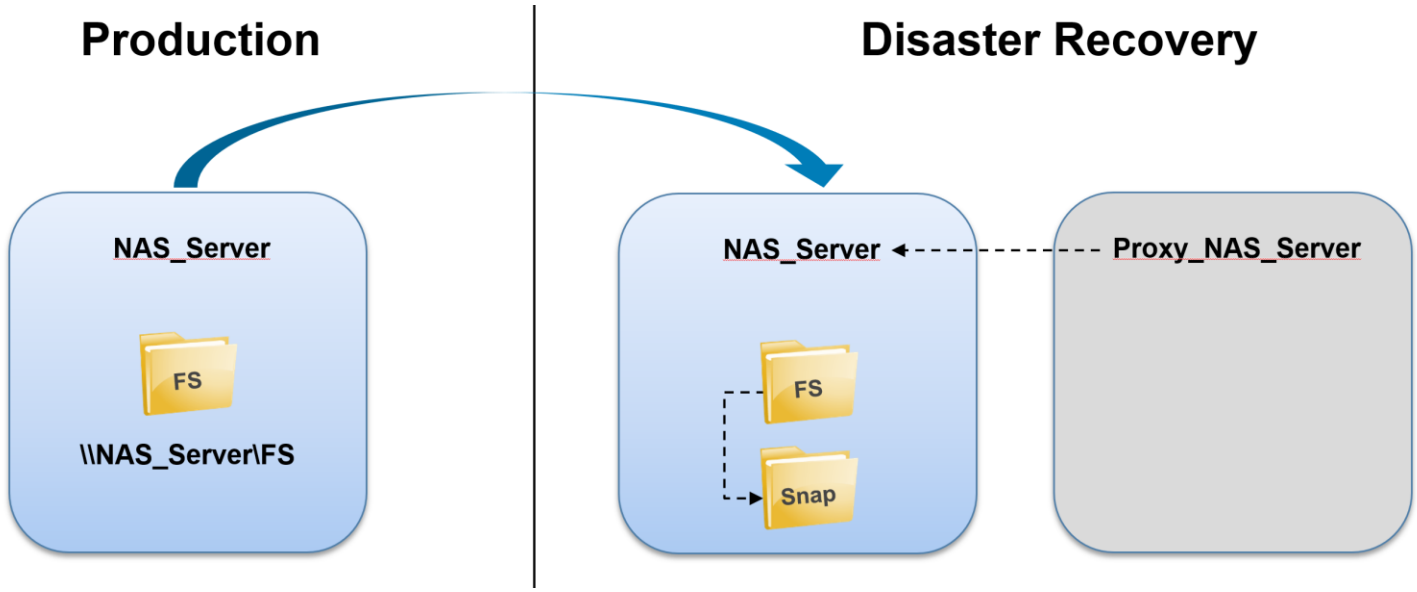
- Name - The name of the feature
- Access Type - Read-Only or Read-Wite Access
- Protocols - The protocol can be used to access the share
- Resource - Which resources can be accessed using this method
- Interface - Which interface is used to provide access to the share

Your requirements for access type, protocols, and what resources you want to access will determine which method you should use. For example, if you only need read-only access for either SMB and/or NFS, a Proxy NAS Server can be configured. However, if you need read-write access, a SMB Proxy NAS Share or NFS access should be configured for SMB and NFS, respectively. FTP/SFP should be configured if you application or environment leverages FTP/SFTP. Finally, NDMPCopy can be used if you want to create a full copy of the file system and present it to the application for the DR test.

PROXY NAS SERVERS

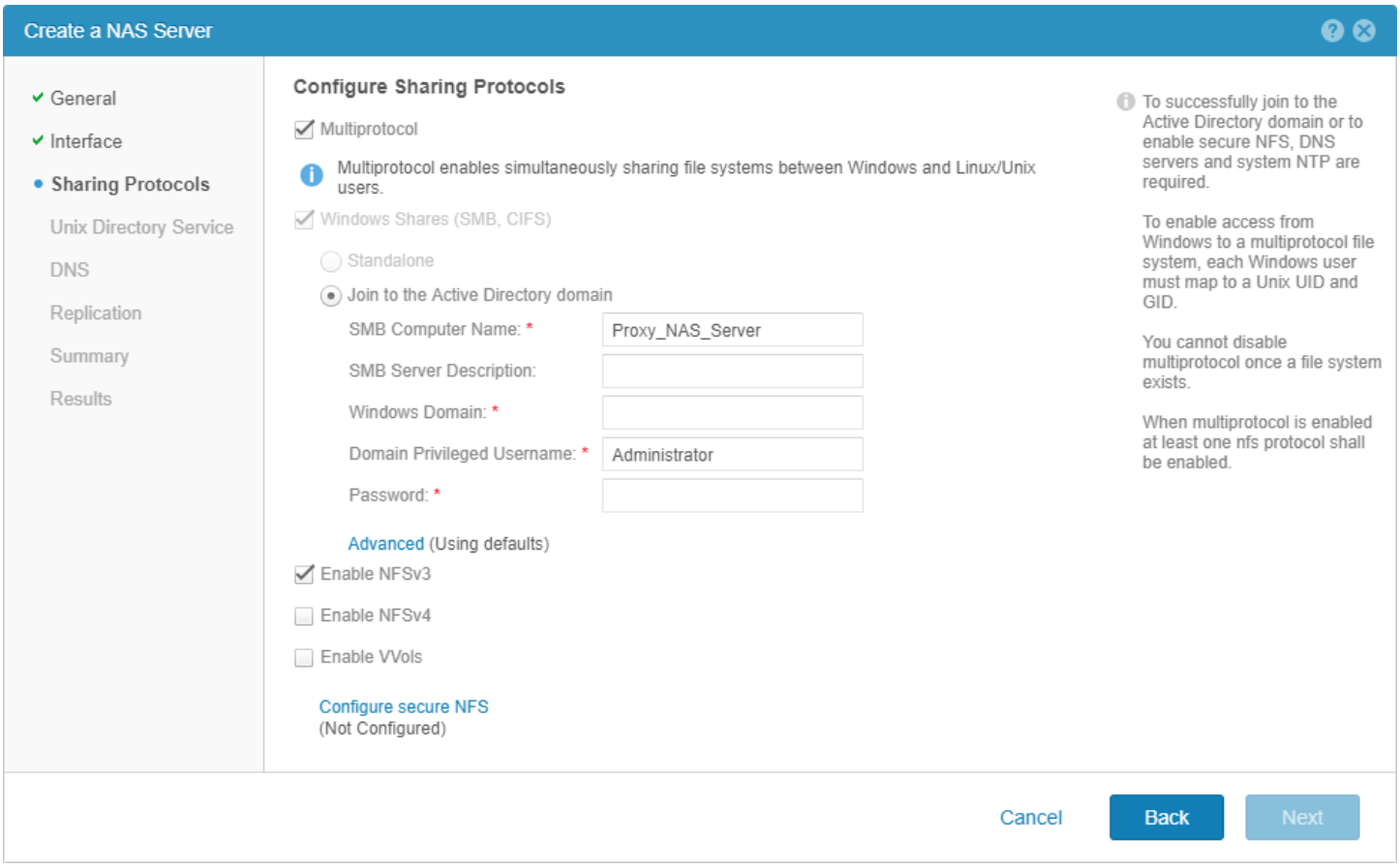
Dell EMC Unity OE version 4.3 introduces Proxy NAS Servers, providing the ability to access files on the destination side of a replicated file resource. This feature provides read-only access to file system and snapshot data through SMB and NFS. There is no ability to write to the file systems or snapshots using the proxy NAS server, even if the snapshot is read/write.

All the NAS Servers' file systems and their snapshots are displayed when connecting to the proxy NAS Server. Due to this, the user must be part of the Local Administrators group for SMB or root for NFS. You can add users and groups to the local Administrators group of the proxy NAS server through MMC, just like a regular SMB server. The figure below shows the Proxy NAS Server configuration.



Although it may be possible to directly access the file system data using the proxy NAS server, it is recommended to use this feature to access data residing on snapshots. This is due to the fact that the destination file system is still being actively replicated. For asynchronous replication, there may be instances where the destination file system needs to be frozen due to a replication sync.

In order to create a proxy NAS server, create a new NAS server on the system with an interface, the appropriate protocols, and configure the appropriate services such as DNS and LDAP. The new proxy NAS server should be configured the same way as the NAS servers that it is providing access to such as protocols, tenants, and so on. Note that the new proxy NAS server must reside on the same SP as the NAS server that it will be providing access to.



In order to designate the new NAS server as a proxy NAS server, a CLI Service Command must be used. SSH into the system and run the `svc_nas <Proxy_NAS_Server> -proxy -add <Target_NAS_Server>` command, where:

- `<Proxy_NAS_Server>` - The name of the new proxy NAS server you just created
- `<Target_NAS_Server>` - The name of the destination NAS server you want users to access
- `-NFSRoot <Allowed_Nodes>` - For NFS access, also include this option to specify the nodes that should have access over NFS. Multiple options can be specified in the command if they are separated by a space. Valid options are:
    - minSecurity - <Security_Mode>
    - host - <Hostname>
    - ip - <IPv4 or IPv6 Address>
    - subnet - <IP/Mask>
    - netgroup - <Netgroup>

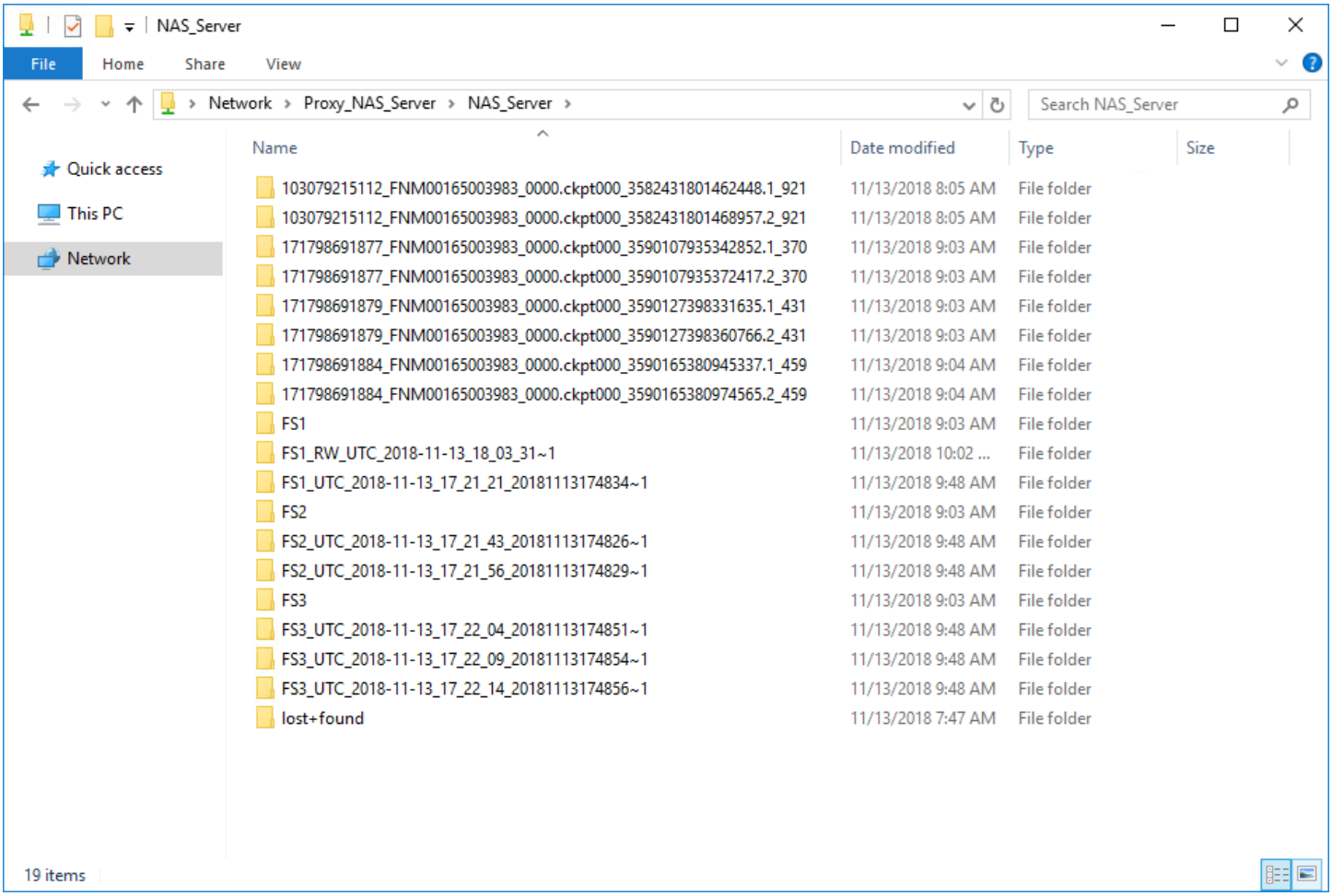
For example, run `svc_nas Proxy_NAS_Server -proxy -add NAS_Server -NFSRoot ip=10.10.10.10` to configure the proxy NAS server for NFS access and limit access to client IP 10.10.10.10.

To view the proxy NAS server configuration on the system, run the `svc_nas Proxy_NAS_Server -proxy -show` command, as shown in the figure below.

```
- PuTTY
16:07:57 service@Chen2390 spa:~/user> svc_nas Proxy_NAS_Server -proxy -show

Proxy_NAS_Server : commands processed: 1
command(s) succeeded
output is complete

 The proxy configuration allows accessing the following NAS server(s):
  NAS server: NAS_Server  State: Started  Mode: Destination
    SMB share: NAS_Server
    NFS export: NAS_Server  allowed root clients: ip=10.10.10.10


Command succeeded


16:07:58 service@Chen2390 spa:~/user>
```

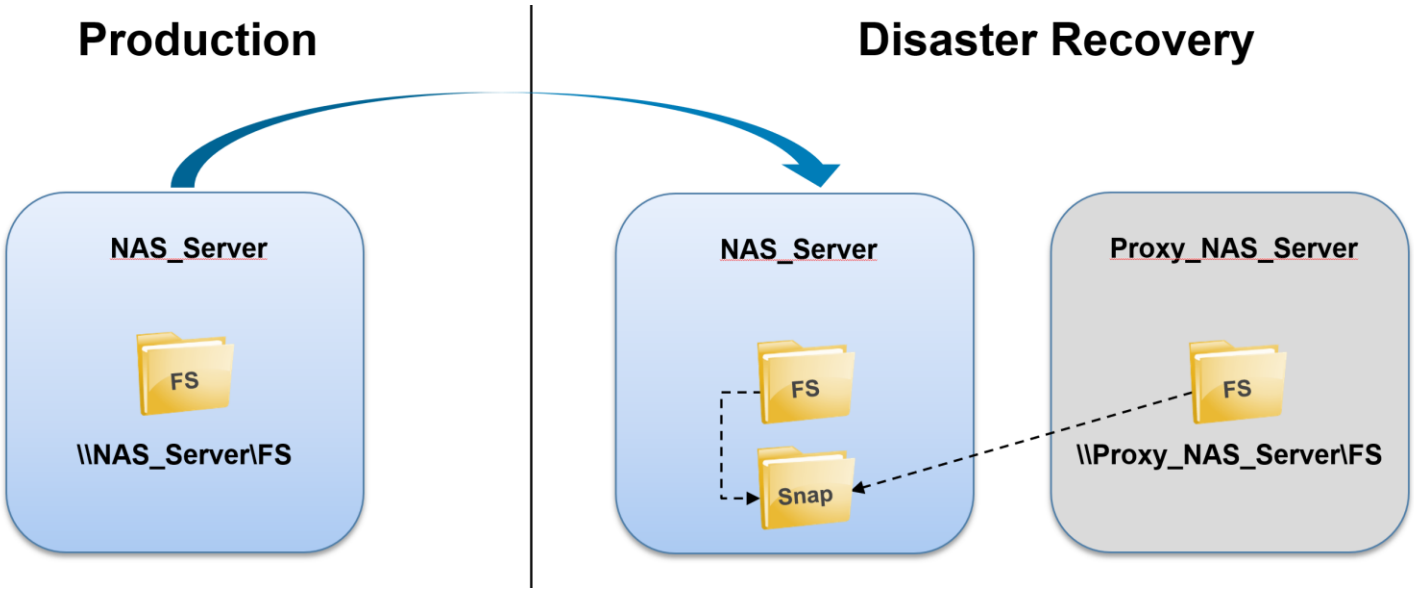
This indiciates the Proxy NAS Server is properly configured and accessible. Run `mount Proxy_NAS_Server:/NAS_Server /mnt` on the host that is provided access or `\\Proxy_NAS_Server\NAS_Server` from a SMB client to mount the proxy NAS server and view the contents. Note that the proxy NAS server configuration and details are only available through the `svc_nas` CLI command. This information is not available through UEMCLI or Unisphere.

Each proxy NAS server can be configured to provide access to one or more NAS servers' data. Each NAS server that you add to the proxy NAS server is displayed as a subdirectory with the name of the NAS server. All of the NAS servers' file systems and their snapshots are displayed when connecting to the proxy NAS server, as shown in the figure below.


NAS_Server
File
Home
Share
View
Network › Proxy_NAS_Server › NAS_Server ›
Search NAS_Server
Quick access
This PC
Network
Name
Date modified
Type
Size
103079215112_FNM00165003983_0000.ckpt000_3582431801462448.1_921 11/13/2018 8:05 AM File folder
103079215112_FNM00165003983_0000.ckpt000_3582431801468957.2_921 11/13/2018 8:05 AM File folder
171798691877_FNM00165003983_0000.ckpt000_3590107935342852.1_370 11/13/2018 9:03 AM File folder
171798691877_FNM00165003983_0000.ckpt000_3590107935372417.2_370 11/13/2018 9:03 AM File folder
171798691879_FNM00165003983_0000.ckpt000_3590127398331635.1_431 11/13/2018 9:03 AM File folder
171798691879_FNM00165003983_0000.ckpt000_3590127398360766.2_431 11/13/2018 9:03 AM File folder
171798691884_FNM00165003983_0000.ckpt000_3590165380945337.1_459 11/13/2018 9:04 AM File folder
171798691884_FNM00165003983_0000.ckpt000_3590165380974565.2_459 11/13/2018 9:04 AM File folder
FS1 11/13/2018 9:03 AM File folder
FS1_RW_UTC_2018-11-13_18_03_31~1 11/13/2018 10:02 ... File folder
FS1_UTC_2018-11-13_17_21_21_20181113174834~1 11/13/2018 9:48 AM File folder
FS2 11/13/2018 9:03 AM File folder
FS2_UTC_2018-11-13_17_21_43_20181113174826~1 11/13/2018 9:48 AM File folder
FS2_UTC_2018-11-13_17_21_56_20181113174829~1 11/13/2018 9:48 AM File folder
FS3 11/13/2018 9:03 AM File folder
FS3_UTC_2018-11-13_17_22_04_20181113174851~1 11/13/2018 9:48 AM File folder
FS3_UTC_2018-11-13_17_22_09_20181113174854~1 11/13/2018 9:48 AM File folder
FS3_UTC_2018-11-13_17_22_14_20181113174856~1 11/13/2018 9:48 AM File folder
lost+found 11/13/2018 7:47 AM File folder
19 items

SMB PROXY NAS SHARES

Dell EMC Unity OE version 4.5 introduces the ability to create SMB shares for writeable and read-only snapshots on the destination NAS Server. This feature is designed to enable DR testing without any impact to the ongoing replication session. It allows customers to confirm that an application can be brought online and write to a share hosted on the destination system. This feature works with both asynchronous and synchronous replication. This feature leverages a Proxy NAS Server and Proxy share created on the destination system to provide access to the snapshot, as shown in the figure below.



In contrast to the read-only Proxy NAS Server feature, this feature allows any domain user to access the share and is not limited to Administrators or root. This is because each share points to a specific snapshot, as opposed to the entire contents of the NAS Server. The proxy share can be configured to point to either a Read-Only (RO) or Read-Write (RW) snapshot that exists on the destination file system. If a RW snapshot is selected, then the client can write to the share.

To configure a proxy share, a new Proxy NAS Server must be created on the destination Dell EMC Unity system. The NAS Server must reside on the same SP it is providing access to and must be joined to the same SMB domain as the destination NAS Server. If these requirements are met, a single Proxy NAS Server can be used to access data on one or more destination NAS Servers.

Once the Proxy NAS Server is configured, SMB shares can be created for snapshots. These special Proxy SMB shares can only be configured and managed by using the `svc_nas` command. Once created, these shares are not visible through normal interfaces such as Unisphere, UEMCLI, or REST API. These shares also do not count towards the system limits and there is no hard limit on how many Proxy SMB shares can be created.

To create a Proxy SMB share, use the `svc_nas <Proxy_NAS_Server> -proxy_share -add <Target_NAS_Server> -share <Share_Name> -path <Snapshot_Path>` command, where:

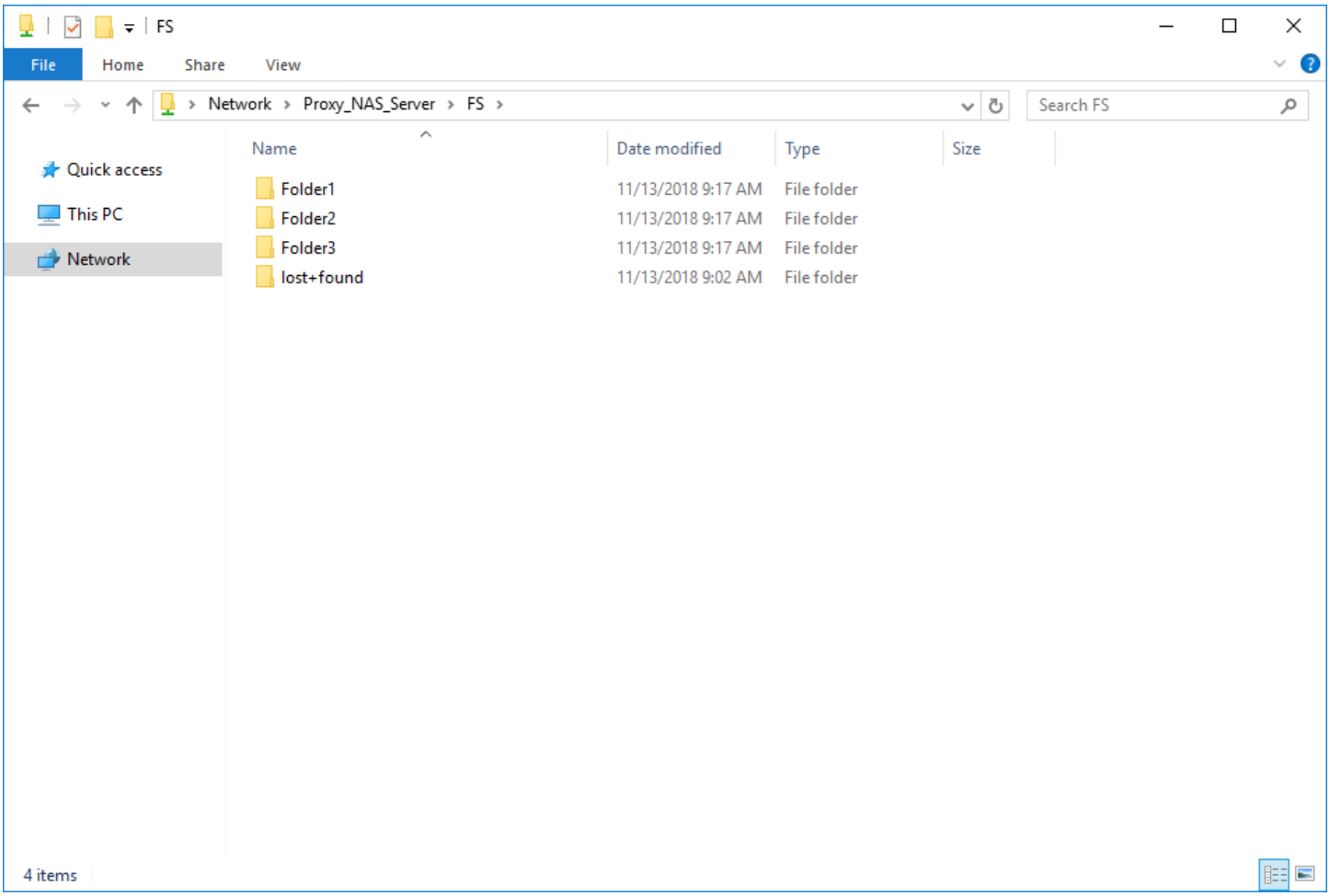
- `<Proxy_NAS_Server>` - Name of the Proxy NAS Server
- `<Target_NAS_Server>` - Name of the NAS Server it is providing access to
- `<Share_Name>` - Name of the share that the client uses to mount
- `<Snapshot_Path>` - Path to the RO or RW snapshot, usually this is the name of the snapshot prefixed with a /

For example, `svc_nas Proxy_NAS_Server -proxy_share -add NAS_Server -share FS -path /UTC_2018-11-13_15:58:57`.

To view the proxy NAS server configuration on the system, run the `svc_nas Proxy_NAS_Server -proxy_share -show`, as shown in the figure below.

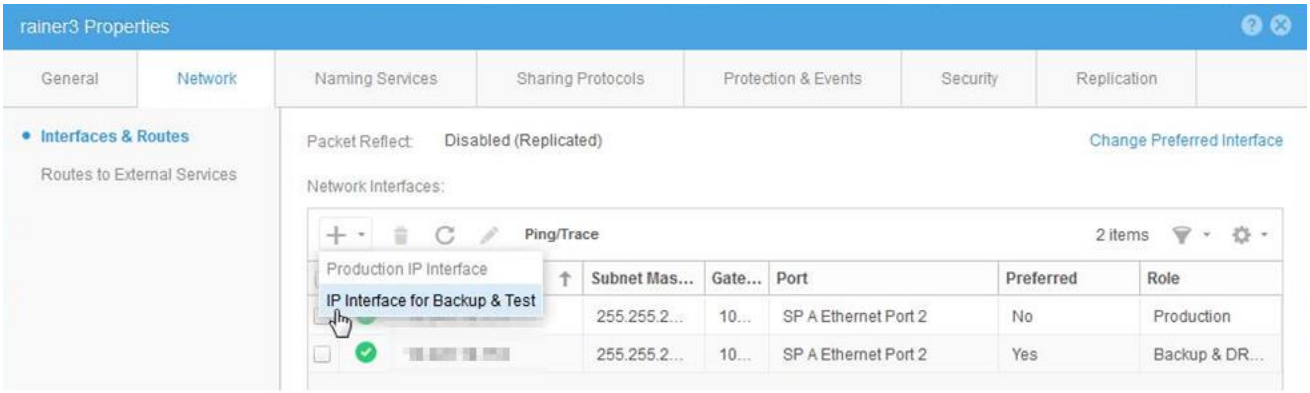
```
- PuTTY
16:49:35 service@Chen2390 spa:~/user> svc_nas Proxy_NAS_Server -proxy_share -show

Proxy_NAS_Server : commands processed: 1
command(s) succeeded
output is complete

 The proxy configuration allows accessing the following NAS server(s):
  NAS server: NAS_Server  State: Started  Mode: Destination
    SMB share: FS -- target=NAS_Server path=/UTC_2018-11-13_15:58:57


Command succeeded


16:49:36 service@Chen2390 spa:~/user>
```

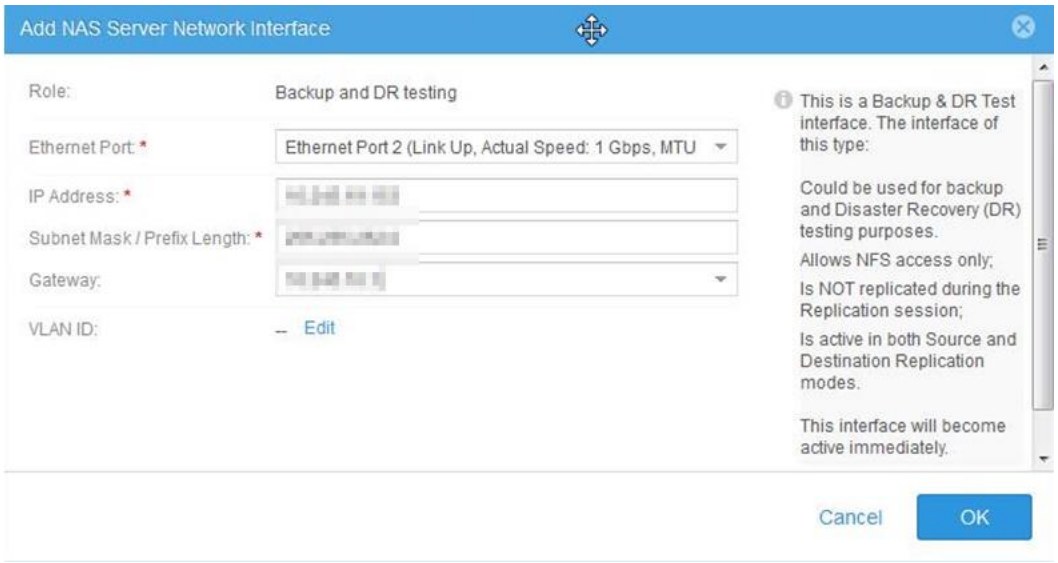
Once this is created, any domain user can access the snapshot by mapping the UNC path `\\Proxy_NAS_Server\FS`. The snapshot data is accessible for read/write access, as shown in the figure below.


FS
File
Home
Share
View
Network › Proxy_NAS_Server › FS ›
Search FS
Quick access
This PC
Network
Name
Date modified
Type
Size
Folder1
11/13/2018 9:17 AM
File folder
Folder2
11/13/2018 9:17 AM
File folder
Folder3
11/13/2018 9:17 AM
File folder
lost+found
11/13/2018 9:02 AM
File folder
4 items

BACKUP AND TEST INTERFACE

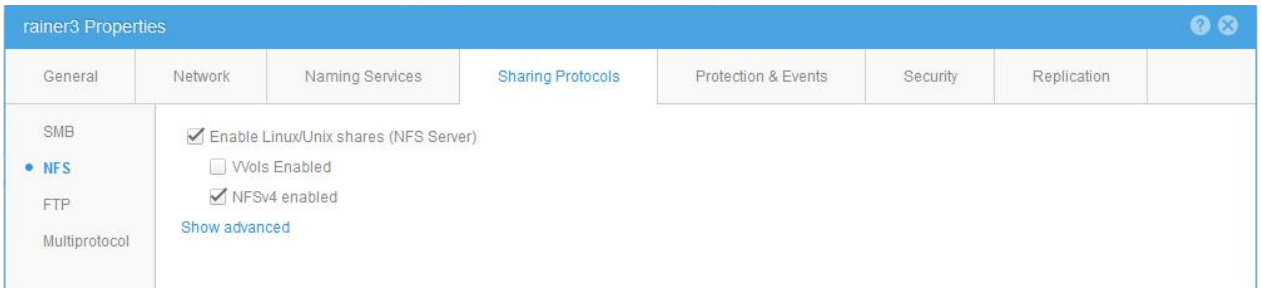
For NFS, FTP/SFTP, or NDMPCopy access, a “Backup and Test” interface must be created on the destination NAS server. This is necessary since the regular production interfaces are not available on a destination unless the NAS server is failed over.

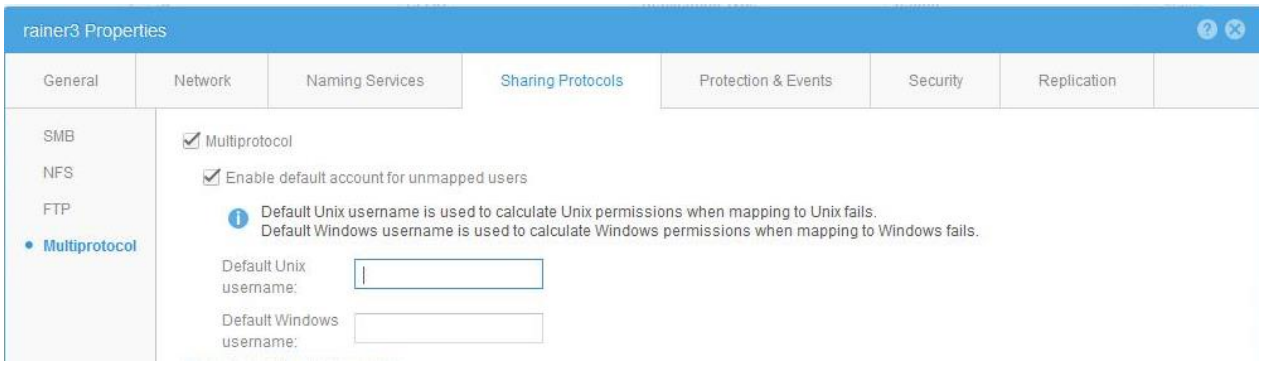




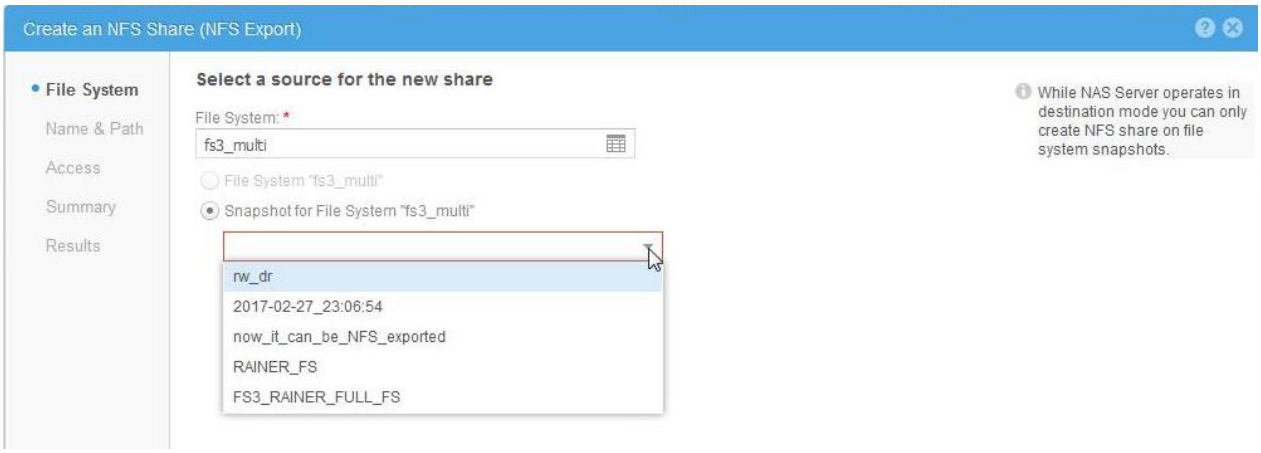
CONFIGURING NFS ACCESS

You can use NFS to access writeable snapshots of NFS file systems on the DR NAS server. If you want to use this method to access snapshots of SMB file systems, you will need multiprotocol configured on the primary NAS Server. The multiprotocol and NFS base configuration is applied on the primary NAS server and is automatically replicated to the DR NAS server:

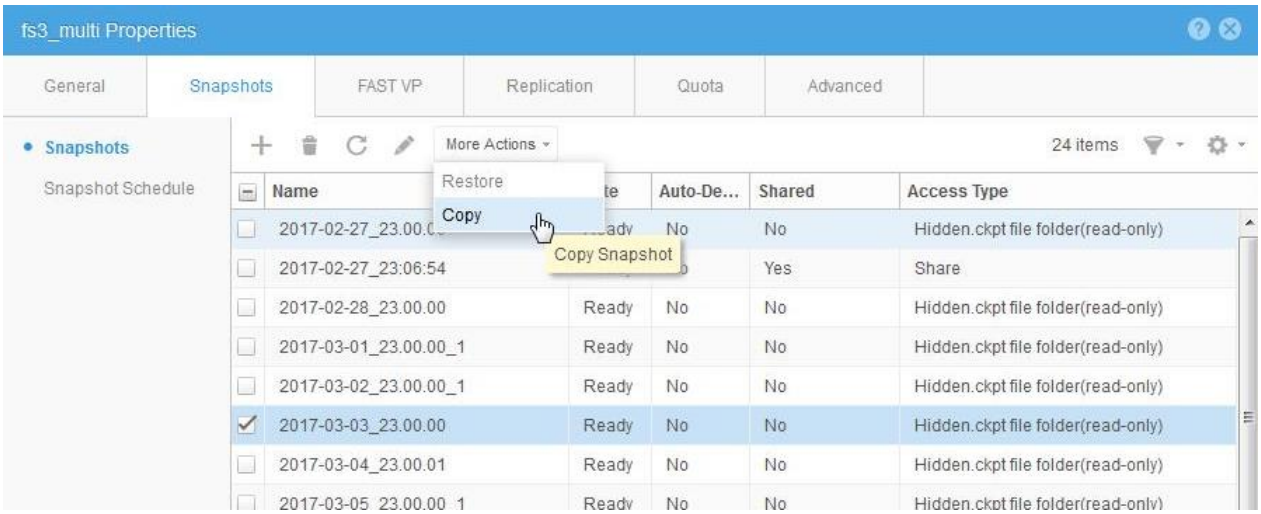


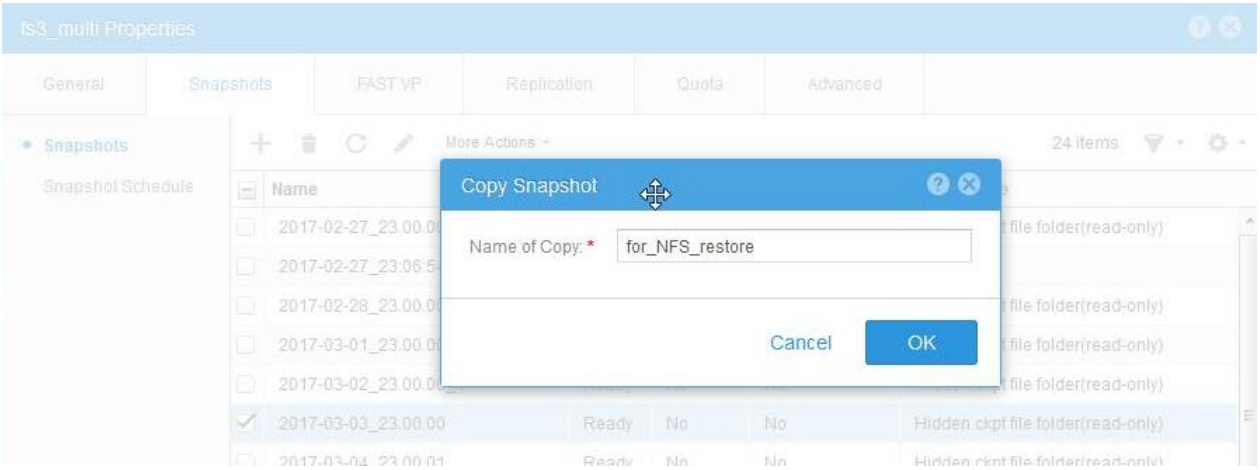


The next step is to create an NFS share on the DR NAS server:

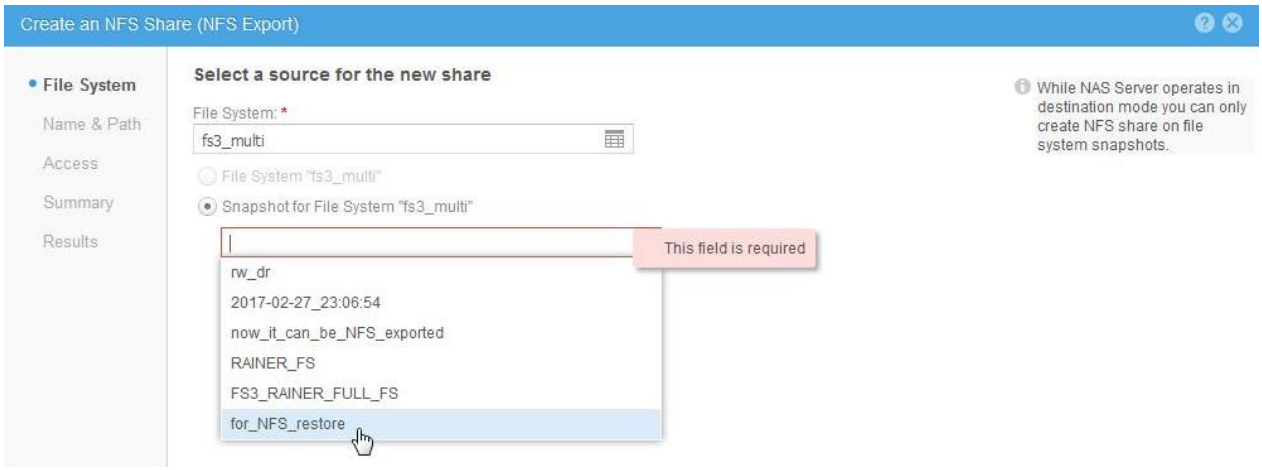


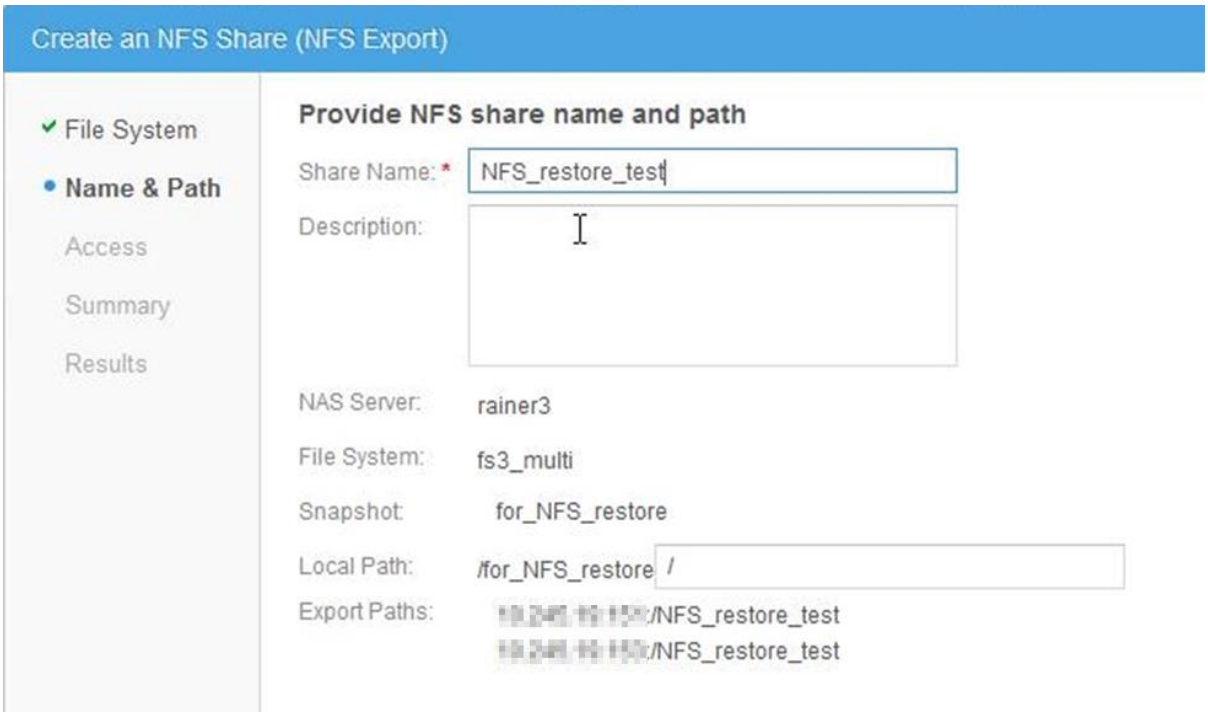
Note that only read-write protocol snapshots can be NFS exported. In order to access the data from a read-only snapshot, simply create a read/write snapshot from it. In the GUI, this is done via the “Copy snapshot” action in the Snapshots tab of the file system properties:



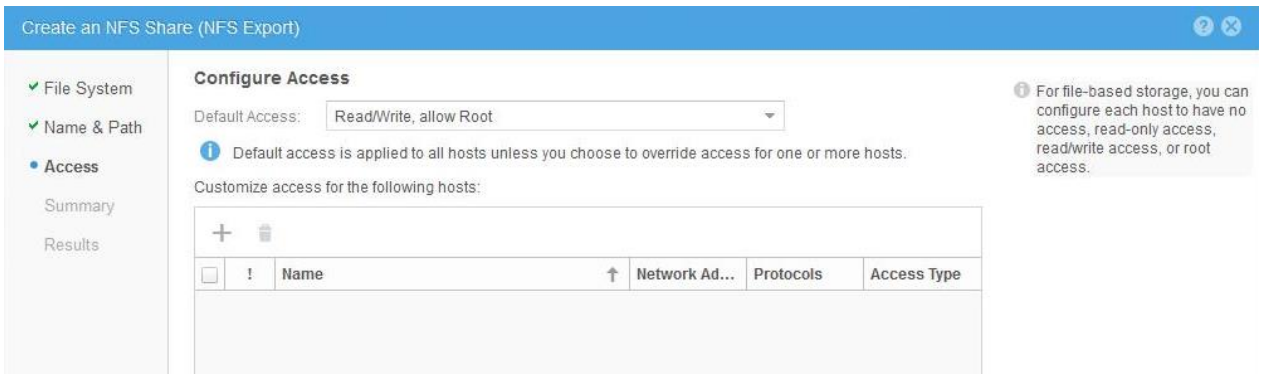


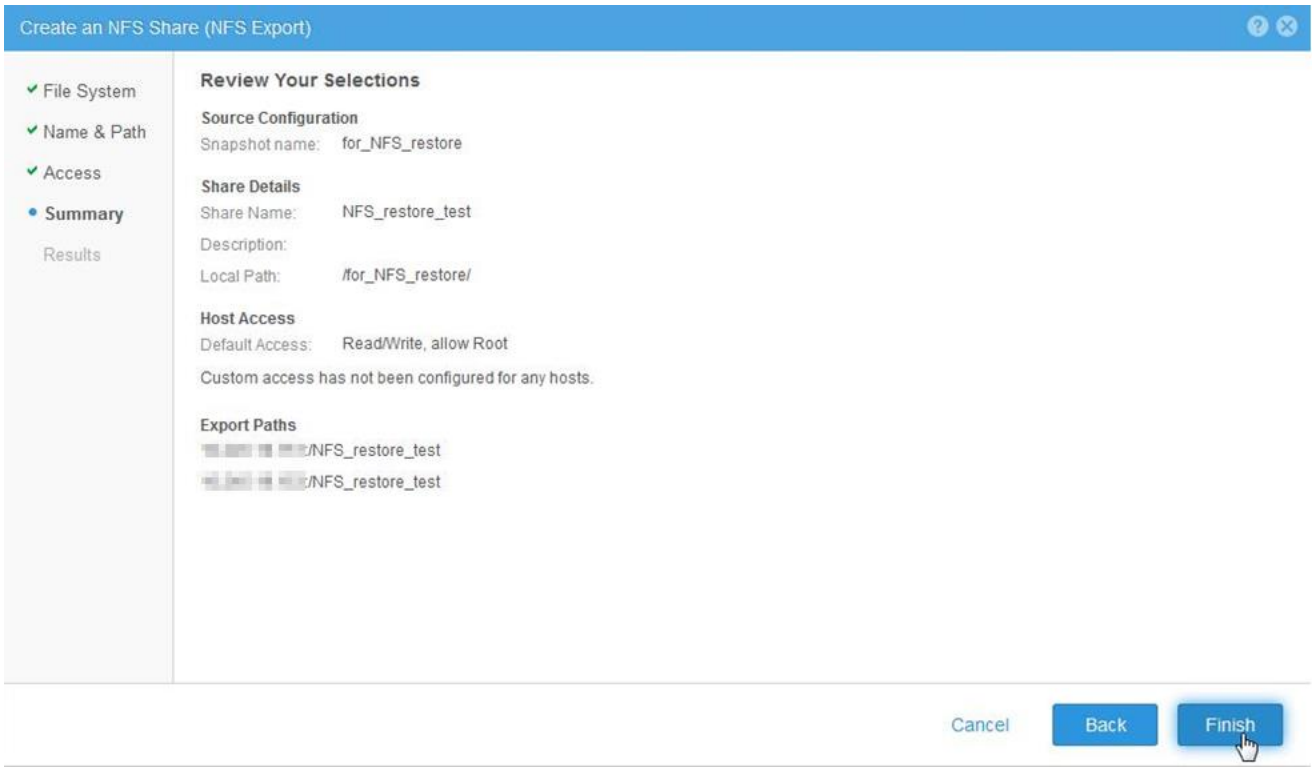
Now we can create a NFS share for it:





Configure access permissions for your NFS client. In this case, I am just simply exporting it with read/write + root permissions for everybody. This is not recommended for security reasons:





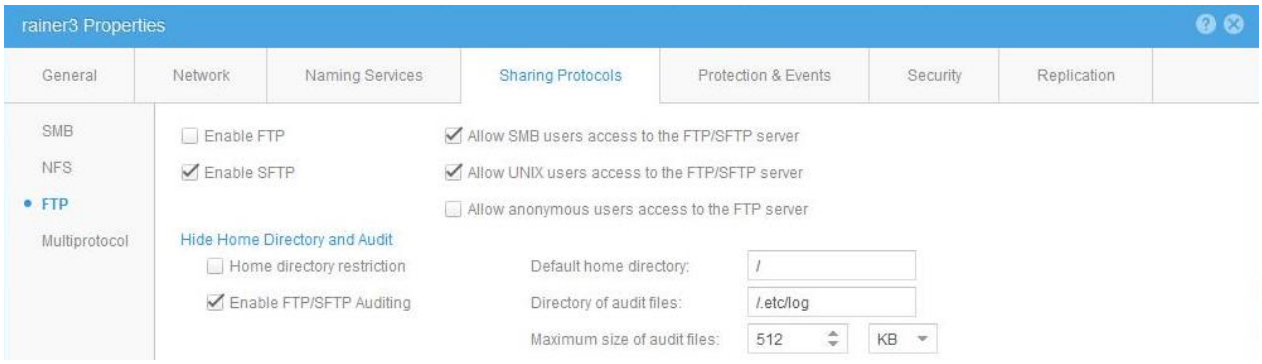
Let's look at the NFS client's point of view:

```
[root@centos-asia fs3_rw_dr]# showmount -e 10.0.0.1
Export list for 10.0.0.1:
/for_NFS_restore            (everyone)
/NFS_restore_test           (everyone)

[root@centos-asia fs3_rw_dr]# mkdir /mnt/NFS_restore_test

[root@centos-asia fs3_rw_dr]# mount 10.0.0.1:/NFS_restore_test /mnt/NFS_restore_test/

[root@centos-asia fs3_rw_dr]# ls -l  /mnt/NFS_restore_test/

total 64

-rw-r--r--.  1 root       root                0 Feb 28 06:12  aaa
-rwxr-xr-x.  1 root root          372 Feb 27 08:51  AclDedupDB
-rwxr-xr-x.  1 root root          477 Feb 27 08:51  AclRecordsDB
-rwxrwxrwx.  1 1001 1001            0  Feb 27 08:40  addfaf.txt
-rwxrwxrwx.  1 leberr               9  Mar  3 08:31  file_created_by_CIFS.txt.txt
-rwxrwxrwx.  1 1001 1001           12  Feb 27 08:22  leberr.txt - Copy.txt
-rwxrwxrwx.  1 1001 1001           12  Feb 27 08:22  leberr.txt.txt
drwxr-xr-x.  2 root root        8192  Feb 27 06:20  lost+found
drwxr-xr-x.  2 root root        8192  Mar  3 05:38  test
drwxrwxrwx.  2 leberr      leberr      152   Feb 27 17:03  test_fs3
drwxrwxrwx.  2 1001 1001        152   Feb 27 06:20  ttttttt
```

From here on, just use your regular UNIX commands to access and restore the data.

CONFIGURING FTP/SFTP ACCESS

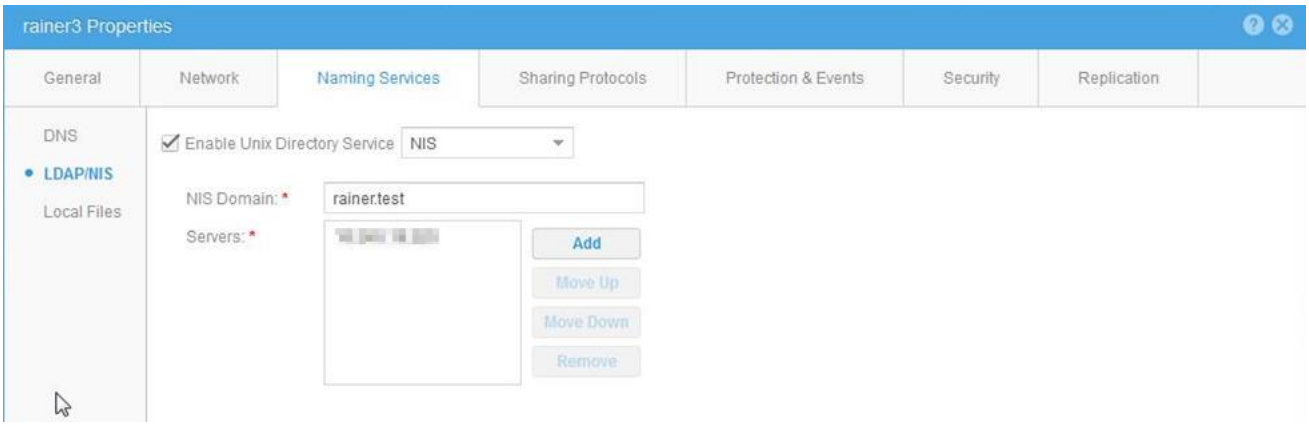
FTP/SFTP must be enabled on the source NAS server (production). Its configuration is automatically replicated to the destination NAS server (DR). Select the **NAS server → Edit → Sharing Protocols → Enable FTP/SFTP**. I recommend using SFTP instead of FTP since it is more secure (FTP transfers data and passwords in clear text).



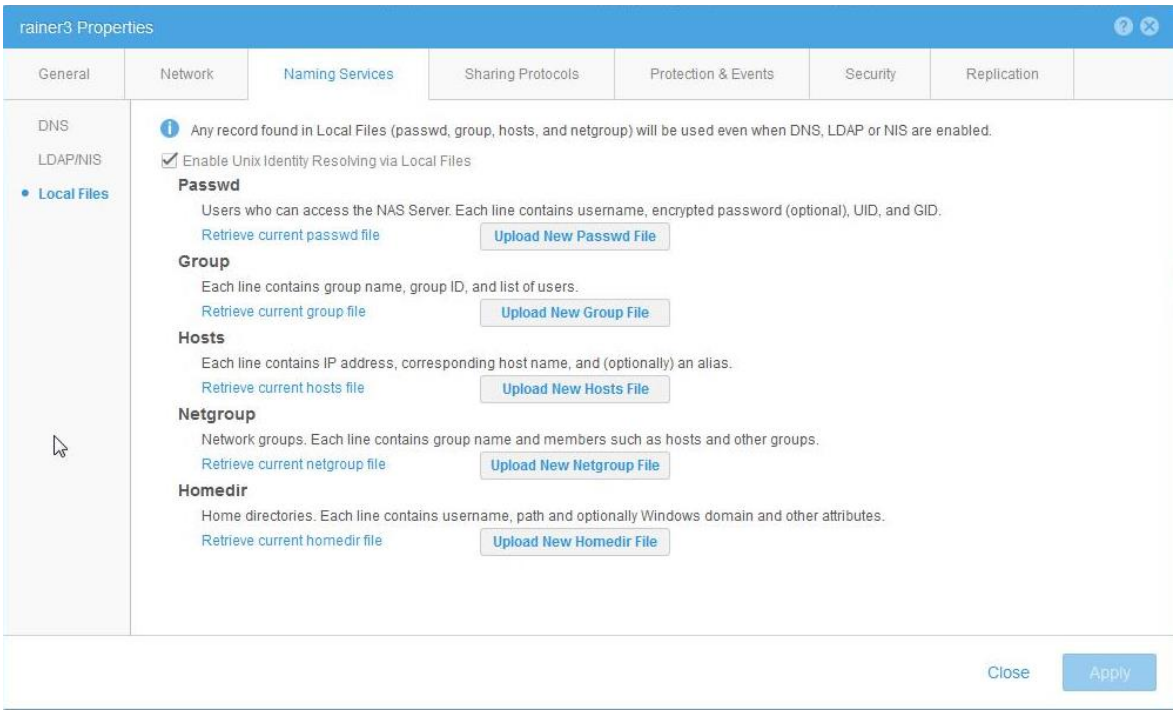
For SFTP authentication, we need to configure access for UNIX users in order to access the DR NAS server since CIFS authentication isn't possible there. You probably also want to uncheck the home directory restriction unless your user account only needs to access their home directory and nothing else.

For UNIX user authentication, the following sources can be configured in the Naming services tab:

- NIS
- LDAP
- Local password file



If you do not already have NIS set up, the simplest way is to use a local password file on the NAS server.



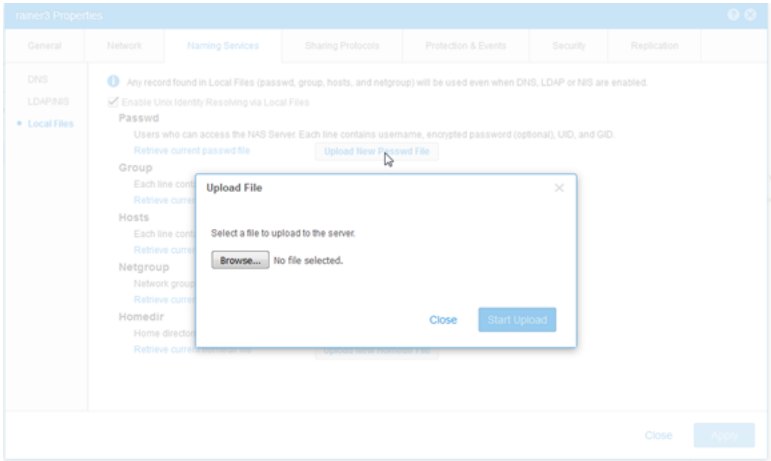
Download the current passwd file and add a line for the user account using an editor capable of handling UNIX files like Windows WordPad:

```
# The passwd file contains the users who can access the NAS server.

#

# Each line of the passwd file defines a user and has the format:

#   username:password:uid:gid:gcos:homedir:shell

# where:

# - username is the user's login name.

# - password is the encrypted password for the user.

# - uid is the user's unique numerical ID for the system.

# - gid is the unique numerical ID of the group to which the user belongs.

# - gcos, homedir and shell are not used and should be empty.

#

# Examples:

# vlad1:CDJcOn1/51jIM:124:100:::

# ivan2:TnH/56fy43hIp:125:100:::


admin:$6$InYgtqfx$QGqek/leEPvX0ThbQHN5nH5tKyQUXDQmpTTrslBJCOZ7UQL0A9eiK0tq4rSA9jUTXVruXxO4nOrwfI3sh
tCfA.:0:0::/home/service:/bin/bash
```

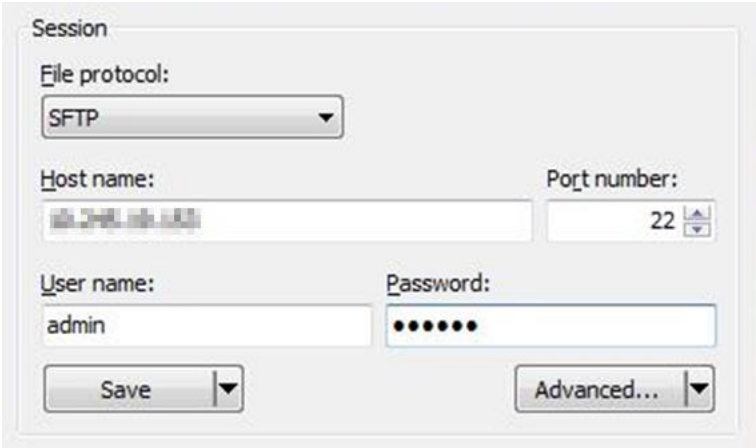
The highlighted part is the encrypted password (MD5 hash UNIX style). The easiest way is to get this is to generate a test account on a Linux system that you have root access on and then copy and paste it into the passwd file like this:

```
[root@centos-asia fs3_rw_dr]# useradd just_for_passwd

[root@centos-asia fs3_rw_dr]# passwd just_for_passwd

Changing password for user just_for_passwd.

New password:

Retype new password:

passwd: all authentication tokens updated successfully.

[root@centos-asia fs3_rw_dr]# grep just_for_passwd /etc/shadow

just_for_passwd:$6$RnQLp4pJ$iauafBJErkZccCwK2fBNXusdRlsMM4f1s5Si1N8nOs00hqQVIQqVzy5t6L5knPLVSOJmDcv
jWWRBTSuKHEYt7/:17231:0:99999:7:::

[root@centos-asia fs3_rw_dr]# userdel just_for_passwd
```

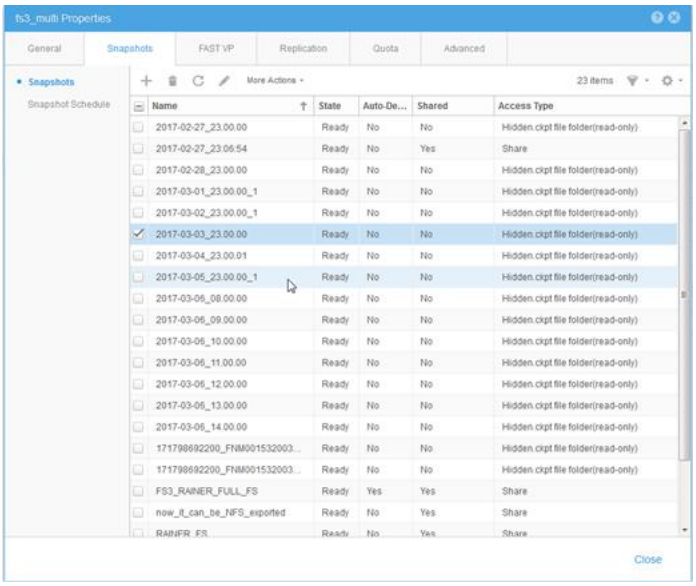
After that, upload the modified passwd file to the NAS server:

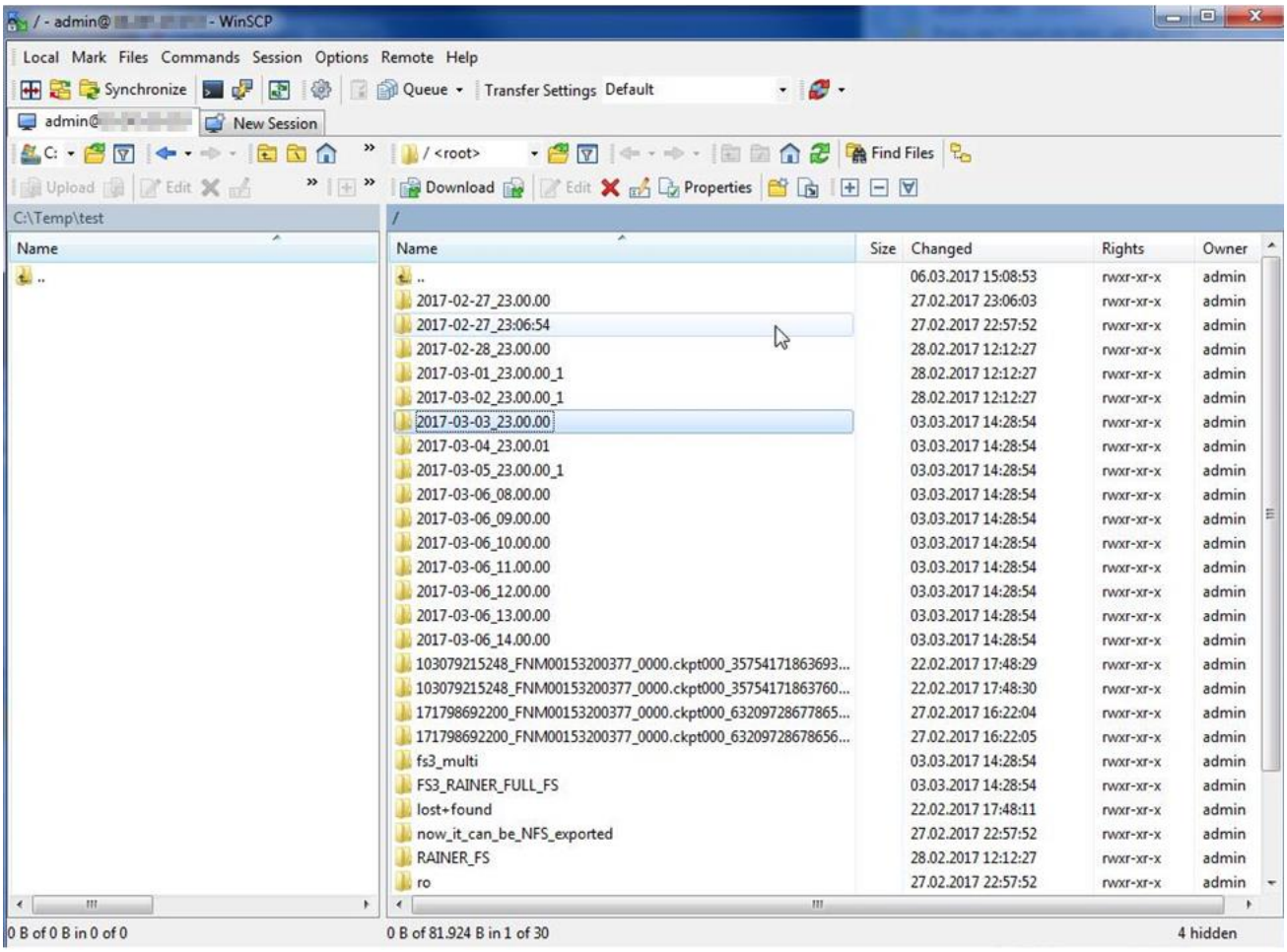


Now you can access your DR NAS server using any tool that supports FTP/SFTP, such as your web browser. For additional convenience, use a tool like WinSCP or Total Commander to connect to the IP address of the Backup & Test interface on the DR NAS server:



Without home directory restriction enabled, this will drop you into the root of the NAS server where then can navigate to the individual file systems and snapshots. Note that you will see each snapshot on the NAS server displayed as a directory on the root like this:

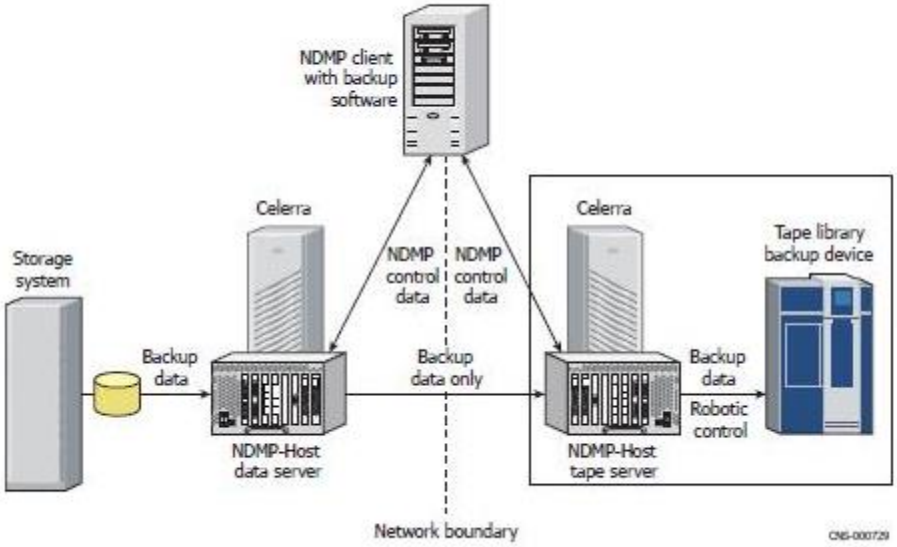




Note that when connecting through SFTP, the user credentials that are supplied are used for permissions purposes. The UNIX access rights mode bits are used to grant access to files and directories.

ACCESS VIA NDMPCOPY

Another option for restoring from any Unity system is via NDMPCopy. This basically creates a 3-way NDMP session where the source backs up the files via TCP/IP to the destination system, which restores them. Additional free capacity is required on the destination system to restore the data to. For NDMPCopy, both the source and destination work as a NDMP data server.



The advantage of using NDMPCopy is that it retains the CIFS file owner and ACLs, just like a NDMP backup would. It is recommended to run NDMPCopy from a Linux client that has connectivity to both the source and destination systems. A Linux version of NDMPCopy is available from Dell EMC Online Support.

https://download.emc.com/downloads/DL32451_NDMPCopy.zip

A couple of tips:

- You need to configure a NDMP password both on the source and destination NAS server
- Source path can be a file system or a snapshot
    - Check using NFS or FTP that it's a valid path
- Destination path has to be a writeable file system
    - You cannot write directly into root (/) since that is the NAS server root, which isn't writeable
- Destination path directory will be created automatically if it doesn't exist
    - Unless it's on the NAS server root
- NDMPCopy doesn't support a single file as the source
    - You need to restore at least a directory

RESTORE EXAMPLE

Restoring from a read-only manual checkpoint called “ro” of file system “fs3_multi” located on a read-only destination NAS server.

Restoring to a writeable file system fs1_multi on another Unity system into directory restored_fs3

```
[root@ centos-asia ~]$ ./ndmpcopy 10.0.0.1:/ro/test_fs3 10.0.0.2:/fs1_multi/restored_fs3 -sa
ndmp:NdmpNdmp1! -da ndmp:NdmpNdmp1! -sport 10000 -dport 10000 -level 0

Connecting to 10.0.0.1.
Connecting to 10.0.0.2.
10.0.0.1: CONNECT: Connection established.

10.0.0.2: CONNECT: Connection established.

10.0.0.1: LOG: SnapSure file system creation succeeds

10.0.0.1: LOG: server_archive: emctar vol 1, 13 files, 0 bytes read, 1983480 bytes written

10.0.0.1: HALT: The operation was successful!

Waiting for 10.0.0.2to halt too.

10.0.0.2: LOG: server_archive: emctar vol 1, 13 files, 1983480 bytes read, 0 bytes written

10.0.0.2: HALT: The operation was successful!

The transfer is complete.

Elapsed time: 0 hours, 0 minutes, 7 seconds.
```