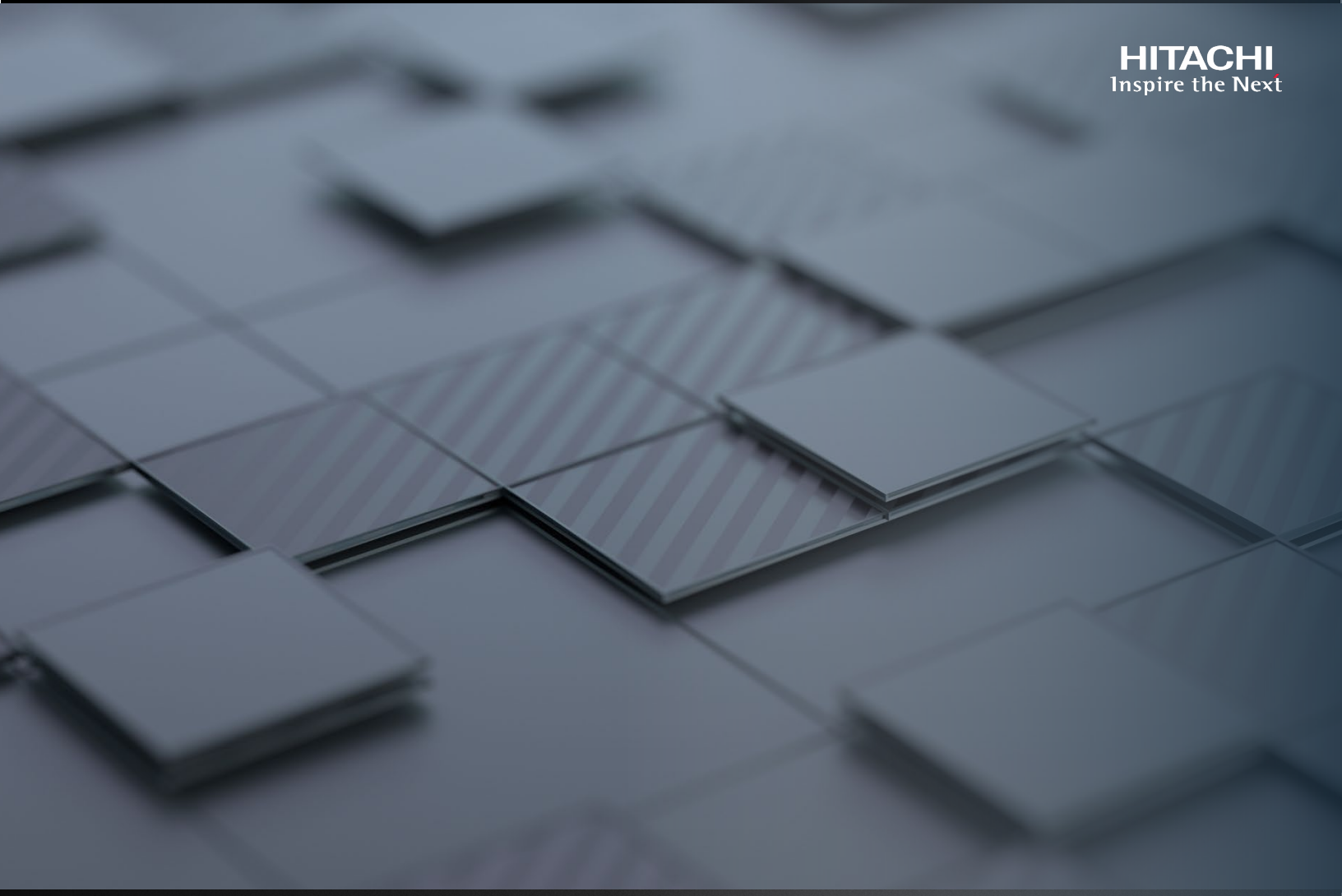


HITACHI
Inspire the Next

Disaster Recovery in Hybrid Cloud Environments with HNAS Object Replication

Using Hitachi Cloud Connect for Equinix

Hitachi Vantara
May 2023

HITACHI
Inspire the Next

Table of Contents

Notices and Disclaimer

About This Guide

This reference architecture documents how to set up a disaster recovery solution using Hitachi Network Attached Storage (HNAS) Object Replication. In addition, it describes the test procedures to validate the solution resiliency, which you can leverage for your proof-of-concept before deploying the solution.

Intended Audience

This document is intended for Hitachi Vantara staff and IT professionals of Hitachi Vantara customers and partners who are responsible for planning and deploying this type of solution.

Document Revisions

Revision Number	Date	Author	Details
v1.0	May 2023	Hitachi Vantara	Initial release

References

- HNAS Virtual SMU Administration Guide: https://knowledge.hitachivantara.com/Documents/Storage/NAS_Platform/14.4/NAS_Installation_and_Configuration_Guides/Virtual_SMU_Administration_Guide
- HNAS Administration Guide: https://knowledge.hitachivantara.com/Documents/Storage/NAS_Platform/14.4/NAS_Administration_Guides
- HNAS Replication and Disaster Recovery Administration Guide: https://knowledge.hitachivantara.com/Documents/Storage/NAS_Platform/14.4/NAS_Administration_Guides/Replication_and_Disaster_Recovery_Administration_Guide
- HNAS Replication Best Practices Guide: https://support.hitachivantara.com/download/epcra/hnas0700.pdf

Comments

Send us any comments on this document to GPSE-Docs-Feedback@hitachivantara.com. Include the document title, including the revision level, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

Thank you.

Executive Summary

This reference architecture documents how to set up a disaster recovery solution using HNAS Object Replication. HNAS Object Replication provides high-speed asynchronous replication and configuration of file systems such as SMB shares and NFS exports between data centers. HNAS operates at the file system level by copying the objects that make up the files, directories, and metadata. Object-level replication detects and replicates only changes; therefore, fewer system resources are used.

The environment used for this validation includes an HNAS 5300 cluster with a Hitachi Virtual Storage Platform E790 (VSP E790) storage system at the on-premises data center, and an HNAS 5300 cluster with a VSP 5200 storage system at the near-cloud data center. The near-cloud data center is an Equinix colocation.

We selected the Equinix colocation because it offers high-speed and low latency connections to major hyperscalers, such as Amazon Web Services (AWS). Hitachi Vantara collaborated with Equinix to offer a near-cloud hybrid solution called **Hitachi Cloud Connect for Equinix**.

This offering allows clients to locate Hitachi products such as the VSP storage system family and HNAS platform at Equinix International Business Exchange™ (IBX) data centers worldwide and includes the option for customers to procure this solution through an agreement and invoice, greatly simplifying and accelerating their time to market. By using Equinix IBX data centers and Equinix Fabric™ to interconnect sources of data to applications, organizations can locate their data stored on VSP storage systems and HNAS systems next to clouds to leverage hybrid- or multi-cloud capabilities while still maintaining physical control of the data.

If you want to discuss options for hosting a disaster recovery solution at Equinix, contact your Hitachi Vantara sales team. For more information, visit the Hitachi Cloud Connect for Equinix webpage at: https://hitachivantara.com/en-us/products/storage/flash-storage/cloud-connect-for-equinix.html.

Introduction

The environment used for this validation includes an HNAS 5300 cluster with a VSP E790 storage system at the on-premises data center and an HNAS 5300 cluster with a VSP 5200 storage system at the near-cloud data center. The near-cloud data center is an Equinix colocation. The HNAS file services (SMB shares and NFS exports) were accessed by using Windows and Linux virtual machines in the two data centers. In addition, we used Equinix Fabric to provide AWS EC2 instances access to the data on the secondary HNAS cluster.

Our hybrid-cloud environment consists of three domains as shown in in *Figure 1*.

- An on-premises data center, located in Englewood, Colorado.
- A near-cloud Equinix colocation data center (named SV5), located in San Jose, California.
- A cloud hosted by AWS in Northern California.

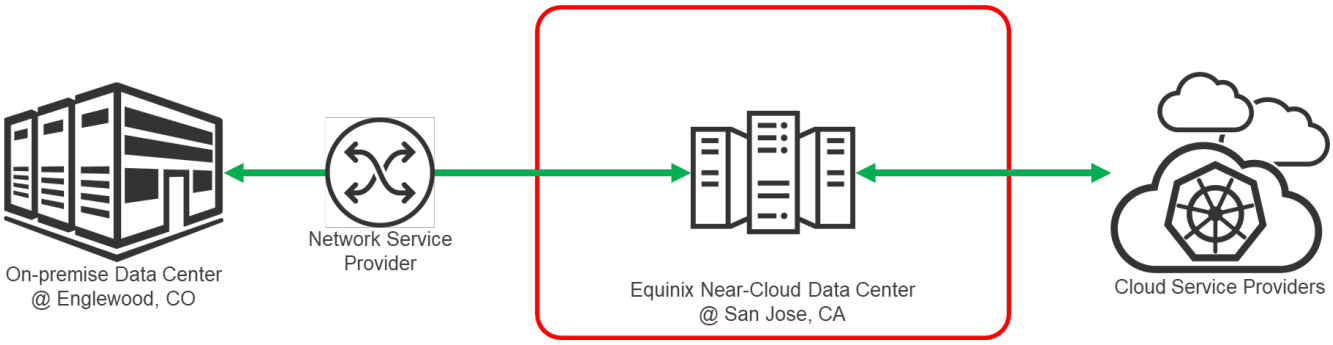


Figure 1: *Hybrid Cloud Environment*

Note: The information shared here is specific to our requirements. It can be used as a guideline or a starting point, but we recommend conducting a proof-of-concept in a non-production, isolated test environment matching your production environment before implementing this solution.

Solution Overview

HNAS Object Replication provides a high-speed means of asynchronously replicating file systems and related configurations, such as SMB shares and NFS exports, between data centers. It operates at the file system level by copying the objects that make up the files, directories, and metadata. Object-level replication detects and replicates only changes so less system resources is used.

The first time a replication is performed, a snapshot is taken (the initial snapshot), and the first replication operation replicates all objects on the source to the target. All following (incremental) replications take a snapshot of the changes to the file system and replicate only the objects that have changed.

The replicated files are immediately available for use in a disaster recovery situation. Additionally, the roles of the source and target HNAS systems can be reversed, allowing the target system to quickly take over the responsibilities of the source system.

Benefits

The following describes the benefits of a disaster recovery solution using HNAS Object Replication:

- Resume business operations quickly when a disaster shuts down the on-premises data center.
- Recover against ransomware attacks: granular, schedule-based snapshots allow the administrator to recover from a point in time before the attack.
- Maintain the replication status on both the source and the target file systems using object replication. If the replication connection is broken such as during a system shutdown or move, incremental replication can continue rather than requiring a full re-sync of the file system when the connection is re-established.
- HNAS provides SMB and NFS file services that are inherently compatible with virtual machines in the cloud, such as AWS EC2 instances. This enables the option of operating the secondary HNAS cluster with less physical compute hardware and leverage compute in the cloud as needed instead.

Key Components

The following lists the key components of the solution. The specifications are provided in the Hardware and Software section.

- Hitachi NAS Platform: Four HNAS 5300 systems were used. Two systems were configured in a cluster at the on-premises data center and two systems were configured in a cluster at the near-cloud data center.
- VSP storage system: A VSP E790 was used as the backend storage system for the on-premises HNAS cluster. A VSP 5200 storage system was used as the backend storage system for the near-cloud HNAS cluster.
- System Management Unit (SMU): A virtual SMU was used to manage the HNAS clusters.
- Network Switches: Cisco Nexus 9000 Series switches were used to connect the two data centers as well as to AWS Direct Connect. The following accessories are needed for establishing a WAN between the two sites.
- 10/25Gbase-LR-S Optics: Long Range transceivers to connect long distances.
- Single-Mode Fiber Cables: For long distance communications.
- Equinix Fabric: Equipment at the Equinix near-cloud data center for connecting to AWS cloud and other hyperscalers.
- AWS Cloud: Equipment at Equinix was connected to AWS cloud via a 10 Gbps Direct Connect link. On AWS, a Virtual Private Cloud was created in the region us-west-1.

Validation

This section describes the method, test environment, hardware and software, and test scenarios used in the validation.

Validation Method

To validate the solution, SMB shares and NFS exports were created on the HNAS file system at the on-premises cluster. New data was written to the on-premise file system prior to the replication operation, and after replication, the file system contents were verified at the near-cloud site to ensure data consistency.

Another test case involved creating an NFS datastore on the near-cloud HNAS filesystem and provisioning a Linux virtual machine on it. Afterwards, Object Replication was configured and a replication operation was run. On the near-cloud HNAS cluster, the target file system was promoted and verified that the Linux virtual machine was copied to the secondary HNAS cluster successfully.

High Level Diagram

Figure 2 shows the test environment used to run the validation.

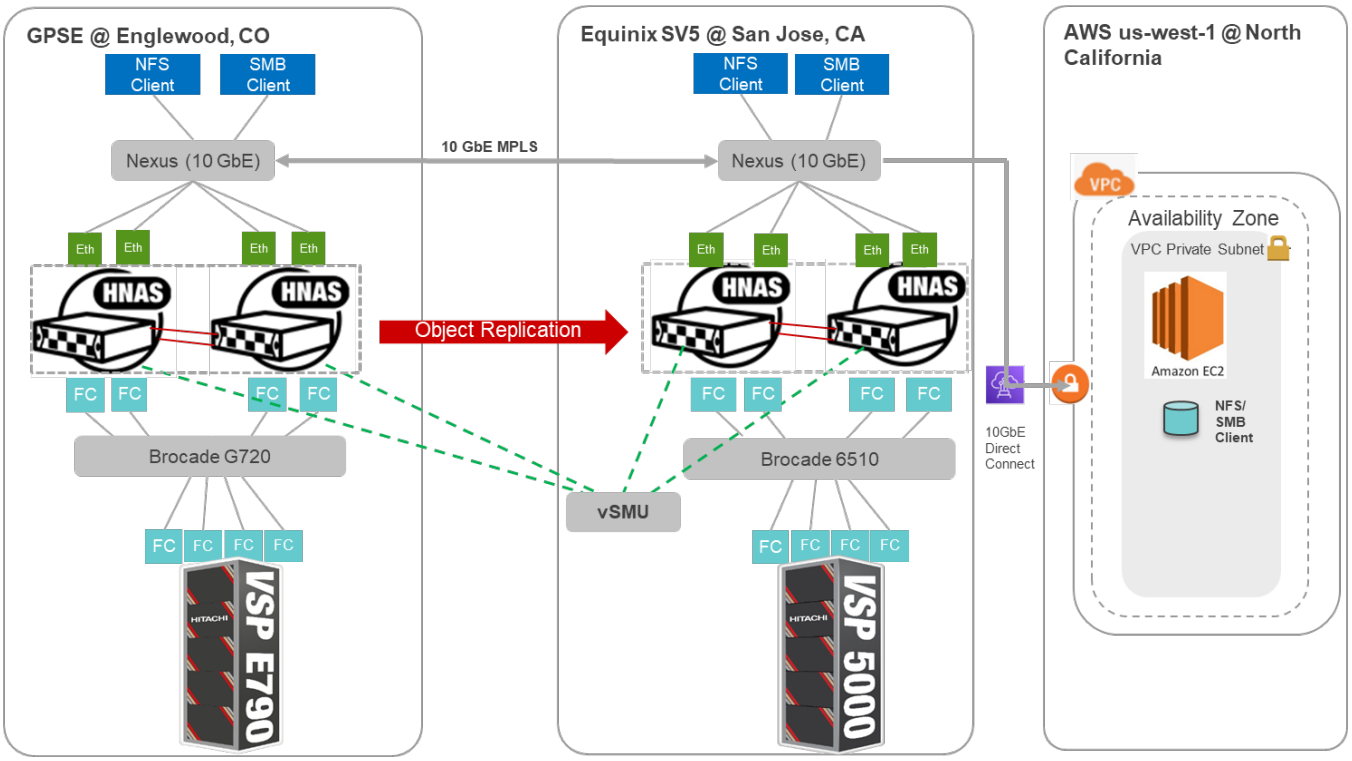


Figure 2: *Test Environment*

Hardware and Software

Table 1 provides the hardware specifications of the equipment used in this validation.

	Item	Description	Version	Function
On-Premises Data Center	**Hitachi VSP E790**	768 GB cache (2) 32-core MPUs (3) RAID6 6D+2P parity groups (4) 32 Gbps FC ports	SVOS RF 9.8.2 93-06-42-40/00-M062	Primary storage system
	HNAS 5300	HNAS 5300	Firmware 14.4.7322.05	2-node primary HNAS cluster
	Brocade G720	Gen 7 Fiber Channel switch	FOS 9.0.1a	Provided FC connectivity between the VSP E790 and the primary HNAS cluster
	Cisco Nexus 93180YC-EX	(48) 1/10/25-Gbps fiber ports (6) 40/100-Gbps QSFP28 ports	NXOS 9.2(3)	Network switch
Equinix Near-Cloud Data Center	**Hitachi VSP 5200**	1 TB cache (2) 20-core MPUs (4) RAID6 6D+2P parity groups (4) 32 Gbps FC ports	SVOS RF 9.8.2 90-08-61-00/00-M104	Secondary storage system
	HNAS 5300	HNAS 5300	Firmware 14.4.7322.05	2-node secondary HNAS cluster
	Brocade 6510	16 Gbps FC switch	FOS 8.2.1c	Provided FC connectivity between the VSP 5200 and the secondary HNAS cluster
	Cisco Nexus C93180YC-FX	Cisco Nexus C93180YC-FX 10 GbE Switch	NXOS 9.3(4)	Network switch

Table 1: *Hardware Components*

Table 2 provides the software specifications used in this validation.

Item	Version	Function
Virtual System Management Unit	14.4.7322.05	Manages HNAS clusters, replication policies and replication schedules
Red Hat Enterprise Linux	Red Hat Enterprise Linux 8.6	Operating system of virtual machines and Amazon EC2 instances used as NFS clients
Microsoft Windows Server 2019 Datacenter	Windows Server 2019 Datacenter	Operating system of virtual machines and Amazon EC2 instances used as SMB clients
KnowBe4 Simulator	2.2.1.3	Simulate ransomware infection

Table 2: *Software Components*

Table 3 provides the HNAS 5300 configuration details.

Item	Description
HNAS Model	HNAS 5300
HNAS Firmware	14.4.7322.05
Number of HNAS Nodes	2 per site
Number of System Drives	32
Capacity per System Drive	VSP E790: 4 TB VSP 5200: 6 TB
Number of Storage Pools	1
Capacity per Storage Pool	VSP E790: 128 TB VSP 5200: 192 TB
Number of File System	1
Capacity per File System	5 TB
Number of NFS Export per File System	1
Number of SMB Share per File System	1
Number of Backend FC Ports	2 per HNAS node
Number of Frontend 10 GbE Ports	2 per HNAS node
HNAS Deduplication	Enabled

Table 3: *HNAS 5300 Configuration Details*

Test Scenarios

Table 4 lists the test scenarios performed in the validation.

#	Description	Success Criteria
1	Prepare VSP storage systems for HNAS: 1. Provision (32) 4 TB DP volumes on VSP E790 storage system to the primary HNAS cluster. 2. Provision (32) 6 TB DP volumes on VSP 5200 storage system to the secondary HNAS cluster. Configure HNAS clusters: 1. Deploy the virtual SMU at Equinix near-cloud data center. 2. Register HNAS clusters as managed devices under SMU. 3. Create an Enterprise Virtual Server (EVS) on HNAS clusters. 4. Create the storage pool from VSP storage system volumes and create file system on HNAS clusters. 5. Create SMB network shares and NFS network shares on HNAS clusters. Prepare network clients: 1. Deploy one Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine at the on-premises data center. 2. Deploy one Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine at the Equinix near-cloud data center. 3. Deploy one Windows Server 2019 EC2 instance and one RHEL 8.6 EC2 instance on AWS cloud.	Environment is set up as per specifications.
2	Configure HNAS Object Replication: 1. Create the HNAS file system to use as replication target. 2. Create the Object Replication policy and schedule. 3. Trigger the replication schedule.	Replication is performed successfully.
3	Define multiple Object Replication schedules: 1. Replicate every six hours. 2. Replicate daily at 04:00.	Replication policies co-exist and run successfully.
4	Perform planned outage: 1. Fail over to the near-cloud data center by promoting Object Replication target file system. 2. Ensure that AWS clients can access and write to the promoted file system. 3. Fail back to the on-premises data center.	• Target file systems is promoted, allowing data to be accessed at near-cloud data center. • New data is replicated back to the primary HNAS cluster.
5	Recover from an unplanned outage: 1. Abruptly disable the data connection at the on-premises data center (or similar method) to create an unplanned outage. 2. Identify the desired file system version to recover. Promote the desired version. 3. Ensure that clients can access file shares on the promoted file system.	Target file systems can be promoted as primary filesystem.
6	Migrate virtual machine using object replication: 1. Create an NFS datastore with a file system on the primary HNAS cluster and provision a virtual machine on the datastore. 2. Configure an HNAS Object Replication policy for the file system. 3. Promote the target file system on the secondary HNAS cluster. 4. Mount the NFS datastore with the promoted file system. 5. Register the virtual machine to an ESXi host in the near-cloud data center.	Virtual machine can be migrated by HNAS Object Replication.
7	Recover from a ransomware attack: 1. Prepare a sample virtual machine running on HNAS NFS datastore. Configure an HNAS Object Replication policy for the file system. 2. Simulate a ransomware attack. 3. Recover by reversing the HNAS Object Replication using a clean snapshot on the secondary HNAS cluster.	Revert to clean virtual machine from replicated data.

Table 4: *Test Scenarios*

Guidelines and Recommendations

This section describes the lessons learned from this validation, along with guidelines and recommendations.

- Object Replication only works at the file system level. All file systems are replicated using Object Replication; therefore, you cannot select individual files or directories for replication.
- During a disaster recovery failover, target file systems are not accessible until they are promoted. Because the file system is replicated as constituent objects, the file system may appear to be corrupted if you attempt to access it during a replication operation before all file system objects are replicated.
- Ensure that the replication target file system is as large as the source file system so everything can be replicated. This is especially important if there are more snapshots because they consume more capacity on the target file system.
- For snapshot rule-based replications, the schedule for the snapshot rule must ensure that a snapshot is created before the replication runs, so the new snapshot is available for the replication operation.

  For example, sometimes an administrator may want to keep hourly snapshots for the last day and daily snapshots for the last month on the replication target. This can be achieved with two policies between the same source and target file systems. The first policy would use a destination snapshot rule with a queue size of 24 and be scheduled hourly. The second policy would use a destination snapshot rule with a queue size of 30 and be scheduled daily. Precautions must be taken with the scheduling to ensure that the daily policy does not start while the hourly policy is running because this would prevent it from running.
- When creating the file systems to use with Object Replication, note the following considerations regarding the source and target file systems:
  - File systems at the source must have access points enabled.
  - File systems at the target must be formatted as a replication target.

Validation Results

This section contains specific steps and screenshots for each test scenario.

Test 1: Prepare the Environment

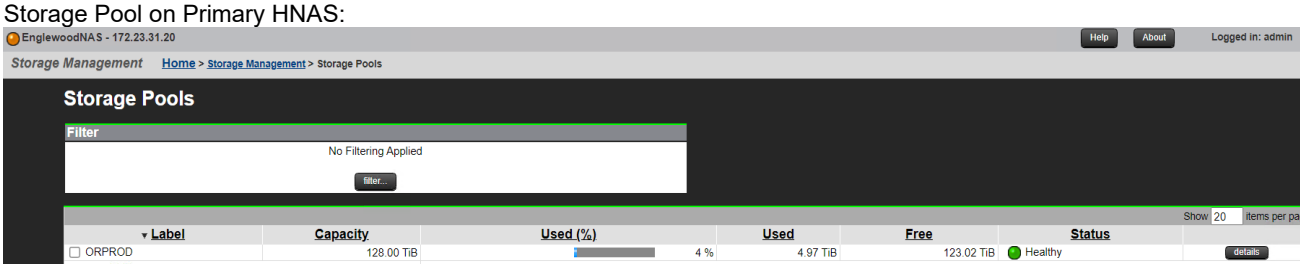
This test case describes the configuration of the components used in the validation.

Prerequisites

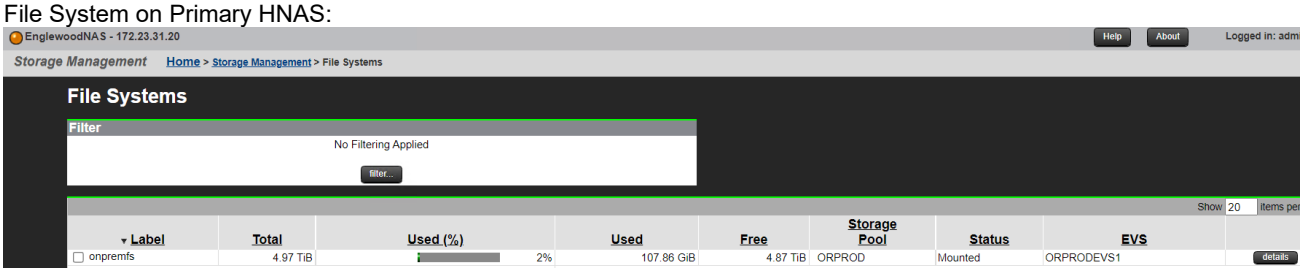
Note that the following prerequisites are outside the scope of this document, so we do not describe them in detail.

- Physical LAN and FC connections for HNAS clusters.
- Virtual SMU: See Installing and Configuring Virtual SMU.
- Configure HNAS clusters: See Create HNAS Cluster using NAS manager.
- Provision volumes from VSP storage systems to HNAS clusters.
- Create virtual machines that will act as file share clients:
  - On-premises data center: One Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine.
  - Near-cloud data center: One Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine.
  - AWS cloud: One Windows Server 2019 EC2 instance and one RHEL 8.6 EC2 instance.
- The following screenshots show the status of the storage pool, file system, and EVS created on the primary HNAS cluster at the on-premises data center. For steps on how to set up these objects, see the HNAS Administration Guide.

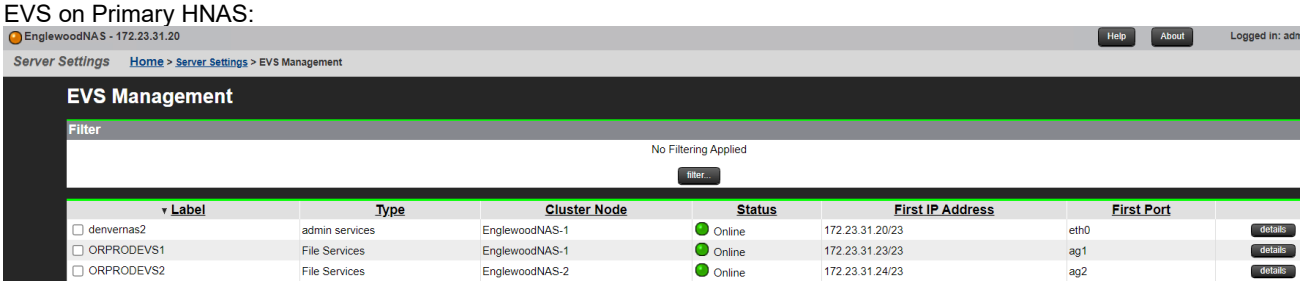
Storage Pool on Primary HNAS:



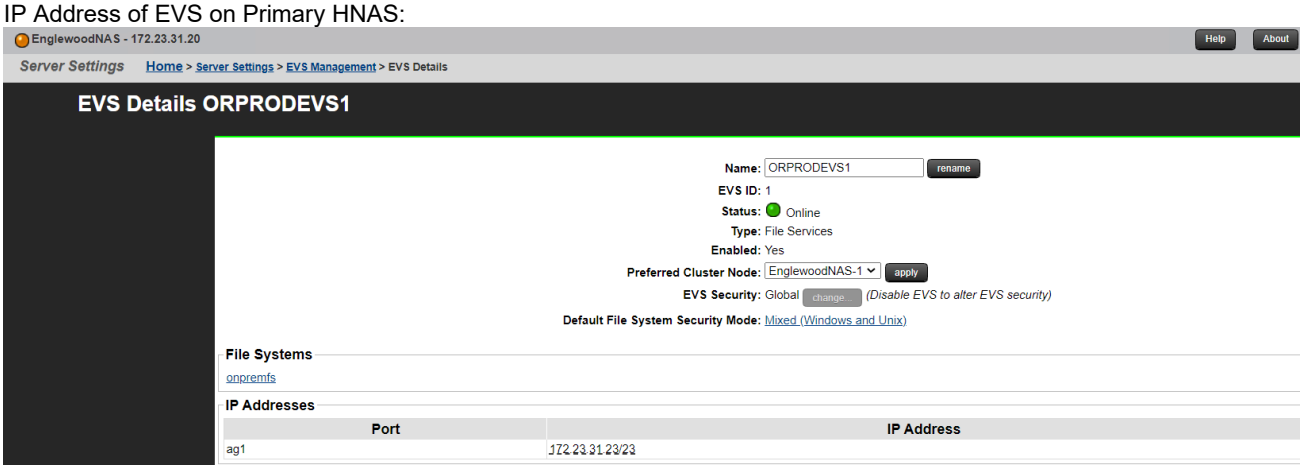
File System on Primary HNAS:



EVS on Primary HNAS:

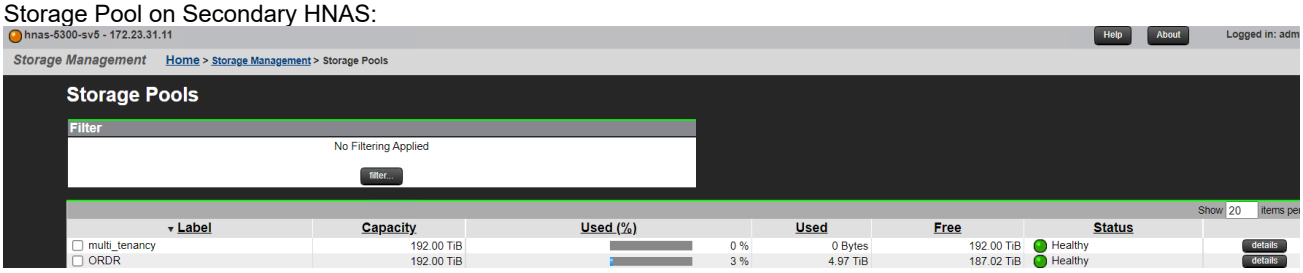


IP Address of EVS on Primary HNAS:

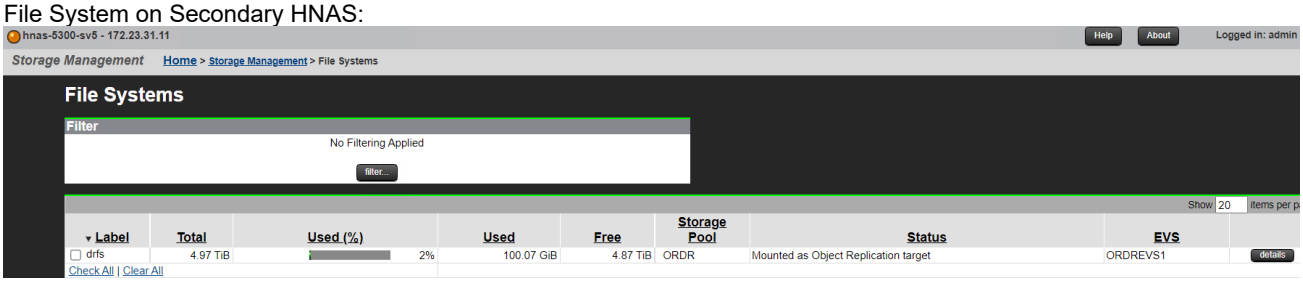


- The following screenshots show the storage pool, file system, and EVS created on the secondary HNAS cluster at the near-cloud data center:

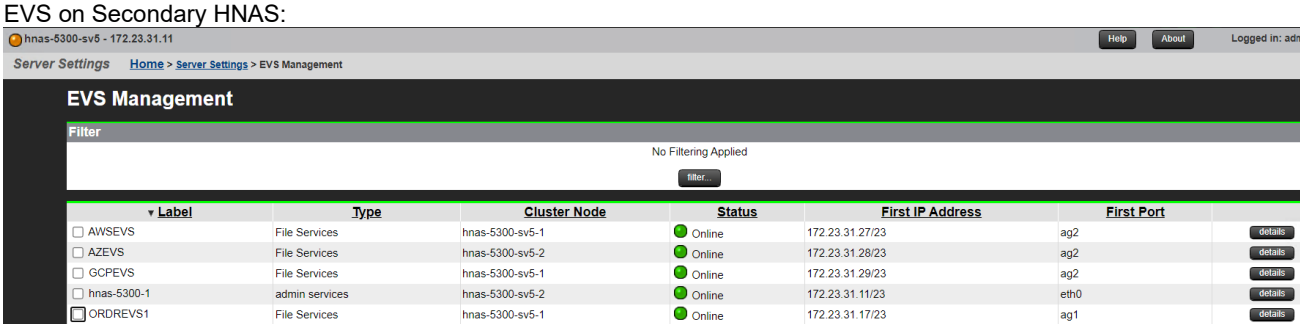
Storage Pool on Secondary HNAS:



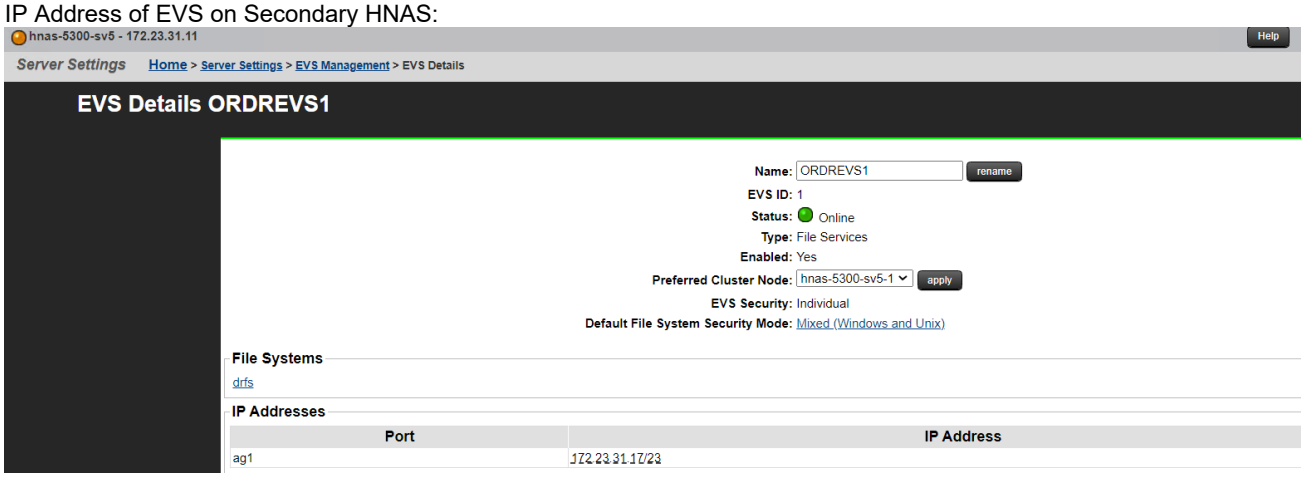
File System on Secondary HNAS:



EVS on Secondary HNAS:

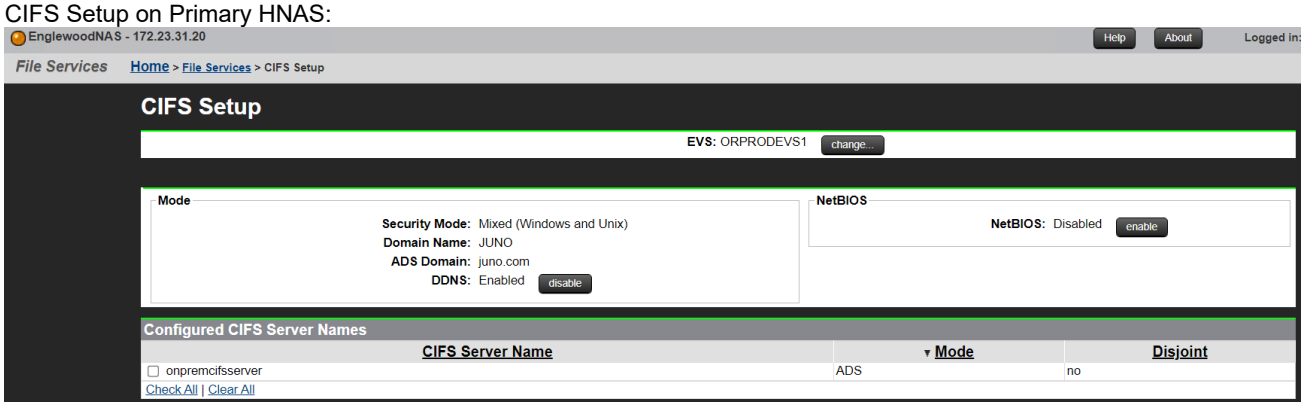


IP Address of EVS on Secondary HNAS:

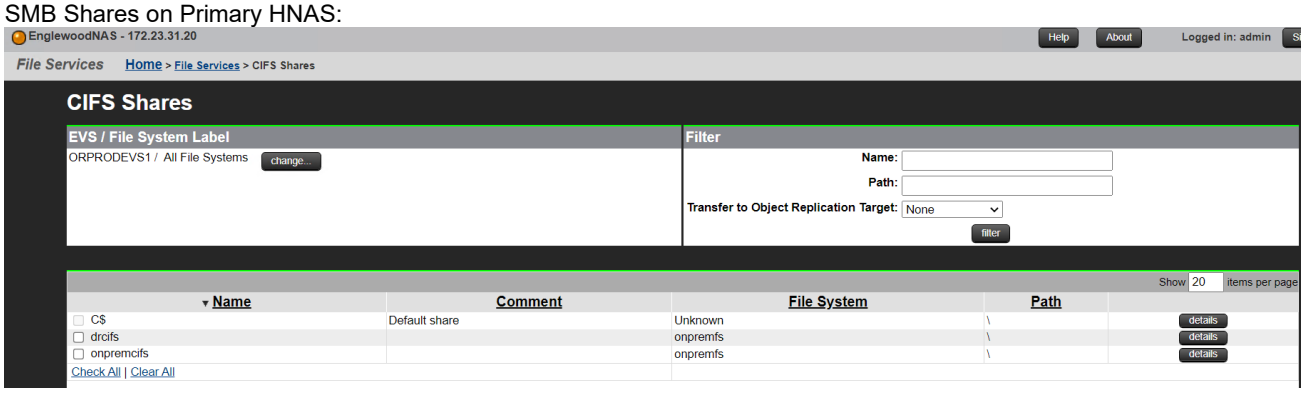


- To enable file sharing to the HNAS file systems, we created SMB shares and NFS exports. The following screenshots show these objects:

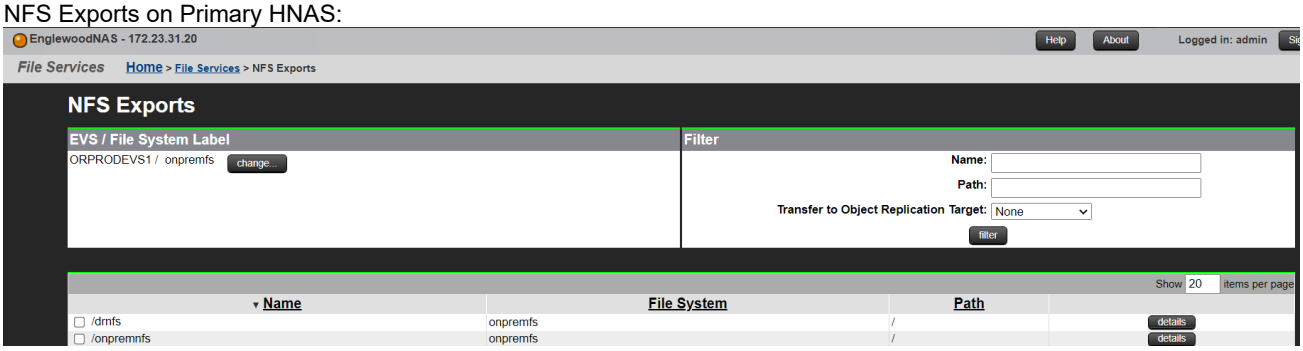
CIFS Setup on Primary HNAS:



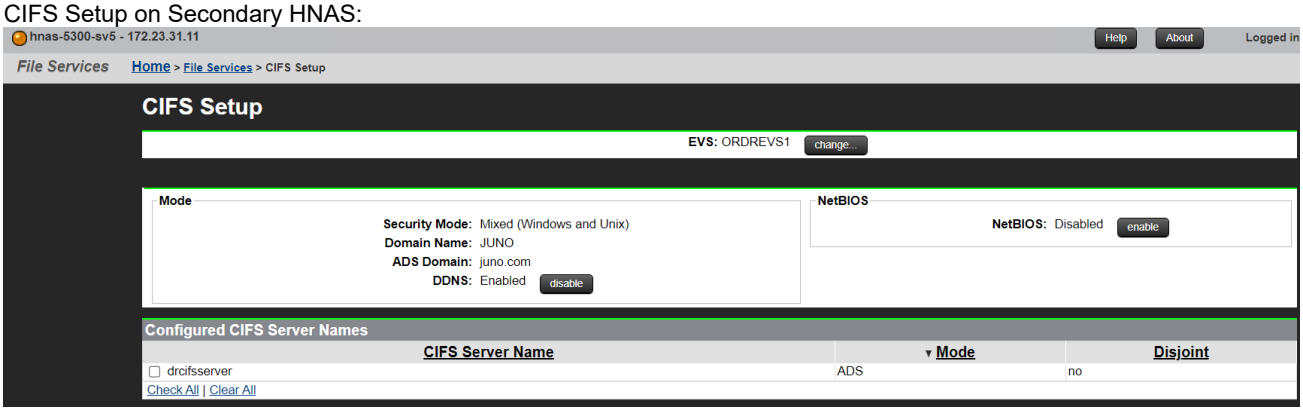
SMB Shares on Primary HNAS:



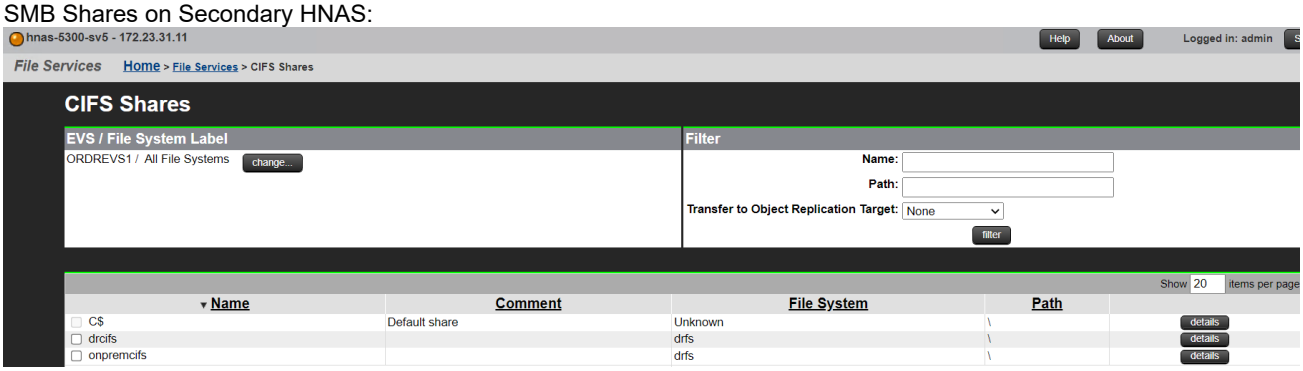
NFS Exports on Primary HNAS:



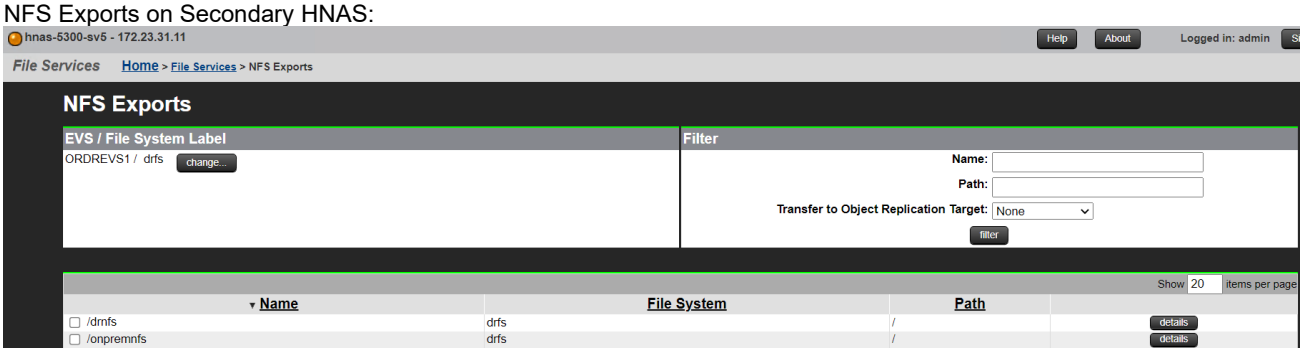
CIFS Setup on Secondary HNAS:



SMB Shares on Secondary HNAS:

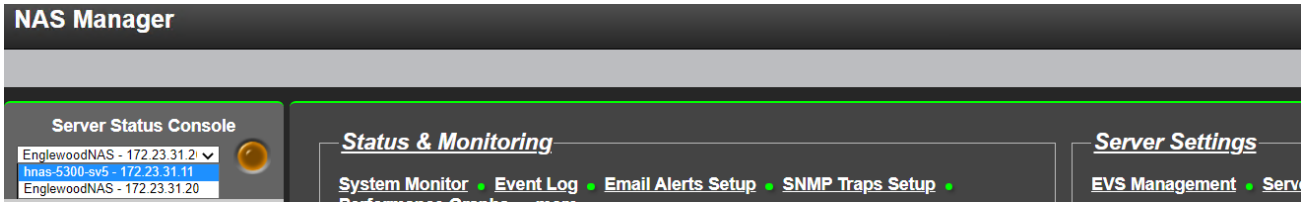


NFS Exports on Secondary HNAS:

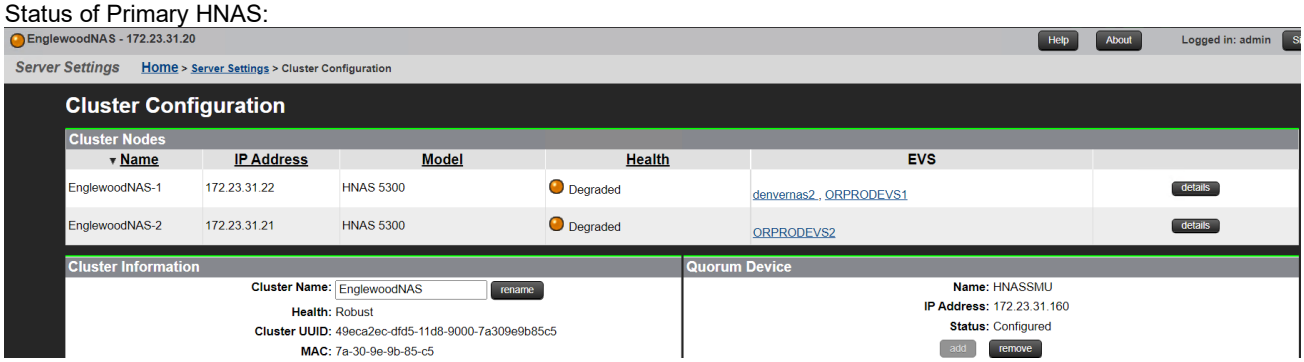


- The following screenshots show the HNAS clusters being managed by one virtual SMU. For usage details, see Virtual SMU Administration Guide.

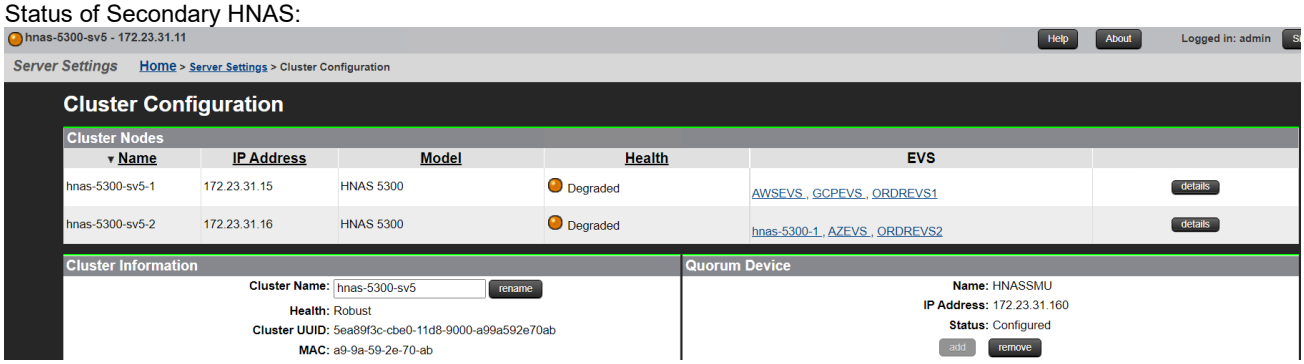
Virtual SMU:



Status of Primary HNAS:



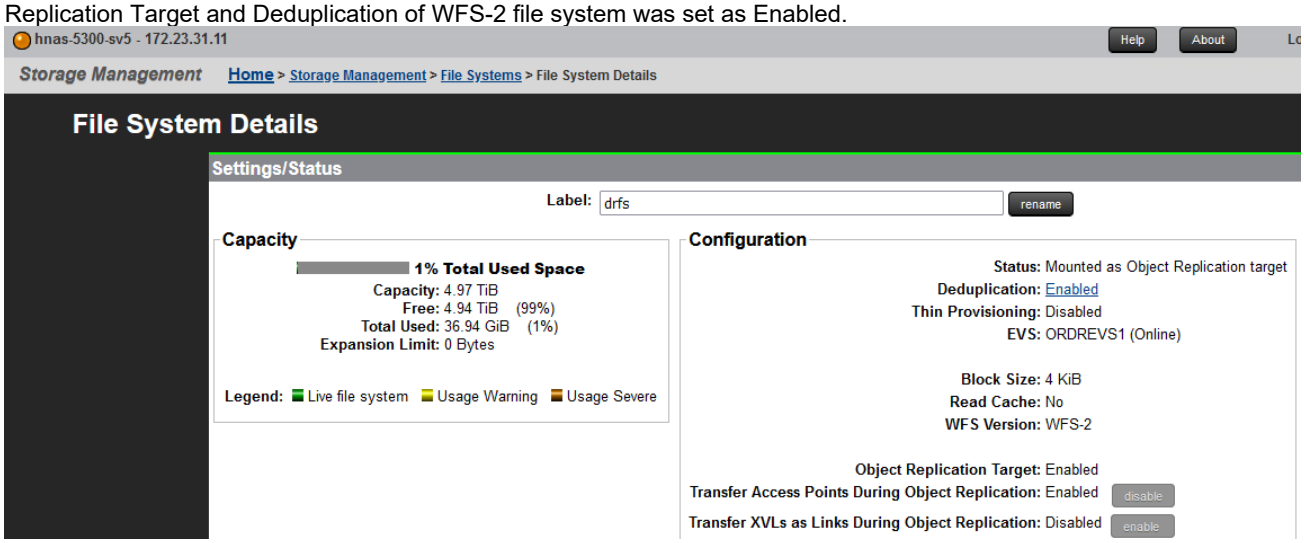
Status of Secondary HNAS:

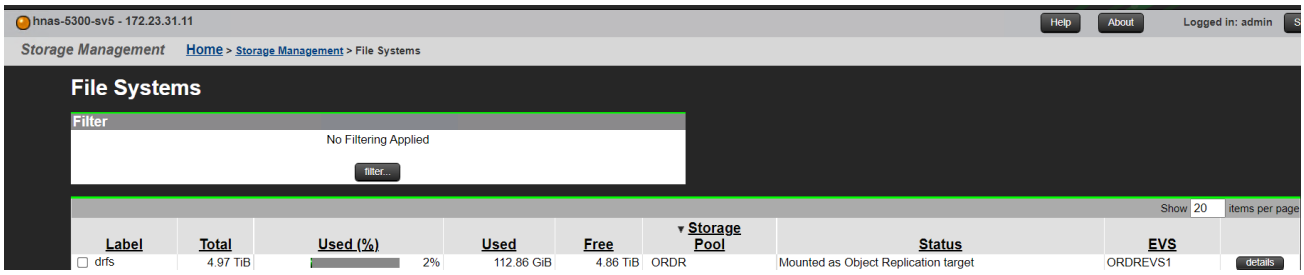


Test 2: Configure HNAS Object Replication

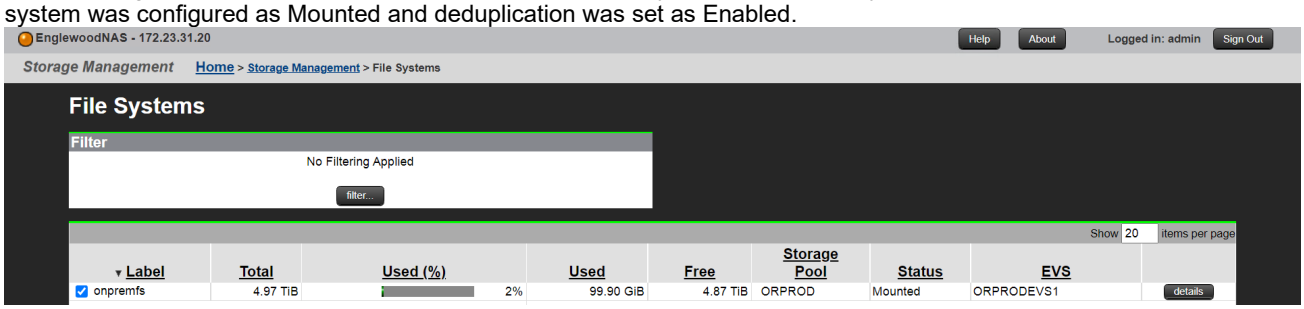
This test case describes the process of configuring an HNAS Object Replication policy, replication schedules and executing object replication between source and target site. For more information on Object Replication, see HNAS Replication Best Practices Guide.

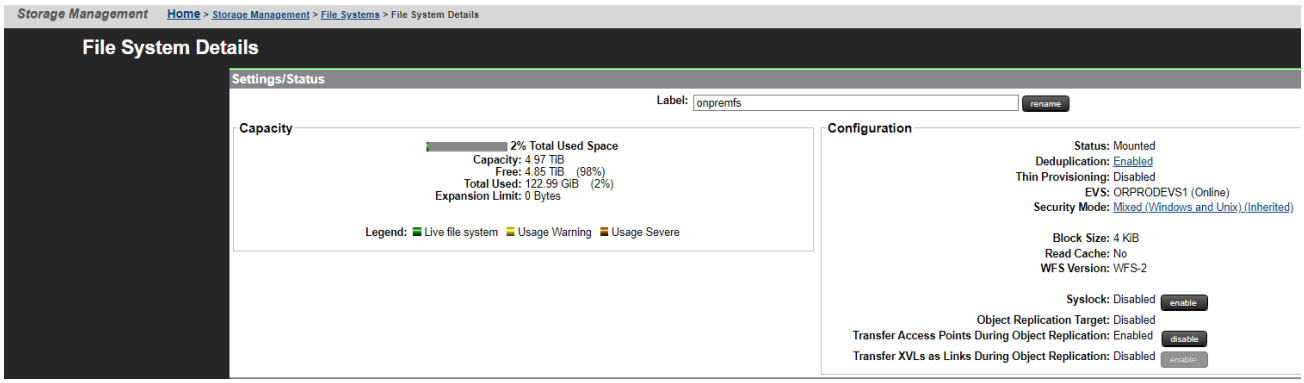
- The following screenshots show the configuration of the target file system on the secondary HNAS cluster. The Object Replication Target and Deduplication of WFS-2 file system was set as Enabled.





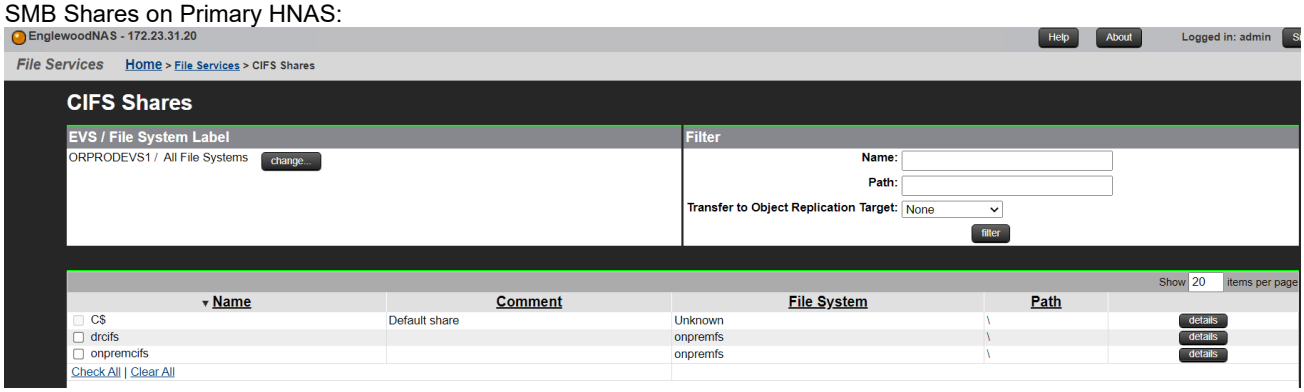
- The following screenshots show the status of the source file system on the primary HNAS cluster. The WFS-2 source file system was configured as Mounted and deduplication was set as Enabled.



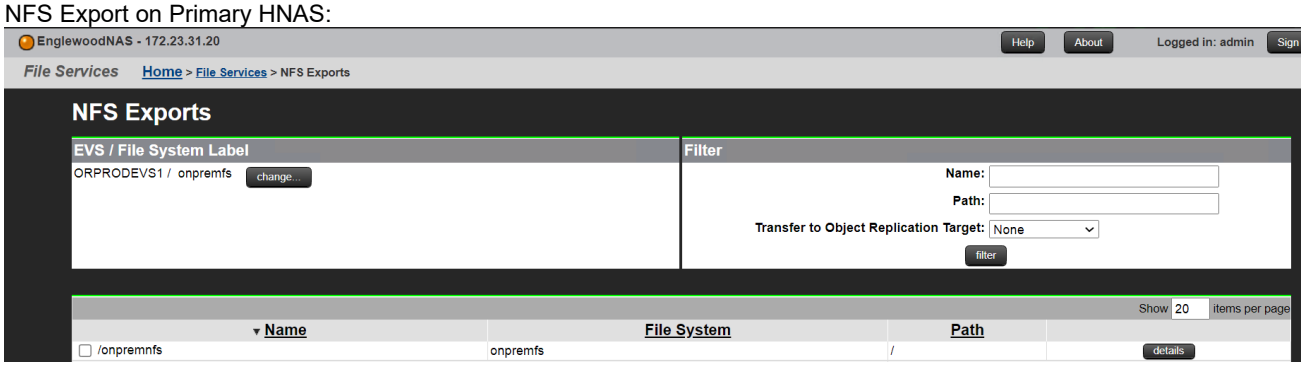


- The following screenshots show the status of the file services on the primary HNAS cluster:

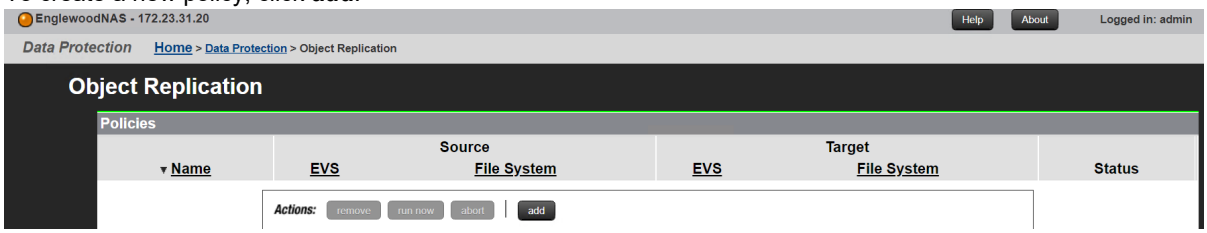
SMB Shares on Primary HNAS:



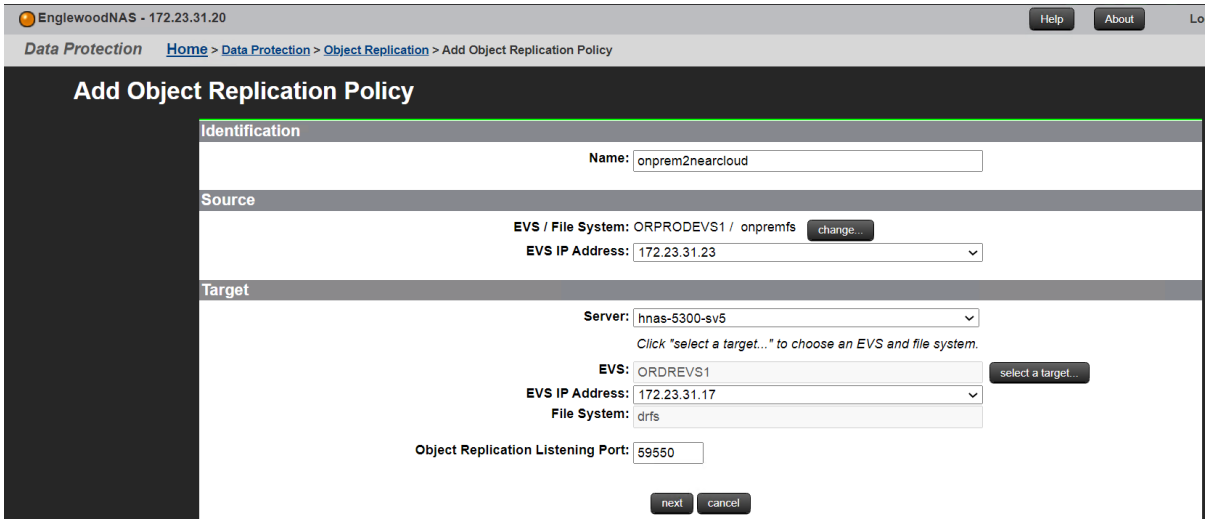
NFS Export on Primary HNAS:



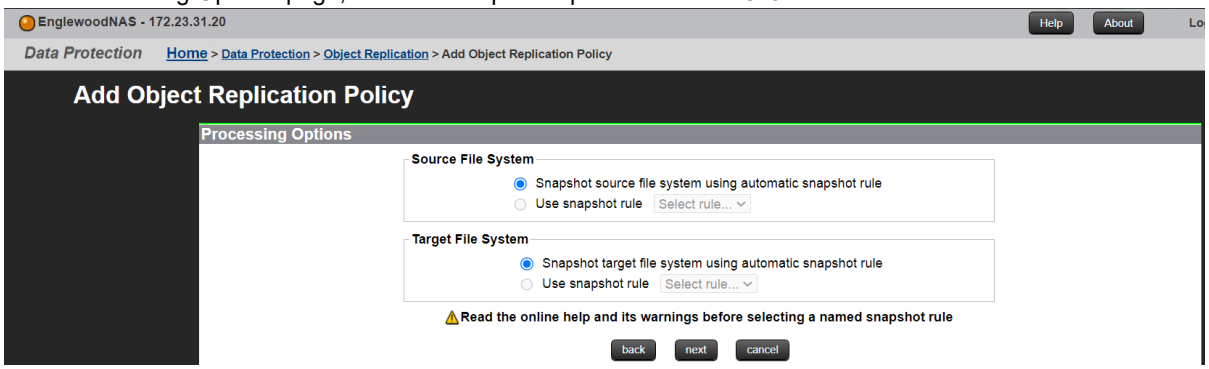
1. Log in to the SMU. From **Home**, click **Data Protection**, and then click **Object Replication**.
   a. To create a new policy, click **add**.



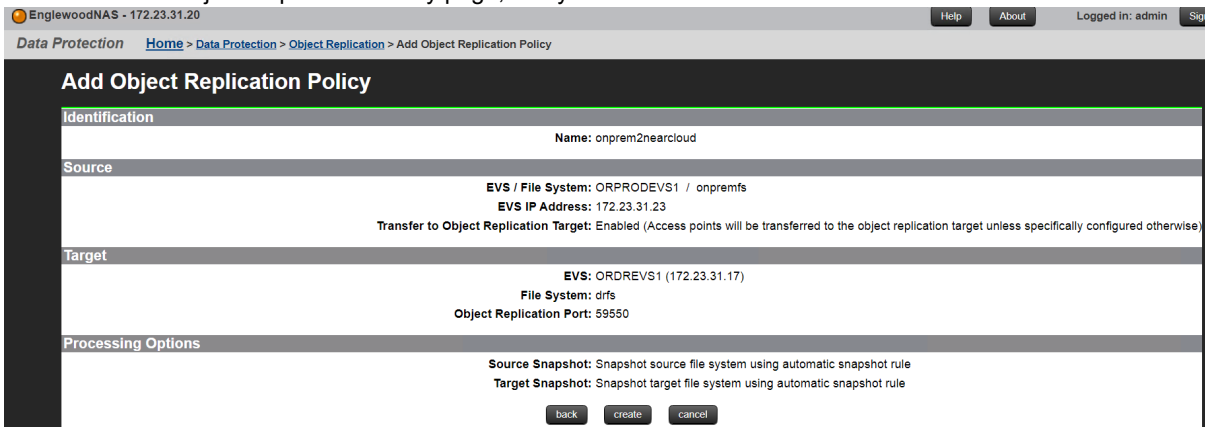
b. In the Add Object Replication Policy page, enter the required information such as source and target, and then click **next**.



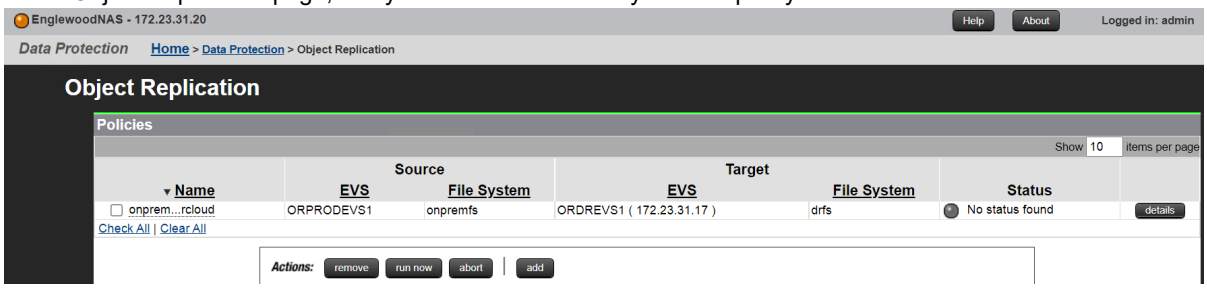
c. In the Processing Options page, select the required option and click **next**.



d. In the next Add Object Replication Policy page, verify the entered information and then click **create**.

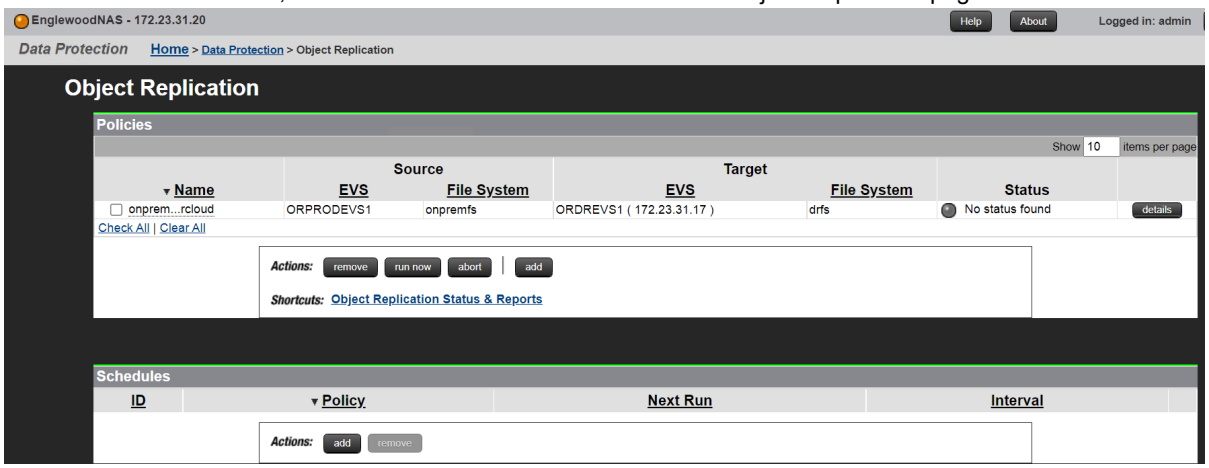


e. In the Object Replication page, verify the status of the newly created policy.

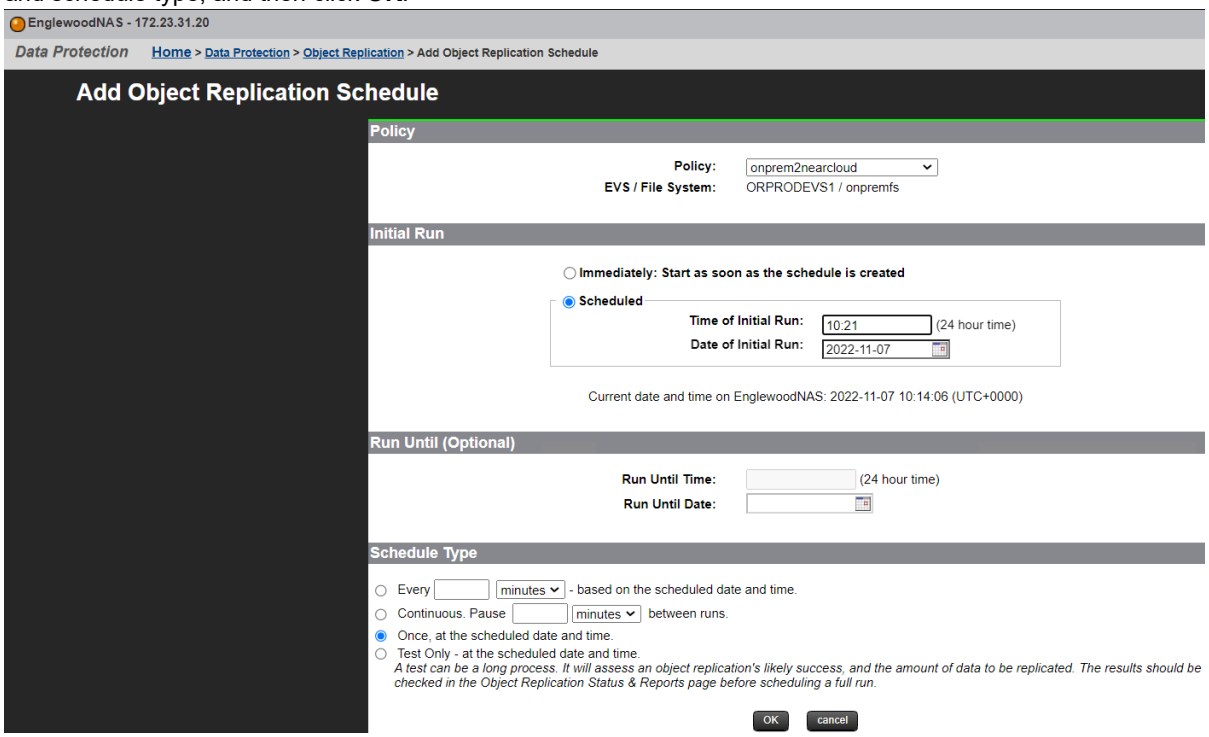


2. Create a schedule for the new policy.

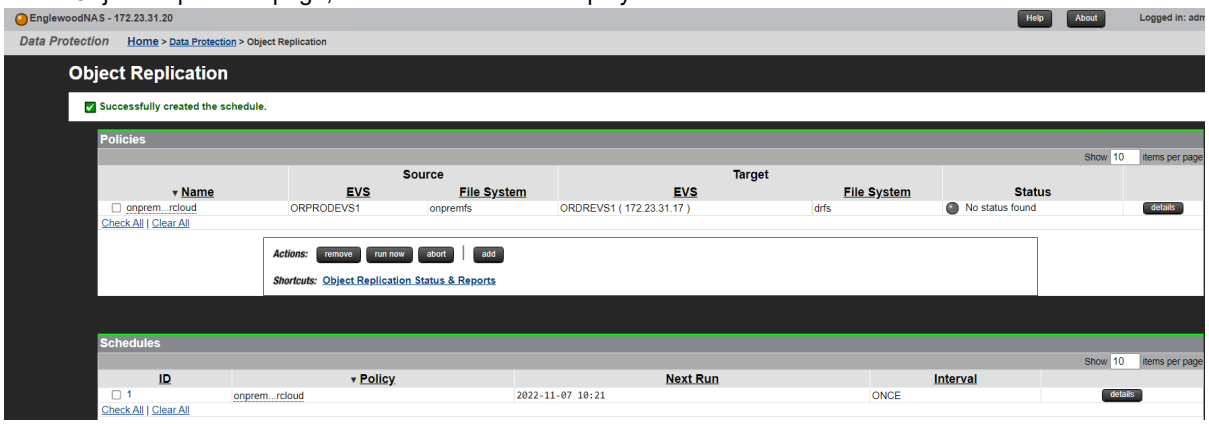
a. To create a new schedule, click **add** in the Schedules section of the Object Replication page.



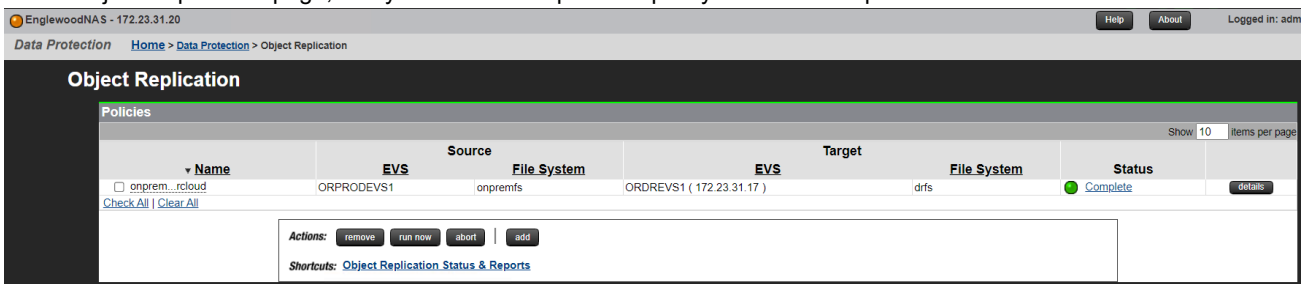
b. In the Add Object Replication Schedule page, enter the required information such as policy name, schedule time, and schedule type, and then click **OK**.



In the Object Replication page, the new schedule is displayed.



3. In the Object Replication page, verify whether the replication policy shows a Complete status.

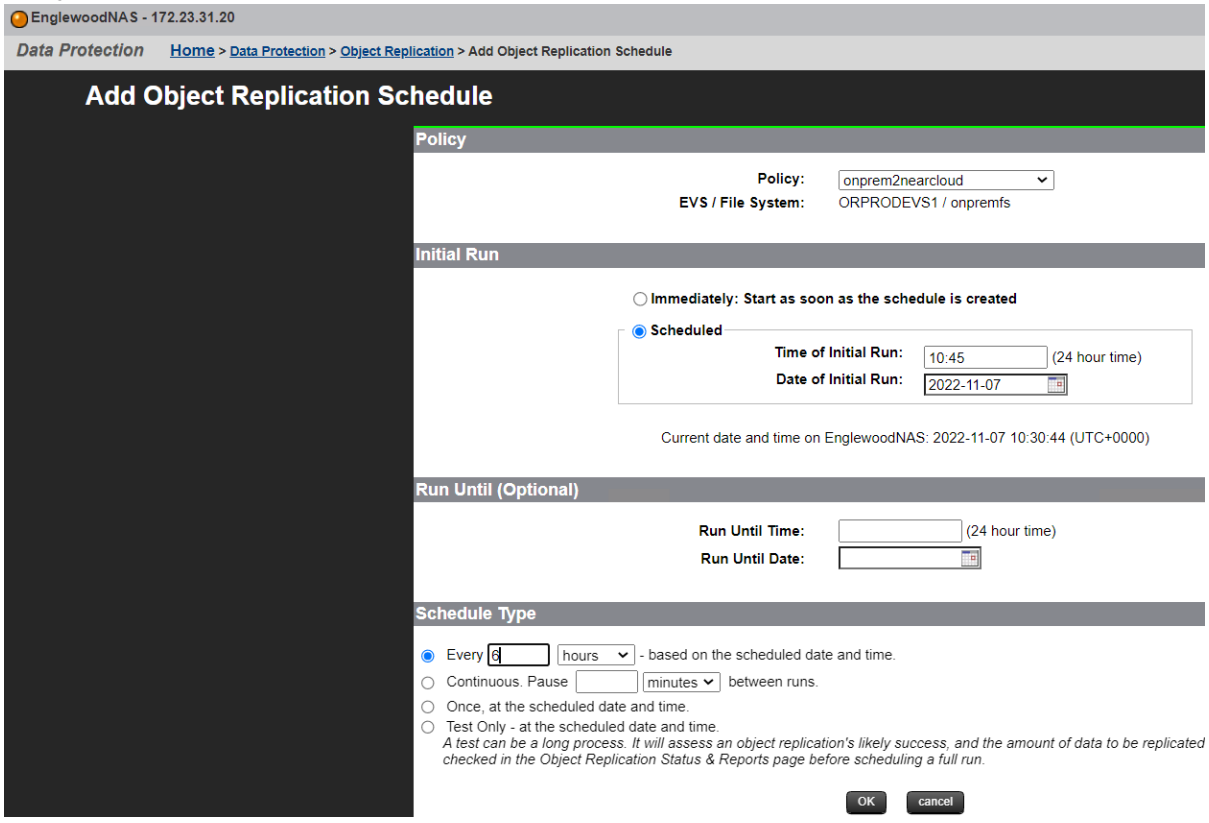


Test 3: Define Multiple Object Replication Schedules

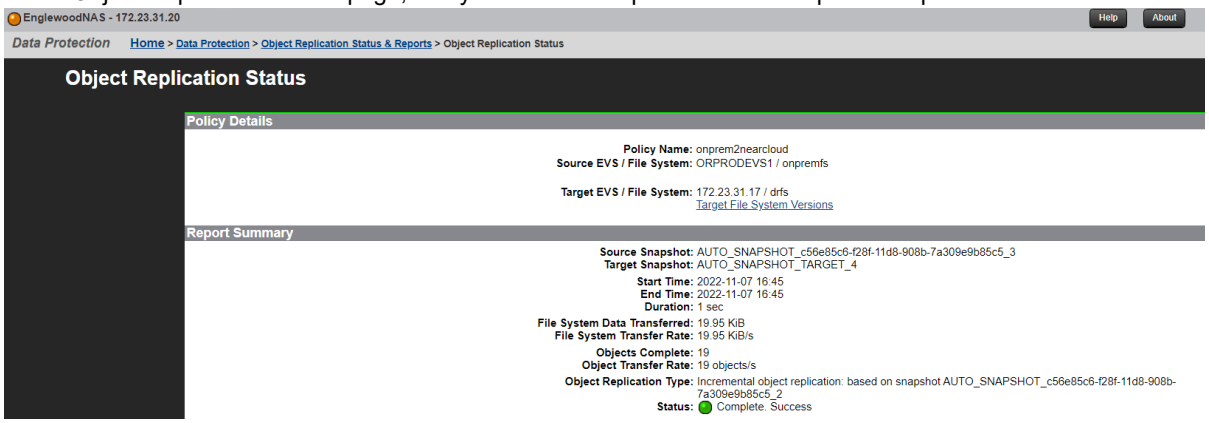
This test case describes the process of defining two object replication schedules on the same object replication policy.

To define Object Replication Schedules, complete the following steps:

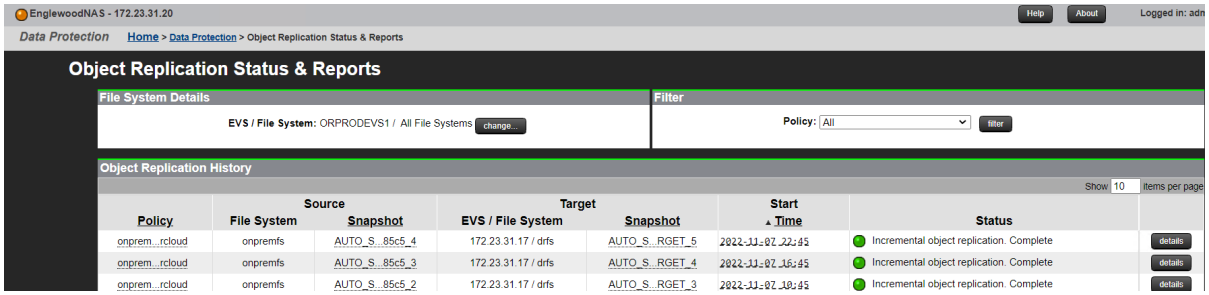
1. First schedule: Replicate every 6 hours.
   a. In the Add Object Replication Schedule page, locate the object replication policy. Under Schedule Type, select **Every**, enter **6**, and select **hours.** Click **OK**.



   b. In the Object Replication Status page, verify whether the replication has completed as per the schedule.

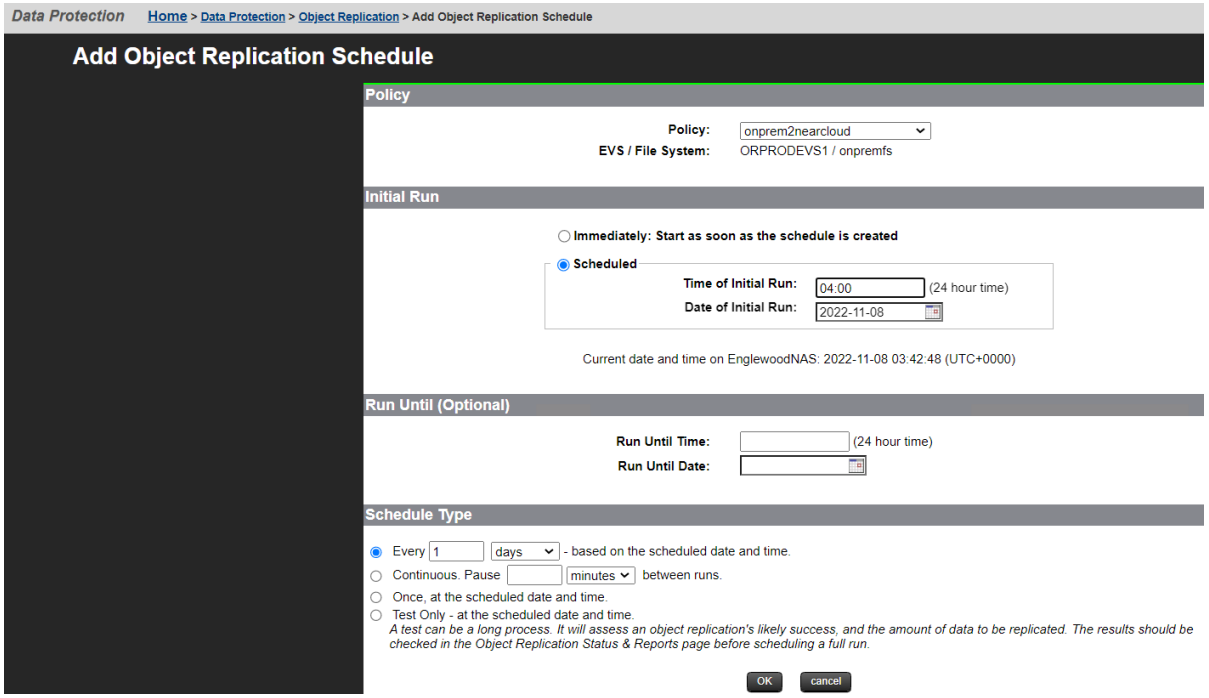


c. In the Object Replication Status & Reports page, verify whether the replication runs every 6 hours as per the schedule.

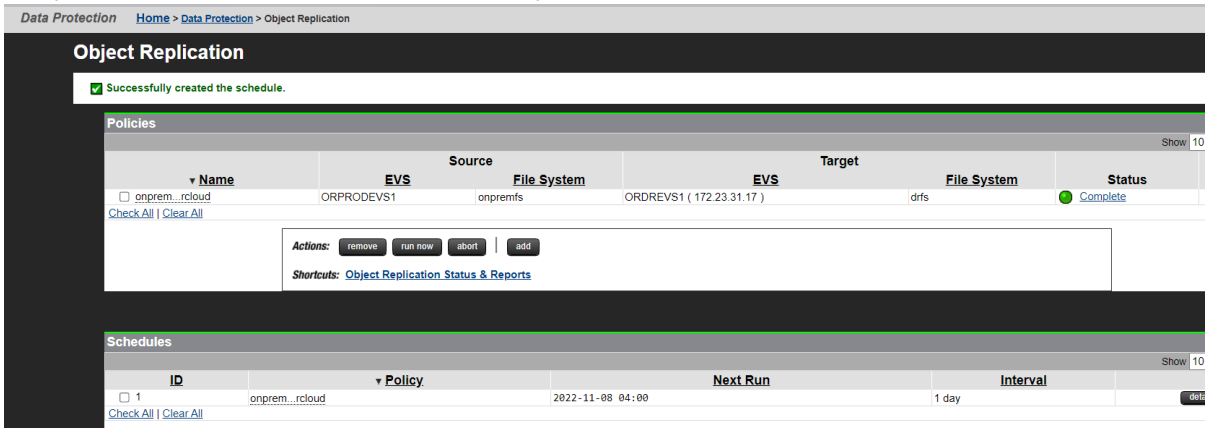


2. Second schedule: Replicate daily at 04:00.

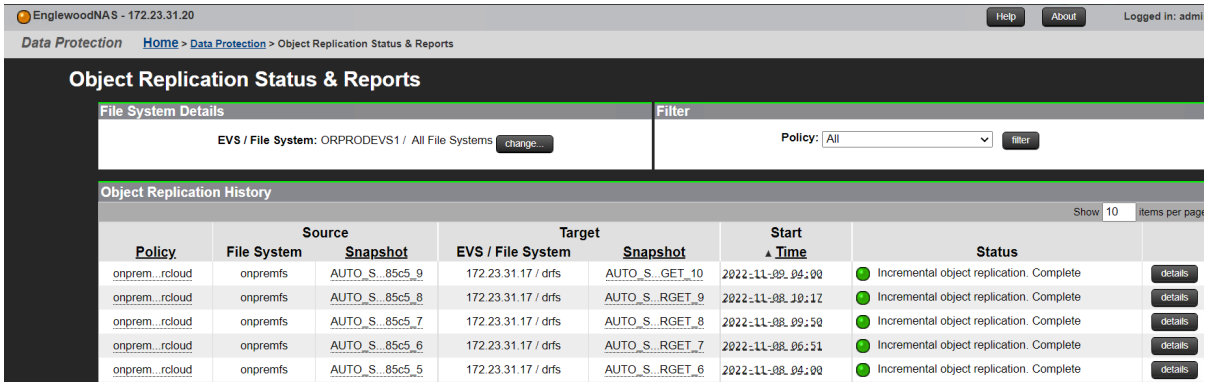
a. In the Add Object Replication Schedule page, locate the object replication policy. Under Initial Run, select **Scheduled** and enter 04:00. Under Schedule Type, select **Every**, enter 1, and select **days**. Click **OK**.



b. Verify whether the schedule is created successfully.



c. In the Object Replication Status & Reports page, verify whether the replication runs daily at 04:00 as per the schedule.



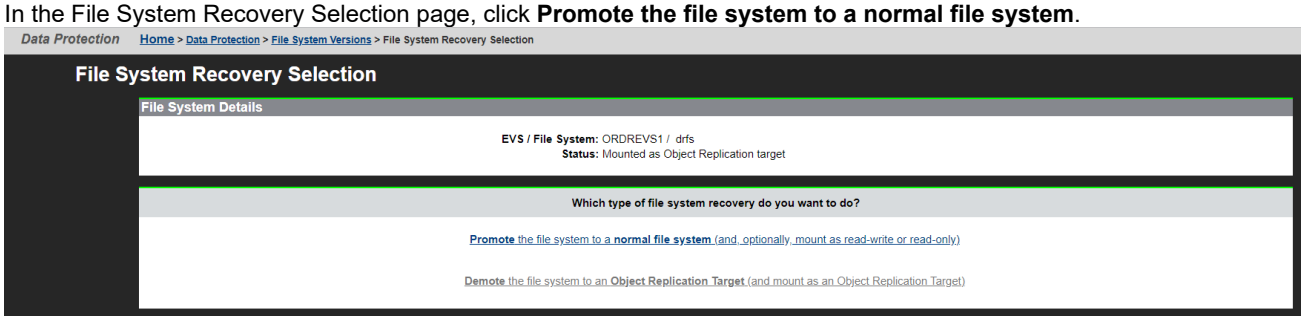
Test 4: Perform Planned Outage

This test case describes the process of performing a planned outage with HNAS Object Replication. This procedure promotes the target HNAS file system and allows clients to access the content. To demonstrate this, we will write to the promoted file system using clients running in the AWS cloud. In addition, we will perform a failback operation to bring the newly created data back to the source HNAS file system.

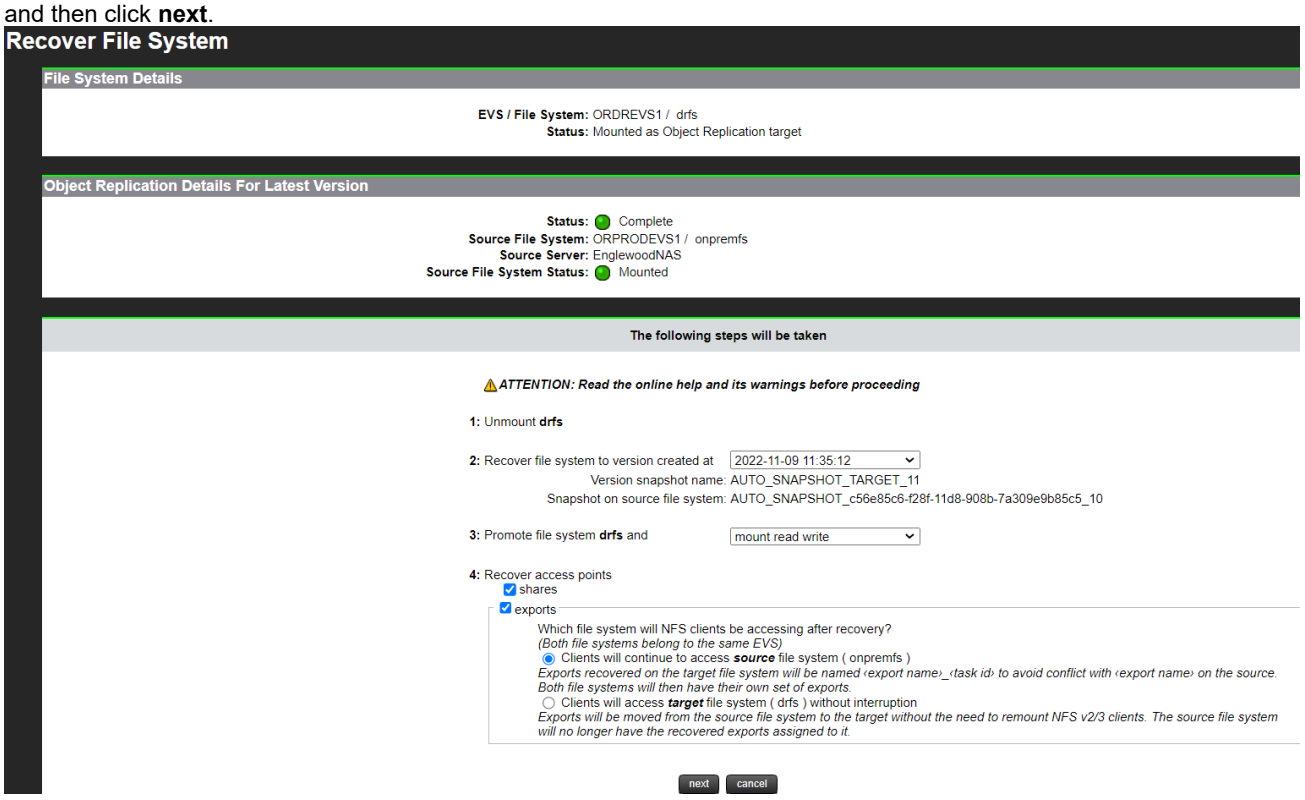
Failover

To start the planned outage by promoting the target HNAS file system, complete the following steps:

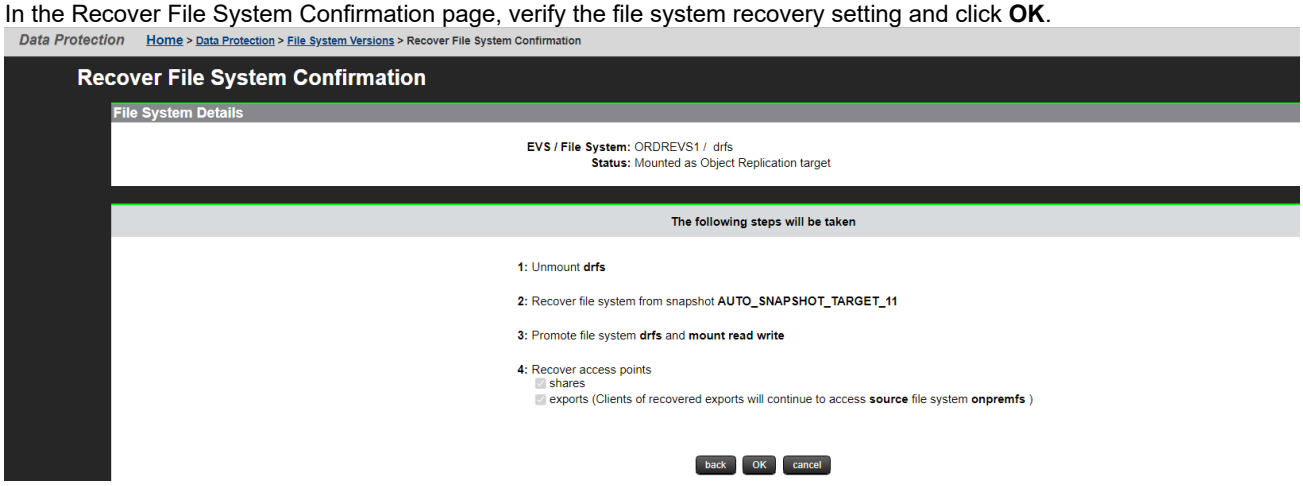
1. Navigate to **Data Protection**, click **File System Versions,** and then click **File System Recovery Selection**.
2. In the File System Recovery Selection page, click **Promote the file system to a normal file system**.



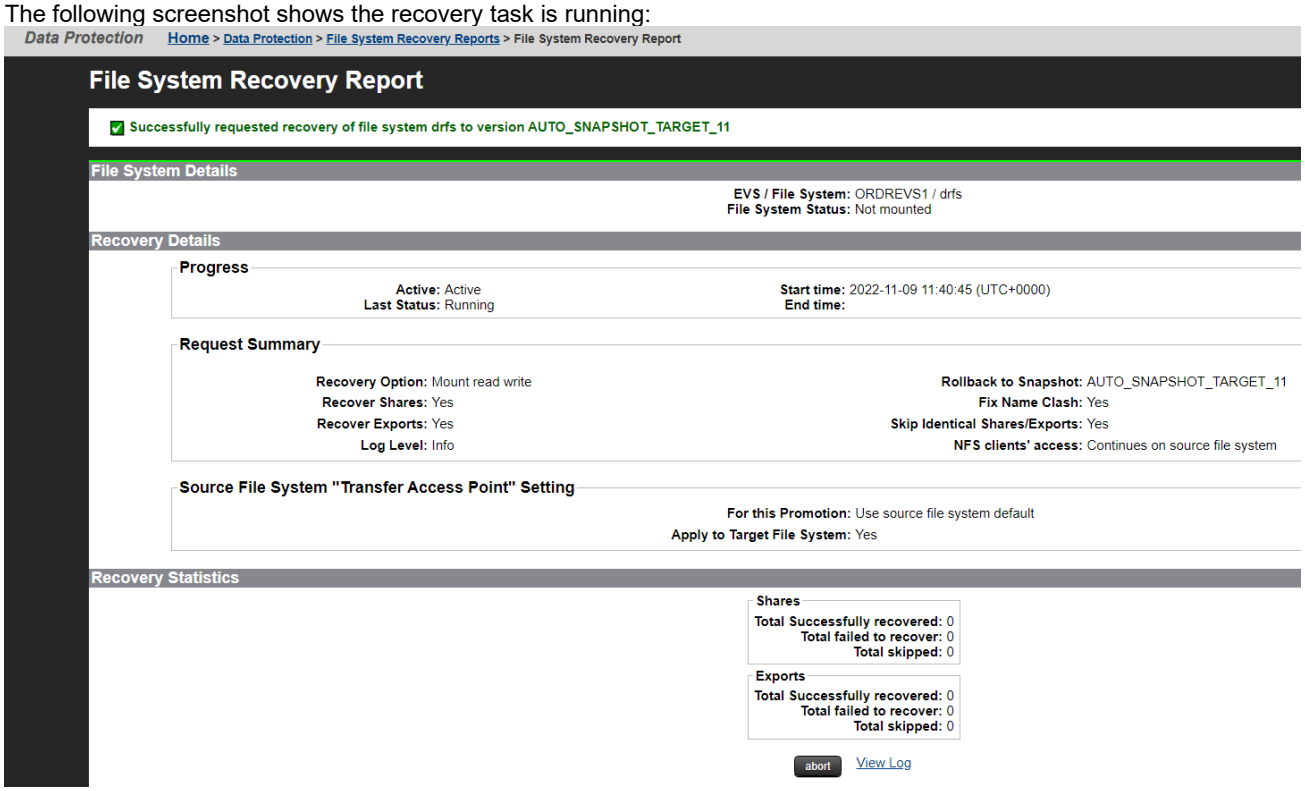
3. In the Recover File System page, enter the required information such as file system version and recover access points, and then click **next**.



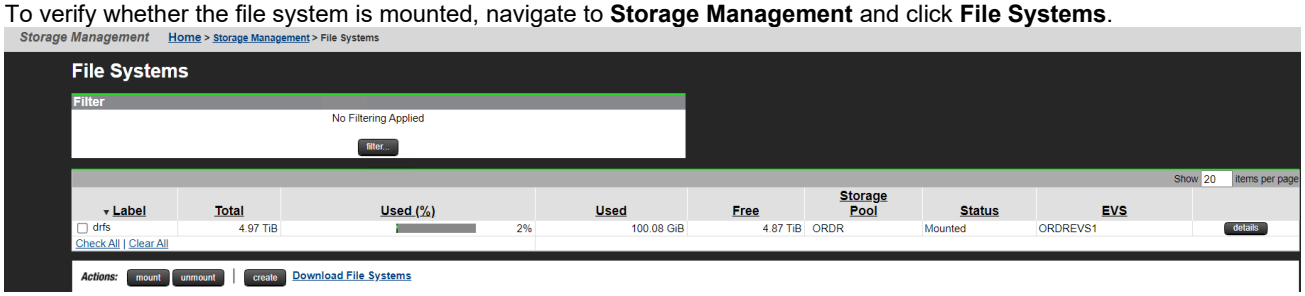
4. In the Recover File System Confirmation page, verify the file system recovery setting and click **OK**.



The following screenshot shows the recovery task is running:



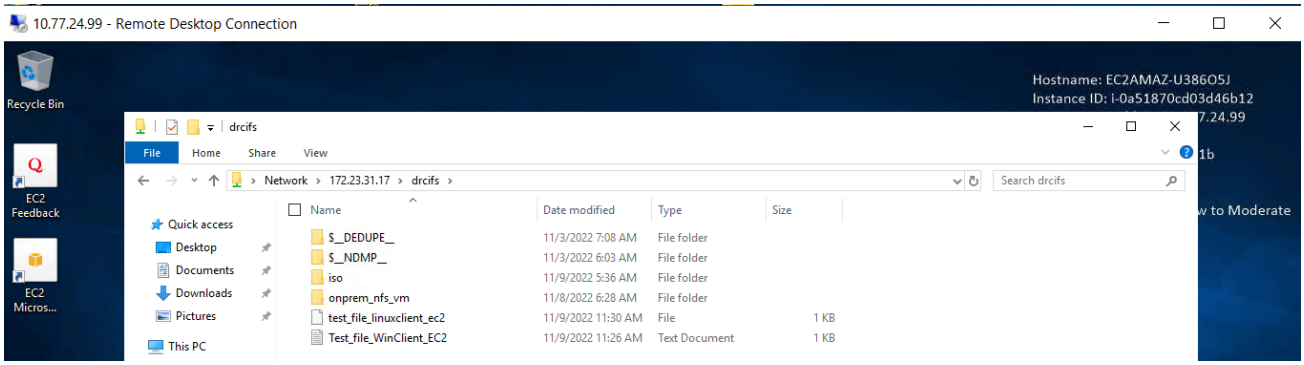
5. To verify whether the file system is mounted, navigate to **Storage Management** and click **File Systems**.



Write Data from Clients in AWS

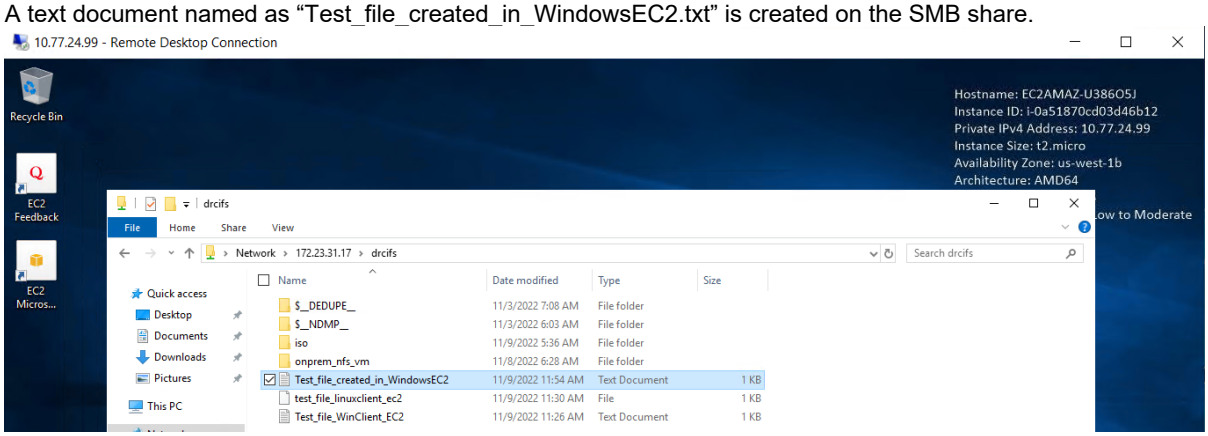
In this section, we will access the HNAS file system that is mounted at the near-cloud data center and ingest new data from clients in the AWS cloud.

- The following screenshots show the SMB share mounted by a Windows EC2 instance and the NFS export mounted by a RHEL EC2 instance:




```
[root@ip-10-77-25-18 ~]# hostname
ip-10-77-25-18.us-west-1.compute.internal
[root@ip-10-77-25-18 ~]# showmount -e 172.23.31.17
Export list for 172.23.31.17:
/drnfs     *
/onpremnfs *
[root@ip-10-77-25-18 ~]# mount -t nfs 172.23.31.17:/drnfs /fs1
[root@ip-10-77-25-18 ~]# df -k
Filesystem           1K-blocks      Used  Available Use% Mounted on
devtmpfs               1844608         0    1844608   0% /dev
tmpfs                  1879956         0    1879956   0% /dev/shm
tmpfs                  1879956      8636    1871320   1% /run
tmpfs                  1879956         0    1879956   0% /sys/fs/cgroup
/dev/nvme0n1p2        31444972   2239732   29205240   8% /
tmpfs                   375988         0     375988   0% /run/user/1000
172.23.31.17:/drnfs 5339226112 104930240 5234295872   2% /fs1
[root@ip-10-77-25-18 ~]# cd /fs1
[root@ip-10-77-25-18 fs1]# ls
'$__DEDUPE__'  '$__NDMP__'   iso   onprem_nfs_vm   Test_file_created_in_WindowsEC2.txt   test_file_linuxclient_ec2   Test_file_WinClient_EC2.txt
```

- The following screenshots show new data being written to the HNAS file system using EC2 instances:
  - A text document named as “Test_file_created_in_WindowsEC2.txt” is created on the SMB share.



- A text document named as “test_file_created_in_linuxEC2.txt” is created on the NFS export.

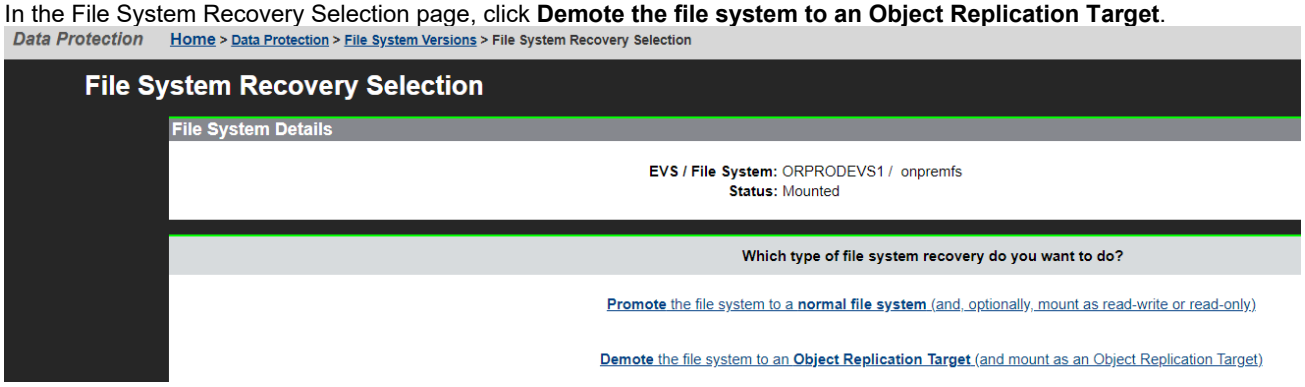
```
[root@ip-10-77-25-18 ~]# cd /fs1
[root@ip-10-77-25-18 fs1]# ls
'$__DEDUPE__'  '$__NDMP__'   iso   onprem_nfs_vm   Test_file_created_in_WindowsEC2.txt   test_file_linuxclient_ec2   Test_file_WinClient_EC2.txt
[root@ip-10-77-25-18 fs1]# vi test_file_created_in_linuxEC2
[root@ip-10-77-25-18 fs1]#
[root@ip-10-77-25-18 fs1]# ls -l
total 32
drwxr-xr-x. 3 root root 2048 Nov  3 07:08 '$__DEDUPE__'
d---------. 3 root root 2048 Nov  3 06:03 '$__NDMP__'
drwxrwxrwx. 2 root root 4096 Nov  9 05:36  iso
drwxr-xr-x. 2 root root 4096 Nov  8 06:28  onprem_nfs_vm
-rw-r--r--. 1 root root   35 Nov  9 12:00  test_file_created_in_linuxEC2
-rwxrwxrwx. 1 root root   35 Nov  9 11:54  Test_file_created_in_WindowsEC2.txt
-rw-r--r--. 1 root root   68 Nov  9 11:30  test_file_linuxclient_ec2
-rwxrwxrwx. 1 root root   94 Nov  9 11:26  Test_file_WinClient_EC2.txt
[root@ip-10-77-25-18 fs1]# date
Wed Nov  9 12:01:03 UTC 2022
[root@ip-10-77-25-18 fs1]#
```

Failback

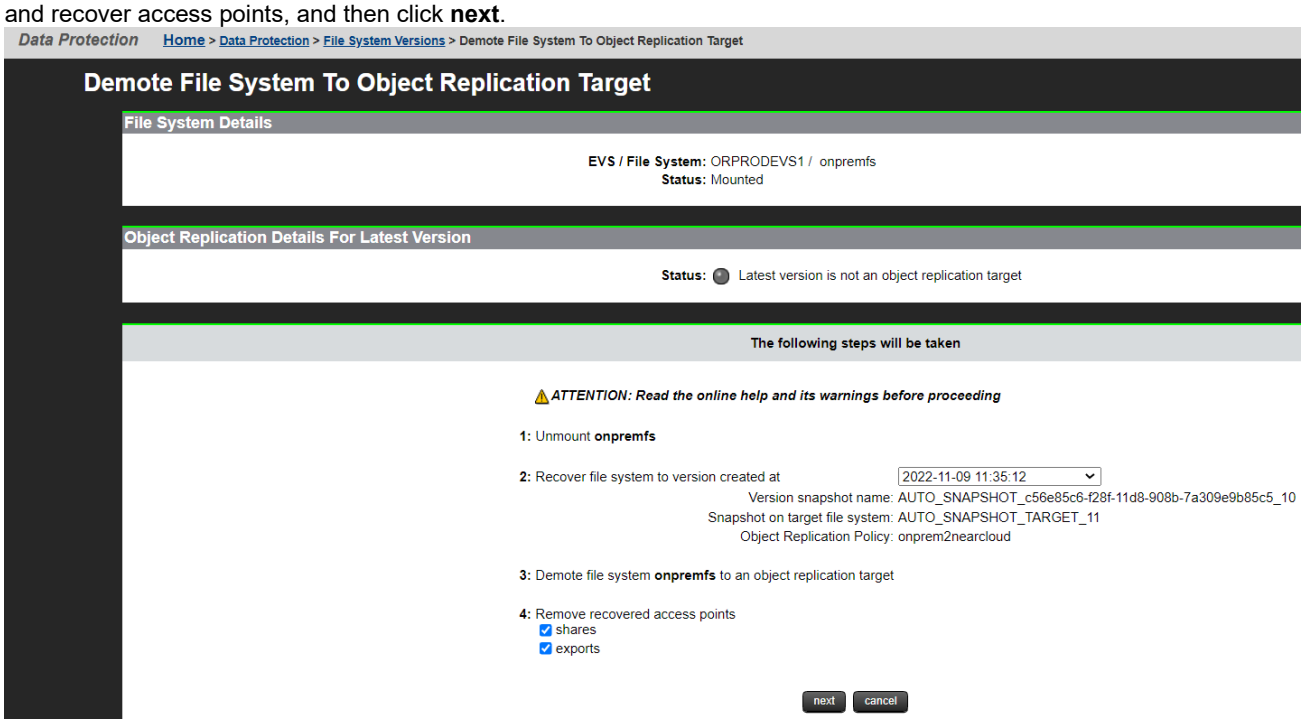
In this section, we will perform a failback operation to bring the newly created data back to the source HNAS file system and verify whether the data is stored.

To perform the planned outage by demoting the HNAS file system, complete the following steps:

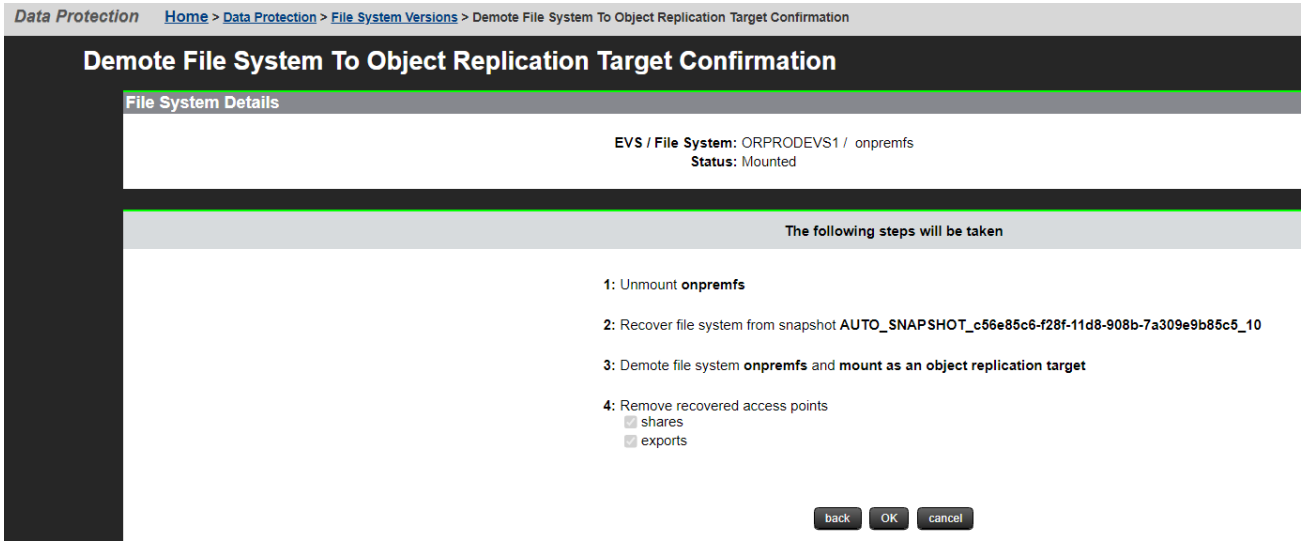
1. Navigate to **Data Protection**, click **File System Versions**, and then click **File System Recovery Selection**.
2. In the File System Recovery Selection page, click **Demote the file system to an Object Replication Target**.



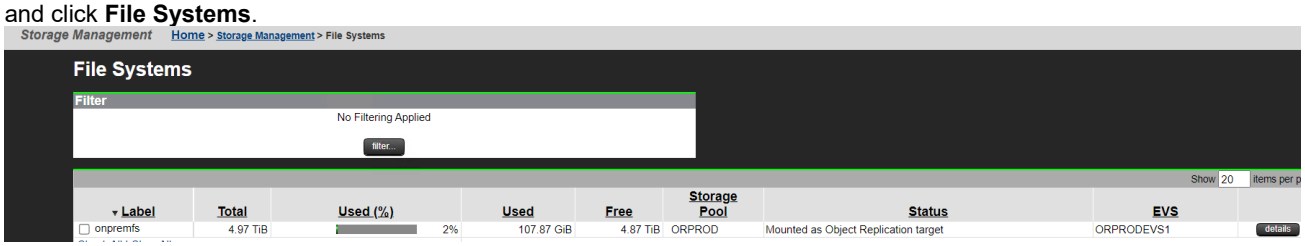
3. In the Demote File System to Object Replication Target page, enter the required information such as file system version and recover access points, and then click **next**.



4. In the Demote File System To Object Replication Target Confirmation page, verify the file system recovery setting and click **OK**.

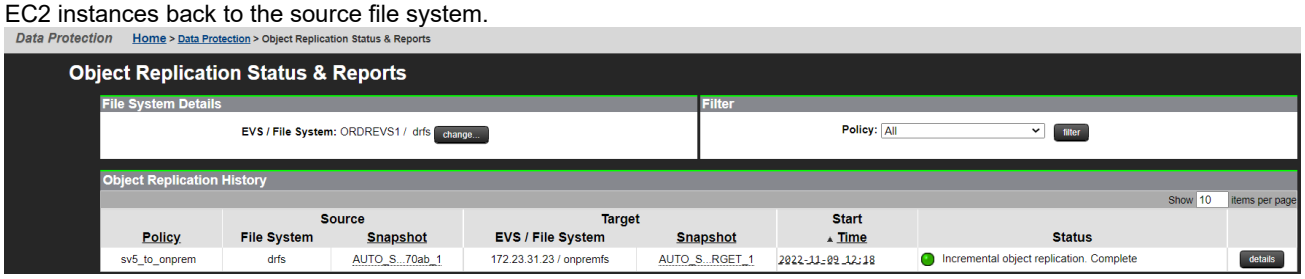


5. To verify whether the primary file system is mounted as an Object Replication target, navigate to **Storage Management** and click **File Systems**.

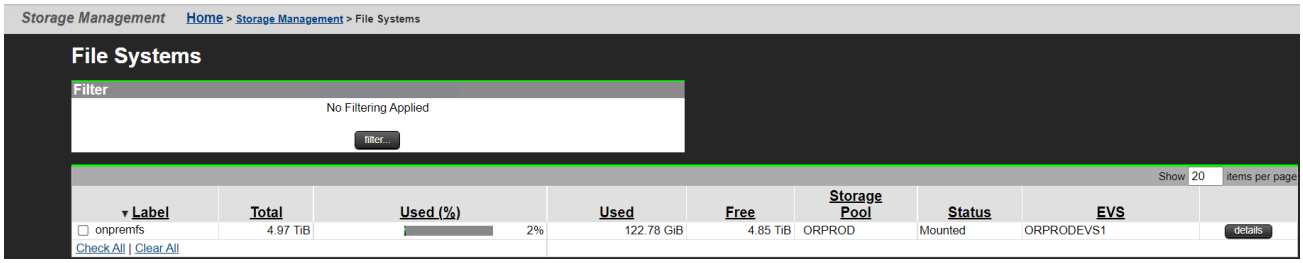


6. Switch to the secondary HNAS cluster, create an Object Replication policy, and schedule using the instructions in the Configure HNAS Object Replication section. Trigger the replication schedule to copy the data that was written by the AWS

EC2 instances back to the source file system.

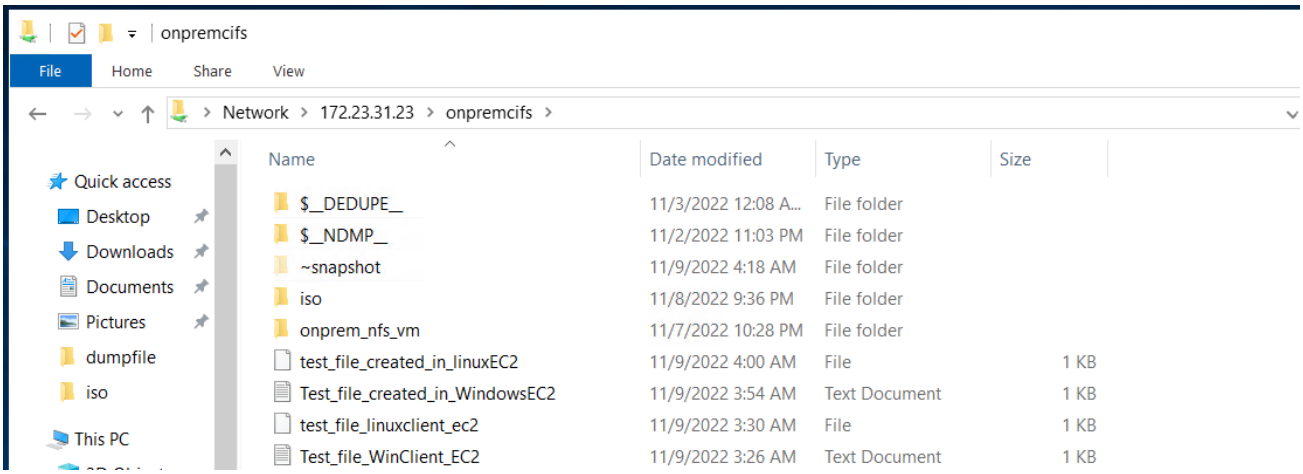


7. Promote the source file system so it becomes usable again with the instructions in the Perform Planned Outage: Failover section.



The following screenshots show that the data written by the AWS EC2 instances to the target file system is present on the source file system and can be access by clients at the on-premises data center.

SMB Share:



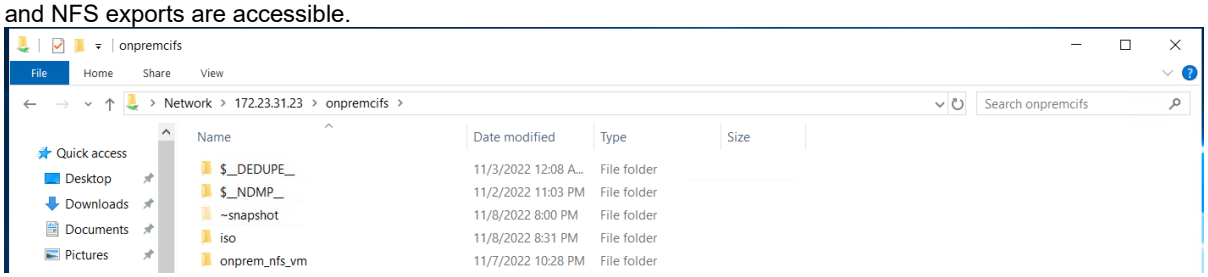
NFS Export:

```
[root@nasclientlinuxeng /]# showmount -e 172.23.31.23
Export list for 172.23.31.23:
/onpremnfs *
[root@nasclientlinuxeng /]# mount -t  nfs 172.23.31.23:/onpremnfs /fs15
[root@nasclientlinuxeng /]# df -k
df: /fs0: Stale file handle
Filesystem              1K-blocks      Used  Available Use% Mounted on
devtmpfs                  1880028         0    1880028   0% /dev
tmpfs                     1910380         0    1910380   0% /dev/shm
tmpfs                     1910380     10164    1900216   1% /run
tmpfs                     1910380         0    1910380   0% /sys/fs/cgroup
/dev/mapper/rhel-root    17197056  10262828    6934228  60% /
/dev/sda2                 1038336    254144     784192  25% /boot
/dev/sda1                  613184      5940     607244   1% /boot/efi
tmpfs                      382076        24     382052   1% /run/user/975
tmpfs                      382076         0     382076   0% /run/user/0
172.23.31.23:/onpremnfs 5339226112 113919424 5225306688   3% /fs15
[root@nasclientlinuxeng /]# cd /fs15
[root@nasclientlinuxeng fs15]# ls
'$__DEDUPE__'  '$__NDMP__'   iso   onprem_nfs_vm   test_file_created_in_linuxEC2   Test_file_created_in_WindowsEC2.txt   test_file_linuxclient_ec2   Test_file_WinClient_EC2.txt
[root@nasclientlinuxeng fs15]#
```

Test 5: Recover from Unplanned Outage

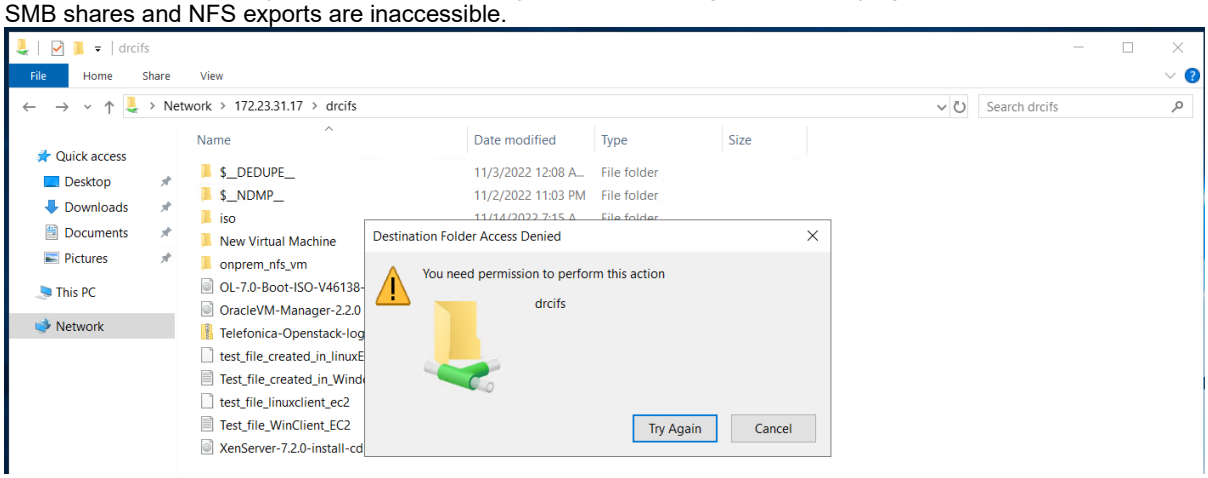
This test case describes how to restore operations after an unplanned outage by utilizing HNAS data that is replicated to the near-cloud data center. This involves promoting the Object Replication target file system to access the replicated data.

- The following screenshots show the status of the HNAS file services during normal operations:
  - On-premises HNAS: File system is mounted as normal and is accepting clients' read and write requests. SMB shares and NFS exports are accessible.



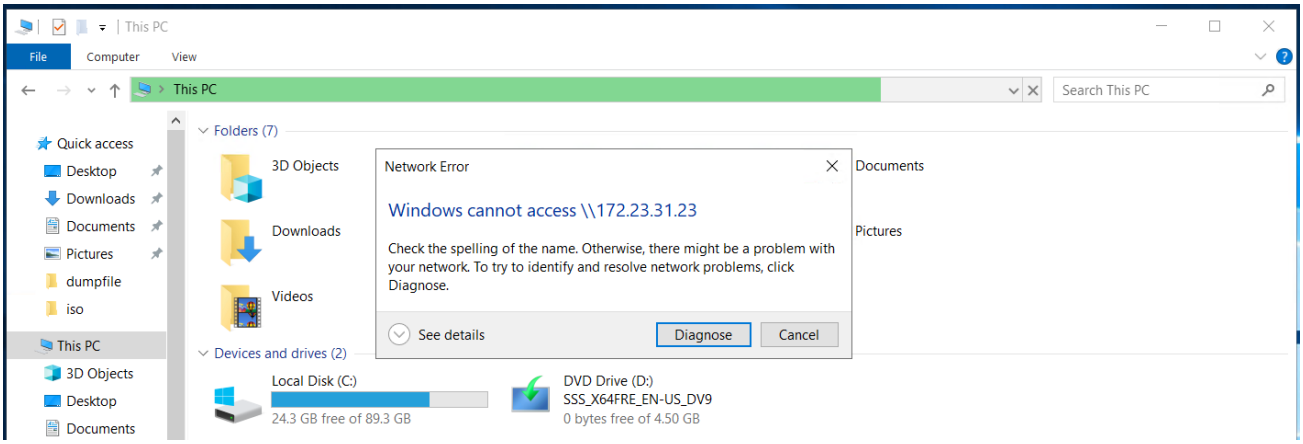

```
[root@nasclientlinuxeng /]# mount -t nfs 172.23.31.23:/onpremnfs /fs15
[root@nasclientlinuxeng /]# df -k
df: /fs0: Stale file handle
Filesystem              1K-blocks      Used  Available Use% Mounted on
devtmpfs                  1880028         0    1880028   0% /dev
tmpfs                     1910380         0    1910380   0% /dev/shm
tmpfs                     1910380     10164    1900216   1% /run
tmpfs                     1910380         0    1910380   0% /sys/fs/cgroup
/dev/mapper/rhel-root    17197056  10262744    6934312  60% /
/dev/sda2                 1038336    254144     784192  25% /boot
/dev/sda1                  613184      5940     607244   1% /boot/efi
tmpfs                      382076        24     382052   1% /run/user/975
tmpfs                      382076         0     382076   0% /run/user/0
172.23.31.23:/onpremnfs 5339226112 113102720 5226123392   3% /fs15
[root@nasclientlinuxeng /]# cd /fs15
[root@nasclientlinuxeng /]# ls
'$__DEDUPE__'  '$__NDMP__'   iso   onprem_nfs_vm
[root@nasclientlinuxeng fs15]# cd iso
[root@nasclientlinuxeng iso]# ls
AW013_RDM_3.1.0.172.iso                 file_at_1045                                        rhel-8.3-x86_64-dvd.iso         test5
comps-4AS-0.20071108.src.rpm            mongodb-windows-x86_64-enterprise-6.0.2-signed.msi  rhel-8.4-x86_64-dvd.iso         VMware-ESXi-7.0-update2a-17867351-hitachi-1301.iso
coreos_production_iso_image.iso         primary_site_fs.txt                                 rhel-baseos-9.0-x86_64-dvd.iso  VMware-VMvisor-Installer-7.0U2-17630552.x86_64.iso
duck-14.4.7322.05-hds.iso               rhel-8.1-x86_64-dvd.iso                             rhel-server-7.9-x86_64-dvd.iso
elx-lpfc-dd-sles15sp-12.6.240.27-ds-1.tar.gz  rhel-8.2-x86_64-dvd.iso                       test01
[root@nasclientlinuxeng iso]# touch test_file_testcase5
[root@nasclientlinuxeng iso]# date
Wed Nov  9 00:35:11 EST 2022
[root@nasclientlinuxeng iso]#
```

  - Near-cloud HNAS: File system is mounted as object replication target and is denying clients' read and write requests. SMB shares and NFS exports are inaccessible.



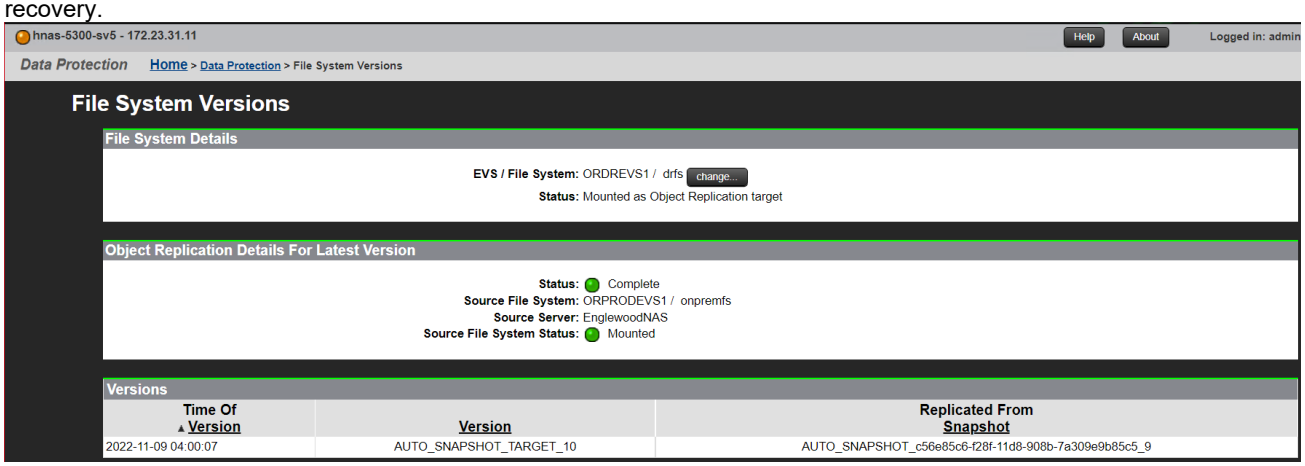

```
[root@nasclientlinuxeng ~]# mount -t nfs 172.23.31.17:/drnfs /fs05
[root@nasclientlinuxeng ~]# cd /fs05
[root@nasclientlinuxeng fs05]# ls
'$__DEDUPE__'  'New Virtual Machine'          OracleVM-Manager-2.2.0.iso      Test_file_created_in_WindowsEC2.txt   XenServer-7.2.0-install-cd.iso
'$__NDMP__'     OL-7.0-Boot-ISO-V46138-01.iso  Telefonica-Openstack-logs.zip   test_file_linuxclient_ec2
 lost+found     onprem_nfs_vm                 test_file_created_in_linuxEC2   Test_file_WinClient_EC2.txt
[root@nasclientlinuxeng fs05]# touch tset5
touch: cannot touch 'tset5': Read-only file system
[root@nasclientlinuxeng fs05]#
```

- The following screenshots show that the on-premises HNAS file services are no longer accessible after an outage:



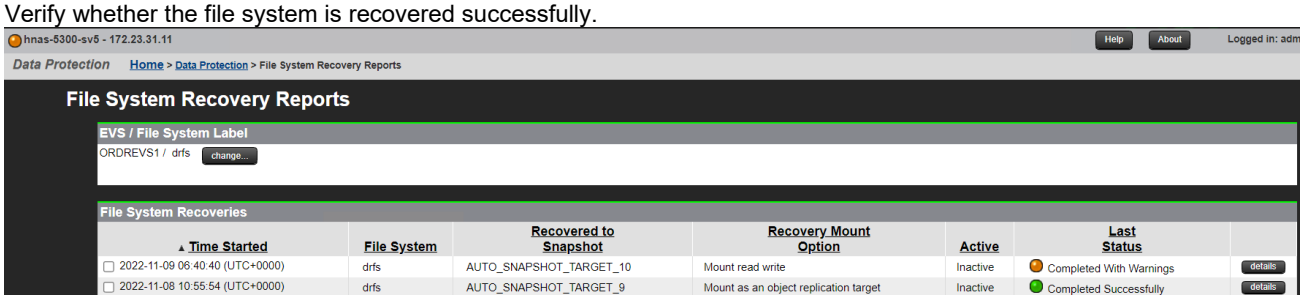

```
[root@nasclientlinuxeng /]# ping 172.23.31.23
PING 172.23.31.23 (172.23.31.23) 56(84) bytes of data.
From 172.23.31.31 icmp_seq=10 Destination Host Unreachable
From 172.23.31.31 icmp_seq=11 Destination Host Unreachable
From 172.23.31.31 icmp_seq=12 Destination Host Unreachable
From 172.23.31.31 icmp_seq=13 Destination Host Unreachable
From 172.23.31.31 icmp_seq=14 Destination Host Unreachable
From 172.23.31.31 icmp_seq=15 Destination Host Unreachable
^C
--- 172.23.31.23 ping statistics ---
17 packets transmitted, 0 received, +6 errors, 100% packet loss, time 16394ms
pipe 3
[root@nasclientlinuxeng /]# showmount -e 172.23.31.23
clnt_create: RPC: Unable to receive
```

1. To begin recovery, navigate to **Data Protection** > **File System Versions** and select the file system version you want to recover. For example, the following screenshot shows that version “AUTO_SNAPSHOT_TARGET_10” is used for the recovery.



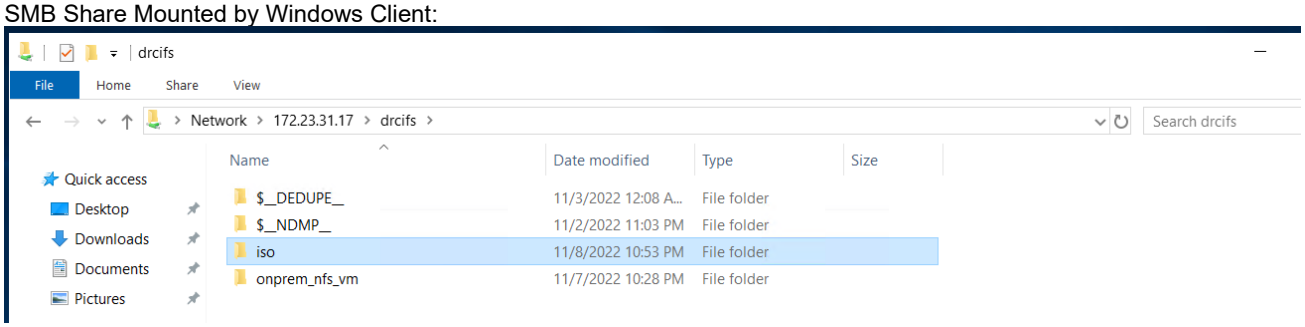
2. Promote the target file system on the secondary HNAS cluster. For instructions, see Perform Planned Outage: Failover section.

3. Verify whether the file system is recovered successfully.



The following screenshots show the SMB share mounted by a Windows client and the NFS export mounted by a RHEL client at the near-cloud data center after a successful recovery.

SMB Share Mounted by Windows Client:



NFS Export Mounted by Linux Client:

```
[root@linuxnfscl2 /]# showmount -e 172.23.31.17
Export list for 172.23.31.17:
/drnfs     *
/onpremnfs *
[root@linuxnfscl2 /]# mkdir /fs10
[root@linuxnfscl2 /]# mount -t nfs 172.23.31.17:/drnfs /fs10
[root@linuxnfscl2 /]# df -kh
df: /fs0: Stale file handle
Filesystem             Size  Used Avail Use% Mounted on
devtmpfs               1.8G     0  1.8G   0% /dev
tmpfs                  1.9G     0  1.9G   0% /dev/shm
tmpfs                  1.9G   10M  1.9G   1% /run
tmpfs                  1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/mapper/rhel-root   13G  5.9G  7.0G  46% /
/dev/sda2             1014M  249M  766M  25% /boot
/dev/sda1              599M  5.9M  594M   1% /boot/efi
tmpfs                  374M   20K  374M   1% /run/user/975
tmpfs                  374M     0  374M   0% /run/user/0
172.23.31.17:/drnfs    5.0T  101G  4.9T   2% /fs10
[root@linuxnfscl2 /]# cd  /fs10
[root@linuxnfscl2 fs10]# ls
'$__DEDUPE__'  '$__NDMP__'   iso   onprem_nfs_vm
[root@linuxnfscl2 fs10]# cd iso
[root@linuxnfscl2 iso]# ls
AW013_RDM_3.1.0.172.iso                      mongodb-windows-x86_64-enterprise-6.0.2-signed.msi  rhel-8.4-x86_64-dvd.iso         VMware-ESXi-7.0-update2a-17867351-hitachi-1301.iso
coreos_production_iso_image.iso              primary_site_fs.txt                                 rhel-baseos-9.0-x86_64-dvd.iso  VMware-VMvisor-Installer-7.0U2-17630552.x86_64.iso
duck-14.4.7322.05-hds.iso                    rhel-8.1-x86_64-dvd.iso                             rhel-server-7.9-x86_64-dvd.iso
elx-lpfc-dd-sles15sp-12.6.240.27-ds-1.tar.gz rhel-8.2-x86_64-dvd.iso                             test01
file_at_1045                                 rhel-8.3-x86_64-dvd.iso                             test5
[root@linuxnfscl2 iso]#
```

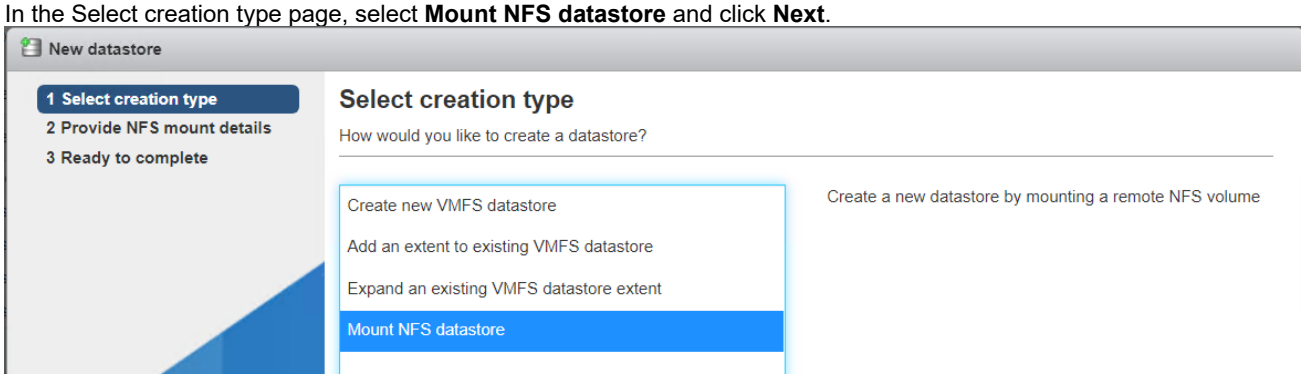
Test 6: Migrate Virtual Machine Using Object Replication

This test case describes the use of HNAS Object Replication as a data mover to migrate virtual machines between sites.

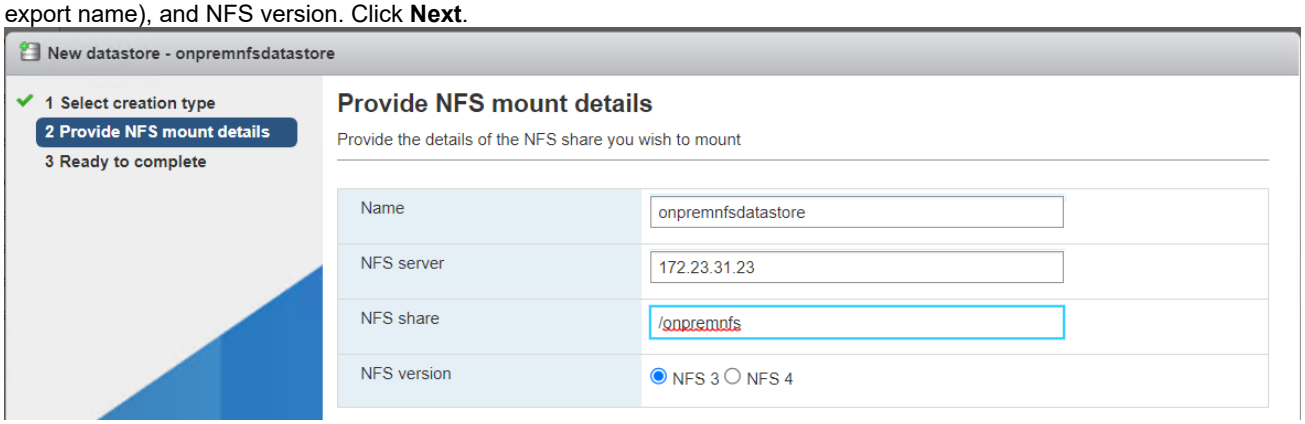
Create Virtual Machine

Mount NFS export from the source HNAS file system as a VMware datastore and then create a virtual machine on the datastore.

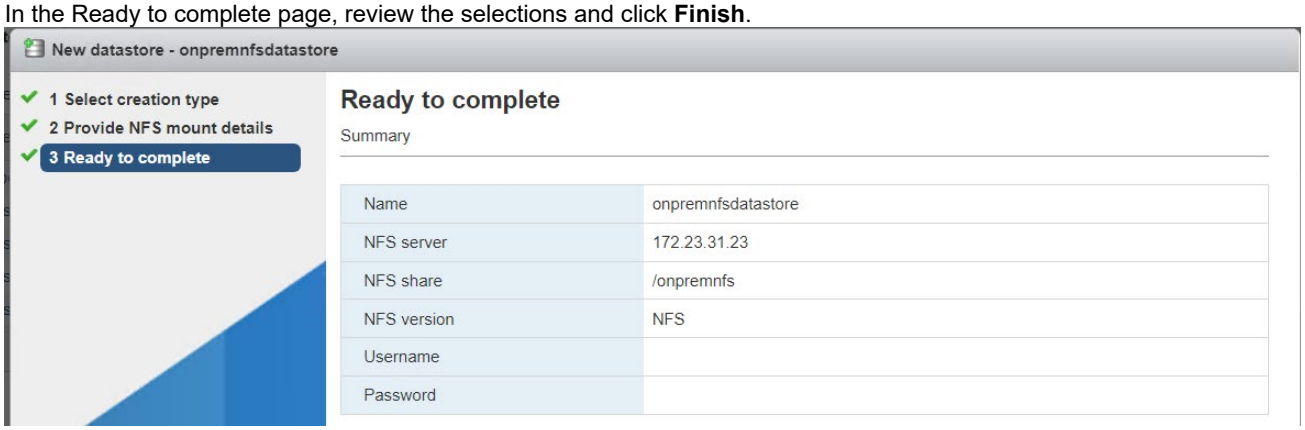
1. Log in to the vSphere client and select the VMware ESXi host to mount the NFS export on.
2. Navigate to **Storage**, right-click, and select **New Datastore**.
3. In the Select creation type page, select **Mount NFS datastore** and click **Next**.



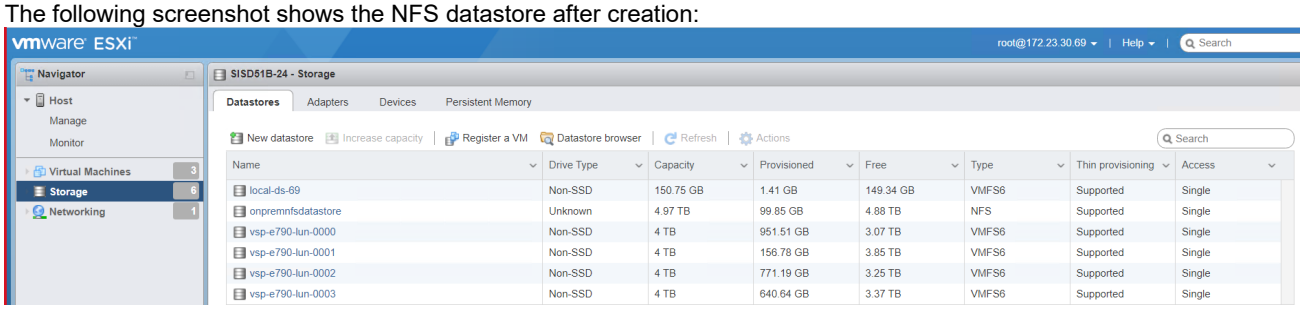
4. In the Provide NFS mount details page, enter the datastore name, NFS server (HNAS EVS), NFS share (HNAS NFS export name), and NFS version. Click **Next**.



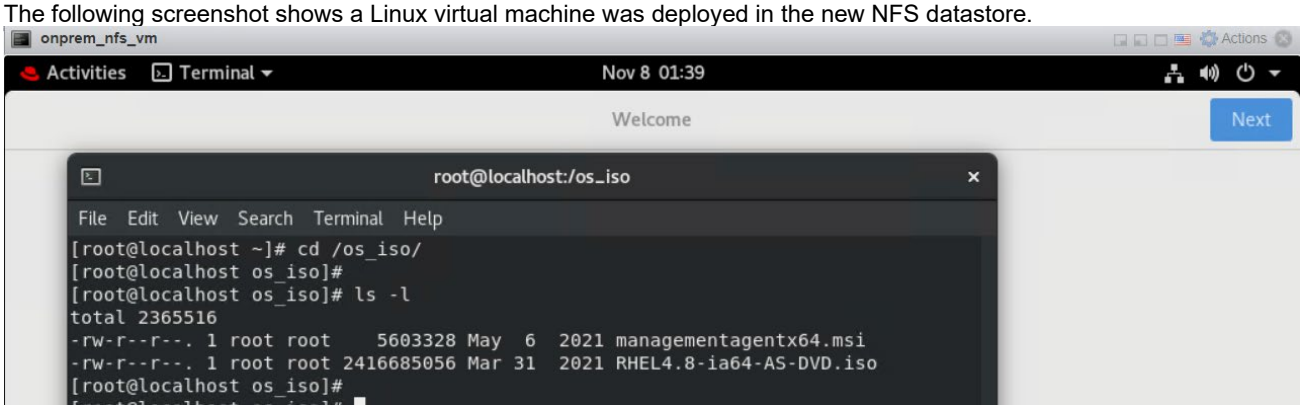
5. In the Ready to complete page, review the selections and click **Finish**.



The following screenshot shows the NFS datastore after creation:



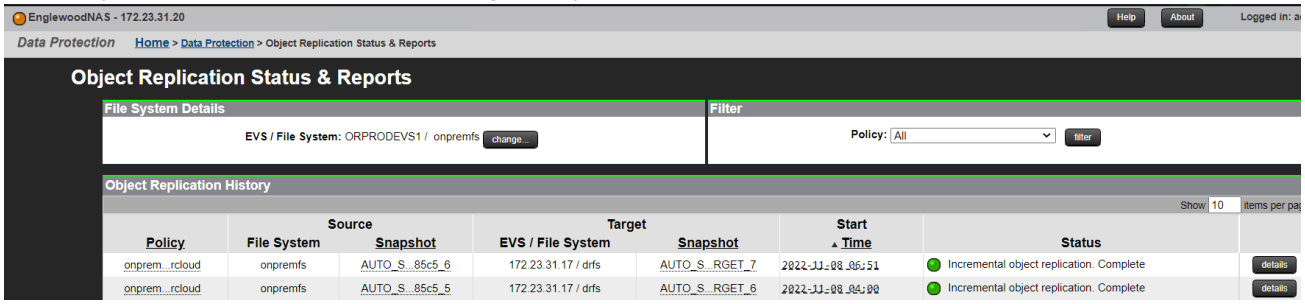
The following screenshot shows a Linux virtual machine was deployed in the new NFS datastore.



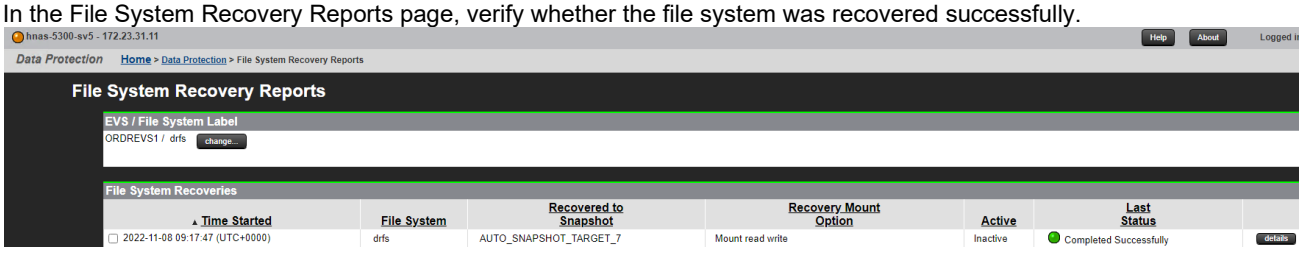
Replicate File System

To create an HNAS Object Replication policy to copy the file system being used as the NFS datastore to the secondary site, complete the following steps:

1. Create an Object Replication policy. For the procedure, see Configure HNAS Object Replication section.
2. In the Object Replication Status & Reports page, verify whether the replication has completed as per the schedule.



3. To make the target file system reusable, promote the target file system. For the procedure, see Perform Planned Outage: Failover section.
4. In the File System Recovery Reports page, verify whether the file system was recovered successfully.

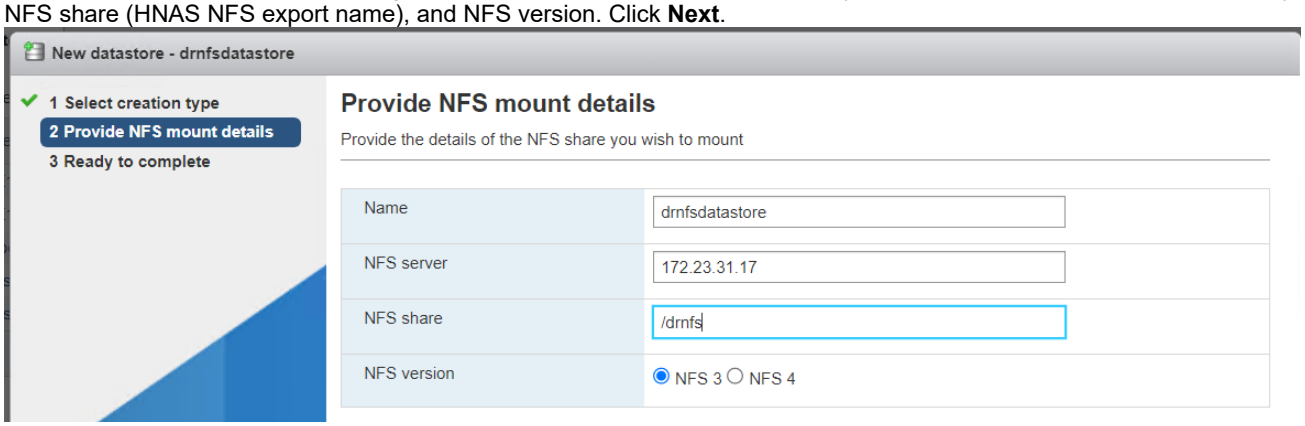


Register Replicated Virtual Machine

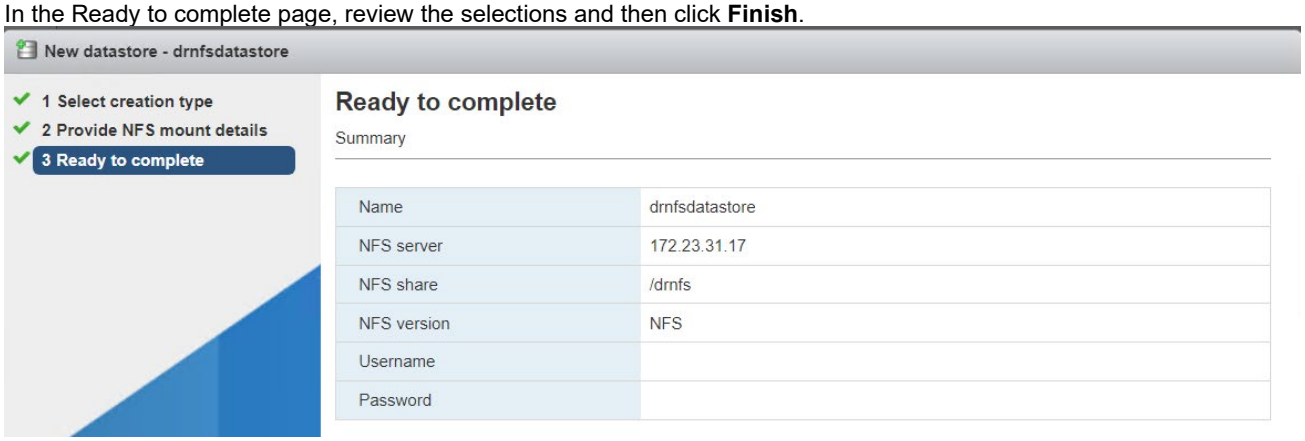
To discover and register the replicated NFS datastore at the secondary site and import the virtual machine, complete the following steps:

1. Log in to the vSphere client and select the VMware ESXi host to mount the NFS export on.

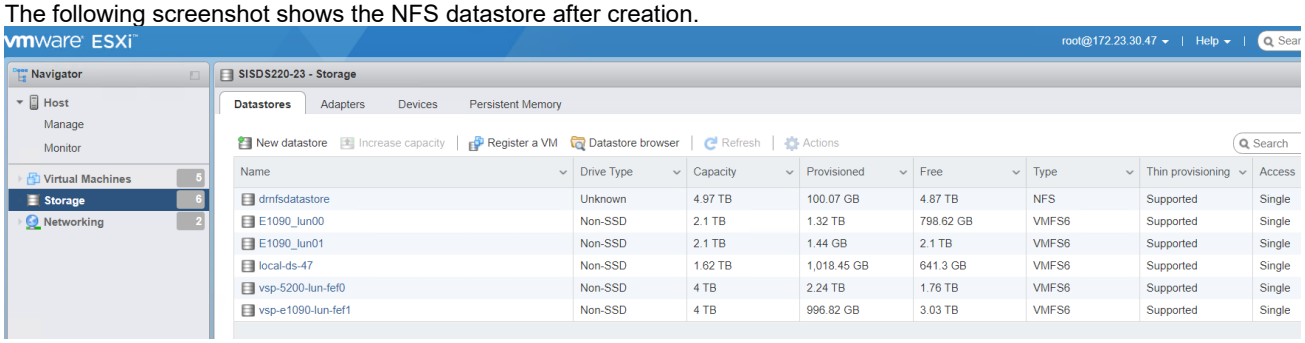
2. Navigate to **Storage**, right-click, and select **New Datastore**.
3. Select **Mount NFS datastore** and click **Next**.
4. In the Provide NFS mount details page, enter the datastore name, NFS server (HNAS EVS at the near-cloud data center), NFS share (HNAS NFS export name), and NFS version. Click **Next**.



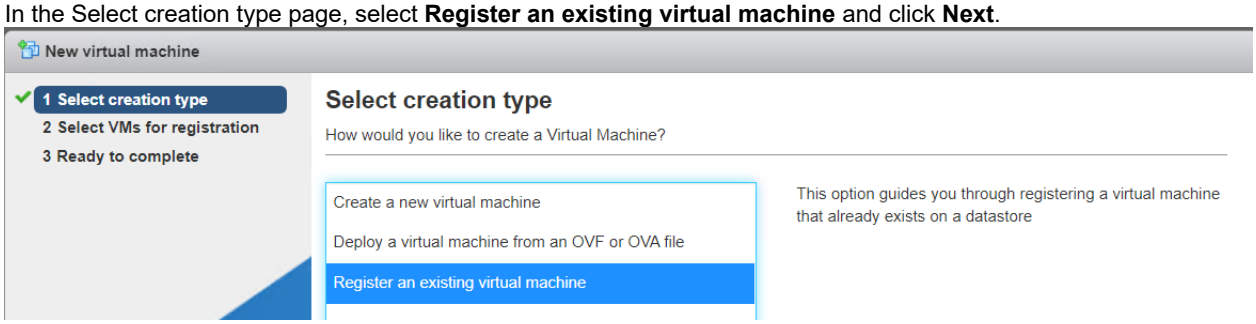
5. In the Ready to complete page, review the selections and then click **Finish**.



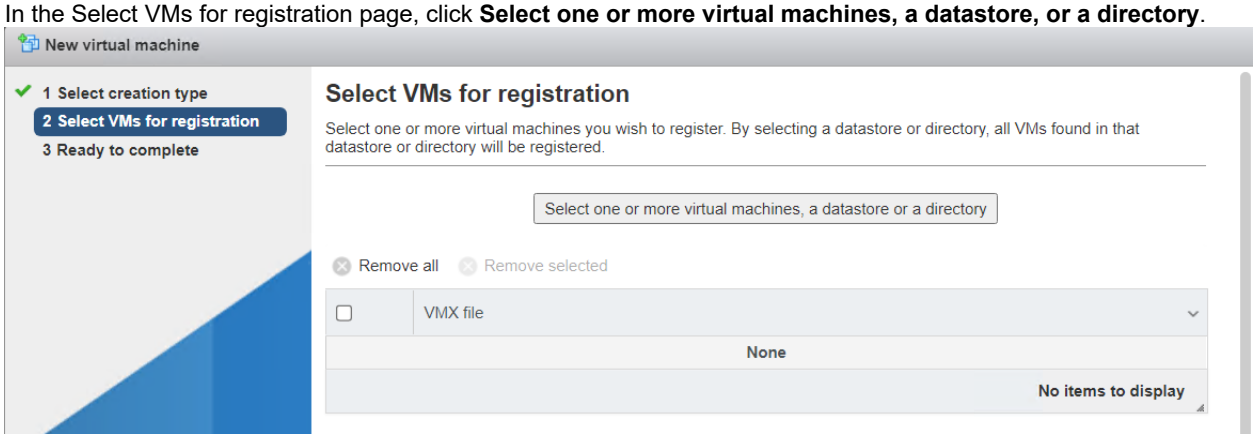
The following screenshot shows the NFS datastore after creation.



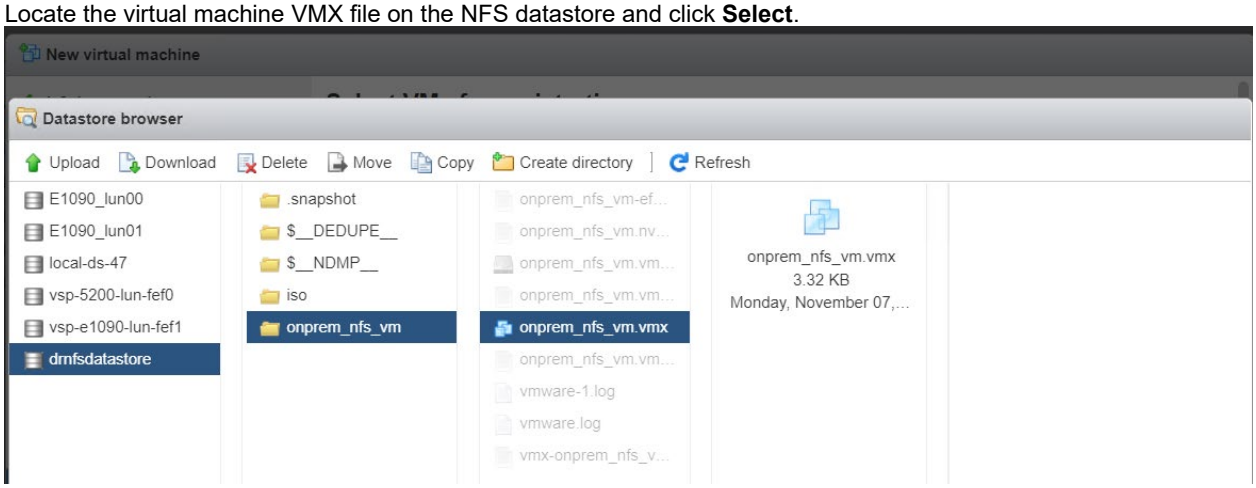
6. Navigate to **Virtual machines**, right-click, and select **Create/Register VM**.
7. In the Select creation type page, select **Register an existing virtual machine** and click **Next**.



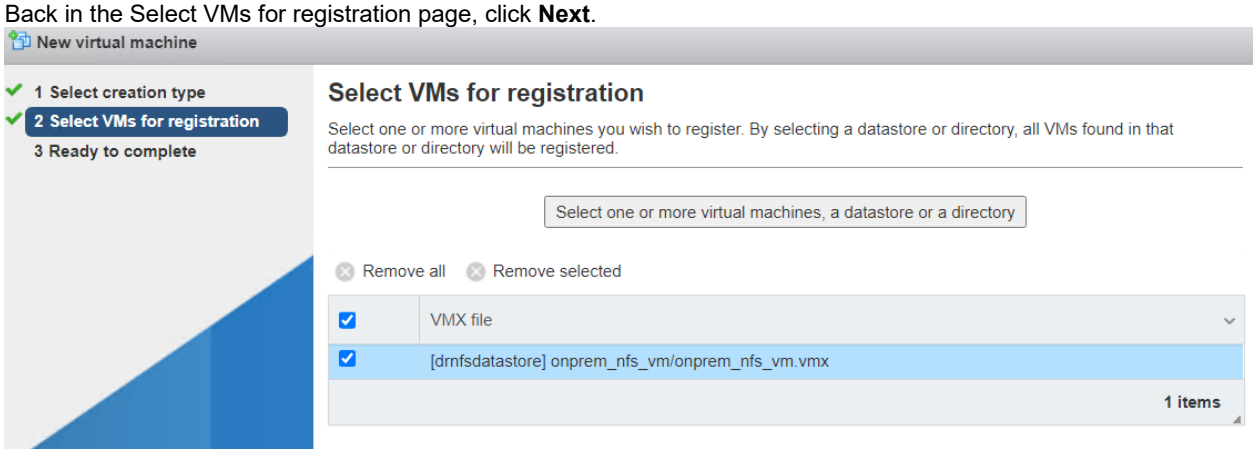
8. In the Select VMs for registration page, click **Select one or more virtual machines, a datastore, or a directory**.



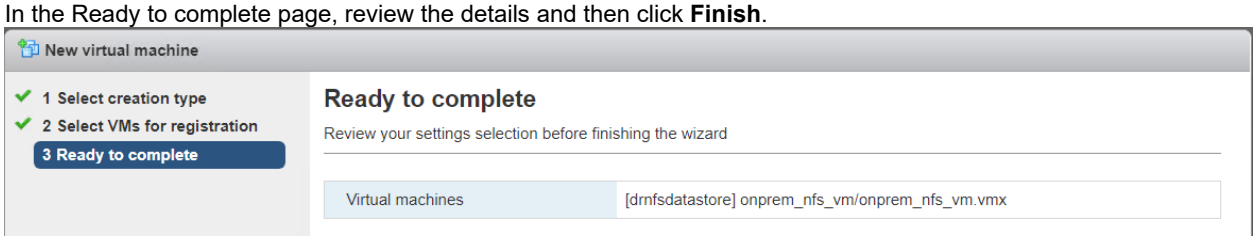
9. Locate the virtual machine VMX file on the NFS datastore and click **Select**.



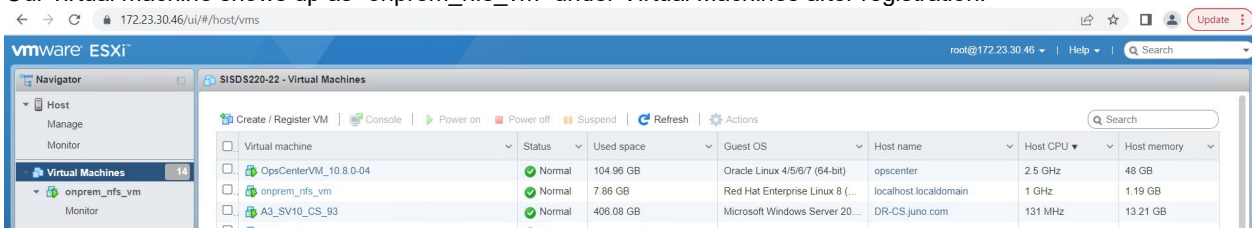
10. Back in the Select VMs for registration page, click **Next**.



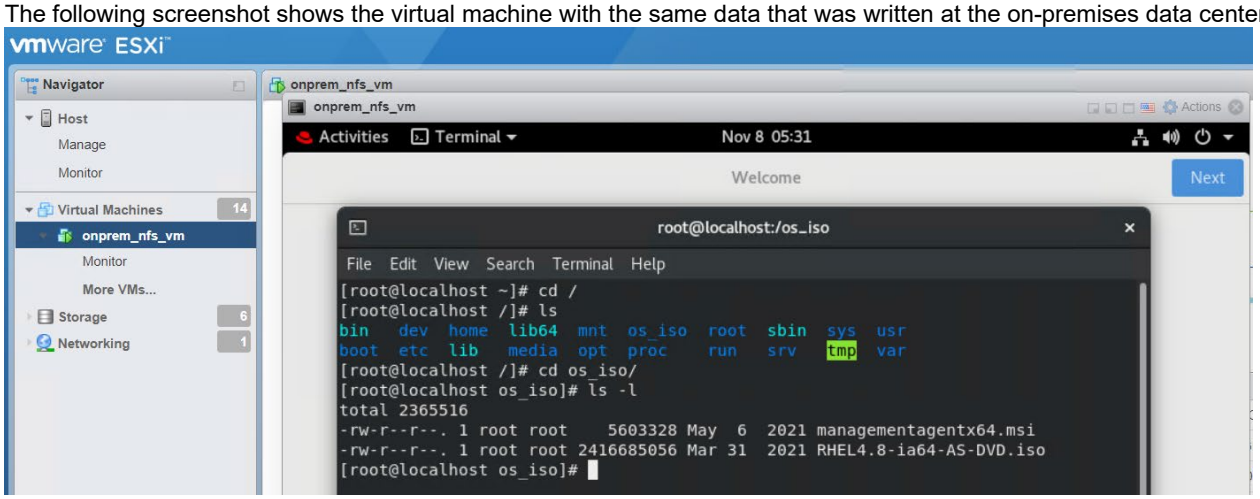
11. In the Ready to complete page, review the details and then click **Finish**.



Our virtual machine shows up as “onprem_nfs_vm” under Virtual Machines after registration.



The following screenshot shows the virtual machine with the same data that was written at the on-premises data center.



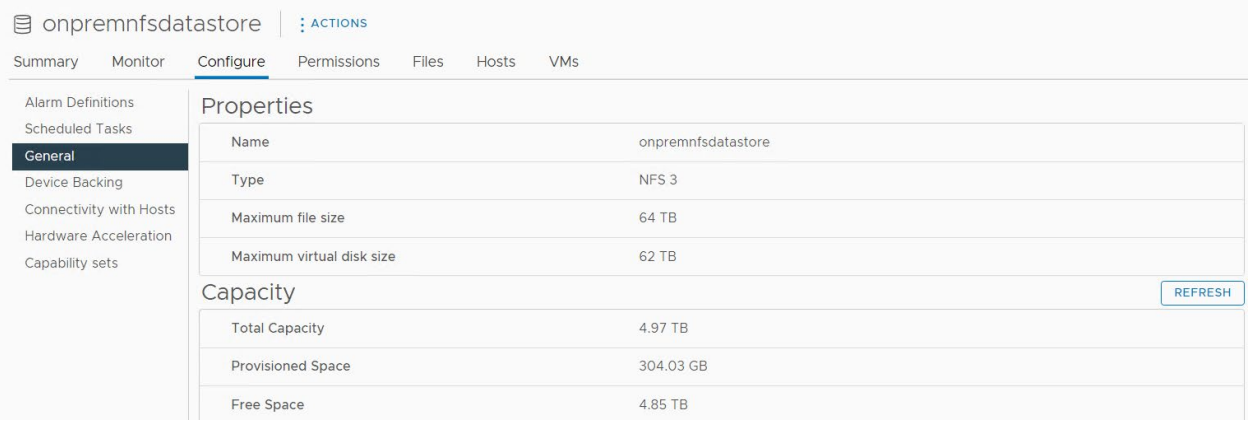
Test 7: Recover from Ransomware Attack

This test case describes how HNAS Object Replication can be used to recover virtual machines infected by a ransomware attack.

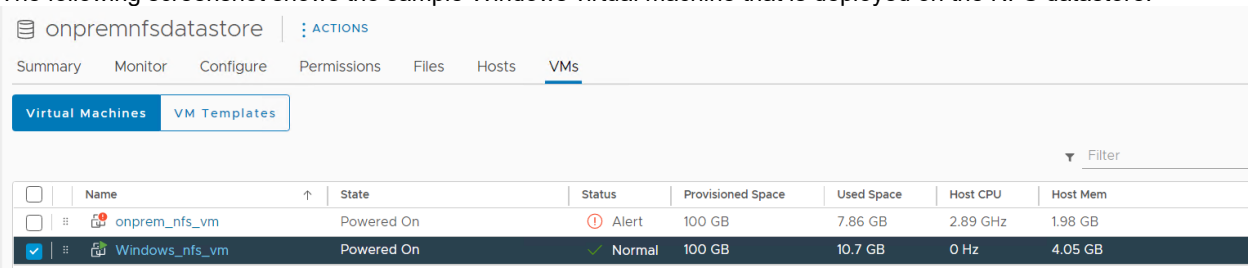
Set up

In this section, we will initiate the preparation of the test environment.

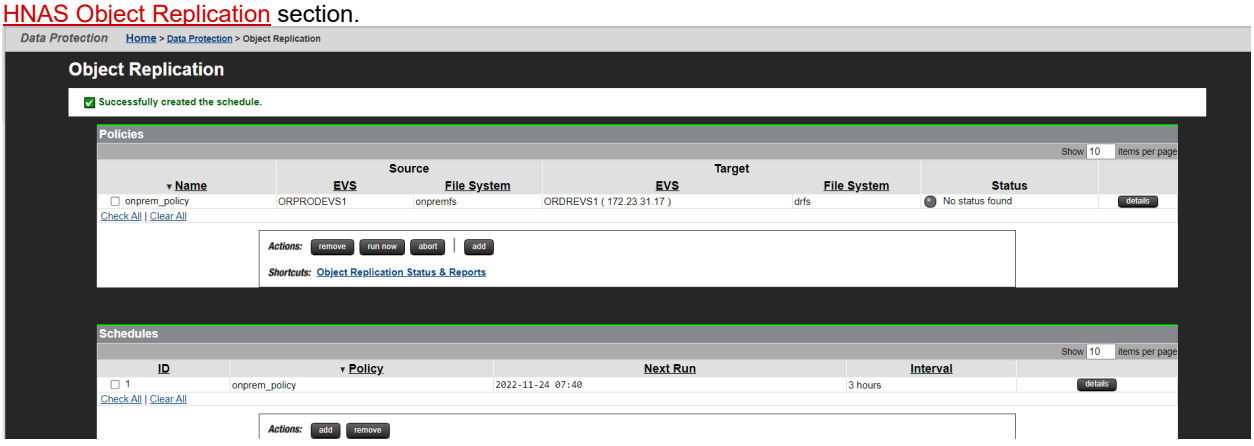
- The following screenshot shows an NFS datastore that is stored in the primary HNAS file system. For instructions, see Create Virtual Machine section.



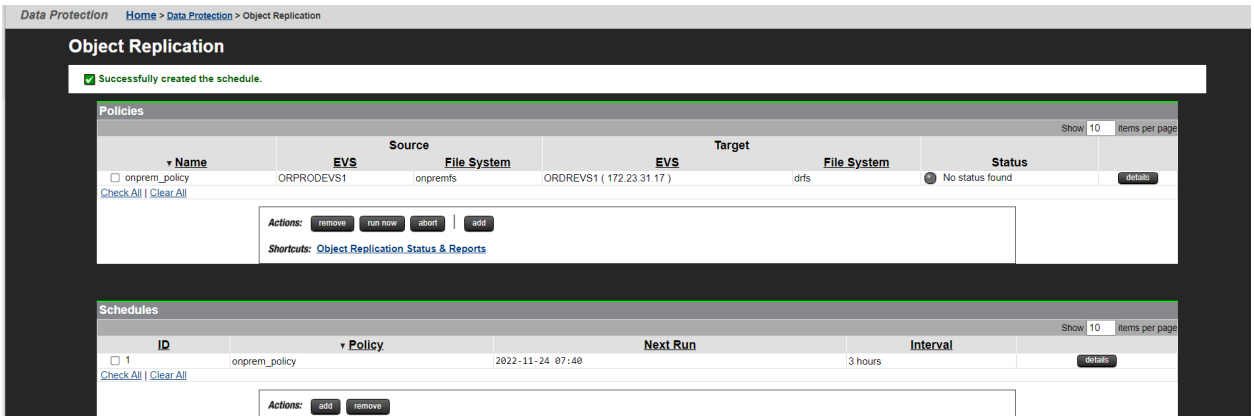
- The following screenshot shows the sample Windows virtual machine that is deployed on the NFS datastore.



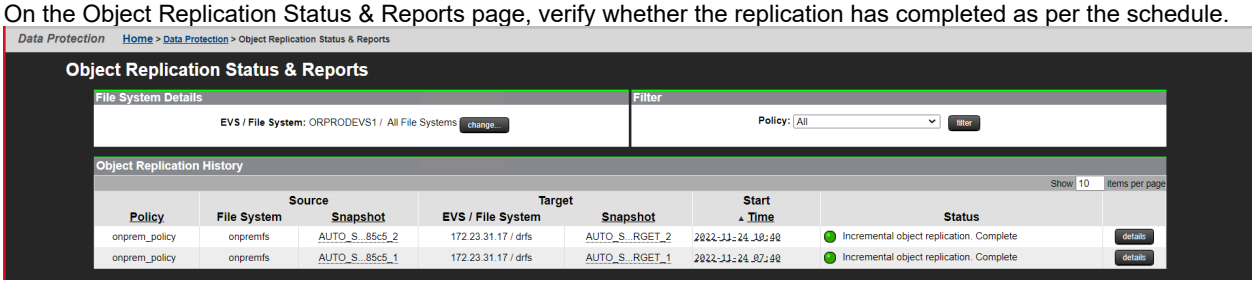
1. Create an Object Replication policy to replicate the primary and secondary file systems. For instructions, see Configure HNAS Object Replication section.



2. Configure a replication schedule that runs every three hours. For instructions, see Define Object Replication Schedules section.



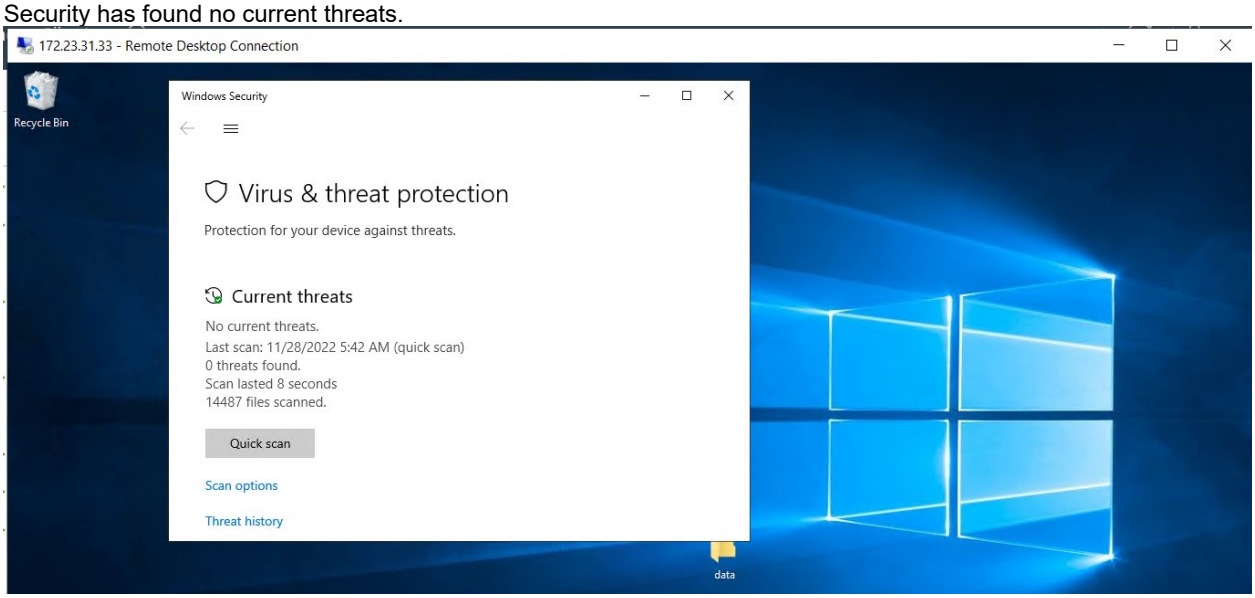
3. On the Object Replication Status & Reports page, verify whether the replication has completed as per the schedule.



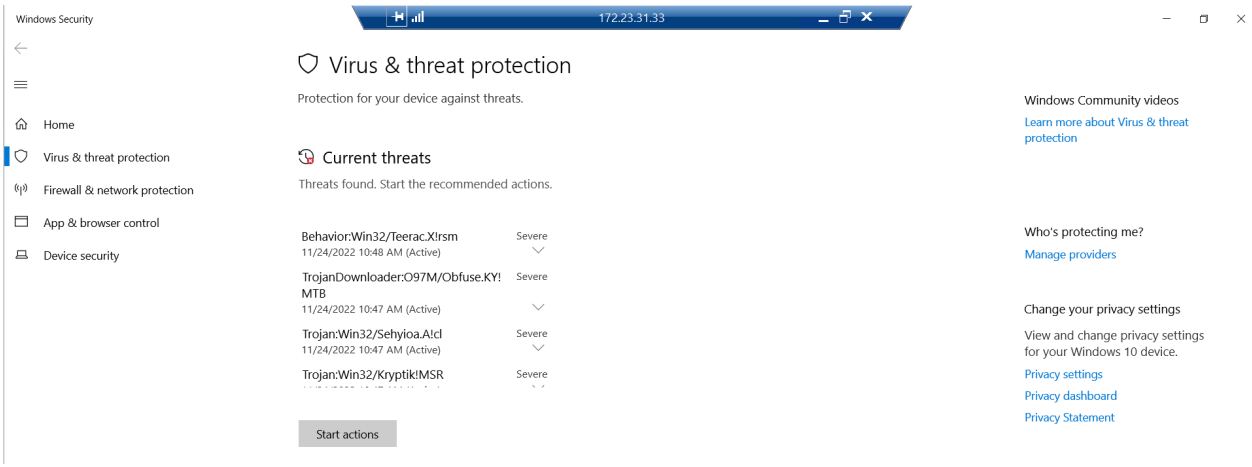
Inject Ransomware

In this section, we will inject ransomware into the virtual machine.

- The following screenshot shows the status of the Windows virtual machine before the ransomware injection. Windows Security has found no current threats.



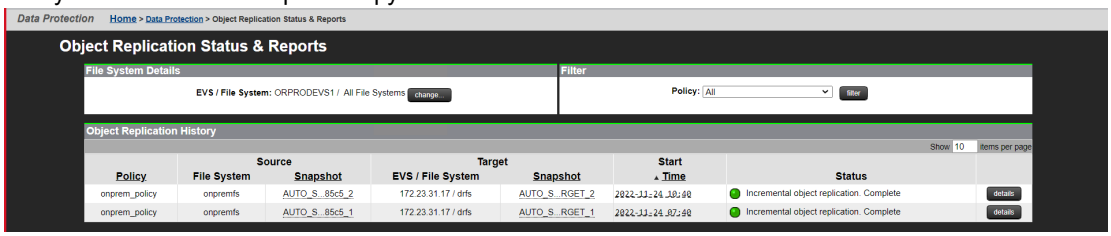
- After a ransomware simulator is used on the virtual machine, Windows Security has picked up severe ransomware threats.



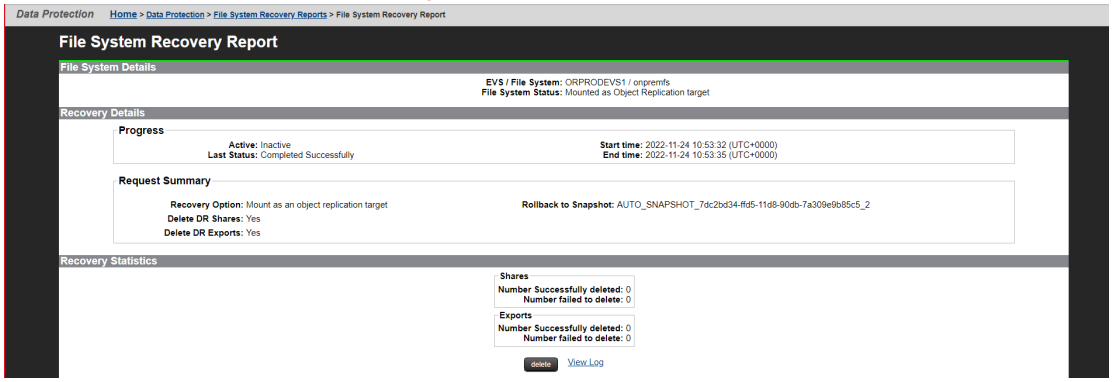
Recovery

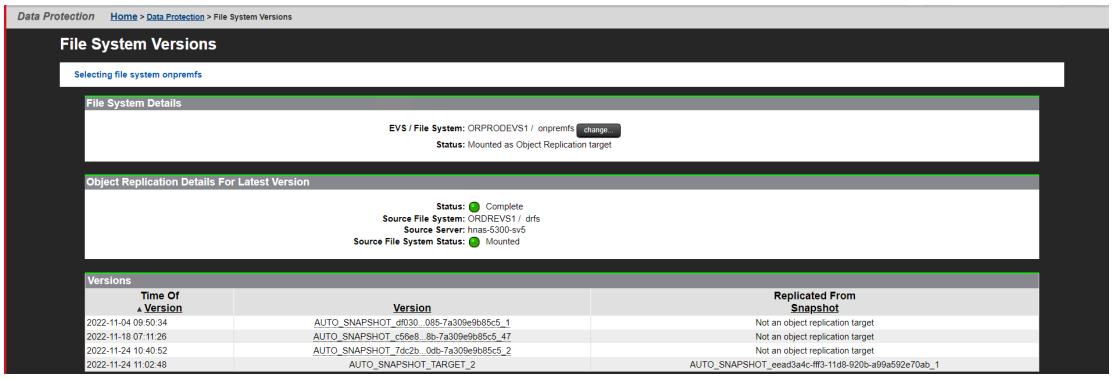
In this section, we will recover the virtual machine.

1. Promote the secondary file system running in the near-cloud data center.
   a. Verify the most recent snapshot copy.



   b. Demote the primary file system running in the on-premises data center to an Object Replication target. For instructions, see Perform Planned Outage: Failback section.

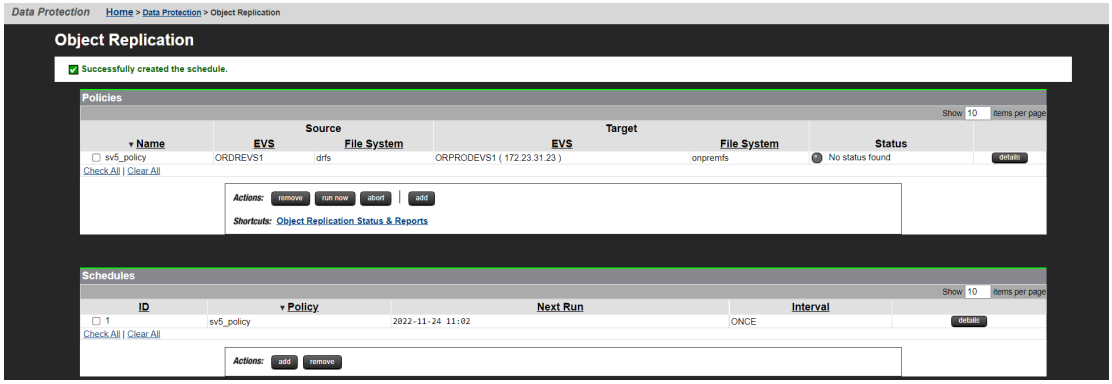




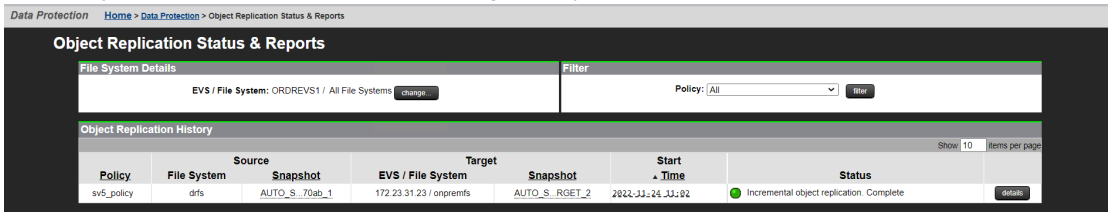
c. Promote the secondary file system running in the near-cloud data center. For instructions, see Perform Planned Outage: Failover section.

d. In the File System Recovery Reports page, verify whether the file system is recovered successfully.

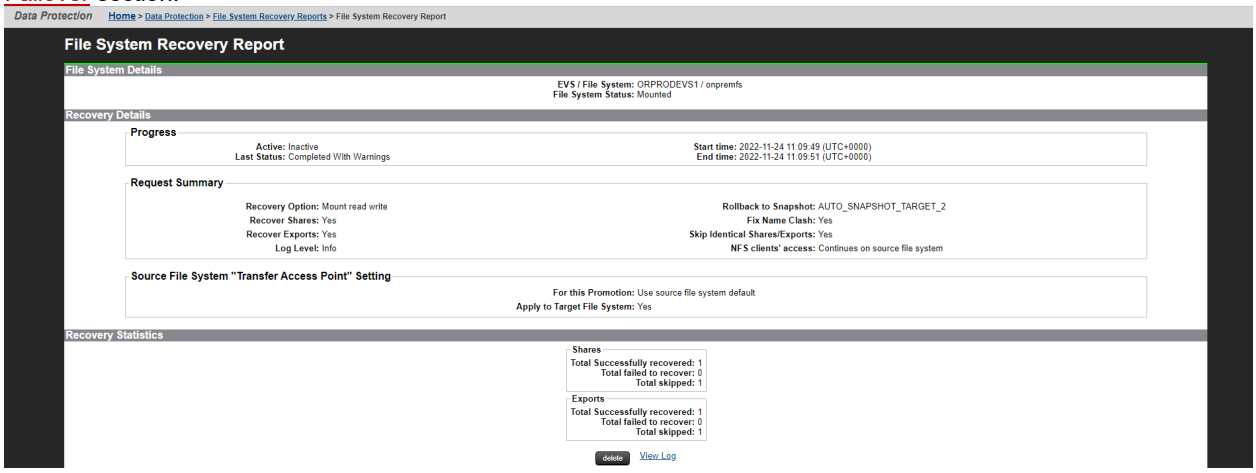
e. Create a reverse replication policy (from near-cloud to on-premises) and schedule. For instructions, see Configure HNAS Object Replication section.



f. In the Object Replication Status & Reports page, verify whether the replication is completed at least once.



2. Promote the primary file system running in the on-premises data center. For procedure, see Perform Planned Outage: Failover section.



3. After promoting, verify whether the Windows virtual machine is recovered. The following screenshot shows a new scan by Windows Security with no current threats.