Using Hitachi Cloud Connect for Equinix

Hitachi Vantara May 2023



Table of **Contents**

Notices and Disclaimer	2
About This Guide	3
Intended Audience	
Document Revisions	
References	
Comments	
Executive Summary	4
Introduction	5
Solution Overview	5
Benefits	5
Key Components	6
Validation	7
Validation Method	7
High Level Diagram	7
Hardware and Software	
Test Scenarios	
Guidelines and Recommendations	11
Validation Results	12
Test 1: Prepare the Environment	
Test 2: Configure HNAS Object Replication	
Test 3: Define Multiple Object Replication Schedules	
Test 4: Perform Planned Outage	
Test 5: Recover from Unplanned Outage	
Test 6: Migrate Virtual Machine Using Object Replication	
Test 7: Recover from Ransomware Attack	39

Notices and Disclaimer

© 2023 Hitachi Vantara LLC. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara (collectively, "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee maynot make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara at https://support.HitachiVantara.com/ en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara.

By using this software, you agree that you are responsible for:

- 1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and
- 2) Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

Hitachi is a registered trademark of Hitachi, Ltd., In the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, Flash Copy, IBM, Lotus, MVS, OS/390, PowerPC, RS6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, BCPii[™] and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or web site are properties of their respective owners.

IMPORTANT: This document can only be used as Hitachi Vantara internal documentation for informational purposes only. This documentation is not meant to be disclosed to customers or discussed without a proper non-disclosure agreement (NDA).

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: <u>https://knowledge.hitachivantara.com/Documents/Storage/NAS Platform/14.4/NAS Installation and Configuration Guide</u> s/Virtual SMU Administration Guide
- HNAS Administration Guide: <u>https://knowledge.hitachivantara.com/Documents/Storage/NAS_Platform/14.4/NAS_Administration_Guides</u>
- HNAS Replication and Disaster Recovery Administration Guide: <u>https://knowledge.hitachivantara.com/Documents/Storage/NAS Platform/14.4/NAS Administration Guides/Replication a</u> <u>nd_Disaster_Recovery Administration_Guide</u>
- HNAS Replication Best Practices Guide: https://support.hitachivantara.com/download/epcra/hnas0700.pdf

Comments

Send us any comments on this document to <u>GPSE-Docs-Feedback@hitachivantara.com</u>. 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: <u>https://hitachivantara.com/en-us/products/storage/flash-storage/cloud-connect-for-equinix.html</u>.

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-Pren	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
nises Data Cente	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
٩r	Cisco Nexus 93180YC-EX	(48) 1/10/25-Gbps fiber ports (6) 40/100-Gbps QSFP28 ports	NXOS 9.2(3)	Network switch
Equinix Ne	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
ear-Clo	HNAS 5300	HNAS 5300	Firmware 14.4.7322.05	2-node secondary HNAS cluster
oud Data	Brocade 6510	16 Gbps FC switch	FOS 8.2.1c	Provided FC connectivity between the VSP 5200 and the secondary HNAS cluster
Center	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: Provision (32) 4 TB DP volumes on VSP E790 storage system to the primary HNAS cluster. Provision (32) 6 TB DP volumes on VSP 5200 storage system to the secondary HNAS cluster. 	Environment is set up as per specifications.
	 Configure HNAS clusters: Deploy the virtual SMU at Equinix near-cloud data center. Register HNAS clusters as managed devices under SMU. Create an Enterprise Virtual Server (EVS) on HNAS clusters. Create the storage pool from VSP storage system volumes and create file system on HNAS clusters. Create SMB network shares and NFS network shares on HNAS clusters. 	
	 Deploy one Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine at the Equinix near-cloud data center. Deploy one Windows Server 2019 EC2 instance and one RHEL 8.6 EC2 instance on AWS cloud. 	
2	 Configure HNAS Object Replication: Create the HNAS file system to use as replication target. Create the Object Replication policy and schedule. 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: Fail over to the near-cloud data center by promoting Object Replication target file system. Ensure that AWS clients can access and write to the promoted file system. 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: Abruptly disable the data connection at the on-premises data center (or similar method) to create an unplanned outage. Identify the desired file system version to recover. Promote the desired version. 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: Create an NFS datastore with a file system on the primary HNAS cluster and provision a virtual machine on the datastore. Configure an HNAS Object Replication policy for the file system. Promote the target file system on the secondary HNAS cluster. Mount the NFS datastore with the promoted file system. 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: Prepare a sample virtual machine running on HNAS NFS datastore. Configure an HNAS Object Replication policy for the file system. Simulate a ransomware attack. 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.



File System on Primary HNAS:



EVS on Primary HNAS:

woodNAS - 172.23.31.20					Help About	Logged in: adn		
r Settings Home > Server Settings > I	EVS Management							
EVS Management								
Filter								
		No	Filtering Applied					
filter								
▼ Label	<u>Type</u>	Cluster Node	<u>Status</u>	First IP Address	First Port			
denvernas2	admin services	EnglewoodNAS-1	Online	172.23.31.20/23	eth0	details		
ORPRODEVS1	File Services	EnglewoodNAS-1	Online	172.23.31.23/23	ag1	details		
ORPRODEVS2	File Services	EnglewoodNAS-2	Online	172.23.31.24/23	ag2	details		



IP Address of EVS on Primary HNAS:

EnglewoodNAS - 1	72.23.31.20	Heip About
Server Settings	Home > Server Settings > EVS Management > EVS Details	
EVS D	Details ORPRODEVS1	
		Name: ORPRODEVS1 rename
		Status: © Online Tune: File Services
		Enabled: Yes
		EVS Security: Global change (Disable EVS to alter EVS security)
		Default File System Security Mode: <u>Mixed (Windows and Unix)</u>
	File Systems	
	onpremfs	
	IP Addresses	
	Port	IP Address
	ag1	172.23.31.23/23

• 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:

Ohnas-5	300-sv5 - 172.23.31.11						Help	About	Logged	i in: adm
Storage	Management <u>Home</u> > <u>Storage Management</u>	t > Storage Pools								
	Storage Pools									
	Filter									
	No Filtering Applied									
		filter								
								Sho	w 20	items pe
		<u>Capacity</u>	<u>Used (%)</u>		Used	Free	Status			
	multi_tenancy	192.00 TiB		0 %	0 Bytes	192.00 TiB	Healthy		de	etails
	ORDR	192.00 TiB		3 %	4.97 TiB	187.02 TiB	Healthy		de	etails

File System on Secondary HNAS:

Ohnas-5300-sv5 - 172.23	is-5300-sv5 - 172.23.31.11						Help	About Log	ged in: admin
Storage Management	Storage Management Home > Storage Management > File Systems								
File Systems									
Filter									
		No Filtering App	lied						
		filter							
								Show 20	items per pa
+ <u>Label</u>	Total	<u>Used (%)</u>	Used	Free	Storage Pool	Status		EVS	
Check All I Clea	4.97 TiB		2% 100.07 G	B 4.87 TiB	ORDR	Mounted as Object Replication target	ORD	REVS1	details
<u>OTECK AII</u> <u>OTE</u>	u Ali								

EVS on Secondary HNAS:

inas-5300-sv5 - 172.23.3	31.11					Help	About	Logged in: adn
rver Settings <u>Hor</u>	<u>ne > Server Settings</u> > EV	S Management						
EVS Man	agement							
Filter								
			No	Filtering Applied				
				filter				
	Label	<u>Type</u>	Cluster Node	<u>Status</u>	First IP Address	First Po	ort	
AWSEVS		File Services	hnas-5300-sv5-1	Online	172.23.31.27/23	ag2		details
AZEVS		File Services	hnas-5300-sv5-2	Online	172.23.31.28/23	ag2		details
GCPEVS		File Services	hnas-5300-sv5-1	Online	172.23.31.29/23	ag2		details
hnas-5300-1		admin services	hnas-5300-sv5-2	Online	172.23.31.11/23	eth0		details
ORDREVS1		File Services	hnas-5300-sv5-1	Online	172.23.31.17/23	ag1		details



IP Address of EVS on Secondary HNAS:

Ohnas-5300-sv5 - 17	72.23.31.11					Help
Server Settings	Home > Server Settings > EVS Management > E	/S Details				
EVS	Details ORDREVS1					
			Name:	ORDREVS1 renam	e	
			EVS ID: Status:	Online		
			Enabled:	Yes		
			EVS Security:	Individual		
		Defa	ult File System Security Mode:	Mixed (Windows and Unix)		
	File Systems					
	drfs					
	IP Addresses					
	Por			IP Address		
	ag1	172.23	31.17/23			

• 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:

EnglewoodNAS	- 172.23.31.20			Help About	Logged in
File Services	Home > File Services > CIFS Setup				
	CIFS Setup				
		EVS: ORPRODEVS1	change		
	Mode	[¹	NetBIOS		
	Security Mode: Mixed (Wir	dows and Unix)	NetB	IOS: Disabled enable	
	ADS Domain: juno.com				
	DDNS: Enabled	disable			
	Configured CIES Server Names				
	CIFS Server Nan	<u>IE</u>	▼ <u>Mode</u>	Disjoint	
	onpremcifsserver		ADS	no	
	Check All Clear All				

SMB Shares on Primary HNAS:

EnglewoodNAS - 172.23.31.20			Help	About Logged in: admin Si
ile Services Home > File Services > CIFS Shares				
CIFS Shares				
EVS / File System Label		Filter		
ORPRODEVS1 / All File Systems change		Name:		
		Path:		
		Transfer to Object Replication Target: None	~	
			ilter	
				Show 20 items per page
▼ <u>Name</u>	Comment	File System	Path	
C\$	Default share	Unknown	V	details
□ drcifs		onpremfs	1	details
onpremcifs		onpremfs	V. Contraction of the second s	details
Check All Clear All				

NFS Exports on Primary HNAS:

O EnglewoodNAS - 172.23.31.20			Hel	About Logge	d in: admin Sig
File Services Home > File Services > NFS Exports					
NFS Exports					
EVS / File System Label		Filter			
ORPRODEVS1 / onpremfs change			Name:		
			Path:		
		Transfer to Object Re	eplication Target: None	~	
			filter		
				Show 20	items per page
▼ <u>Name</u>	File S	<u>System</u>	Path		
/dmfs	onpremfs	/	1	details	
/onpremnfs	onpremfs	/	/	details	

CIFS Setup on Secondary HNAS:

as-5300-sv5 -	172.23.31.11					нер	About	Logged in
Services	Home > File Services > CIFS Setup							
	CIFS Setup							
			EVS: ORDREVS1	change				
	Mode	Security Mode: Mixed (Windows and Unix)		NetBIOS	NetBIOS: Di	sabled enable	e	
		ADS Domain: juno.com DDNS: Enabled disable						
	Configured CIFS Server Name	S					_	
		CIFS Server Name			▼ <u>Mode</u>		<u>Disjoint</u>	
	drcifsserver			ADS		no		
	Check All Clear All							

SMB Shares on Secondary HNAS:

s-5300-sv5 - 172.23.31.11			Help	About Logged in: admin S
ervices Home > File Services > CIFS Shares				
CIFS Shares				
EVS / File System Label		Filter		
ORDREVS1 / All File Systems change		Name:]
		Path:		1
		Transfer to Object Replication Target:	None V]
			filter	
				Show 20 items per page
▼ <u>Name</u>	Comment	File System	Path	
C\$	Default share	Unknown	V	details
drcifs		drfs	1	details
onpremcifs		drfs	N I I I I I I I I I I I I I I I I I I I	details

NFS Exports on Secondary HNAS:

Ohnas-5300-sv5 - 172.23.31.11				Help About Logg	ged in: admin 🛛 S
File Services Home > File Services > NFS Exports					
NFS Exports					
EVS / File System Label		Filter			
ORDREVS1 / drfs change			Name:		
			Path:		
		Transfer to Object	Replication Target: None	~	
			filter		
				Show 20	items per page
▼ <u>Name</u>	File	<u>System</u>	Path		
/dmfs	drfs		1	details	
/onpremnfs	drfs		1	details	

• The following screenshots show the HNAS clusters being managed by one virtual SMU. For usage details, see <u>Virtual</u> <u>SMU Administration Guide</u>.

Virtual SMU: NAS Manager		
Server Status Console EnglewoodNAS - 172.23.31.21 V Innas-5300-ev5 - 172.23.31.21 V EnglewoodNAS - 172.23.31.20	System Monitor • Event Log • Email Alerts Setup • SNMP Traps Setup •	Server Settings EVS Management • Server

Status of Primary HNAS:

Engle	woodNAS - 172.23.31.20	1		Нер	About	Logged in: admin Si				
Server	erver Settings Home > Server Settings > Cluster Configuration									
	Cluster Conf	iguration								
	Cluster Nodes									
	▼ <u>Name</u>	IP Address	Model	Health		EVS				
	EnglewoodNAS-1	172.23.31.22	HNAS 5300	Degraded		denvernas2., ORPRODEVS1		details		
	EnglewoodNAS-2	172.23.31.21	HNAS 5300	Degraded		ORPRODEVS2		details		
	Cluster Information	n			Quorum	Device				
		Cluster Name:	EnglewoodNAS			Name: HNASSMU				
		Health:	Robust			IP Address: 172.23.31.160 Status: Configured				
		Cluster UUID:	49eca2ec-dfd5-11d8-9000-7a309e9b85	ōc5		add remove				
	•	WAC.	19-20-28-20-02-02	I	I			· · · · ·		
Statu	s of Seconda	ary HNAS								
Ohnas-6	5300-sv5 - 172.23.31.11	ary 110.00.				Help	About	Logged in: admin S		
Server	Settings <u>Home</u> > s	ierver Settings > Cluster Co	nfiguration							
	Cluster Conf	iguration								
	Cluster Nodes									
	▼ <u>Name</u>	IP Address	Model	<u>Health</u>		EVS				
	hnas-5300-sv5-1	172.23.31.15	HNAS 5300	Degraded		AWSEVS., GCPEVS., ORDREVS1		details		
	hnas-5300-sv5-2	172.23.31.16	HNAS 5300	Degraded		hnas-5300-1, AZEVS, ORDREVS2		details		
	Cluster Information	1			Quorum	Device				
		Cluster Name:	hnas-5300-sv5 rename			Name: HNASSMU				
		Health:	Robust		IP Address: 172.23.31.160					
		Cluster UUID:	5ea89f3c-cbe0-11d8-9000-a99a592e70	lab	Status: Configured					
		MAC:	a9-9a-59-2e-70-ab	add remove						

-11

Inspire the Next

Lo

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 <u>HNAS Replication Best</u> <u>Practices Guide</u>.

 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.

 hnas-5300-sv5 - 172.23.31.11

Storage Management	Home > <u>Storage Management</u> > <u>File Systems</u> > File System Details	
File System	n Details	
	Settings/Status	
	Label: drfs	rename
	Capacity	Configuration
	1% Total Used Space Capacity: 4.97 TiB Free: 4.94 TiB (99%) Total Used: 36.94 GiB (1%) Expansion Limit: 0 Bytes Legend: Live file system Usage Warning Usage Severe	Status: Mounted as Object Replication target Deduplication: <u>Enabled</u> Thin Provisioning: Disabled EVS: ORDREVS1 (Online) Block Size: 4 KiB Read Cache: No WFS Version: WFS-2
Inas-5300-sv5 - 172.23.31.11 Storage Management Hom	16 > Storage Management > File Systems	Object Replication Target: Enabled Transfer Access Points During Object Replication: Enabled Transfer XVLs as Links During Object Replication: Disabled Hep About Logged in: admin S
Storage Management <u>Hom</u>	<u>10 > Storage Management</u> > File Systems	

File Syster	ms							
Filter								
		No Filtering Appl	lied					
		filter						
							Show 20	items per page
Label	Total	Used (%)	lise	ed Free	• <u>Storage</u> Pool	Status	EVS	
☐ drfs	4.97 TiB	<u>03cu (70)</u>	2% 11	2.86 GiB 4.86 Til	B ORDR	Mounted as Object Replication target	ORDREVS1	details

• 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.

nglewoodNAS - 172.23.31.2	20							Help About	Logged	in: admin Sig
rage Management 🛛 💾	Home > Storage Mana	gement > File Systems								
File Systems	;									
Filter										
	No	Filtering Applied								
		filter								
									Show 20	items per page
▼ Label	<u>Total</u>	<u>Used (%)</u>		Used	Free	<u>Storage</u> <u>Pool</u>	<u>Status</u>	EVS		
🔽 onpremfs	4.97 TiB		2%	99.90 GiB	4.87 TiB	ORPROD	Mounted	ORPRODEVS1		details

HITACHI Inspire the Next

Disaster Recovery in Hybrid Cloud Environments with HNAS Object Replication

Storage Management Home > Storage Management > File Systems > File System Details	
File System Details	
Settings/Status	
Label: onpremfs	rename
Capacity	Configuration
Legend: Worf file system Usage Warning Usage Severe	Status: Mounted Deduplication: <u>Enabled</u> Thin Provisioning: Disabled EVS: ORPRODEVS1 (Online) Security Mode: Mixed (Vindows and Unix) (Inherited) Block Size: 4 KiB Read Cache: No WFS Version: WFS-2 Syslock: Disabled Chipet Replication: Enabled Transfer Access Points During Object Replication: Enabled Transfer XVLs as Links During Object Replication: Disabled Transfer XVLs as Links During Object Replication: Disabled

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

SMB Shares on Primary HNAS:				
O EnglewoodNAS - 172.23.31.20			Help	About Logged in: admin S
File Services Home > File Services > CIFS Shares				
CIFS Shares				
EVS / File System Label		Filter		
ORPRODEVS1 / All File Systems change		Name:		
		Path:		
		Transfer to Object Replication Target:	None 🗸	
			filter	
				Show 20 items per page
▼ <u>Name</u>	Comment	File System	Path	
C\$	Default share	Unknown	ν.	details
☐ drcifs		onpremfs	۱.	details
onpremcifs		onpremfs	1	details
Check All Clear All				

NFS Export on Primary HNAS:

EnglewoodNAS - 172.23.31.20			Help	About Logged in: a	admin Sign
File Services Home > File Services > NFS Exp	orts				
NFS Exports					
EVS / File System Label		Filter			
ORPRODEVS1 / onpremfs change			Name:		
			Path:		
		Transfer to Object R	eplication Target: None	~	
			filter		
				Show 20 ite	ems per page
▼ <u>Name</u>	File	<u>System</u>	<u>Path</u>		
/onpremnfs	onpremfs		1	details	

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

EnglewoodNAS -	172.23.31.20				Help	About	Logged in: admin	
Data Protection	Home > Data Protec	tion > Object Replication	1					
Object	Dbject Replication							
Polic	ies							
			Source		Target			
	▼ <u>Name</u>	EVS	File System	EVS	File System		Status	
		Actions: remove	run now abort add					



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

EnglewoodNAS -	172.23.31.20		Help	About	Lo
Data Protection	Home > Data Protection > Object Replication > Add Object Replication Policy			_	
Add Ol	oject Replication Policy				
	Identification				
	Name:	onprem2nearcloud			
	Source				
	EVS / File System:	ORPRODEVS1 / onpremfs change			
	EVS IP Address:	172.23.31.23			
	Target				
	Server:	hnas-5300-sv5 ~			
		Click "select a target" to choose an EVS and file system.			
	EVS:	ORDREVS1	select a target	J	
	EVS IP Address: File System:	172.23.31.17 V			
	Object Replication Listening Port:	59550			
		next cancel			
In the Process	sing Ontions name, select the required ontion	and click peyt			
EnglewoodNAS -	172.23.31.20		Help	About	1.
Data Protection	Home > Data Protection > Object Replication > Add Object Replication Policy		- nop	- About	
Data Flotection	Tome > Data Protection > Object Replication > Add Object Replication Policy				
Add Ol	piect Replication Policy				

Processing Options	
Source	e File System
	Snapshot source file system using automatic snapshot rule
	○ Use snapshot rule Select rule ✓
Targe	t File System
	Snapshot target file system using automatic snapshot rule
	○ Use snapshot rule Select rule ∨
	Read the online help and its warnings before selecting a named snapshot rule
	back next cancel

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

Data Protection Home > Data Protection > Object Replication > Add Object Replication Policy

The form some some some some some some some som
Add Object Replication Policy
Identification
Name: onprem2nearcloud
Source
EVS / File System: ORPRODEVS1 / onpremfs
EVS IP Address: 172.23.31.23
Transfer to Object Replication Target: Enabled (Access points will be transferred to the object replication target unless specifically configured otherwis
Target
EVS: ORDREVS1 (172.23.31.17)
File System: drfs
Object Replication Port: 59550
Processing Options
Source Snapshot: Snapshot source file system using automatic snapshot rule
Target Snapshot: Snapshot target file system using automatic snapshot rule
back create cancel

c.



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

EnglewoodNAS - 1	72.23.31.20					Help About	Logged in: admin
Data Protection	Home > Data Protec	tion > Object Replication					
Object	Replication						
Policie	s						
						Show 1	0 items per page
		5	Source		Target		
	▼ <u>Name</u>	EVS	File System	EVS	File System	Status	
🗆 on	premrcloud	ORPRODEVS1	onpremfs	ORDREVS1 (172.23.31.17)	drfs	No status found	details
Check A	II <u>Clear All</u>						
		Actions: remove r	run now abort add)			

- 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.

EnglewoodNAS - 17	2.23.31.20					Help Ab	out Lo	ogged in: admin
ata Protection	Home > Data Prote	ction > Object Replication						
Object F	Replication	l.						
Policie	s							
							Show 10	items per page
		:	Source		Target			
	▼ <u>Name</u>	EVS	File System	EVS	File	<u>System</u> Stat	us	
	premrcloud	ORPRODEVS1	onpremfs	ORDREVS1 (172.23.31.17)	drfs	No status for	ind	details
Check A	I Clear All							
		Actions: remove	run now abort add					
		Shortcuts: Object Rep	lication Status & Reports					
Schedu	iles	_	_					
ID		▼ Policy		<u>Next Run</u>		Interva	al	
		Actions: add rem	ove					

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**.

	2.23.31.20	
Data Protection	Home > Data Protection > Object Replication	1 > Add Object Replication Schedule
Add O	bject Replication Schec	lule
	Poli	cy
		Policy: onprem2nearcloud EVS / File System: ORPRODEVS1 / onpremfs
	Initia	al Run
		Immediately: Start as soon as the schedule is created Scheduled
		Time of Initial Run: 10:21 (24 hour time) Date of Initial Run: 2022-11-07 Image: Compare the second s
		Current date and time on EnglewoodNAS: 2022-11-07 10:14:06 (UTC+0000)
	Run	Until (Optional)
		Run Until Time: (24 hour time) Run Until Date: III
	Sch	edule Type
		Every Iminutes v - based on the scheduled date and time. Continuous. Pause Iminutes v between runs. Once, at the scheduled date and time. Test Only - at the scheduled date and time. test can be a long process. It will assess an object replication's likely success, and the amount of data to be replicated. The results should be hecked in the Object Replication Status & Reports page before scheduling a full run. OK cancel



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

	Englewo	oodNAS - 172.23.31.20	10,				Help	About	Logged in: adm
	Data Pro	tection Home > Data Protection >	Dbject Replication						
		Object Replication							
		Successfully created the sched	ule.						
		Policies							
								Show 10	items per page
		- Nomo	EVC	Source	Targ	get File Svotem	Ctatua		
			ORPRODEVS1	onpremfs	ORDREVS1 (172 23 31 17)	difs	No status found		details
		Check All Clear All	01111002101	onpromo		0110			
			Actions: remove run now	abort					
			Shortcuts: Object Replication	n Status & Reports					
		Schedules							
								Show 10	items per page
		ID	▼ <u>Policy</u>		Next Run		Interval		
		1 ong	remrcloud	2022-11	-07 10:21	ONCE		detail	
		Check All Clear All							
3.	In the Object R	eplication page, v	erify whether t	he replication	policy shows a Cor	mplete status.			
	EnglewoodNAS - 172.23.31	1.20					Help /	About	Logged in: adm
	Data Protection Home	Data Protection > Object Replication	L. C.						
	Object Rej	plication							

Policies							
						Show 1	10 items per page
		Source		Target			
	EVS	File System	EVS		File System	Status	
onpremrcloud	ORPRODEVS1	onpremfs	ORDREVS1 (172.23.31.17)	drf	s	Complete	details
Check All Clear All							
	Actional Common Common						
	Actions. Temove Tun now	add					
	Shortcuts: Object Replication	Status & Reports					

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**.

EnglewoodNAS - 17	2.23.31.20	
Data Protection	Home > Data Protection > Object R	eplication > Add Object Replication Schedule
Add O	bject Replication S	chedule
		Policy
		Policy: onprem2nearcloud EVS / File System: ORPRODEVS1 / onpremfs
		Initial Run
		Immediately: Start as soon as the schedule is created Scheduled
		Time of Initial Run: 10:45 (24 hour time) Date of Initial Run: 2022-11-07 Image: Compare the second
		Current date and time on EnglewoodNAS: 2022-11-07 10:30:44 (UTC+0000)
		Run Until (Optional)
		Run Until Time: (24 hour time) Run Until Date: Image:
		Schedule Type
		 Every A hours - based on the scheduled date and time. Continuous. Pause minutes between runs. Once, at the scheduled date and time. Test Only - at the scheduled date and time. A test can be a long process. It will assess an object replication's likely success, and the amount of data to be replicated checked in the Object Replication Status & Reports page before scheduling a full run.
		OK cancel

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

Data Protection	Home > Data Protection > Object Replication Status & Reports > Object Replication Status
Objec	t Replication Status
	Policy Details
	Policy Name: onprem2nearcloud Source EVS / File System: ORPRODEVS1 / onpremfs
	Target EVS / File System: 172.23.31.17 / drfs Target File System Versions
	Report Summary
	Source Snapshot: AUTO_SNAPSHOT_c56e85c6-f28f-11d8-908b-7a309e9b85c5_3 Target Snapshot: AUTO_SNAPSHOT_TARGET_4
	Start Time: 2022-11-07 16:45 End Time: 2022-11-07 16:45 Duration: 1 sec
	File System Data Transferred: 19.95 KiB File System Transfer Rate: 19.95 KiB/s
	Objects Complete: 19 Object Transfer Rate: 19 objects/s
	Object Replication Type: Incremental object replication: based on snapshot AUTO_SNAPSHOT_c56e85c6.428f-11d8-908b- 7a300e8b85c5_2 Status: Complete: Success



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

EnglewoodNAS - 1	172.23.31.20						Help	About	Logged in: adn
Data Protection	Home > Data Prote	ection > Object Replicati	on Status & Reports						
Objec	t Replicatio	on Status & I	Reports						
File	e System Details				Filter				
		EVS / File System:	ORPRODEVS1 / All File S	Systems change		Policy: Al	↓ v fitter		
Ob	ject Replication I	History							
								Show 10	items per page
		Sc	ource	Targ	et	Start			
	Policy	File System	Snapshot	EVS / File System	Snapshot	.▲ <u>Time</u>	Status		
	onpremrcloud	onpremfs	AUTO_S85c5_4	172.23.31.17 / drfs	AUTO_SRGET_5	2022-11-07-22:45	Incremental object replication. Complete		details
	onpremrcloud	onpremfs	AUTO_S85c5_3	172.23.31.17 / drfs	AUTO_SRGET_4	2022-11-07-16:45	Incremental object replication. Complete		details

- 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**. *Data Protection* Home > Data Protection > Object Replication > Add Object Replication Schedule

Add Object Replicat	ion Schedule			
	Policy			
		Policy: or EVS / File System: OF	nprem2nearcloud RPRODEVS1 / onpremfs	
	Initial Run			
		Immediately: Start as soon as Scheduled Time of Initia Date of Initia	the schedule is created ial Run: 04:00 (24 hour to 10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	ime)
		Current date and time on Engle	ewooanas: 2022-11-08 03:42:48 (UTC+	0000)
	Run Until (Optional)			
		Run Until Time: Run Until Date:	(24 hour time)	
	Schedule Type			
	 Every 1 days Continuous Pause Once, at the scheduled date Test Only - at the scheduled A test can be a long process checked in the Object Replice 	- based on the scheduled date and minutes ➤ between runs. and time. date and time. <i>t</i> will assess an object replication's ation Status & Reports page before schedule	d time. Ilikely success, and the amount of data t scheduling a full run. OK cancel	o be replicated. The results should be
Data Protection Home > Data Protection > Object				
Object Replication				
Successfully created the schedule.				
Policies				
v Name onpremrcloud Check All Clear All	Source EVS File Sy ORPRODEVS1 onpremfs	vstem I ORDREVS1 (172.23.31.17	Target EVS File Sy Africe	ystem Status Complete
	Actions: remove run now abort add Shortcuts: Object Replication Status & Reports			
Schedules				
	• Policy	Next R	lun	Show 10

2022-11-08 04:00

1 day

deta

b.

1 Check All | Clear All

onprem...rcloud



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

EnglewoodNAS - 17	72.23.31.20						Help	About	Logged in: admi
Data Protection	Home > Data	Protection > Object F	Replication Status & Repo	orts					
Object	Replica	tion Status	& Reports						
File S	ystem Detai	ls			Filter				
		EVS / File System:	ORPRODEVS1 / All Fil	e Systems change		Policy: All	▼ filter		
Objec	t Replicatio	n History							
		0.0		Tean	- 4	04-rt		Show 10	items per page
1	Policy	File System	Snapshot	EVS / File System	Snapshot	start ▲ <u>Time</u>	Status		
onpre	emrcloud	onpremfs	AUTO_S85c5_9	172.23.31.17 / drfs	AUTO_SGET_10	2022-11-09_04:00	Incremental object replication.	Complete	details
onpre	emrcloud	onpremfs	AUTO_S85c5_8	172.23.31.17 / drfs	AUTO_SRGET_9	2022-11-08_10:17	Incremental object replication.	Complete	details
onpre	emrcloud	onpremfs	AUTO_S85c5_7	172.23.31.17 / drfs	AUTO_SRGET_8	2022-11-08-09:50	Incremental object replication.	Complete	details
onpre	emrcloud	onpremfs	AUTO_S85c5_6	172.23.31.17 / drfs	AUTO_SRGET_7	2022-11-08-06:51	Incremental object replication.	Complete	details
onpre	emrcloud	onpremfs	AUTO_S85c5_5	172.23.31.17 / drfs	AUTO_SRGET_6	2022-11-08-04:00	Incremental object replication.	Complete	details

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**. Data Protection Home > Data Protection > File System Recovery Selection

File System Recovery Selection	
File System Details	
EVS / File System: ORDREVS1 / drfs Status: Mounted as Object Replication target	
Which type of file system recovery do you want to do?	
Promote the file system to a normal file system (and optionally, mount as read-write or read-only)	
Demote the file system to an Object Replication Target (and mount as an Object Replication Target)	

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

ile System Details		
	EVS / File System: ORDREVS1 / drf Status: Mounted as Objer	fs ct Replication target
Dbject Replication Details For Latest Version		
	Status: Complete Source File System: ORPRODEVS1 / Source Server: EnglewoodNAS Source File System Status: Mounted	onpremfs
	The follow	ving steps will be taken
	ATTENTION: Read the online he	Ip and its warnings before proceeding
	1: Unmount drfs	
	2: Recover file system to version create Version snapshot Snapshot on source file s	ed at 2022-11-09 11:35-12 name: AUTO_SNAPSHOT_TARGET_11 ystem: AUTO_SNAPSHOT_c56e85c6-f28f-11d8-908b-7a309e9b85c5_10
	3: Promote file system drfs and	mount read write
	4: Recover access points	
	 CAPUTS Which file system will NFS (Both file systems belong to © Clients will continue to Exports recovered on the te Both file systems will then h O Clients will access targ Exports will be moved from 	clients be accessing after recovery? o the same EVS) access source file system (onpremfs) arget file system will be named (export name_clask id) to avoid conflict with (export name) on the sou have their own set of exports. pet file system (drfs) without interruption the source file system to the target without the need to remount NFS v2/3 clients. The source file sys



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

ala Frolection Hol	The > Data Protection > File System Versions > Recover File System	Contirmation
Recover	File System Confirmation	
File Sys	tem Details	
		EVS / File System: ORDREVS1 / drfs Status: Mounted as Object Replication target
		The following steps will be taken
		1: Unmount drfs
		2: Recover file system from snapshot AUTO_SNAPSHOT_TARGET_11
		3: Promote file system drfs and mount read write
		Recover access points shares exports (Clients of recovered exports will continue to access source file system onpremfs)
		back OK cancel
ne following s	creenshot shows the recovery ta	sk is running:
Data Protection	Home > Data Protection > File System Recovery Reports >	File System Recovery Report
File Sy	stem Recovery Report	
V Succe	essfully requested recovery of file system drfs to version	n AUTO_SNAPSHOT_TARGET_11
File Syste	m Details	
		EVS / File System: ORDREVS1 / drfs File System Status: Not mounted
Recovery	Details	
	Progress	
	Active: Active Last Status: Running	Start time: 2022-11-09 11:40:45 (UTC+0000) End time:
	Request Summary	
	Recovery Option: Mount read w	rite Rollback to Snapshot: AUTO_SNAPSHOT_TARGET_11
	Recover Shares: Yes	Fix Name Clash: Yes
	Recover Exports: Yes Log Level: Info	Skip Identical Shares/Exports: Yes NFS clients' access: Continues on source file system
	Source File System "Transfer Access Point"	Setting
		For this Promotion: Use source file system default Apply to Target File System: Yes
		· · · · · · · · · · · · · · · · · · ·
Recovery	Statistics	
		Shares Total Successfully recovered: 0 Total failed to recover: 0 Total skipped: 0 Exports
		Total Successfully recovered: 0 Total failed to recover: 0 Total skipped: 0
		abort <u>View Log</u>

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

File System	S									
Filter										
		No Filtering Applied								
		filter								
		into a								
									Show 20	items per page
+ <u>Label</u>	Total	<u>Used (%)</u>		Used	Free	Storage Pool	Status	EVS		
🗌 drfs	4.97 TiB		2%	100.08 GiB	4.87 TiB	ORDR	Mounted	ORDREVS1		details
Check All Clear All										
Actions: mount	unmount create Down	oad 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:**

🌄 10.77.24.99 - Re	emote Desktop Co	nnectio	on										-		×
Recycle Bin											Hostnar Instance	ne: EC2AM 2 ID: i-0a51	AZ-U38 870cd0	3605J)3d46b	12
	💂 📝 📙 🖛 dr	cifs										- 0	×	7.24.99	9
	File Home	Share	View										~ 🕐	1b	
Q		> Net	work > 172.23.31	17 > droifs >						~ 71	Search droifs		0		
EC2		· neu		^						¥ U	Search arens		~		
Feedback	Ouick access		Name			Date modified	Туре	Size						w to M	oderate
	Deckton		\$DEDU	PE_		11/3/2022 7:08 AM	File folder								
1	Desktop	<u></u>	S_NDM	P		11/3/2022 6:03 AM	File folder								
7	Documents		iso			11/9/2022 5:36 AM	File folder								
EC2 Micros	Downloads	R	onprem_	nfs_vm		11/8/2022 6:28 AM	File folder								
	Pictures	*	test_file_l	linuxclient_ec2		11/9/2022 11:30 AM	File		1 KB						
	💻 This PC		Test_file_	WinClient_EC2		11/9/2022 11:26 AM	Text Document		1 KB						
[root@ip-10-7	7-25-18 ~]# h	nostna	ame	1											
[root@in-10-7	7-25-18 ~]# «	showne	unt -e 17	1 2 23 31 17											
Export list f	or 172.23.31.	.17:	June C 17.	2.25.51.17											
/drnfs *															
/onpremnfs *															
[root@ip-10-7	7-25-18 ~]# m	nount	-t nfs 172	2.23.31.17:	/drnfs	s /fs1									
[root@ip-10-7	7-25-18 ~]# 0	lf -k													
Filesystem	1K-b]	locks	Used	Available	Use%	Mounted on									
devtmpfs	184	14608	0	1844608	0%	/dev									
tmpts	18/	79956	9676	1879956	1%	/dev/snm /pup									
tmpfs	107	70056	8050	1870056	0%	/svs/fs/cgroup									
/dev/nyme@n1n	2 3144	14972	2239732	29205240	8%	/ / / / / / / / / / / / /									
tmpfs	37	75988	0	375988	0%	, /run/user/1000									
172.23.31.17:	/drnfs 533922	26112	104930240	5234295872	2%	/fs1									
[noot@in 10 7	7 35 10 . 14 /	d 16	-1												

[root@ip-10-77-25-18 ~]# cd /fs1 [root@ip-10-77-25-18 fs1]# ls '\$__DEDUPE__' '\$__NDMP__' iso 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.

🌄 10.77.24.99 - Remote Desl	ktop Connection
-----------------------------	-----------------

- 10.77.24.99	- Remote Desktop C	onnec	tion						-	-		\times
Recycle Bin								Hostname: E Instance ID: i Private IPv4 / Instance Size Availability Z Architecture:	C2AMA -0a5187 Address : t2.mic one: us- : AMD6-	Z-U3 70cd0 :: 10.7 ro -west 4	8605J 03d46b12 77.24.99 t=1b	2
EC2 Feedback	↓ ↓ </th <th>fs Share</th> <th>View</th> <th></th> <th></th> <th></th> <th></th> <th>-</th> <th>- ></th> <th>× ?</th> <th>ow to Mo</th> <th>derate</th>	fs Share	View					-	- >	× ?	ow to Mo	derate
	← → ~ ↑ 🗜	> Netv	vork > 172.23.31.17 > drcifs				v 0	Search drcifs	م	>		
EC2	🖈 Quick access		Name ^	Date modified	Туре	Size						
Micros	Deskton		\$_DEDUPE_	11/3/2022 7:08 AM	File folder							
	Documents	<u>_</u>	S_NDMP_	11/3/2022 6:03 AM	File folder							
	Documents	~	iso	11/9/2022 5:36 AM	File folder							
	Downloads	R	onprem_nfs_vm	11/8/2022 6:28 AM	File folder							
	Pictures	1	Test_file_created_in_WindowsEC2	11/9/2022 11:54 AM	Text Document	1 KB						
	This PC		test_file_linuxclient_ec2	11/9/2022 11:30 AM	File	1 KB						
			Test_file_WinClient_EC2	11/9/2022 11:26 AM	Text Document	1 KB						



• 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
'$_DEDUPE_' '$_NOMP_' 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]# ls -1
total 32
drwxr-xr-x. 3 root root 2048 Nov 3 07:08 '$_DEDUPE_'
drwxrwxrwx. 2 root root 2048 Nov 3 06:03 '$_NDMP_'
drwxrwxrwx. 2 root root 4096 Nov 9 05:36 iso
drwxr-xr-x. 3 root root tot 4096 Nov 9 05:36 iso
drwxr-xr-x. 1 root root 4096 Nov 9 05:36 iso
drwxr-xr-x. 1 root root 35 Nov 9 11:00 test_file_created_in_linuxEC2
-rwxrwxrwx. 1 root root 35 Nov 9 11:30 test_file_created_in_WindowsEC2.txt
-rw-r-r-r-. 1 root root 68 Nov 9 11:30 test_file_linuxclient_ec2
-rwxrwxrwx.t 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**. *Data Protection* Home > Data Protection > File System Recovery Selection

File Sy	stem Recovery Selection
	File System Details
	EVS / File System: ORPRODEVS1 / onpremfs Status: Mounted
	Which type of file system recovery do you want to do?
	Which type of file system recovery do you want to do? Promote the file system to a normal file system (and, optionally, mount as read-write or read-only.)



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**.

Data Protection	Home > Data Protection > File System Versions > Demote File System To Object Replication Target
Demo	ote File System To Object Replication Target
File	e System Details
	EVS / File System: ORPRODEVS1 / onpremfs Status: Mounted
Ob	ject Replication Details For Latest Version
	Status: Status:
	The following steps will be taken
	ATTENTION: Read the online help and its warnings before proceeding
	1: Unmount onpremfs
	2: Recover file system to version created at Version snapshot name: AUTO_SNAPSHOT_c56e85c6-f28f-11d8-908b-7a309e9b85c5_10 Snapshot on target file system: AUTO_SNAPSHOT_TARGET_11 Object Replication Policy: onprem2nearcloud
	3: Demote file system onpremfs to an object replication target
	4: Remove recovered access points
	next cancel

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

Data Protection	Home > Data Protection > File System Versions > Demote File System	To Object Replication Target Confirmation
Demo	te File System To Object Replication	Target Confirmation
File	e System Details	
		EVS / File System: ORPRODEVS1 / onpremfs Status: Mounted
_		
		The following steps will be taken
		1: Unmount onpremfs
		2: Recover file system from snapshot AUTO_SNAPSHOT_c56e85c6-f28f-11d8-908b-7a309e9b85c5_10
		3: Demote file system onpremfs and mount as an object replication target
		4: Remove recovered access points shares exports
		back OK cancel

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

S	storage Management	Home > Storage Manage	ement > File Systems						
	File Syste	ms							
	Filter								
			No Filtering Applied						
			filter						
								Show 20	items per p
	+ Label	Total	<u>Used (%)</u>	Used	Free	Storage Pool	Status	EVS	
	onpremfs	4.97 TiB	2%	107.87 GiB	4.87 TiB	ORPROD	Mounted as Object Replication target	ORPRODEVS1	details

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.

File System Details File EVS / File System: ORDREVS1 / drfs Change								
Object Replica	tion Status &	Reports						
File System Det	ails			Filter				
EVS / File System: ORDREVS1 / drfs				Policy: All	▼ Titter			
Object Replicat	on History							
							Show 10	items per page
	s	ource	Target	t	Start			
Policy	File System	Snapshot	EVS / File System	Snapshot	<u> ▲ Time</u>	Status		
sv5_to_onprem	drfs	AUTO_S70ab_1	172.23.31.23 / onpremfs	AUTO_SRGET_1	2022-11-09-12:18	Incremental object replication. Complete		details

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

Storage Management	lome > <u>Storage Manage</u>	<u>ment</u> > File Systems							
File Systems	S								
Filter									
		No Filtering Applied							
		filter							
								Show 20	items per page
▼ <u>Label</u>	Total	<u>Used (%)</u>	<u>Used</u>	Free	<u>Storage</u> <u>Pool</u>	<u>Status</u>	EVS		
onpremfs	4.97 TiB	29	6 122.78 GiB	4.85 TiB	ORPROD	Mounted	ORPRODEVS1		details
Check All Clear All									

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:

💄 🛃 📜 🔻 onpremcifs					
File Home Share	View				
← → × ↑ 💄 > Net	work > 172.23.31.23 > onpremcifs >				~
A	Name	Date modified	Туре	Size	
Quick access	\$_DEDUPE	11/3/2022 12:08 A	File folder		
Desktop	\$_NDMP	11/2/2022 11:03 PM	File folder		
	~snapshot	11/9/2022 4:18 AM	File folder		
🛅 Documents 🖈	📕 iso	11/8/2022 9:36 PM	File folder		
N Pictures 🖈	onprem_nfs_vm	11/7/2022 10:28 PM	File folder		
📙 dumpfile	test_file_created_in_linuxEC2	11/9/2022 4:00 AM	File	1 KB	
📙 iso	Test_file_created_in_WindowsEC2	11/9/2022 3:54 AM	Text Document	1 KB	
This DC	test_file_linuxclient_ec2	11/9/2022 3:30 AM	File	1 KB	
	Test_file_WinClient_EC2	11/9/2022 3:26 AM	Text Document	1 KB	

NFS Export:

[root@nasclientlinuxeng	[root@nasclientlinuxeng /]# showmount -e 172.23.31.23									
Export list for 172.23.3	Export list for 172.23.31.23:									
/onpremnfs *										
<pre>[root@nasclientlinuxeng /]# mount -t nfs 172.23.31.23:/onpremnfs /fs15</pre>										
[root@nasclientlinuxeng	[root@nasclientlinuxeng /]# df -k									
df: /fs0: Stale file han	dle									
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 /fs1	15								
[root@nasclientlinuxeng	fs15]# ls									
'\$DEDUPE' '\$NDMP_	_' iso	onprem_nfs	_vm test_	file_created_in_linuxEC2	Test_file_created_in_WindowsEC2.txt	<pre>test_file_linuxclient_ec2</pre>	Test_file_WinClient_EC2.txt			
[root@nasclientlinuxeng	fs15]#									
L										

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.

💄 🗹 📕 🔻 onpremcifs						-		×
File Home Share	View							~ ?
\leftarrow \rightarrow \checkmark \uparrow 💄 > Netw	work > 172.23.31.23 > onpremcifs >				~ Ū	Search onpremcifs		P
^	Name	Date modified	Туре	Size				
📌 Quick access								
📃 Desktop 🛛 🖈	S_DEDUPE_	11/3/2022 12:08 A	File folder					
🖶 Downloads 🖈	\$_NDMP_	11/2/2022 11:03 PM	File folder					
🖹 Documents 🖈	~snapshot	11/8/2022 8:00 PM	File folder					
Documents	🦲 iso	11/8/2022 8:31 PM	File folder					
Pictures 🖈	onprem_nfs_vm	11/7/2022 10:28 PM	File folder					
<pre>[rootgmasclientlinuxemg /]# df:/fs0:Stalefilentlinuxemg /]# df:/fs0:Stalefile handle Filesystem IK devtmpfs IK tmpfs If tmpfs If (dev/mapper/rhel-root If (dev/mapper/rhel-root If (dev/sda1 tmpfs If (rootgmasclientlinuxemg fs1 If (rootgmasclientlinuxemg fs2 If (rootgmasclientlinuxemg fs3 If (rootgmasclientlientlinuxemg fs3 If (rootgmasclientlientlinuxemg fs3 If (rootgmasclientlientlinuxemg fs3 If (rootgmasclientlientlinuxemg fs3 If (rootgmasclientlinuxemg fs3 If (rootgmasclientlientlinuxemg fs3 If (rootgmasclientlientlientlientlientlientlientlient</pre>	<pre>mount -t nfs 172.23.31.23:/onpremmts /ts1 df -k blocks Used Available Use% Mounted 1 1880028 0 1880028 0% /dev/shm 1910380 01910300 0% /dev/shm 1910380 10164 1900216 1% /run 1910380 0 1910300 0% /sys/fs/ 190380 254144 764192 25% /boot 613184 5940 607244 1% /boot/ef 382076 24 382072 0% /run/use 32076 24 382072 0% /run/use 32076 0 382076 0% /run/use 320712 113102720 5226123392 3% /fs15 cd /fs15 cd /fs15 cf /s15 fj# ls file_at_1045 m mongodb-windows-x86_64 .iso primary_site_fs.txt rhel=8.1.x86_64-dvd.iso j# date 2 j# date 2 j# date</pre>	5 cgroup i r/975 r/0 enterprise-6.0.2-siį	rh gned.msi rh rh te	el-8.3-x86_64-dvd.iso el-8.4-x86_66-dvd.iso el-baseos-9.0-x86_64-dvd.iso el-server-7.9-x86_64-dvd.iso st01	test5 VWware-CSXI-7.0- VPWware-VMvisor-I	update2a-17867351-hit nstaller-7.002-176305	achi-130 52.x86_(01.iso 64.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.

N A	> Not	work > 172.22.21.17 > dreife						7.	Cooreb draifs	
→ v 1 🭝	/ INCI	work > 172.25.51.17 > dicits						v 0	Search dichs	
10:1		Name		Date modified	Туре	Size				
Quick access		S_DEDUPE_		11/3/2022 12:08 A	File folder					
Desktop	×.	\$ NDMP		11/2/2022 11:03 PM	File folder					
Downloads	*	iso		11/14/2022 7-15 Δ	File folder			7		
Documents	*	New Virtual Machine	Destinat	ion Folder Access Denied			\times			
E Pictures	*	onprem nfs vm								
This PC		OL-7.0-Boot-ISO-V46138-		You need permission to perfor	m this action					
S mis re		OracleVM-Manager-2.2.0	_	drcifs						
🥩 Network		Telefonica-Openstack-log								
		test_file_created_in_linuxE								
		Test file created in Wind								
		test_file_linuxclient_ec2								
		Test_file_WinClient_EC2			Try Again	Cance	1			
		XenServer-7.2.0-install-cd			ity Again	Cance				

/[root@nasclientlinuxeng ~]# mount -t nfs 172.23.31.17:/drnfs /fs05									
[root@nasclientlinuxeng ~]# cd /fs05									
[root@nasclientlinuxeng fs05]# 1s									
OracleVM-Manager-2.2.0.iso	Test_file_created_in_WindowsEC2.txt	XenServer-7.2.0-install-cd.iso							
Telefonica-Openstack-logs.zip	test_file_linuxclient_ec2								
<pre>test_file_created_in_linuxEC2</pre>	Test_file_WinClient_EC2.txt								
touch: cannot touch 'tset5': Read-only file system									
	3.31.17:/drnfs /fs05 OracleVM-Manager-2.2.0.iso Telefonica-Openstack-logs.zip test_file_created_in_linuxEC2 stem	3.31.17:/drnfs /fs05 OracleVM-Manager-2.2.0.iso Telefonica-Openstack-logs.zip test_file_created_in_linuxEC2 test_file_winClient_EC2.txt stem							



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



recovery.								
Ohnas-5300-sv5 - 172.23.31.11		Help About Logged in	n: admin					
Data Protection Home > Data Protection > File	e System Versions							
File System Versions								
File System Details								
	EVS / File System: ORDREVS1 /	drfs change						
	Status: Mounted as C	Dbject Replication target						
Object Replication Details Fo	r Latest Version							
Status: O Complete / Source File System: ORPRODEVS1 / onpremfs Source Server: EnglewoodNAS Source File System Status: Mounted								
Versions								
Time Of ▲ <u>Version</u>	Version	Replicated From <u>Snapshot</u>						
2022-11-09 04:00:07	AUTO_SNAPSHOT_TARGET_10	AUTO_SNAPSHOT_c56e85c6-f28f-11d8-908b-7a309e9b85c5_9						

17 packets transmitted, 0 received, +6 errors, 100% packet loss, time 16394ms

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

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

^C

1.

pipe 3

--- 172.23.31.23 ping statistics ---

clnt create: RPC: Unable to receive

[root@nasclientlinuxeng /]# showmount -e 172.23.31.23



3. Verify whether the file system is recovered successfully.

Ohnas-5300-sv5 - 172.23.31.11	Help	About Logged in: adn								
Data Protection Home > Data Protection > File System Recovery Reports										
File System Recovery Reports										
EVS / File System La	EVS / File System Label									
ORDREVS1 / drfs ch	ORDREVS1 / drfs									
File System Recove	ries									
▲ <u>Time</u>	Started	File System	Recovered to Snapshot	<u>Recovery Mount</u> <u>Option</u>	Active	Last Status				
2022-11-09 06:40:40	(UTC+0000)	drfs	AUTO_SNAPSHOT_TARGET_10	Mount read write	Inactive	Completed With Wa	irnings details			
2022-11-08 10:55:54	(UTC+0000)	drfs	AUTO_SNAPSHOT_TARGET_9	Mount as an object replication target	Inactive	Completed Success	fully details			

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:

💄 🗹 📕 = drcif File Home 🗧	s Share	View				_
← → • ↑ 🕹	> Netv	vork > 172.23.31.17 > drcifs >				✓ Ů Search drcifs
		Name	Date modified	Туре	Size	
	*	\$_DEDUPE_	11/3/2022 12:08 A	File folder		
	<u>_</u>	\$_NDMP	11/2/2022 11:03 PM	File folder		
Downloads	<i>.</i>	📜 iso	11/8/2022 10:53 PM	File folder		
Documents Pictures	Я Я	onprem_nfs_vm	11/7/2022 10:28 PM	File folder		

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.

New datastore					
1 Select creation type 2 Provide NFS mount details 3 Ready to complete	Select creation type How would you like to create a datastore?				
	Create new VMFS datastore Add an extent to existing VMFS datastore Expand an existing VMFS datastore extent	Create a new datastore by mounting a remote NFS volume			
	Mount NFS datastore				

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**.

1 N	1 New datastore - onpremnfsdatastore							
✓ 1 2 3	Select creation type Provide NFS mount details Ready to complete	Provide NFS mount details Provide the details of the NFS share you wish to mount						
	Name	onpremnfsdatastore						
	NFS server	172.23.31.23						
	NFS share	/onpremnfs						
	NFS version	● NFS 3 ○ NFS 4						

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

1 Select creation type 2 Provide NFS mount details 3 Ready to complete	Ready to complete Summary					
	Name	onpremnfsdatastore				
	NFS server	172.23.31.23				
	NFS share	/onpremnfs				
	NFS version	NFS				
	Username					
	Password					



Actions of

The following screenshot shows the NFS datastore after creation:

vm ware [,] ESXi ^{**}						root@172.23.30	0.69 🕶 Help 🕶	Q Search
Navigator	SISD51B-24 - Storage							
▼ 🗐 Host	Datastores Adapters Devices Persistent Memory							
Manage	1 New datastore 📧 Increase canacity 🎝 Register a VM	🕽 Datastore browser	Refresh 🛛 🖄	Actions			0	Search
Monitor					-	-	<u> </u>	
> 🔂 Virtual Machines	Name	Drive Type V	Capacity ~	Provisioned ~	Free v	Туре 🗸	Thin provisioning ~	Access ~
📑 Storage 🛛 🗖	local-ds-69	Non-SSD	150.75 GB	1.41 GB	149.34 GB	VMFS6	Supported	Single
> 🧕 Networking	onpremnfsdatastore	Unknown	4.97 TB	99.85 GB	4.88 TB	NFS	Supported	Single
	sp-e790-lun-0000	Non-SSD	4 TB	951.51 GB	3.07 TB	VMFS6	Supported	Single
	E vsp-e790-lun-0001	Non-SSD	4 TB	156.78 GB	3.85 TB	VMFS6	Supported	Single
	🗐 vsp-e790-lun-0002	Non-SSD	4 TB	771.19 GB	3.25 TB	VMFS6	Supported	Single
	🗐 vsp-e790-lun-0003	Non-SSD	4 TB	640.64 GB	3.37 TB	VMFS6	Supported	Single

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

Activities	🔈 Terminal 🛨	Nov 8 01:39		よ もの し ・
		Welcome		Next
	root@localho	ost:/os_iso	×	
File E	dit View Search Terminal Help			
[root@ [root@ [root@ total	localhost ~]# cd /os_iso/ localhost os_iso]# localhost os_iso]# ls -l 2365516			
- rw- r- - rw- r- [root@	-r 1 root root 5603328 May 6 -r 1 root root 2416685056 Mar 31 localhost os_iso]#	2021 managementagentx64.msi 2021 RHEL4.8-ia64-AS-DVD.iso		

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 <u>Configure HNAS Object Replication</u> section.
- 2. In the Object Replication Status & Reports page, verify whether the replication has completed as per the schedule.

EnglewoodNAS - 1	172.23.31.20						Help	About	Logged in: a
Data Protection	Home > Data Prote	ction > Object Replicati	on Status & Reports						
Object Replication Status & Reports									
File	e System Details				Filter				
EVS / File System: ORPRODEVS1 / onpremfs change						Policy: All	▼ filter		
Ob	ject Replication H	listory							
								Show 10	items per pag
		Sc	ource	Targe	et	Start			
	Policy	File System	Snapshot	EVS / File System	<u>Snapshot</u>	. <u>⊼ Time</u>	Status		
	onpremrcloud	onpremfs	AUTO_S85c5_6	172.23.31.17 / drfs	AUTO_SRGET_7	2022-11-08-06:51	Incremental object replication. Complete		details
	opprem reloud	oppremfe	AUTO S 85c5 5	172 23 21 17 / defe	AUTO S RGET 6	2022 11 08 04-00	Incremental object replication. Complete		details

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

0						nep sour	roadeau
Data Protection	Home > Data Protection > File System Recovery Reports						
File	System Recovery Reports						
E	EVS / File System Label						
Q	ORDREVS1 / drfs change						
_							
	File System Recoveries						
	▲ Time Started	File System	Recovered to Snapshot	Recovery Mount Option	Active	<u>Last</u> <u>Status</u>	
0	2022-11-08 09:17:47 (UTC+0000)	drfs	AUTO_SNAPSHOT_TARGET_7	Mount read write	Inactive	Completed Successfully	details

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**.

1 New datastore - drnfsdatastore						
 1 Select creation type 2 Provide NFS mount details 3 Ready to complete 	Provide NFS mount details Provide the details of the NFS share you wish to mount					
	Name	drnfsdatastore				
	NFS server	172.23.31.17				
	NFS share	/drnfs				
	NFS version	● NFS 3 ○ NFS 4				

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

1 Select creation type 2 Provide NFS mount details 3 Ready to complete	Ready to complete	3	
	Name	drnfsdatastore	
	NFS server	172.23.31.17	
	NFS share	/drnfs	
	NFS version	NFS	
	Username		
	Password		

The following screenshot shows the NFS datastore after creation.

vm ware [,] ESXi [®]						root@172.23.3	0.47 - Help -	Q Sea
Navigator	SISD S220-23 - Storage							
▼ 🗒 Host	Datastores Adapters Devices Persistent Memory							
Manage								
Monitor	🔁 New datastore 🛛 Increase capacity 🛛 鹶 Register a VM	C Datastore browser	📔 🕑 Refresh 📔 🙀	Actions			(0	L Search
> 🔂 Virtual Machines 5	Name	Drive Type 🗸 🗸	Capacity ~	Provisioned ~	Free ~	Туре ~	Thin provisioning \sim	Access
🛛 🧮 Storage 🛛 🚺 🚳	drnfsdatastore	Unknown	4.97 TB	100.07 GB	4.87 TB	NFS	Supported	Single
Networking 2	E1090_lun00	Non-SSD	2.1 TB	1.32 TB	798.62 GB	VMFS6	Supported	Single
	E1090_lun01	Non-SSD	2.1 TB	1.44 GB	2.1 TB	VMFS6	Supported	Single
	Iocal-ds-47	Non-SSD	1.62 TB	1,018.45 GB	641.3 GB	VMFS6	Supported	Single
	vsp-5200-lun-fef0	Non-SSD	4 TB	2.24 TB	1.76 TB	VMFS6	Supported	Single
	sys-e1090-lun-fef1	Non-SSD	4 TB	996.82 GB	3.03 TB	VMFS6	Supported	Single

- 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.

🔁 New virtual machine		
 1 Select creation type 2 Select VMs for registration 	Select creation type	
3 Ready to complete		
	Create a new virtual machine	This option guides you through registering a virtual machine that already exists on a datastore
	Deploy a virtual machine from an OVF or OVA file	
	Register an existing virtual machine	



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

1 Select creation type 2 Select VMs for registration	Select V	s for registration
3 Ready to complete	datastore or o	ctory will be registered.
		Select one or more virtual machines, a datastore or a directory
	🛞 Remove	Remove selected
		IX file ~
		None
		No items to display

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

🔁 New virtual machine				
	.	·		1
C Datastore browser				
摿 Upload 🛛 🔒 Download	🛃 Delete 🔒 Move 🗎 Copy	🛅 Create directory 📋 🤁 F	Refresh	
E1090_lun00	🚞 .snapshot	onprem_nfs_vm-ef		
E1090_lun01	a \$DEDUPE	onprem_nfs_vm.nv		
local-ds-47	2 S_NDMP	onprem_nfs_vm.vm	onprem_nfs_vm.vmx	
sp-5200-lun-fef0	🚞 iso	onprem_nfs_vm.vm	3.32 KB Monday, November 07,	
Vsp-e1090-lun-fef1	anprem_nfs_vm	🗿 onprem_nfs_vm.vmx		
drnfsdatastore		onprem_nfs_vm.vm		
		vmware-1.log		
		vmware.log		
		vmx-onprem_nfs_v		
1				

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

 1 Select creation type 2 Select VMs for registration 	Select V	/Ms for registration
3 Ready to complete	Select one datastore o	or more virtual machines you wish to register. By selecting a datastore or directory, all VMs found in that directory will be registered.
		Select one or more virtual machines, a datastore or a directory
	🛞 Remov	e all 💿 Remove selected
		VMX file ~
		[drnfsdatastore] onprem_nfs_vm/onprem_nfs_vm.vmx
		1 items

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

🔁 New virtual machine		
 1 Select creation type 2 Select VMs for registration 3 Ready to complete 	Ready to complete Review your settings selection before finite	shing the wizard
	Virtual machines	[drnfsdatastore] onprem_nfs_vm/onprem_nfs_vm.vmx



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

← → C 🔒 172.23.30.46/	ui/#/host/vms				e i	🗶 🔲 😩 🗘 Update 🔅
vmware [,] ESXi ^{,,}				root@172.23.3	0.46 🕶 Help 🛩	Q Search -
Navigator	🔂 SISDS220-22 - Virtual Machines					
✓ ☐ Host Manage	1 Create / Register VM] 📝 Console 🕨 Power on 🗧 P	Power off 🔢 Suspend 🧲 Refresh	🔅 Actions			iearch
Monitor	Virtual machine Virtual machine	✓ Status ✓ Used space	✓ Guest OS ✓	Host name v	Host CPU 🔻 🗸 🗸	r Host memory V
👻 🚑 Virtual Machines 🛛 🚺	no OpsCenterVM_10.8.0-04	Normal 104.96 GB	Oracle Linux 4/5/6/7 (64-bit)	opscenter	2.5 GHz	48 GB
▼	O fip onprem_nfs_vm	Normal 7.86 GB	Red Hat Enterprise Linux 8 (localhost.localdomain	1 GHz	1.19 GB
Monitor	🗆 🐻 A3_SV10_CS_93	Normal 406.08 GB	Microsoft Windows Server 20	DR-CS.juno.com	131 MHz	13.21 GB

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

Navigator	p onprem_nfs_vm
🕶 🗐 Host	opprem_nfs_vm
Manage	Sectivities 🖸 Terminal - Nov 8 05:31
Monitor	Welcome
Virtual Machines Virtual Machines	root@localhost:/os_iso ×
Monitor	File Edit View Search Terminal Help
More VMs	<pre>[root@localhost ~]# cd / [root@localhost /]# ls bin dev home lib64 mnt os_iso root sbin sys usr boot etc lib media opt proc run srv tmp var [root@localhost /]# cd os_iso/ [root@localhost os_iso]# ls -l total 2365516 -rw-rr 1 root root 5603328 May 6 2021 managementagentx64.msi -rw-rr 1 root root 2416685056 Mar 31 2021 RHEL4.8-ia64-AS-DVD.iso [root@localhost os_iso]#</pre>

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 <u>Create Virtual Machine</u> section.

🛢 onpremnfsda	tastore : Actions	
Summary Monitor	Configure Permissions Files Hosts VMs	
Alarm Definitions	Properties	
Scheduled Tasks General	Name	onpremnfsdatastore
Device Backing	Туре	NFS 3
Connectivity with Hosts	Maximum file size	64 TB
Capability sets	Maximum virtual disk size	62 TB
	Capacity	REFRESH
	Total Capacity	4.97 TB
	Provisioned Space	304.03 GB
	Free Space	4.85 TB

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

onpremnfsdatastore	ACTIONS						
Summary Monitor Configure	Permissions Files	Hosts V	VMs				
Virtual Machines VM Templates							
							¥ Filter
Name	↑ State		Status	Provisioned Space	Used Space	Host CPU	Host Mem
🗌 🗏 🕄 onprem_nfs_vm	Powered On		() Alert	100 GB	7.86 GB	2.89 GHz	1.98 GB
🔽 🗉 👪 Windows_nfs_vm	Powered On		🗸 Normal	100 GB	10.7 GB	0 Hz	4.05 GB

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

Successfully created the schee	dule.						
Policies							
						Show 10	items per page
	Source		Targe	et			
▼ <u>Name</u>	EVS	File System	EVS	File System	Status		
onprem_policy	ORPRODEVS1 onpre	mfs ORDREVS	1 (172.23.31.17)	drfs	No status found		details
Check All Clear All							
	Actions: remove run now abort	add					
	Shortcute: Object Peolication Status	8 Penorte					
	Shortcus. Object Replication Status						
Schedules							
Generaties						Chour 10	Home per per
						Show To	items per page
	* Policy		<u>Next Run</u>		Interval		
	prem_policy	2022-11-24 07:40		3 hours		details	

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

Object Replication	1					
Successfully created the s	chedule.					
Policies						
			Taur			Show 10 items per pa
<u>▼ Name</u>	EVS	File System	EVS	File System	Status	
onprem_policy Check All Class All	ORPRODEVS1	onpremfs	ORDREVS1 (172.23.31.17)	drfs	No status found	details
	Actions: remove run no Shortcuts: Object Replicati	w abort add				
Schedules						Chan 10 internet
ID	• Policy		Next Run		Interval	Show 10 nems per pa
1 Check All Clear All	onprem_policy	2022-11	-24 07:40	3 hours		details
	Actions: add remove					

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

Object Replicat	bject Replication Status & Reports								
File System Detail	s			Filter					
	EVS / File System: ORPRODEVS1 / All File Systems change				Policy: All	✓ filter			
Object Replication	Object Replication History								
	s	ource	Targ	et	Start				
Policy	File System	Snapshot	EVS / File System	Snapshot	<u> ▲ Time</u>	Status			
onprem_policy	onpremfs	AUTO_S85c5_2	172.23.31.17 / drfs	AUTO_SRGET_2	2022-11-24 10:40	Incremental object replication. Complete	details		
onprem_policy	onpremfs	AUTO_S85c5_1	172.23.31.17 / drfs	AUTO_SRGET_1	2022-11-24_07:40	Incremental object replication. Complete	details		

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.

	Windows Security	al 🛨		172.23.31.33	_ 7 ×	- 0	×
	←	Virus & threat prot Protection for your device against three	tection ats.			Windows Community videos	
	☆ Home ○ Virus & threat protection	🚱 Current threats				Learn more about Virus & threat protection	
ſ	^{(c} μ) Firewall & network protection	Threats found. Start the recommended	l actions.				
	App & browser control Device security	Behavior:Win32/Teerac.X!rsm 11/24/2022 10:48 AM (Active)	Severe			Who's protecting me? Manage providers	
		TrojanDownloader:O97M/Obfuse.KY! MTB 11/24/2022 10:47 AM (Active)	Severe			Change your privacy settings	
		Trojan:Win32/Sehyioa.A!cl 11/24/2022 10:47 AM (Active)	Severe			View and change privacy settings for your Windows 10 device.	
		Trojan:Win32/Kryptik!MSR	Severe			Privacy settings Privacy dashboard	
		Start actions				Privacy Statement	

Recovery

In this section, we will recover the virtual machine.

Data P

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

Data Protection Home > Data Protection > Object Replication Status & Reports										
Object Replication Status & Reports										
File System Detail	File System Details					Filter				
	EVS / File System: ORPRODEVS1 / All File Systems etange					▼ [fiter]				
Object Replication History										
							Show 10 items per page			
	So	urce	Targe	ət	Start		Show 10 Items per page			
Policy.	So File System	ource <u>Snapshot</u>	Targ EVS / File System	et <u>Snapshot</u>	Start <u>▲ Time</u>	Status	Show 10 Items per page			
Policy onprem_policy	So File System onpremfs	ource Snapshot AUTO_S85c5_2	Targe EVS / File System 172.23.31.17 / drfs	et <u>Snapshot</u> AUTO_SRGET_2	Start ▲ <u>Time</u> 2022-JJ-24 JØ:40	Status Status	Show 10 Items per page details			

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

File System Details		
	EVS / File System: ORPRODEVS1 / onpremfs File System Status: Mounted as Object Replication target	
Recovery Details		
Progress Active: Inactive Last Status: Completed Successfully	Start time: 2022-11-24 10:53-32 (UTC+0000) End time: 2022-11-24 10:53:35 (UTC+0000)	
Request Summary Recovery Option: Mount as an object replication target Delete DR Starses: Yes Delete DR Storse: Yes	Rollback to Snapshot: AUTO_SNAPSHOT_76c2bd34.fld5-f1d6-90db-7a309e9665c5_2	
Recovery Statistics		
	Shares Number Successfully deleted: 0 Exports Number Successfully deleted: 0 Number Successfully deleted: 0 Number Successfully deleted: 0	

ta Protection Home > Data Protestion > File System Versions										
File System Versions										
Selecting file system onpremfs	Selecting file system onprem/s									
File System Details	File System Details									
	EVS / File System: ORPRODEVS1 / onprendis Compo Status: Mounted as Object Replication target									
Object Replication Details Fo	- Latest Version									
Status:										
Versions										
Time of Replicated From A Version Version Snapshot										
2022-11-04 09:50:34	AUTO_SNAPSHOT_df030085-7a309e9b85c5_1	Not an object replication target								
2022-11-18 07:11:26	AUTO_SNAPSHOT_c56e88b-7a309e9b85c5_47	Not an object replication target								
2022-11-24 10:40:52	AUTO_SNAPSHOT_7dc2b0db-7a309e9b85c5_2	Not an object replication target								
2022-11-24 11:02:48	AUTO_SNAPSHOT_TARGET_2	AUTO_SNAPSHOT_eead3a4c-fff3-11d8-920b-a99a592e70ab_1								

- c. Promote the secondary file system running in the near-cloud data center. For instructions, see <u>Perform Planned</u> <u>Outage: Failover</u> 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 <u>Configure HNAS Object Replication</u> section.

ject Replication									
Successfully created the sch	edule.								
Policies									
	Sour	ce	Target	t	SI	ow 10 items per page			
▼ Name	EVS	File System	EVS	File System	Status				
sv5_policy	ORDREVS1 drfr	or o	ODEVS1 (172.23.31.23)	onpremfs	No status found	details			
	Actions: rannow rannow adort and Shortouts: Object Replication Status & Reports								
Schedules									
					St	ow 10 items per page			
ID	* Policy		Next Run	Ŀ	nterval				
Check All Clear All	sv5_policy	2022-11-24 11:	02	ONCE		details			

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

oject Replication Status & Reports									
File System Details F					Filter				
EVS / File System: ORDREVS1 / All File Systems change					Policy: All	▼ fitter			
Object Replica	tion History								
							Show 10	items per page	
Source Target					Start				
Policy File System Snapshot EVS / File System Snapsh			Snapshot	<u> ▲ Time</u>	Status				
sv5_policy	drfs	AUTO_S70ab_1	172.23.31.23 / onpremfs	AUTO_SRGET_2	2022-11-24-11:02	Incremental object replication. Complete		details	

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

File System Recovery Report	
File System Details	
	EVS / File System: ORPRODEVS1 / onpremfs File System Status: Mounted
Recovery Details	
Progress	
Active: Inactive Last Status: Completed With Warnings	Start time: 2022-11-24 11.09.49 (UTC+0000) End time: 2022-11-24 11.09.51 (UTC+0000)
Request Summary	
Recovery Option: Mount read write	Rollback to Snapshot: AUTO_SNAPSHOT_TARGET_2
Recover Shares: Yes	Fix Name Clash: Yes
Recover Exports: Yes	Skip Identical Shares/Exports: Yes
Log Level: Info	NFS clients' access: Continues on source file system
Source File System "Transfer Access Point" Setting	
	For this Promotion: Use source file system default
	Apply to Target File System: Yes
Recovery Statistics	
	Shares Total Successfully recovered: 1 Total failed to recover: 0 Total skipped: 1
	Exports Total Successfully recovered: 1 Total failed to recover: 0 Total failed to skipped: 1
	detete <u>View Log</u>

HITACHI Inspire the Next

Disaster Recovery in Hybrid Cloud Environments with HNAS Object Replication

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.

Server Manager	H al	172.23.31.3	3	_ 8 × _			-	- 0	×
Ser	ver Manager • Dashboard				- © I	Manage	Tools	View	Help
📰 Dashboard	WELCOME TO SERVER MANAGER								
Local Server All Servers File and Storage Ser	Windows Security $ \leftarrow$ \equiv	□ ×							
	Virus & threat protection Protection for your device against threats.								
	Current threats No current threats Lat scare 11/04/2022 11:20 AM (quick scare)							ŀ	lide
	0 threats found. Scan lasted 12 seconds 34025 files scanned.								
	Quick scan		Il Servers 1						
	Scan options		1anageability vents						
	Threat history		ervices						