

Hitachi Vantara-Veritas NetBackup End-to-End Cyber Protection Solution

v2.0

Implementation Guide

This document describes multilayered Cyber protection and recovery solution using Veritas™ NetBackup™ with Hitachi Virtual Storage Platform (VSP) and Hitachi Content Platform (HCP) for Cloud Scale.

Hitachi Vantara

October 2023

© 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 Corporation (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 may not 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 Corporation 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 Corporation.

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, BCPi™ 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.

Table of Contents

Table of Contents	3
Preface	5
About this document.....	5
Document conventions.....	5
Intended audience	5
Revision History	6
Accessing product downloads.....	6
Getting Help.....	6
Comments	6
Solution Overview	7
Solution Diagram.....	9
Solution Components.....	9
Backup System.....	9
Storage System	10
System Requirements	11
Configuring and Installing Hitachi Components	12
Installing the DNS and CM-REST Servers	13
Configuring the DNS server.....	13
Configuring the CM-REST server.....	13
Configuring and Installing Veritas NetBackup Components	15
Installing the Master server	15
Installing NetBackup Media Server.....	15
Installing NetBackup Client	15
Configuring MSDP-C Storage.....	16
Prepare the environment.....	16
Create an MSDP cloud immutable storage volume	17
Add a Disk pool from the NetBackup WEB UI.....	20
Create a Storage Unit using WORM Lock feature	23
Configuring Storage Life Cycle Policy.....	24
Installing and Configuring the CloudPoint Server to use Snapshot Manager	28
Preparing for CloudPoint Installation	28
Installing CloudPoint using Docker.....	28

Configuring CloudPoint plug-ins	29
Configuring a Policy for using Snapshot Manager	30
Installing NetBackup Malware Scanner	34
Preparing the Scan Host	34
Installing the Malware scanner	34
Configuring Anomaly Detection.....	34
NetBackup Backup and Restore Operations	35
Running a Snapshot Backup Job using a CloudPoint server for VSP 5600 storage system and HCP for Cloud Scale	35
Restoring a Snapshot Backup Job.....	40
Description before restoration	40
Preparation before Restore	40
Restoring from a VSP 5600 storage system	41
Restoring from HCP for Cloud Scale.....	45
Point in time restore.....	47
NetBackup and Hitachi Cyber Security Capabilities	51
Verifying Anomaly Detection during Backup.....	51
Verifying Malware detection after Backup and before Restore Manually.....	53
NetBackup Malware Scanner Test with Non-affected files	53
NetBackup Malware Scanner Test with Virus affected files	58
Data Protection Within the Retention Period	63
Verify WORM lock Feature from NetBackup End	63
Limitations and Troubleshooting.....	65
Limitations	65
Troubleshooting.....	65
Conclusion.....	68

Preface

About this document

The Veritas™ NetBackup™ end-to-end Cyber Protection solution helps to mitigate cyber threats by providing backup and disaster recovery capabilities, security features such as encryption and secure communication, and compliance with industry standards. By backing up data and ensuring the availability of secure and recoverable data, this solution helps organizations in reducing the impact of cyber-attacks, data breaches, and other security incidents. Additionally, their compliance with industry standards and security regulations can ensure that sensitive data is managed correctly and protected against unauthorized access.

Document conventions

This document uses the following typographic convention:

Convention	Description
Bold	<ul style="list-style-type: none">Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK.Indicates emphasized words in list items.
<i>Italic</i>	Indicates a document title or emphasized words in text.
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairdisplay -g oradb</code>

Intended audience

This document is intended for administrators and architects of Hitachi VSP 5000 storage systems and IT professionals who deploy Veritas NetBackup with VSP 5000 storage systems and HCP for Cloud Scale systems. To use this document, you must have the following knowledge and experience:

- Storage Area Networks (SAN)
- Computing
- Networking
- Hitachi Content Platform for Cloud Scale
- Hitachi Storage
- Veritas NetBackup

Revision History

Revision	Changes	Date
v1.0	Initial release	April 2023
v2.0	Added x509 error solution and secured the connection for data transferring in HCP for Cloud Scale	October 2023

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: <https://support.hitachivantara.com/> and Veritas download center: https://www.veritas.com/support/en_US/downloads

Log in and select Product Downloads to access the most current downloads, including updates that may have been made after the release of the product.

Getting Help

[Hitachi Vantara Support Connect](#) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

[Hitachi Vantara Community](#) is a global online community for customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Send us any comments on this document to GPSE-Docs-Feedback@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Solution Overview

The Veritas™ NetBackup™ anomaly detection and faster recovery feature combined with Hitachi Content Platform (HCP) for Cloud Scale immutable copy and Hitachi Virtual Storage Platform (VSP) snapshot technology provides a comprehensive end-to-end cyber protection solution.

Anomaly detection in NetBackup helps by identifying and mitigating potential threats to data, reducing the risk of data loss or corruption.

Fast recovery enables quick restoration of data in case of data loss, minimizing downtime and ensuring data availability.

By ensuring data integrity and adding another layer of protection against cyber threats, HCP for Cloud Scale immutable copy provides a secure, tamper-proof archive of data.

Hitachi VSP snapshots offer a point-in-time view of data, enabling fast and efficient data recovery in case of cyber incidents. These technologies work together to create a secure and reliable data protection and management system, ensuring the confidentiality, integrity, and availability of critical information assets in the event of cyberattacks.



Figure 1: Data recovery framework

Stage 1 (Anomaly detection during backup): NetBackup anomaly detection works as the security engine with Identify, Detect, and Respond features.

Stage 2 (Malware scanning after backup): NetBackup Malware scanner has the same features as anomaly detection. You can scan backup images manually using the NetBackup Malware Scanner.

Stage 3 (Within retention): HCP for Cloud Scale has an object lock feature that protects the backup data. The data cannot be deleted within the retention period during policy creation.

Stage 4 (Malware scanning before recovery): You can scan the requested backup images before restoring using NetBackup Malware scanner.

Stage 5 (During recovery): You can retain backup images and provide restoration for the following cases:

- You can recover copy 1 snapshots that are responsible for point-in-time recovery and are stored on a VSP 5600 storage system.
- You can recover file and directory levels stored on a VSP 5600 storage system (block storage) from the backup of copy 2 snapshots.
- You can recover file and directory levels stored in HCP for Cloud Scale (object storage) from another backup of copy 3. Because of the object lock feature, if any backup data is deleted from block storage, you can recover the same from the HCP for Cloud Scale immutable bucket.

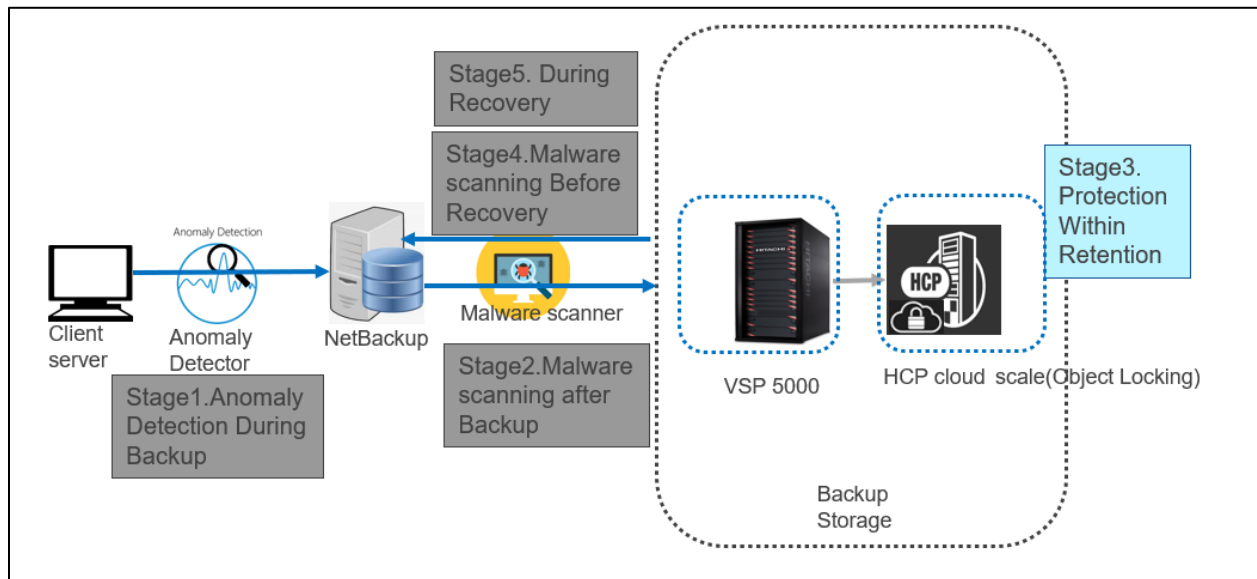


Figure 2: Multi-layered security

Solution Diagram

The following diagram shows the Veritas NetBackup end-to-end cyber protection solution with VSP storage system and HCP for Cloud Scale:

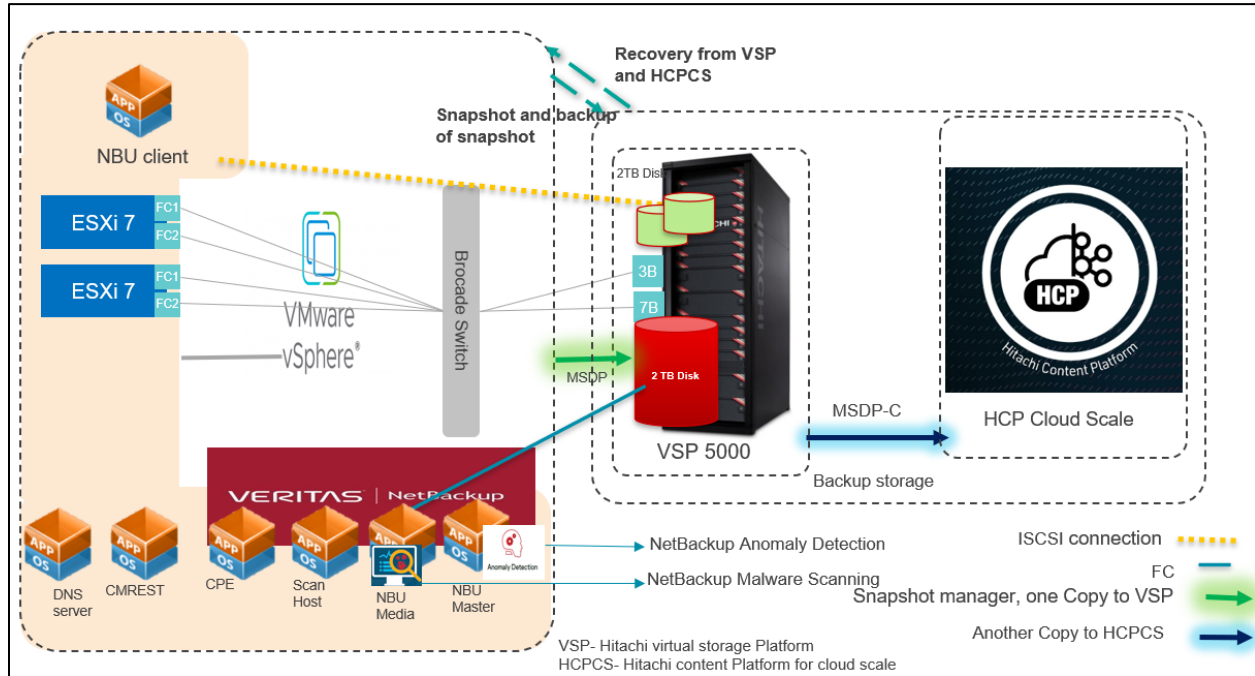


Figure 3: Hitachi Veritas NetBackup end-to-end cyber protection solution overview

Solution Components

Backup System

- **NetBackup Master:** Master server where the NetBackup catalog resides which includes the internal databases that contain information about NetBackup configuration and backups.
- **NetBackup Media:** Server that manages the data movement between the client being backed up and the target backup device (disk, tape, and so on). A storage server is a NetBackup entity that manages the backup storage (for example: the MSDP pool to which you are backing up).
- **NetBackup Client:** Any server protected by NetBackup. The NetBackup software is installed on the media server. During backups, the client sends data across the network to the NetBackup media server, which selects the correct storage media as a backup target.
- **Content Platform Engine (CPE) server:** Cloud-native snapshot management software that integrates with AWS, Azure, and Google Cloud.
- **API Configuration Manager server:** Server that makes it fast and easy to manage a Hitachi storage system using a REST API. There is no need to use an FC or iSCSI connection.

- **Media Server Deduplication Pool (MSDP):** Resource that writes to, and reads from, the storage system. One host functions as the storage server, and only one storage server exists for each NetBackup deduplication node. The host must be a NetBackup media server. Although the storage server components run on a media server, the storage server is a separate logical entity.
- **MSDP Cloud:** Enterprise-class, software-defined storage solution that scales out to any infrastructure.
- **NetBackup Anomaly Detection:** NetBackup detects anomalies in backup metadata such as any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.
- **NetBackup Malware Detection:** NetBackup finds malware in supported backup images and finds the last known good image that is malware free. You can select one or more backup images of the supported policy-types for on-demand scan. In addition, you can use a pre-defined list of scan hosts. If malware is detected during scanning, a notification is generated in the WebUI.

Storage System

Hitachi Virtual Storage Platform (VSP 5000 series)

Hitachi's most powerful data platform delivers industry-leading enterprise storage virtualization in a unified platform for midmarket to global enterprises that need to manage information more efficiently and securely with the best performance in its class.

HCP for Cloud Scale

A software-defined object storage solution that is based on a massively parallel microservice architecture and is compatible with the Amazon S3 application programming interface (API).

System Requirements

This chapter describes the hardware and software components required for setting up a Veritas NetBackup end-to-end cyber protection solution with a VSP 5600 storage system and HCP for Cloud Scale.

Table 1 lists the hardware and software components that are applicable to this solution:

Product	Application	Version
Hitachi Virtual Storage Platform 5000 Series	Hitachi Storage Virtualization Operating System (SVOS)	90-08-61-00/00
VMware	VMware ESXi	VMware ESXi, 6.7.0, 10302608
	VMware vCenter Server	vSphere Client Version 6.7.0.20000
Veritas NetBackup	Veritas NetBackup (Master, Media, Client) server	NetBackup 10.0
	CM-REST server	Ops Center API configuration manager 10.8.3
	NetBackup Malware Scanner server	NetBackup AntiMalwareClient1.0
	Snapshot Manager Server	Veritas_CloudPoint_10.0.0.9818
HCP for Cloud Scale	Hitachi Content Platform for Cloud Scale	version 2.3.1

Table 1: Hardware and software requirements

Table 2 lists the operating systems that are applicable to this test:

Server	Operating System version
Master	RHEL 7.8
Media	
Client	
CPE	
CMREST server	
Scan host	RHEL 8.2
DNS server	Windows 2019

Table 2: Operating systems

Configuring and Installing Hitachi Components

This chapter describes the steps for configuring a VSP 5600 storage system and HCP for Cloud Scale. In addition, it describes the steps for installing DNS and CMREST server.

- Configuring a Hitachi VSP 5600 storage system
- Configuring HCP for Cloud Scale
- Installing DNS and CMREST server

Configuring a Hitachi VSP 5600 storage system

To configure a VSP 5600 storage system, complete the following steps:

1. Set up a Storage Dynamic pool for MSDP and Thin Image Pool for Flex snap for use in NetBackup.

Note: The Dynamic Provisioning pool (DP) is used for the NetBackup media server, and the Thin Image (HTI) pool is used for the NetBackup Snapshot Manager. It is mandatory to name the HTI pool you create as **flexsnap_pool** for the Snapshot Manager server.

Pool Name	Status	Pool Type	Drive Type/RPM	Number of Pool VOLS	Number of V-VOLs	Number of Root VOLS	RAID Level	Capacity			
								Total	Reserved	Used	Used (%)
DP	Normal	DP	SSD,FMD/-	32	30	0	6(6D+2P)	84474.9...	0.00 GB	2223.21 GB	
flexsnap_pool	Normal	TI	SSD,FMD/-	12	-	1	6(6D+2P)	36736.7...	0.00 GB	2.29 GB	

2. Create Storage Volumes for NetBackup servers.
3. Create Host Groups.
4. Add a LUN Path.
5. Set up an iSCSI Connection.

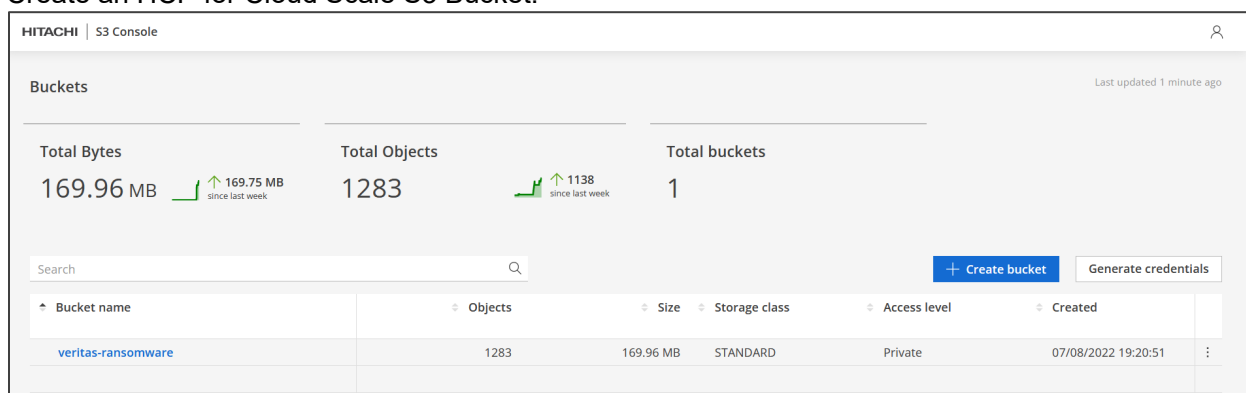
For detailed information, see: [Configuring iSCSI ports - Hitachi Vantara Knowledge](#)

Note: Because the client is a VMware server, there is no direct FC connection to the storage system, and an iSCSI connection is required between the NetBackup Client and the Hitachi VSP 5600 storage system. During Snapshot exports, the Snapshot manager searches for FC or iSCSI.

Configuring HCP for Cloud Scale

This section describes how to configure HCP for Cloud Scale Version 2.3.1 for a NetBackup end-to-end solution. This process consists of the following high-level steps:

1. Create an HCP for Cloud Scale S3 Bucket.



2. Generate an HCP for Cloud Scale S3 credential for NetBackup Media Server.



Note: Copy the credentials of the Access Key and Secret Key because you will use them when configuring HCP for Cloud Scale.

For details about the installation, see the System Requirements section in the HCP for Cloud Scale documentation: [Installing Hitachi Content Platform for Cloud Scale](#)

Installing the DNS and CM-REST Servers

Configuring the DNS server

To configure the DNS server, complete the following steps:

1. Install Windows server.
2. Use the DNS manager to add entries.

Configuring the CM-REST server

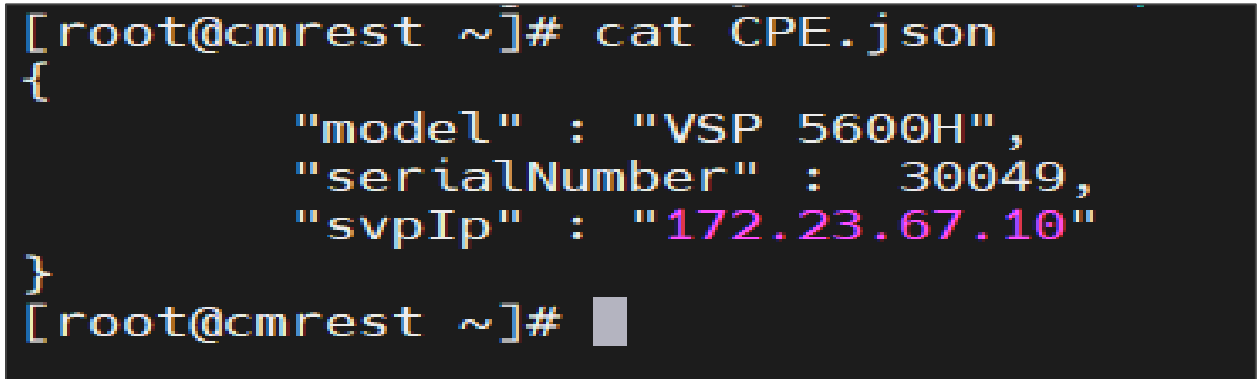
1. To install and configure the CM-REST server, complete the procedure described the following location:

https://knowledge.hitachivantara.com/Documents/Management_Software/Ops_Center/API_Configuration_Manager/10.8.x/Get_started/05_Installing_the_REST_API

2. Register the Hitachi storage system.

- a. To register a Hitachi storage system, create a JSON file with the information for each storage system you want to register and then run the following command:

```
[root@cmrest tmp]# curl -v -k -H "Accept:application/json" -H  
"Content-Type:application/json" -u maintenance:raid-maintenance -X  
POST --data-binary @./CPE.json
```

A terminal window with a black background and white text. The prompt is [root@cmrest ~]#. The command cat CPE.json is entered, and the output is a JSON object: {"model": "VSP 5600H", "serialNumber": 30049, "svpIp": "172.23.67.10"}. The prompt [root@cmrest ~]# is shown again with a grey cursor block.

```
[root@cmrest ~]# cat CPE.json  
{  
    "model" : "VSP 5600H",  
    "serialNumber" : 30049,  
    "svpIp" : "172.23.67.10"  
}  
[root@cmrest ~]# █
```

- b. To check the registered storage system, run the following command:

```
[root@cmrest tmp]#curl -k
```

<https://cmrest.ransomware.net:23451/ConfigurationManager/v1/objects/storages>

Configuring and Installing Veritas NetBackup Components

Configuring Veritas NetBackup consists of the following high-level steps:

- Installing the Master server
- Installing NetBackup Media Server
- Installing NetBackup Client
- Configuring MSDP storage
- Configuring MSDP-C Storage
- Configuring Storage Life Cycle Policy
- Installing and Configuring CloudPoint Server to use Snapshot Manager
- Installing NetBackup Malware Scanner
- Configuring Anomaly Detection

Installing the Master server

To install the NetBackup master server, see the [NetBackup Install Guide](#).

Installing NetBackup Media Server

To install the NetBackup media server, complete the procedure in the [NetBackup™ Installation Guide \(veritas.com\)](#).

Installing NetBackup Client

To install NetBackup on the client, copy the Binary file to the client server.

For more information, see the [NBU installation Guide](#).

Configuring MSDP Storage

To configure the MSDP storage, disk pool, and storage unit, complete the procedure described in the following location:

https://sort.veritas.com/public/documents/isa/7.3.0.1/linux/productguides/html/access_nbu_solutions_7301_lin/ch03s06.htm

Configuring MSDP-C Storage

Configuring the MSDP-C storage consists of the following high-level steps:

- Prepare the environment
- Create an MSDP cloud immutable storage volume
- Add a Disk pool from the NetBackup WEB UI
- Create a Storage Unit using WORM Lock feature

Prepare the environment

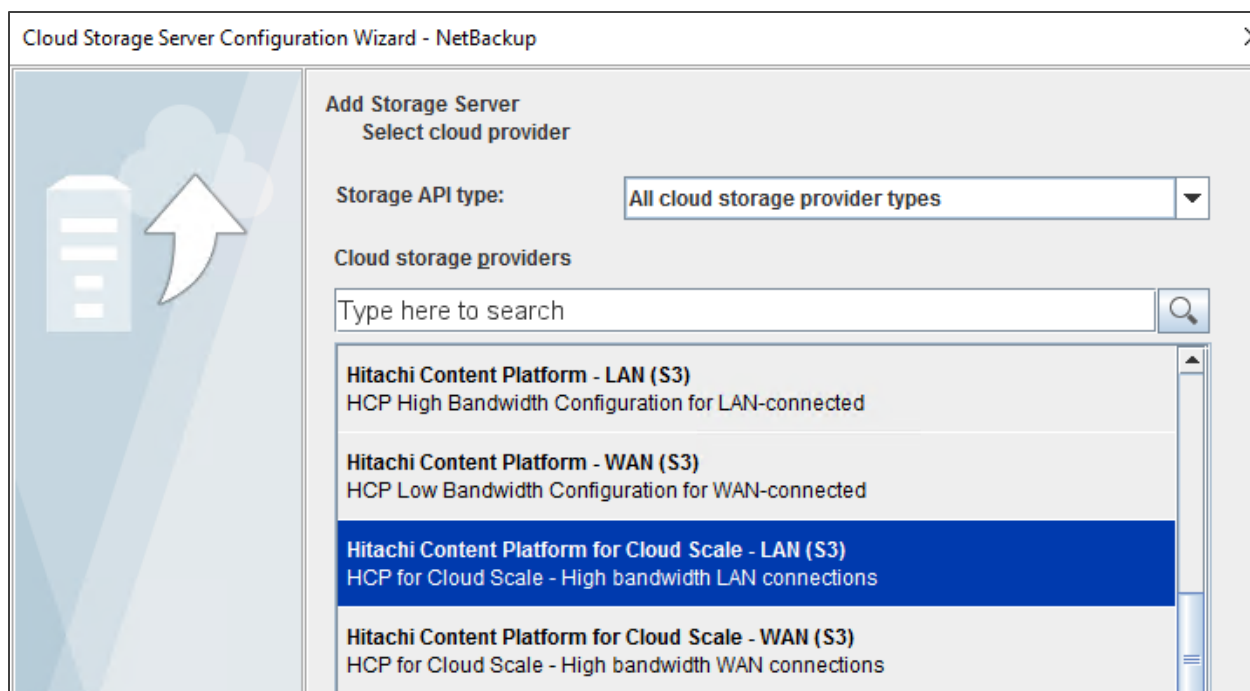
Before you begin, prepare the environment as follows:

1. Create an immutable storage volume from Veritas NetBackup, which creates a bucket in HCP for cloud scale.
2. Verify that HCP for cloud scale has a valid SSL certificate.
3. To perform the system and admin tasks, set up the following environment variables on the MSDP-C server:

```
export MSDPC_ACCESS_KEY=xxxx
export MSDPC_SECRET_KEY=yyyy
export MSDPC_REGION=us-west-2
export MSDPC_PROVIDER= Hitachi-csl
export MSDPC_ENDPOINT= HCP for cloud scale server name
```

4. Verify that the following Veritas NetBackup cloud storage providers for HCP for cloud scale are available:

```
hitachi-csw (HCP for cloud scale, WAN)
hitachi-csl (HCP for cloud scale, LAN)
```



Create an MSDP cloud immutable storage volume

To create and manage immutable cloud volumes, use the Veritas NetBackup MSDP cloud admin tool, `msdpclutil`. This tool is located in the `/usr/openv/pdde/pdcr/bin` folder.

Note: To skip SSL, use “`--disablessl`”. For more details, see the [Troubleshooting](#) section.

1. Create a cloud immutable storage volume using the `msdpclutil` tool. Run the following command:

```
/usr/openv/pdde/pdcr/bin/msdpclutil
```

```
/usr/openv/pdde/pdcr/bin/msdpclutil create -b veritas-ransomware -v veritas_vol --mode COMPLIANCE --min 1D --max 30D --live 2025-08-25 --disablessl
```

```
[root@NBUMEDIA tmp]# /usr/openv/pdde/pdcr/bin/msdpclutil create -b veritas-ransomware -v veritas_vol --mode COMPLIANCE --min 1D --max 30D --live 2025-08-25 --disablessl
```

2. Update the cloud immutable storage volume with the minimum and maximum retention period values. Run the following command:

```
/usr/openv/pdde/pdcr/bin/msdpclutil update range -b veritas-ransomware -v veritas_vol --min 5D --max 30D
```

```
/usr/openv/pdde/pdcr/bin/msdpclutil update -b veritas-ransomware -v veritas_vol --mode COMPLIANCE --min 1D --max 30D --live 2025-08-25 -
```

```
disablessl
```

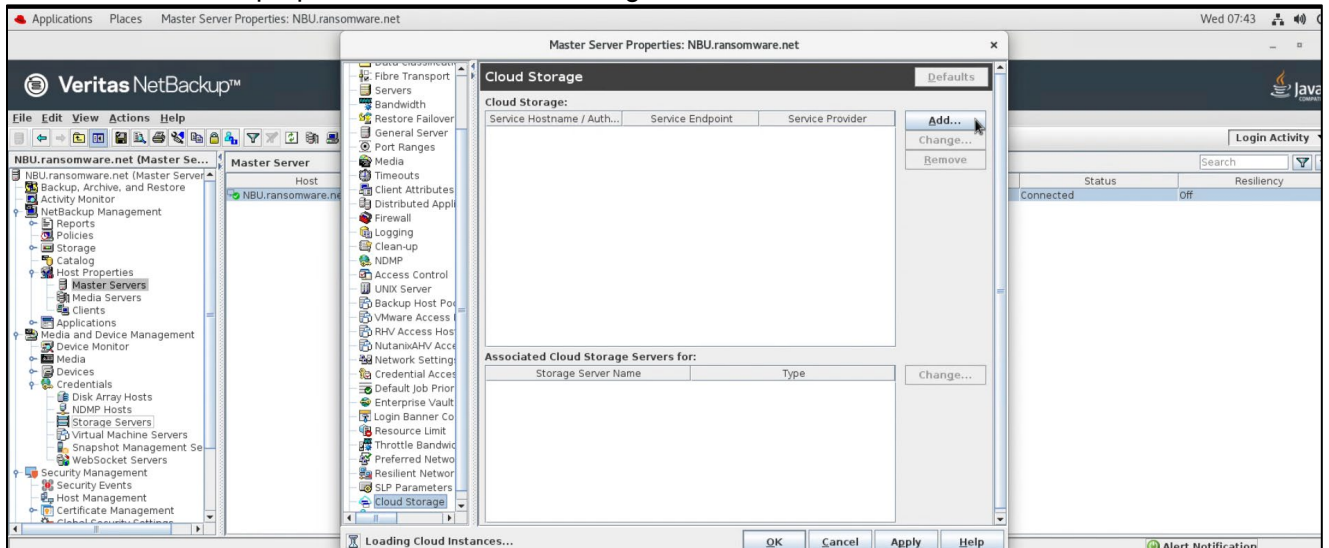
```
[root@NBUMEDIA tmp]# /usr/openv/pdde/pdcr/bin/msdpclutil update -b veritas-ransomware -v veritas_vol --mode COMPLIANCE --min 1D --max 30D --live 2025-08-25 --disablessl
```

3. To view the defined storage parameters, list the immutable bucket that was created using Veritas NetBackup when setting up the environment. Run the following command:

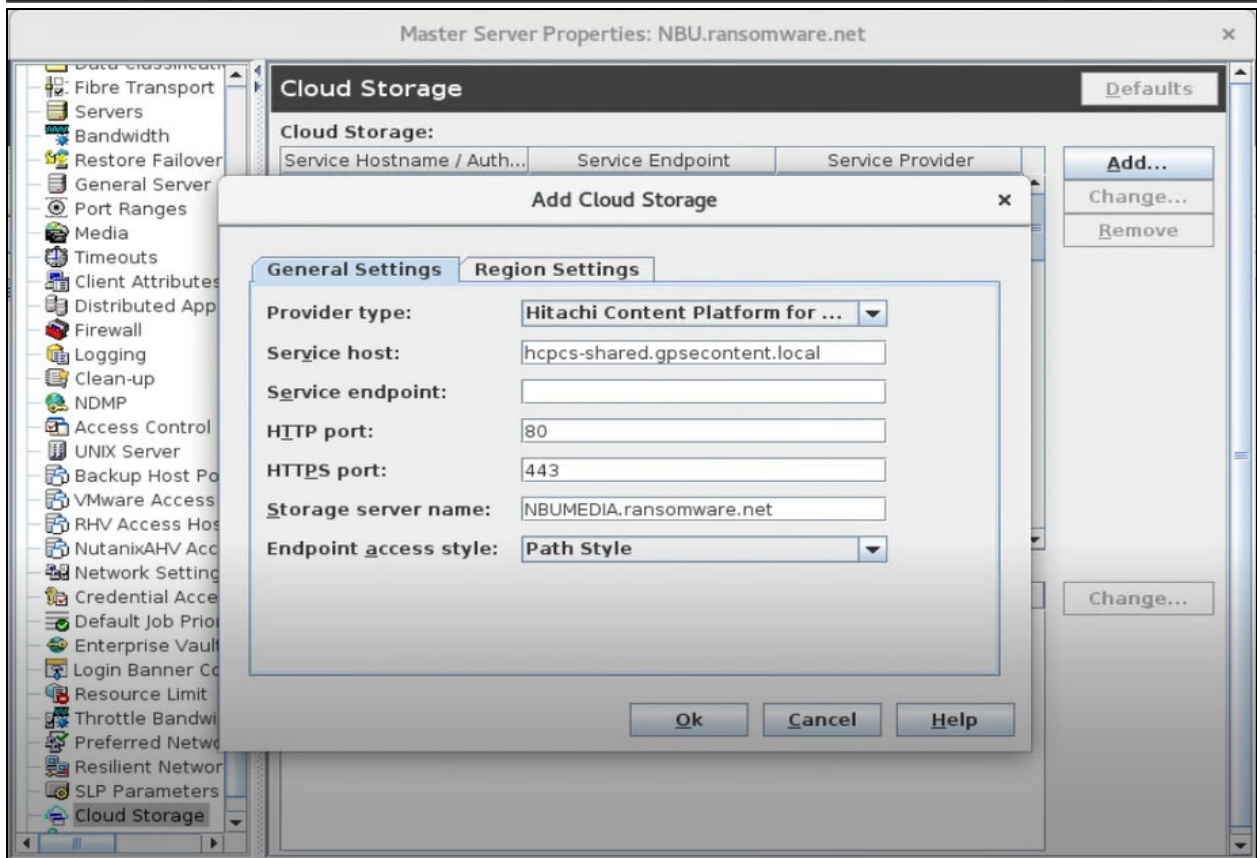
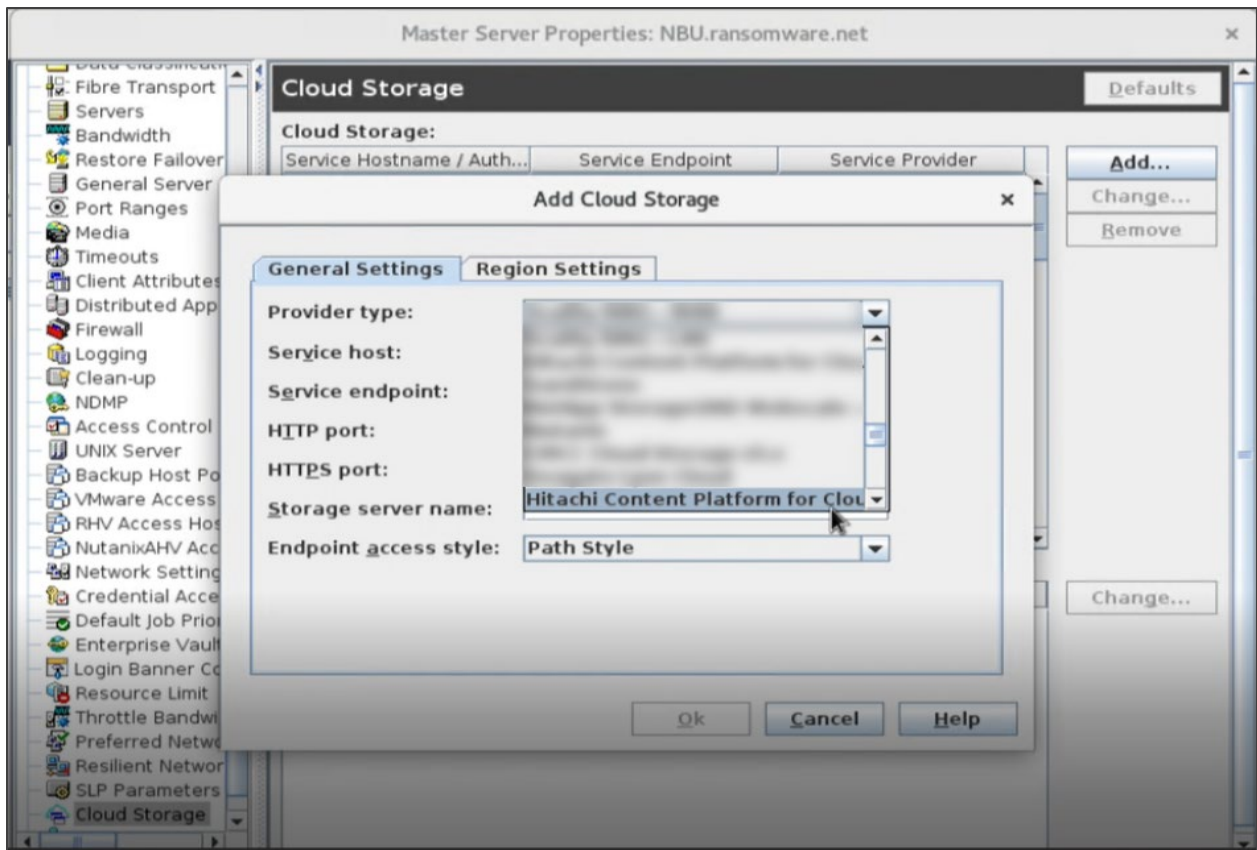
```
/usr/openv/pdde/pdcr/bin/msdpclutil list --disablessl
```

```
[root@NBUMEDIA tmp]# /usr/openv/pdde/pdcr/bin/msdpclutil list --disablessl
Bucket: veritas-ransomware
{
  "Bucket": "veritas-ransomware",
  "Volume": "veritas_vol",
  "Region": "us-west-2",
  "Volume_Mode": "COMPLIANCE",
  "Volume_LiveState": "ON",
  "Volume_LiveUntilDate": "2025-08-25 00:00:00 +0000 UTC",
  "Volume_LiveDuration": "2Y289D",
  "Volume_RetentionTimeInherit": "unknown",
  "Volume_LockMin": "86400",
  "Volume_LockMax": "2592000",
  "Volume_Configured": false
}
```

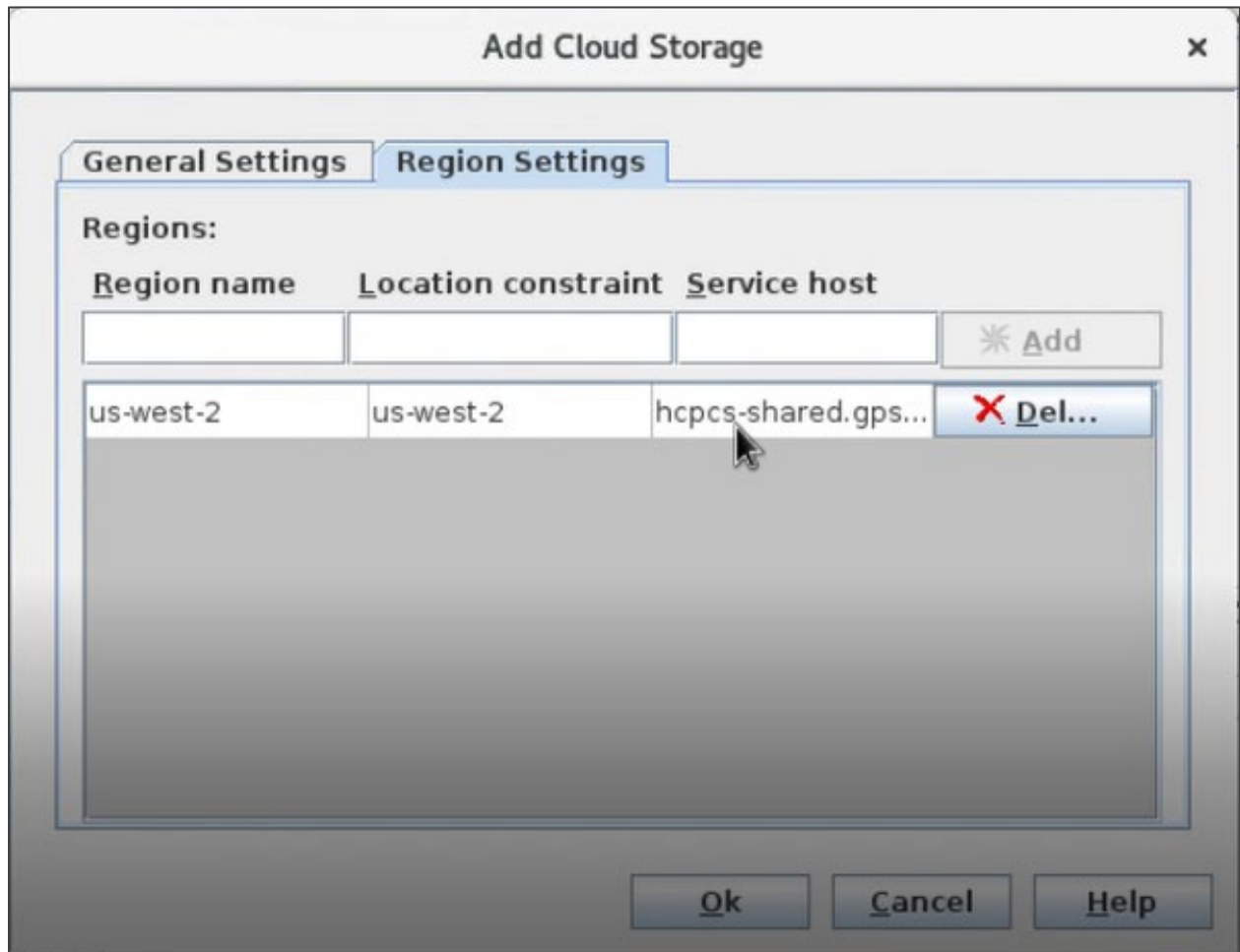
4. From master server properties, select Cloud Storage.



5. Add the Media server to the cloud provider Hitachi Content Platform for cloud scale LAN.



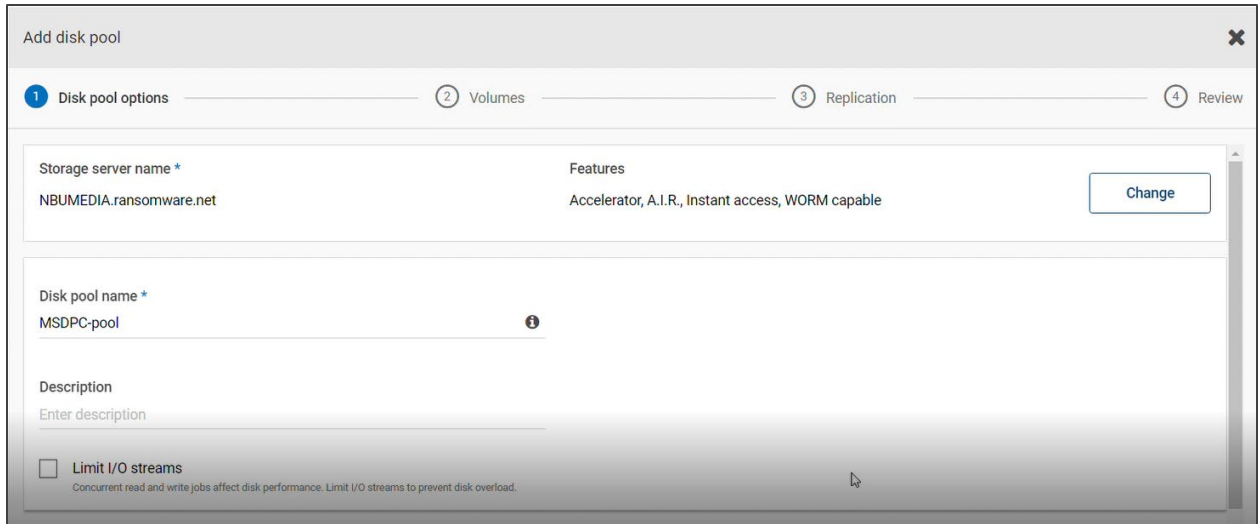
6. Add region settings.



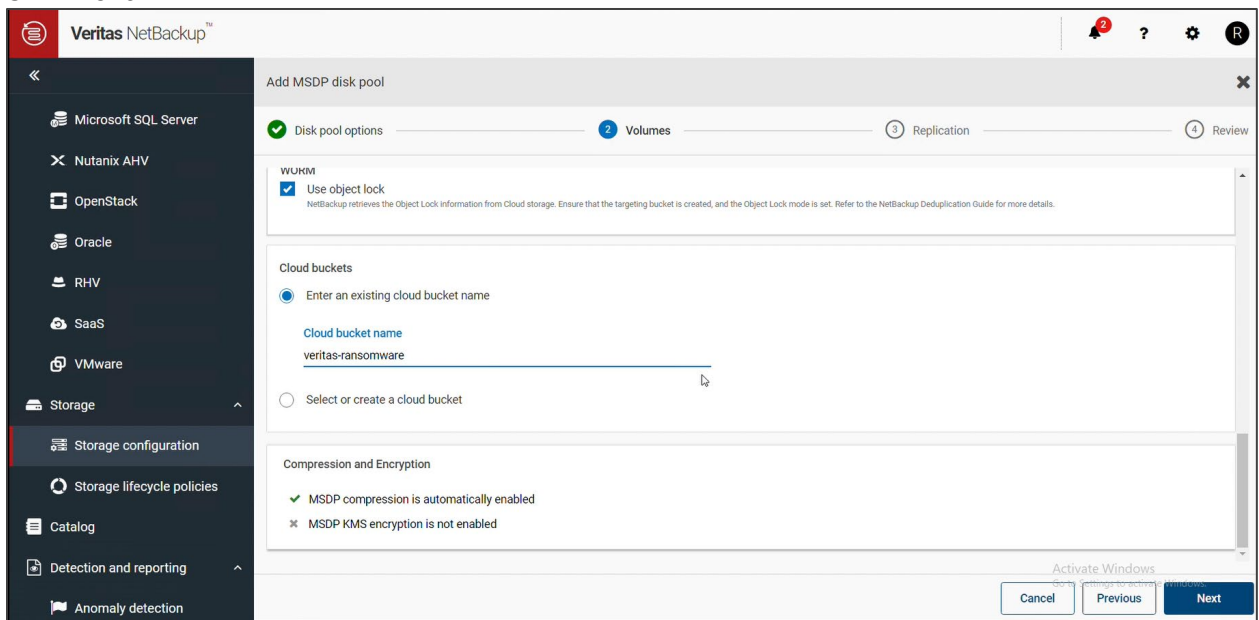
Add a Disk pool from the NetBackup WEB UI

To add a disk pool from the NetBackup UI, complete the following steps:

1. Select a media server.
2. Enter a pool name.

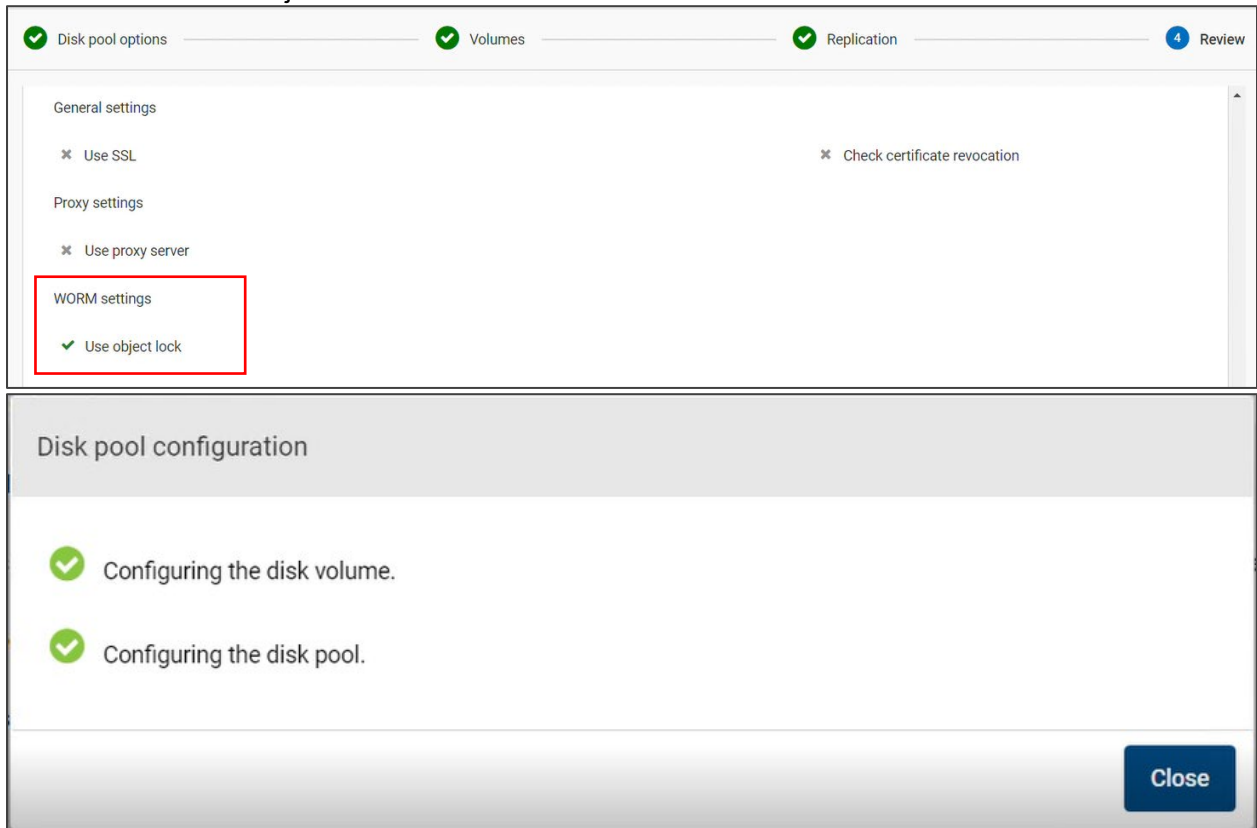


3. Select the WORM lock feature.
4. Select an existing cloud bucket name.
5. Click **Next**.



6. Without adding replication, click **Next**.

7. Ensure that the use object lock feature is enabled.

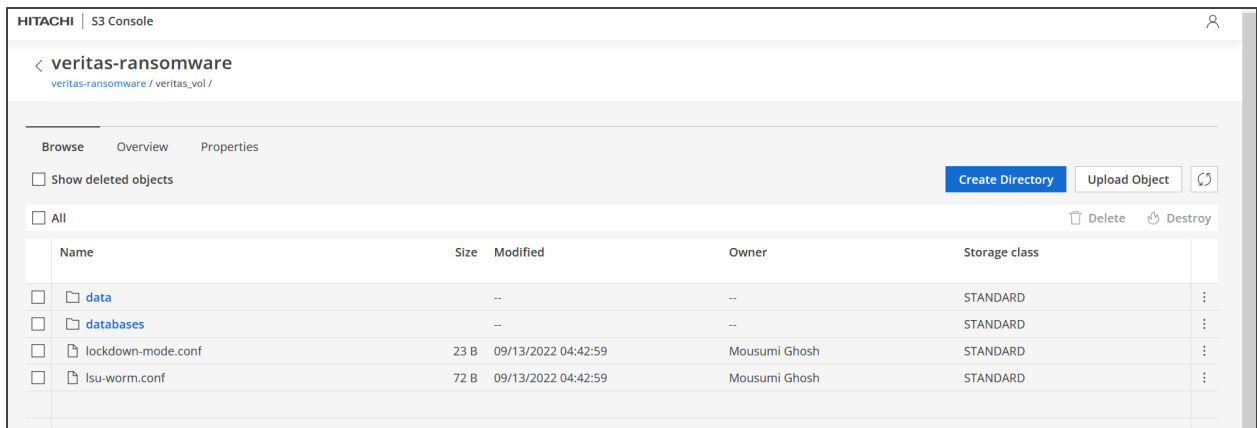


The volume configuration is true only after you add the volume with the same name from the NetBackup UI.

```
[root@NBUMEDIA goodies]# /usr/opensv/pdde/pdcr/bin/msdpclutil list --disablessl
Bucket: veritas-ransomware
{
  "Bucket": "veritas-ransomware",
  "Volume": "veritas_vol",
  "Region": "us-west-2",
  "Volume_Mode": "COMPLIANCE",
  "Volume_LiveState": "ON",
  "Volume_LiveUntilDate": "2025-08-25 00:00:00 +0000 UTC",
  "Volume_LiveDuration": "2Y346D",
  "Volume_RetentionTimeInherit": "unknown",
  "Volume_LockMin": "86400",
  "Volume_LockMax": "2592000",
  "Volume_Configured": true
}
```

Name	Available space	Total size	Encryption	Replication	Bucket name	WORM capable	Minimum lock duratio	Maximum lock durati
PureDiskVolume	1.34 TB	1.34 TB	Yes	None				
veritas_vol	8.00 PB	8.00 PB	No	None	veritas-ransomware	<input checked="" type="checkbox"/>	1 day	30 days

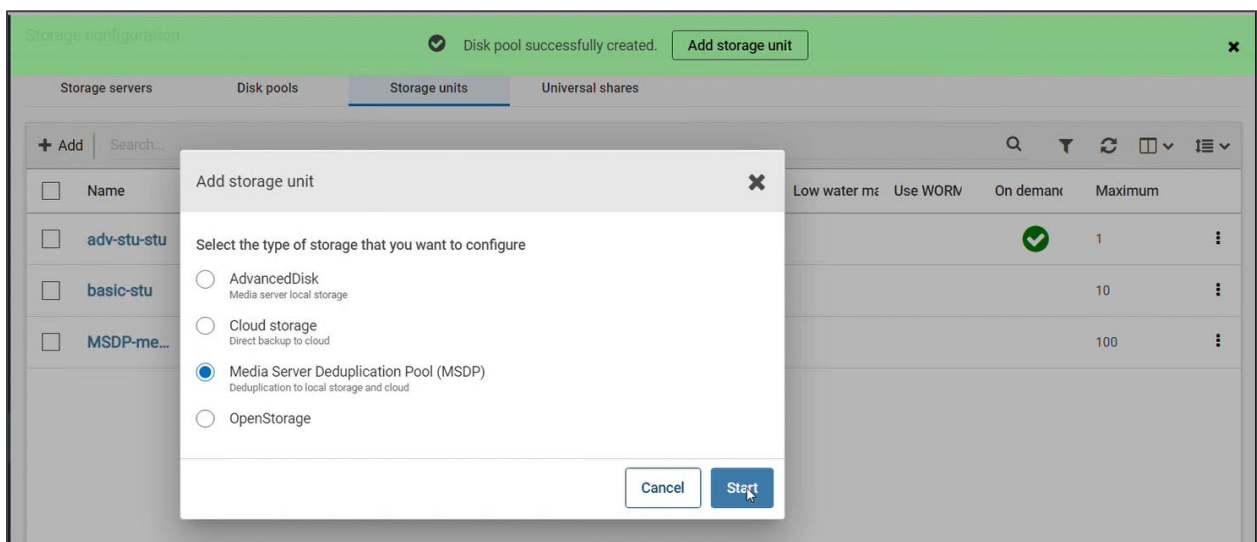
8. Verify the bucket and volume from HCP for Cloud Scale tab.



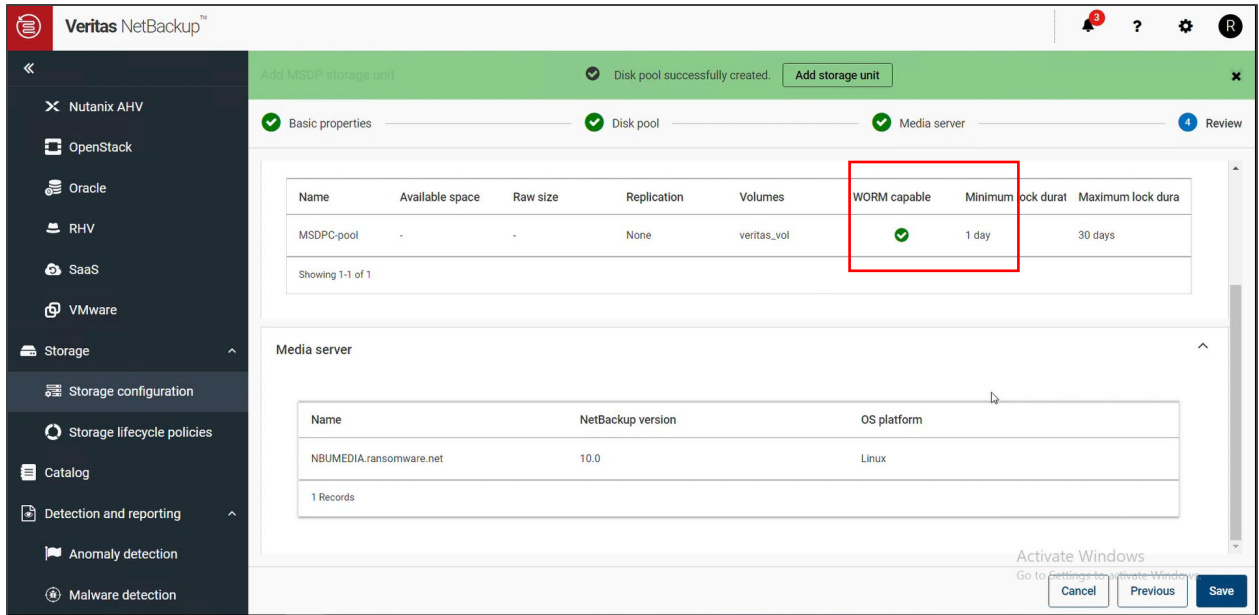
Create a Storage Unit using WORM Lock feature

To create a Storage Unit using WORM Lock feature, complete the following steps:

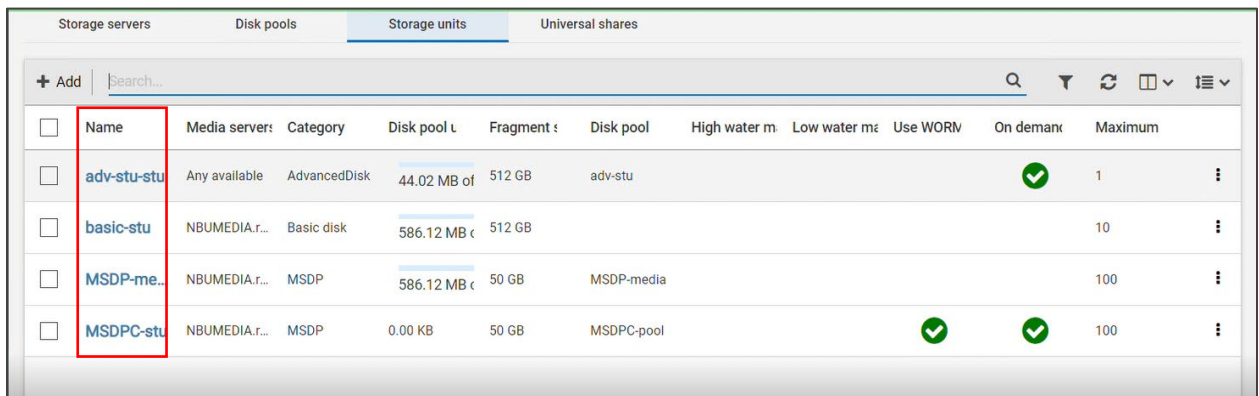
1. Click **Add Storage Unit**.
2. Select the storage type.



3. Click **Start**.
4. Verify that WORM capable is checked.

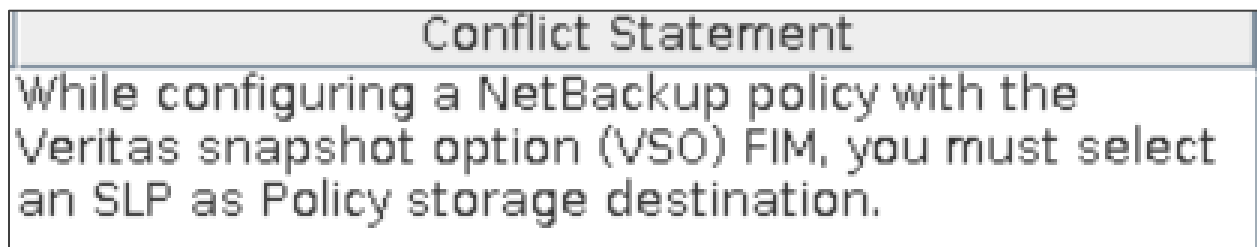


5. Verify that a storage unit is created.



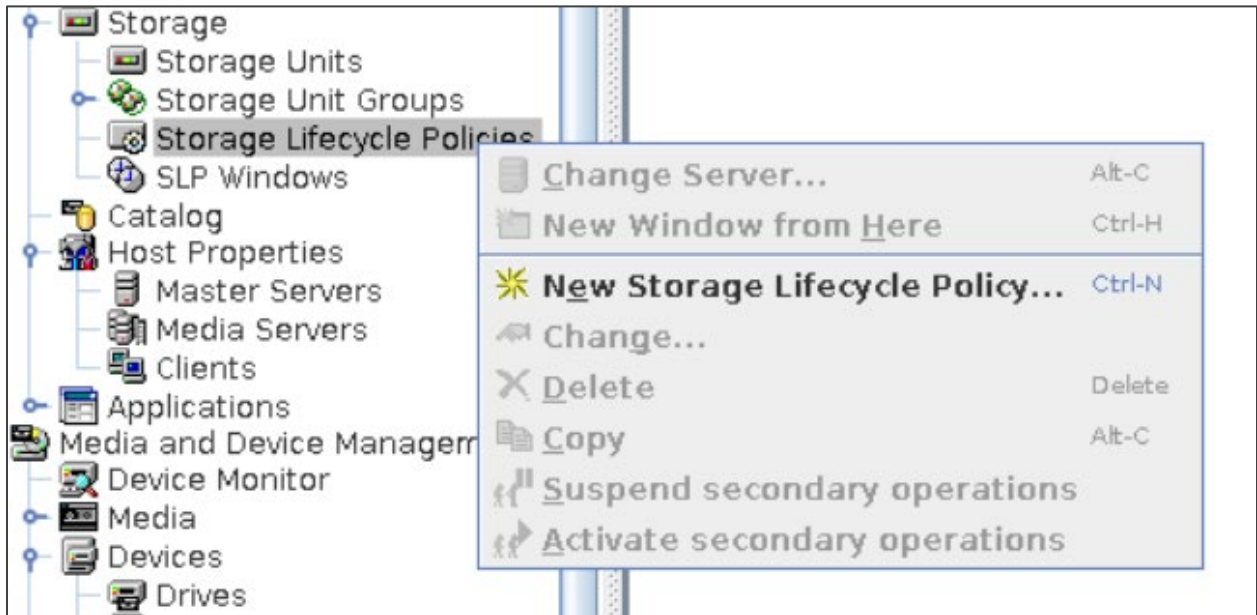
Configuring Storage Life Cycle Policy

A storage lifecycle policy (SLP) is a storage plan for a set of backups that is required to use the Snapshot Manager application.



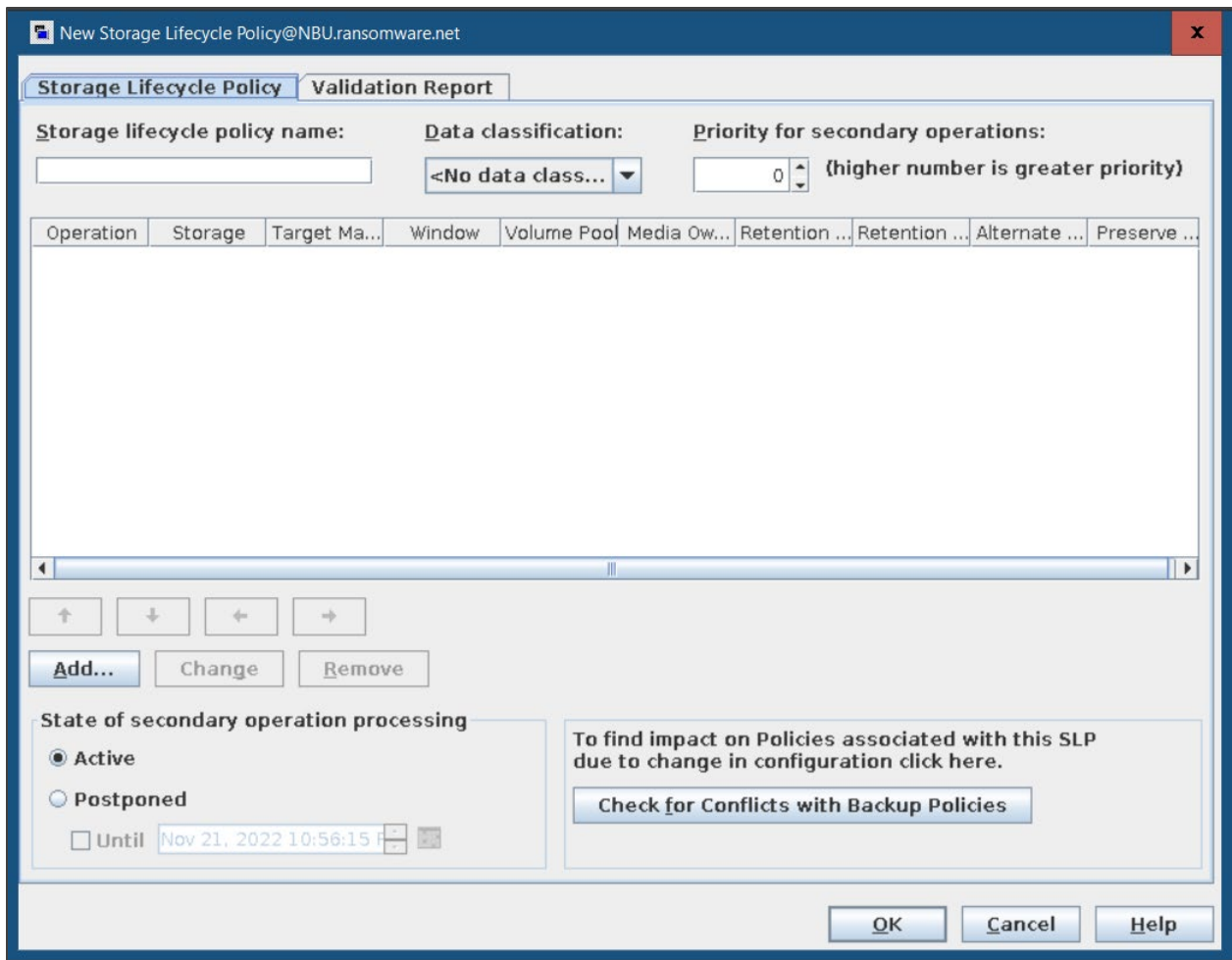
To create a new storage lifecycle policy, complete the following steps:

1. Right-click on **Storage Lifecycle Policies** and then click **New Storage Lifecycle Policy**.

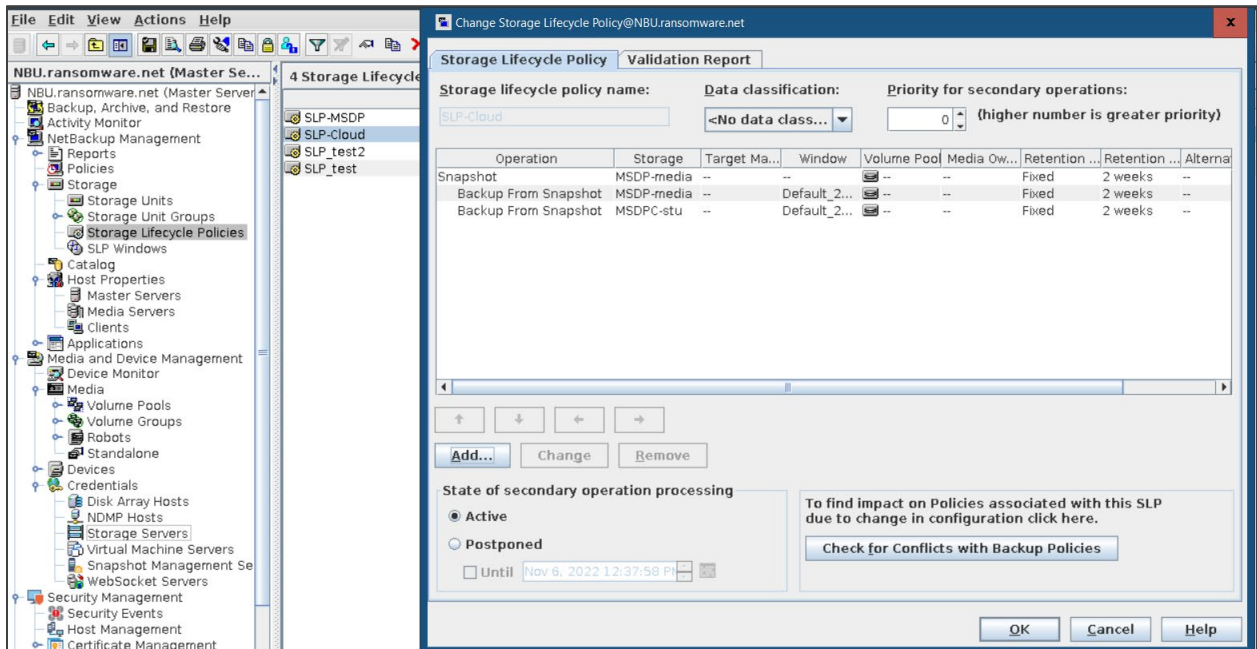
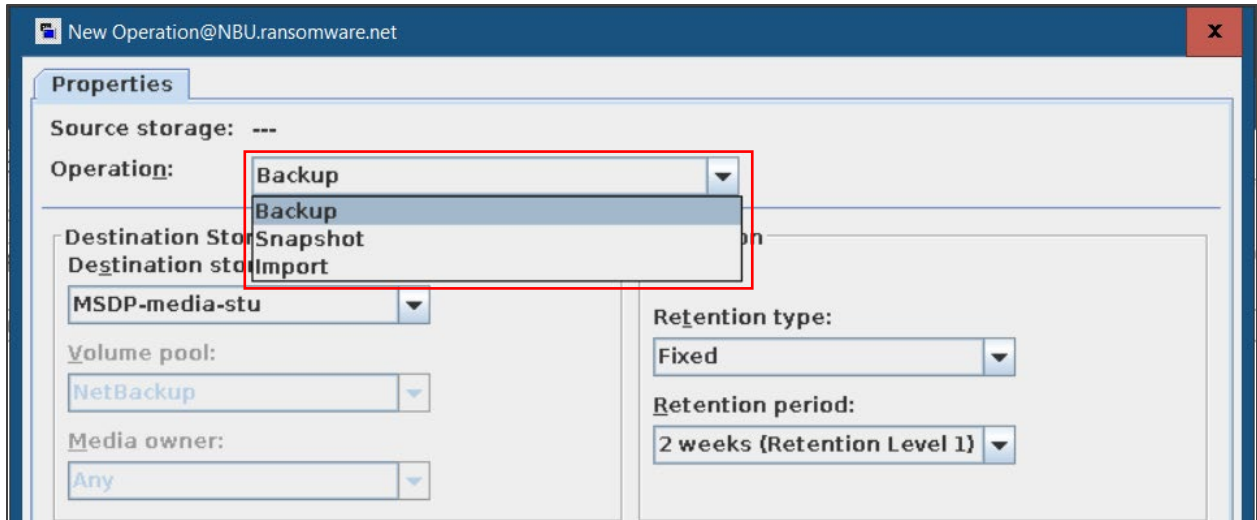


2. Add an SLP name.





3. Select an operation.
 - First operation - Snapshot is created on a Hitachi VSP 5600 storage system.
 - Second operation - Backup of snapshot is stored on NetBackup media server (Hitachi VSP 5600 storage system).
 - Third operation - Backup of snapshot is stored on HCP for cloud scale.
4. Select **Destination Storage**.
5. Select an image expiry retention type and period.



Installing and Configuring the CloudPoint Server to use Snapshot Manager

Configuring the CloudPoint Server consists of the following high-level steps:

- Preparing for CloudPoint Installation
- Installing CloudPoint using Docker
- Configuring CloudPoint plug-ins
- Configuring Policy for using Snapshot Manager

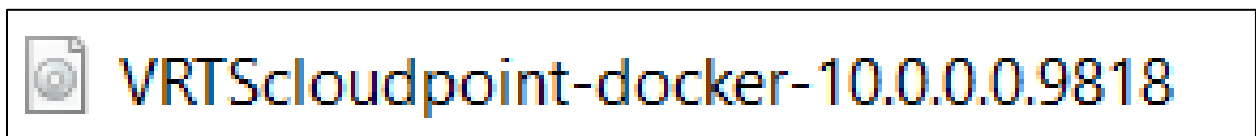
Preparing for CloudPoint Installation

To install the container Platform Docker, complete the described in the following location:
https://www.veritas.com/content/support/en_US/doc/140789355-151836558-0/v140790360-151836558

Installing CloudPoint using Docker

To install CloudPoint using docker, complete the following steps:

1. Download the file from [Veritas download center](#).



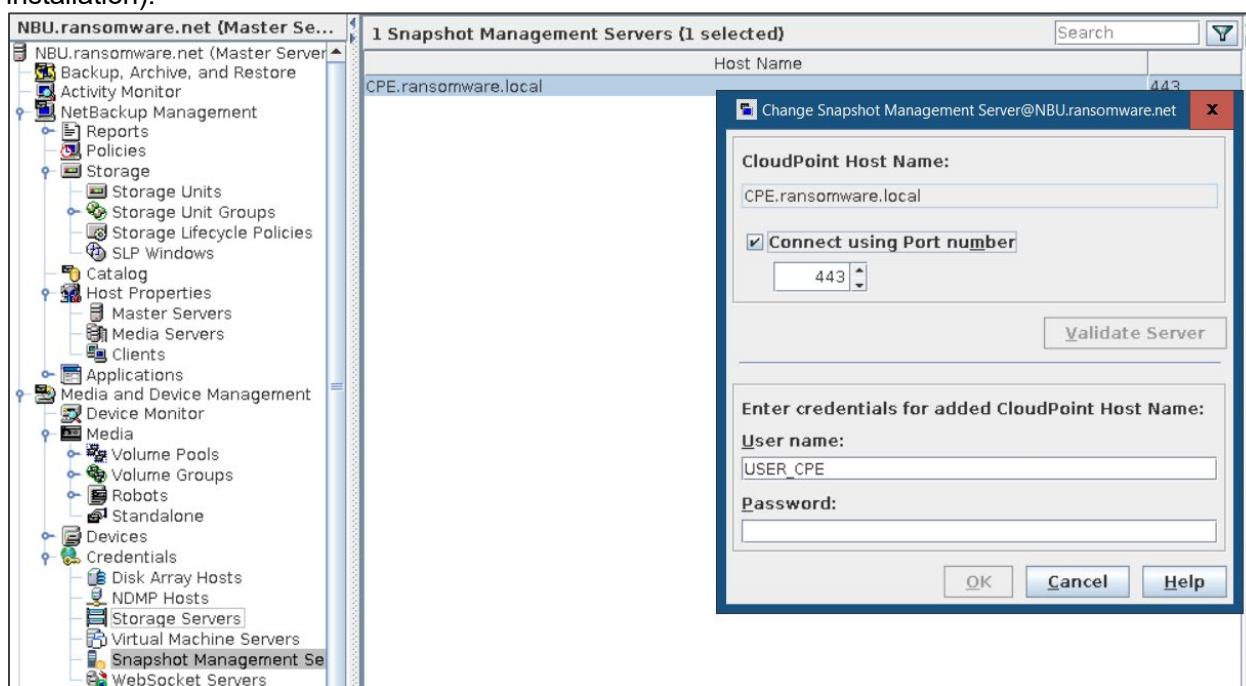
```
docker load -i Veritas_CloudPoint_10.0.0.9818.img.gz
```

```
docker run -it -rm -v /cloudpoint:/cloudpoint -v  
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint: 10.0.0.9818 install
```

```
docker run -it --rm -v /cloudpoint:/cloudpoint -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-cloudpoint:10.0.0.9818 insta
Installing the services
Configuration started at time: Wed Aug 10 04:05:58 UTC 2022
WARNING: You're not using the default seccomp profile
docker server version: 1.13.1
WARNING: You're not using the default seccomp profile
This is a fresh install of NetBackup CloudPoint 10.0.0.9818
CloudPoint currently is not configured. Starting initial services before configuration.
Creating network: flexsnap-network ... done
Starting container: flexsnap-fluentd ... done
Starting container: flexsnap-ipv6config ... done
Creating container: flexsnap-mongodb ... done
Creating container: flexsnap-rabbitmq ... done
Creating container: flexsnap-certauth ... done
Creating container: flexsnap-api-gateway ... done
Creating container: flexsnap-coordinator ... done
```

2. From the NetBackup UI, click **Snapshot Manager**.

3. Enter a CloudPoint server name, user name, and password (which you created during installation).



Configuring CloudPoint plug-ins

To configure CloudPoint plug-ins, complete the following steps:

1. Enter a unique plug-in ID.
2. Enter a Hitachi API Configuration Manager (CMREST) server IP.
3. For server port, enter 23451.
4. Enter an array username and password.
5. Enter the storage device ID that you created during Hitachi storage system registration.

The image shows a 'Configure Plugin' dialog box with the following fields and values:

- CloudPoint Server: NBUCPE.ransomware.local
- Selected Plugin: Hitachi Storage Array
- Credentials section:
 - Enter Plugin ID: VSP5600H
 - Hitachi Configuration Manager Server IP: [Redacted]
 - Hitachi Configuration Manager Server Port: 23451
 - Array Username: [Redacted]
 - Array Password: [Redacted]
 - Array storage Device Id: [Redacted]

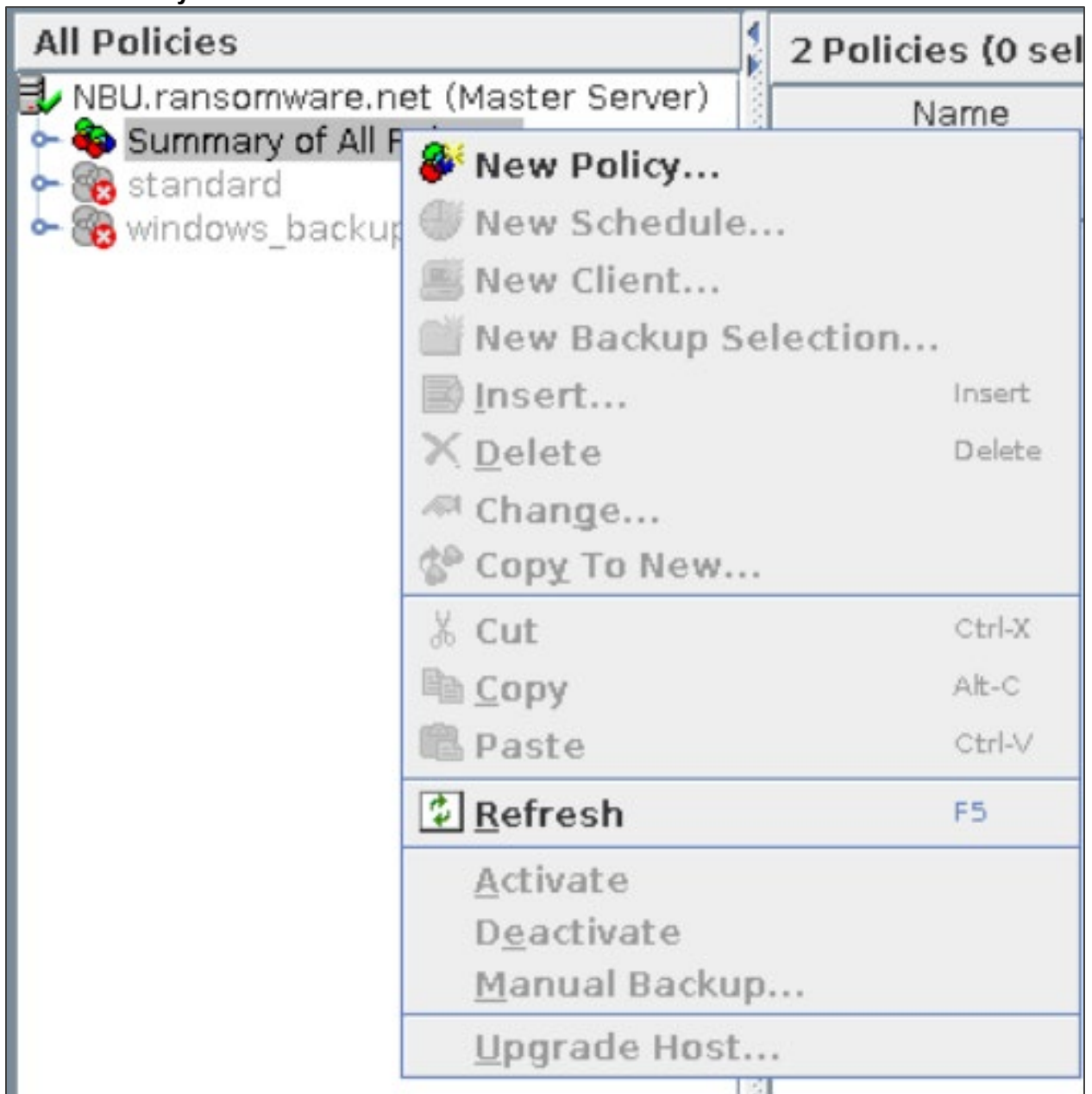
Buttons at the bottom: OK, Cancel, Help.

Configuring a Policy for using Snapshot Manager

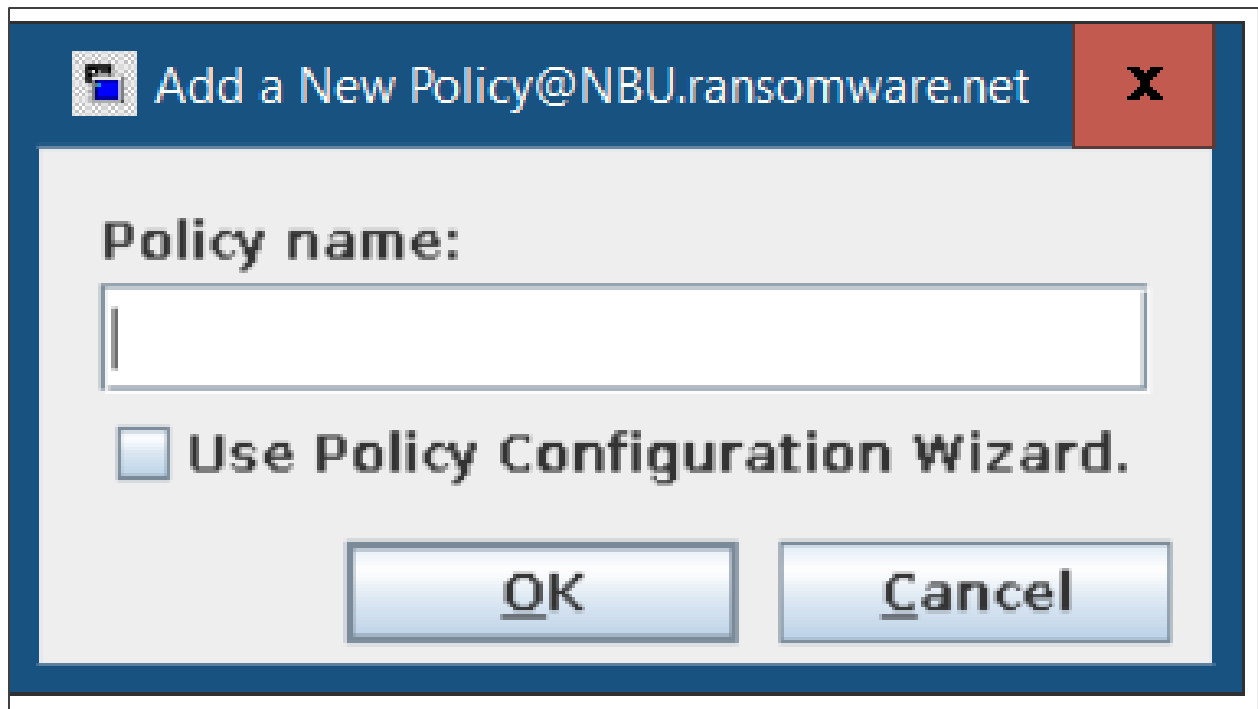
To configure a policy, complete the following steps:

1. Right-click on **Summary of all policies**.

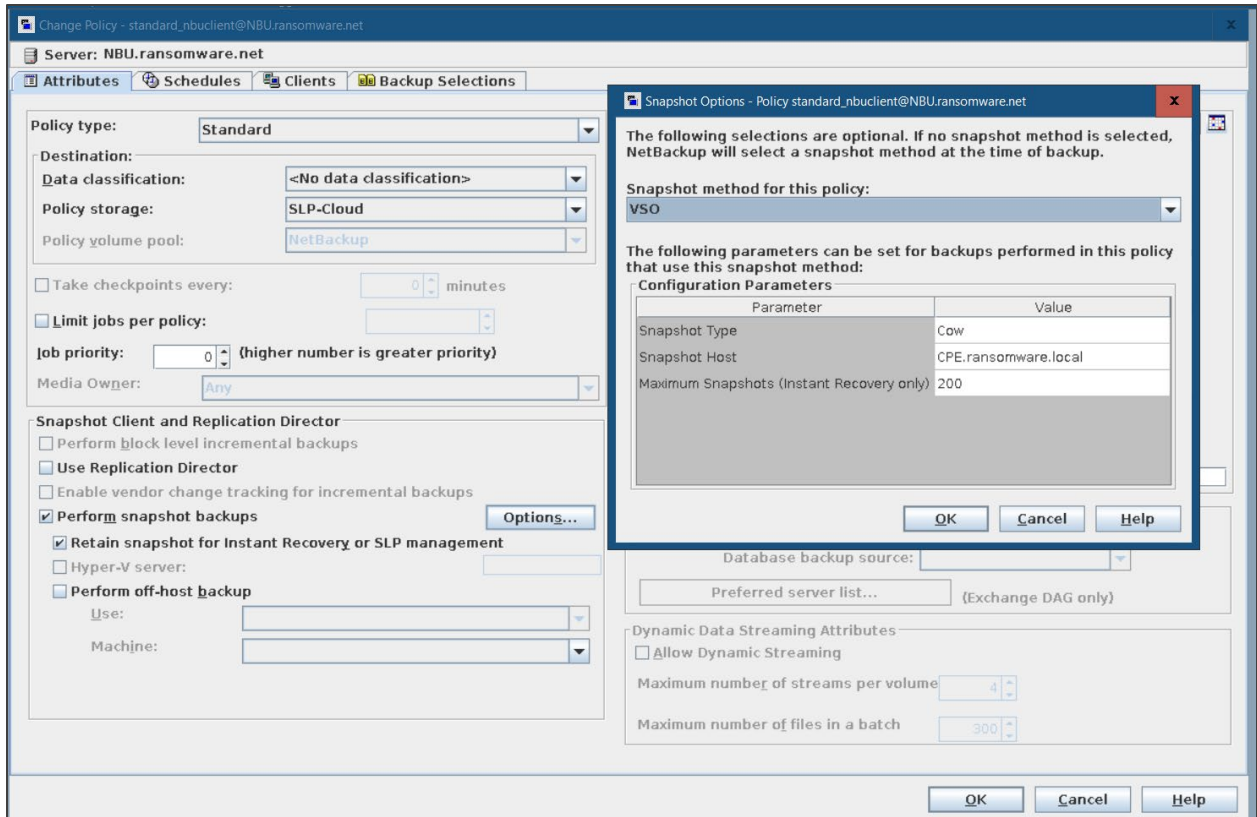
2. Click **New Policy**.



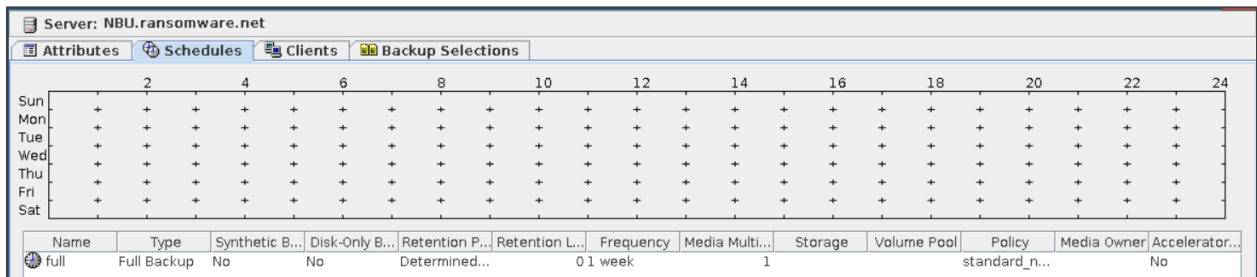
3. Enter a policy name and click **OK**.



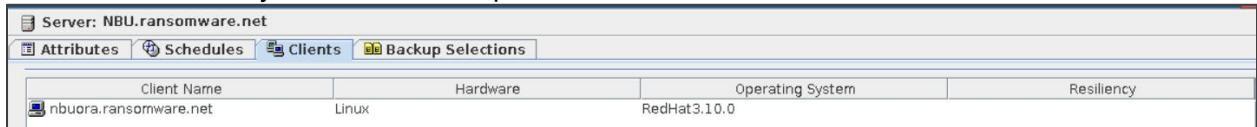
4. Select a policy type.
5. For policy storage, select SLP.
6. Click **Perform Snapshot Backups**.
7. Select snapshot options.
8. For snapshot method, select VSO (applicable for standard policy type).
VSO is used for snapshots that are managed using CloudPoint.
Using the NetBackup Snapshot management framework, you can use CloudPoint for taking snapshots of your images. With this release, you can protect all the on-premises storage systems that are supported by CloudPoint.
9. For snapshot type, select COW (Copy-On-Write). (Ensure that no active COW snapshots are in progress. If there is an active COW snapshot, the snapshot process has a handle open to the volume.)
10. Provide a maximum snapshots number for the policy.



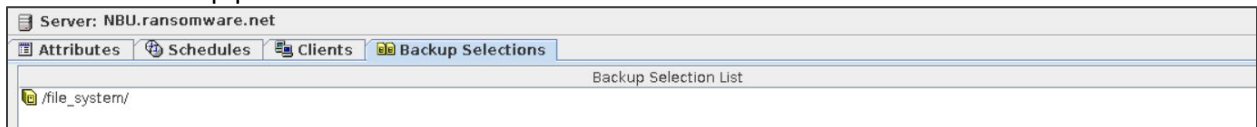
11. Add schedules.



12. Add the client name you want to back up.



13. Select the backup path.



Installing NetBackup Malware Scanner

NetBackup malware scanner installation consists of the following high-level steps:

- Preparing the scan host
- Installing the malware scanner

Preparing the Scan Host

1. Validate the pre-requisites listed in the following URL:

https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v152616050-149123528

2. Before using the Malware scanner, review the following workflow:

https://www.veritas.com/content/support/en_US/doc/21733320-149123528-0/v152646970-149123528

Important: You must configure instant access BYO on the MSDP storage server as described in the following location:

https://www.veritas.com/content/support/en_US/doc/25074086-151874763-0/v144265324-151874763

3. To verify whether the mount is working or not, create NFS from the media server manually as follows:

```
[root@NBU ~]# mkdir /tmp/test  
[root@NBU ~]# mount -t nfs NBUMEDIA.ransomware.net:/malwareshare  
/tmp/test
```

Installing the Malware scanner

To install the Malware Scanner, complete the procedure described in the following location:

https://www.veritas.com/content/support/en_US/doc/21733320-149123528-0/v152254868-149123528

Configuring Anomaly Detection

To configure the Anomaly detection setting from the WebUI, complete the procedure in the following location:

https://www.veritas.com/content/support/en_US/doc/21733320-149123528-0/v152007140-149123528

NetBackup Backup and Restore Operations

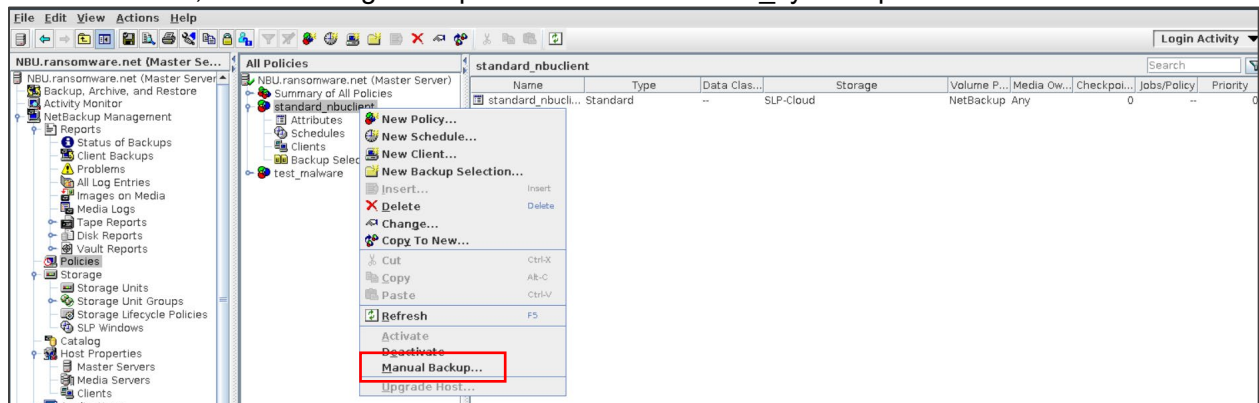
NetBackup Backup and Restore operations consists of the following high-level steps;

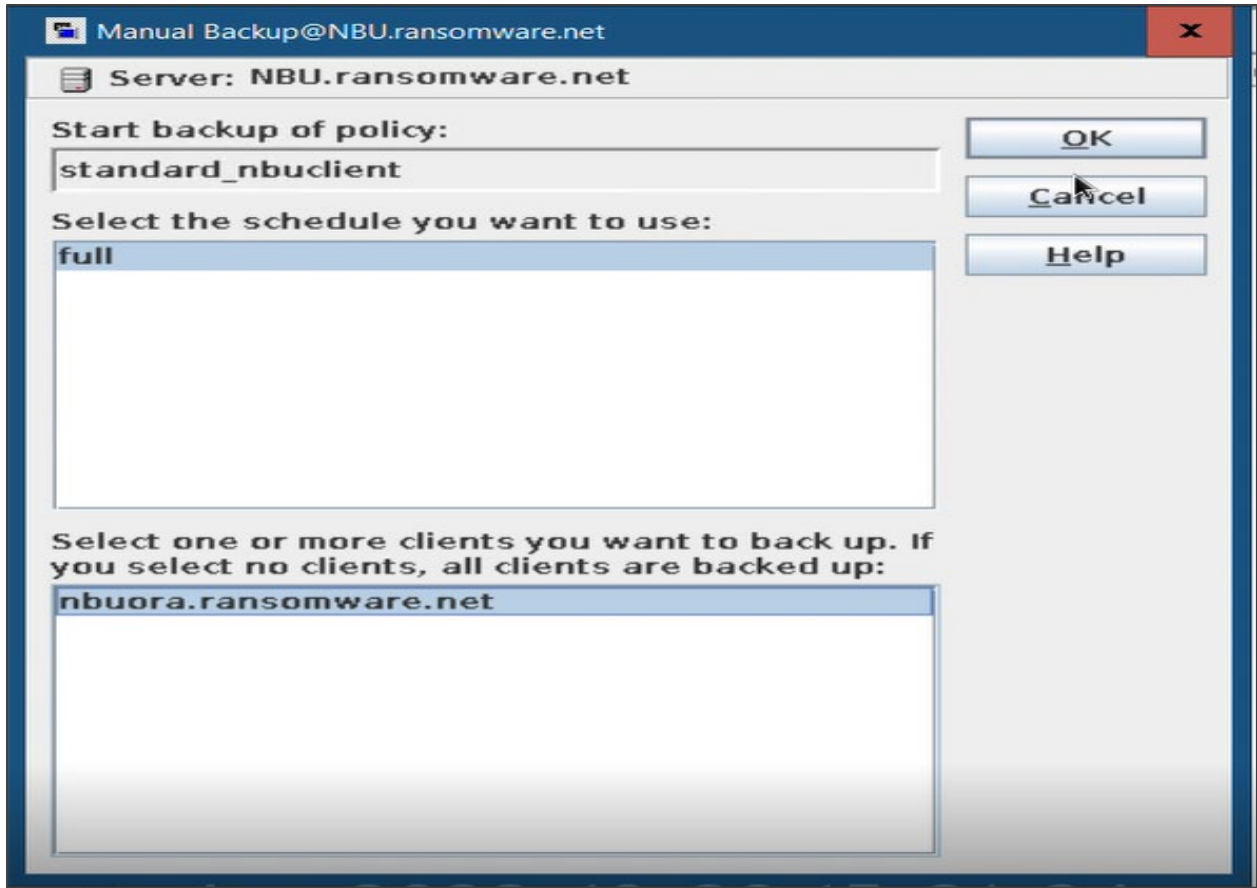
- Running a Snapshot Backup Job using a CloudPoint server for VSP 5600 storage system and HCP for cloud scale
- Restoring a Snapshot Backup Job

Running a Snapshot Backup Job using a CloudPoint server for VSP 5600 storage system and HCP for Cloud Scale

1. To perform snapshot and backups of snapshot, click **Manual Backup**.

In this scenario, we are taking backup of a text file in the '/file_system' path.





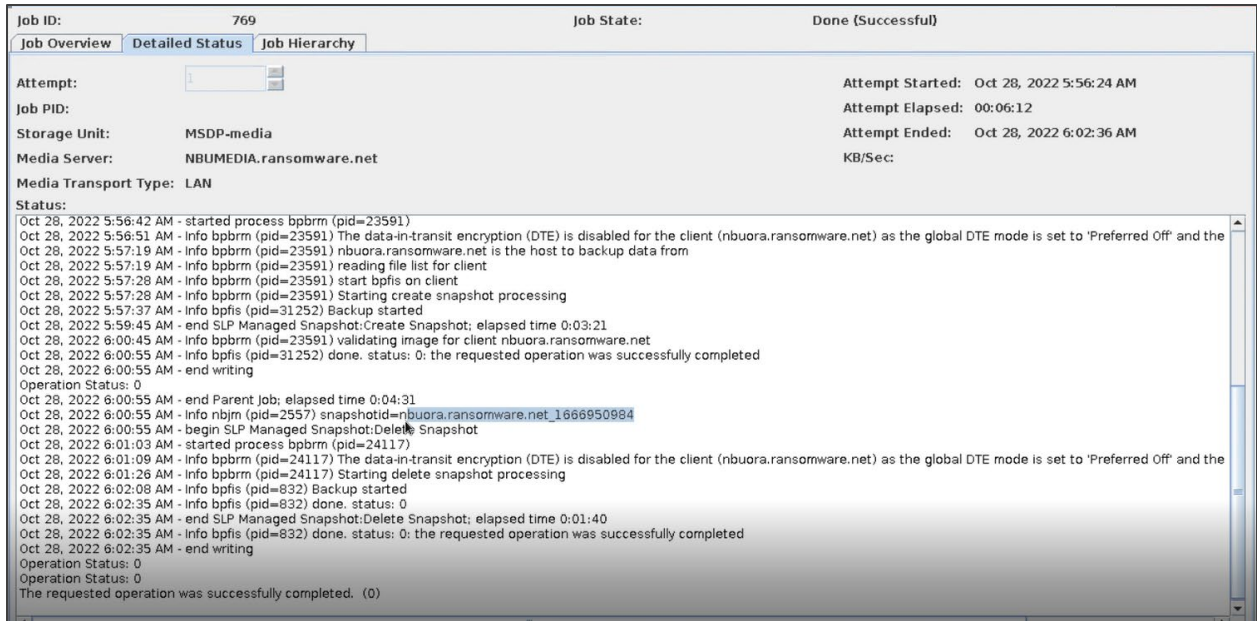
According to SLP, Snapshot job (Copy 1) has been completed successfully.

Job Id	Type	State	Stat...	Status	Job Policy	Job Schedule	Client	Media Se...	Start
769 Snapshot		Active			standard_nbuclient	full	nbuora.ransomware.net	NBUMEDI...	Oct 28, 2022

Job Id	Type	State	Stat...	Status	Job Policy	Job Schedule	Client	Media Se...	Start
769 Snapshot		Done		0	standard_nbuclient	full	nbuora.ransomware.net	NBUMEDI...	Oct 28, 2022

2. Verify the Snapshot job from the NetBackup UI.

Snapshot job (Copy 1) is created in the VSP 5600 storage system as shown in the following image:



- Verify the Snapshot job (Copy 1) from the VSP 5600 storage system.

All TI pairs are created after the snapshot job is completed from NetBackup.

LDEV ID	LDEV Name	Port ID	Host Group Name / iSCSI Target Alias	iSCSI Target Name	LUN ID	Namespace ID	Number of Snapshot Data	Number of Pairs in PSUE status	Cascade
00:00:51	veritas_o...	CL1-H	1H-G01 (01)	iqn.1994-0...	0	-	6	0	Disabled

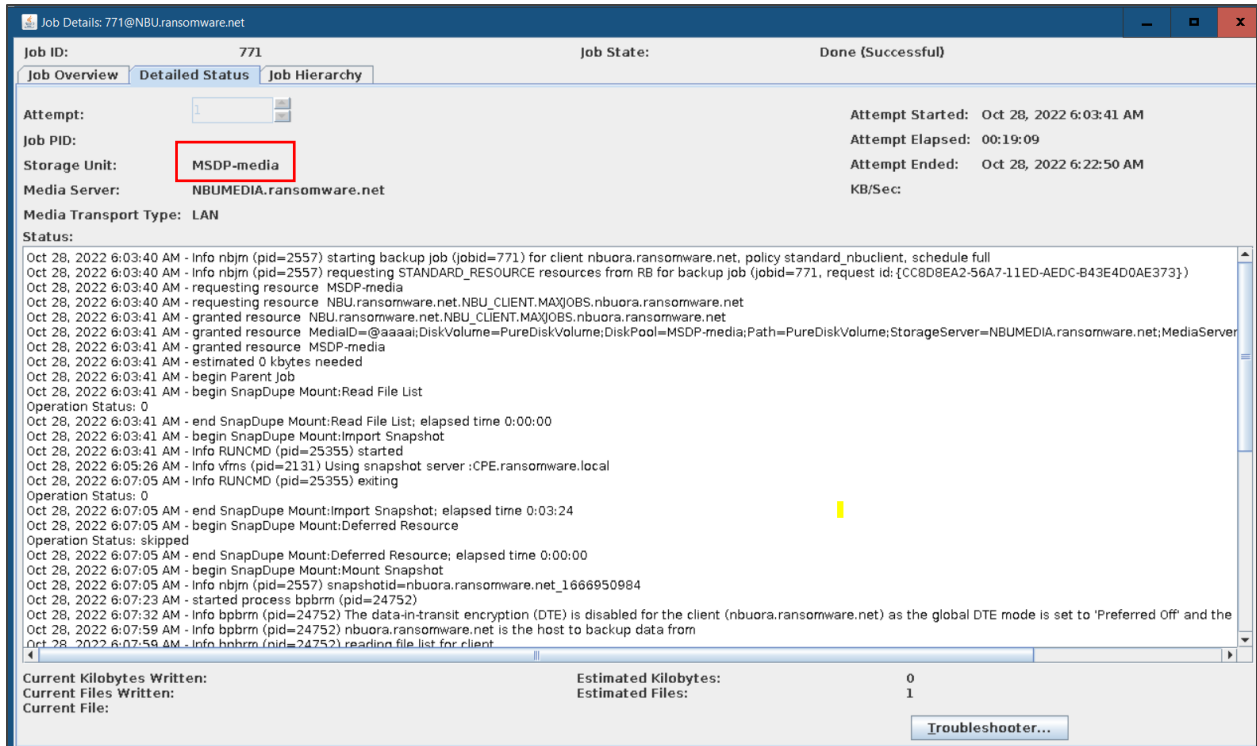
Snapshot Date	Snapshot SLU ID	Secondary Volume						
		LDEV ID	LDEV Name	Port ID	Host Group Name / iSCSI Target Alias	iSCSI Target Name	LUN ID	
2022/09/29 08:35:53	-	00:00:03	NB1664440586044761851	CL1-A	1A-G00 (00)	-	0	
2022/09/29 09:56:10	-	00:00:16	NB16644409540843761990	CL1-A	1A-G00 (00)	-	1	
2022/10/28 09:57:49	-	00:00:18	NB16669509840947258900	CL1-A	1A-G00 (00)	-	2	
2022/10/17 10:46:01	-	00:00:1B	NB16660034850730382724	CL1-A	1A-G00 (00)	-	3	
2022/10/18 05:13:46	-	00:00:1C	NB16660699700720816724	CL1-A	1A-G00 (00)	-	6	
2022/10/18 07:00:43	-	00:00:1D	NB16660763710544598844	CL1-A	1A-G00 (00)	-	7	

According to SLP, Backup of the snapshot job (Copy 2) is completed successfully:

772 Backup From Snapshot	Done	0 SLP_SLP-Cloud	full	nbuora.ransomware.net	NBUMEDIA.r...	Oct 28, 2022
771 Backup From Snapshot	Done	0 SLP_SLP-Cloud	-	nbuora.ransomware.net	NBUMEDIA.r...	Oct 28, 2022

- Verify whether the snapshot job (Copy 2) is created from the NetBackup UI.

The backup of snapshot (Copy 2) is backed up in the VSP 5600 storage system as shown in the following image:



According to SLP Tasks, backup of snapshot (Copy 3) is completed successfully.

776	Backup From Snapshot	Done	0	SLP_SLP-Cloud	full	nbuora.ransomware.net	NBUMEDIA.r...	Oct 28, 2022
775	Backup From Snapshot	Done	0	SLP_SLP-Cloud	-	nbuora.ransomware.net	NBUMEDIA.r...	Oct 28, 2022

- Verify whether the snapshot job (Copy 3) is created from the NetBackup UI.

The backup of snapshot (Copy 3) is backed up on the MSDP-C pool as shown in the following image:

Job ID: 775 Job State: Done (Successful)

Job Overview Detailed Status Job Hierarchy

Attempt: Attempt Started: Oct 28, 2022 6:37:41 AM
 Attempt Elapsed: 00:14:03
 Attempt Ended: Oct 28, 2022 6:51:44 AM
 KB/Sec:

Storage Unit: **MSDPC-stu**
 Media Server: NBUMEDIA.ransomware.net
 Media Transport Type: LAN

Status:

```

Oct 28, 2022 6:37:41 AM - Info nbjrn (pid=2557) starting backup job (jobid=775) for client nbuora.ransomware.net, policy standard_nbuclient, schedule full
Oct 28, 2022 6:37:41 AM - Info nbjrn (pid=2557) requesting STANDARD_RESOURCE resources from RB for backup job (jobid=775, request id:{8CB7CEDC-56AC-11ED-9640-FF62F119ED6A})
Oct 28, 2022 6:37:41 AM - requesting resource MSDPC-stu
Oct 28, 2022 6:37:41 AM - requesting resource NBU.ransomware.net.NBU_CLIENT.MAXJOBS.nbuora.ransomware.net
Oct 28, 2022 6:37:41 AM - granted resource NBU.ransomware.net.NBU_CLIENT.MAXJOBS.nbuora.ransomware.net
Oct 28, 2022 6:37:41 AM - granted resource MediaID=@aaaaw;DiskVolume=veritas_vol;DiskPool=MSDPC-pool;Path=veritas_vol;StorageServer=NBUMEDIA.ransomware.net;MediaServer=NBUMEDIA
Oct 28, 2022 6:37:41 AM - granted resource MSDPC-stu
Oct 28, 2022 6:37:41 AM - estimated 0 kbytes needed
Oct 28, 2022 6:37:41 AM - begin Parent Job
Oct 28, 2022 6:37:41 AM - begin SnapDupe Mount:Read File List
Operation Status: 0
Oct 28, 2022 6:37:41 AM - end SnapDupe Mount:Read File List; elapsed time 0:00:00
Oct 28, 2022 6:37:41 AM - begin SnapDupe Mount:Import Snapshot
Oct 28, 2022 6:37:41 AM - Info RUNCMD (pid=8732) started
Oct 28, 2022 6:38:06 AM - Info RUNCMD (pid=8732) exiting
Operation Status: 0
Oct 28, 2022 6:38:06 AM - end SnapDupe Mount:Import Snapshot; elapsed time 0:00:25
Oct 28, 2022 6:38:06 AM - begin SnapDupe Mount:Deferred Resource
Operation Status: skipped
Oct 28, 2022 6:38:06 AM - end SnapDupe Mount:Deferred Resource; elapsed time 0:00:00
Oct 28, 2022 6:38:06 AM - begin SnapDupe Mount:Mount Snapshot
Oct 28, 2022 6:38:07 AM - Info nbjrn (pid=2557) snapshotid=nbuora.ransomware.net_1666950984
Oct 28, 2022 6:38:24 AM - started process bpbm (pid=28249)
Oct 28, 2022 6:38:33 AM - Info bpbm (pid=28249) The data-in-transit encryption (DTE) is disabled for the client (nbuora.ransomware.net) as the global DTE mode is set to 'Preferred Off' and the
Oct 28, 2022 6:39:00 AM - Info bpbm (pid=28249) nbuora.ransomware.net is the host to backup data from
Oct 28, 2022 6:39:00 AM - Info bpbm (pid=28249) reading file list for client
Oct 28, 2022 6:39:06 AM - Info bpbm (pid=28249) Starting mount_snapshot_processing
  
```

Current Kilobytes Written: 0
 Current Files Written: 1
 Current File: Estimated Files: 1

Troubleshooter...

6. Verify the backups from HCP for cloud scale.

Folders 10 and 11 are created in HCP for cloud scale after backup completion:

HITACHI | S3 Console

veritas-ransomware
 veritas-ransomware / veritas_vol / data /

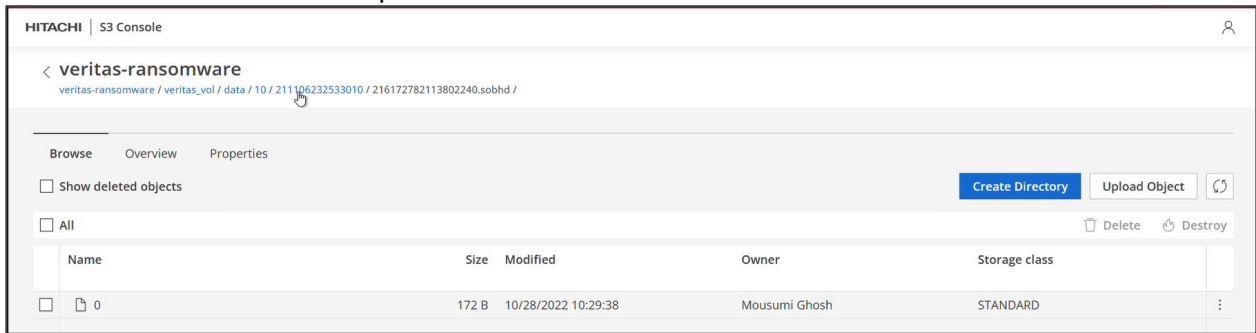
Browse Overview Properties

Show deleted objects Create Directory Upload Object ↻

All Delete Destroy

Name	Size	Modified	Owner	Storage class
<input type="checkbox"/> 10	--	--	--	STANDARD
<input type="checkbox"/> 11	--	--	--	STANDARD
<input type="checkbox"/> 2	--	--	--	STANDARD
<input type="checkbox"/> 6	--	--	--	STANDARD
<input type="checkbox"/> 7	--	--	--	STANDARD
<input type="checkbox"/> 8	--	--	--	STANDARD
<input type="checkbox"/> 9	--	--	--	STANDARD

Folder 10 contains the backup data:



Restoring a Snapshot Backup Job

Description before restoration

According to SLP-cloud configuration:

Storage Lifecycle Policy		Validation Report					
Storage lifecycle policy name: SLP-Cloud		Data classification: <No data class...	Priority for secondary operations: 0 (higher number is greater priority)				
Operation	Storage	Target Ma...	Window	Volume Pool	Media Ow...	Retention ...	Retentio
Snapshot	MSDP-media	--	--	--	--	Fixed	2 weeks
Backup From Snapshot	MSDP-media	--	Default...	--	--	Fixed	2 weeks
Backup From Snapshot	MSDPC-stu	--	Default...	--	--	Fixed	2 weeks

1381 Backup From Snapshot	Done	0 SLP_SLP-Cloud	MSDPC-stu	full	1006	520,128	nbuora.ransomware.net
1380 Backup From Snapshot	Done	0 SLP_SLP-Cloud	MSDPC-stu	-	-	-	nbuora.ransomware.net
1378 Backup From Snapshot	Done	0 SLP_SLP-Cloud	MSDP-media	full	1006	520,128	nbuora.ransomware.net
1377 Backup From Snapshot	Done	0 SLP_SLP-Cloud	MSDP-media	-	-	-	nbuora.ransomware.net
1376 Snapshot	Done	0 standard_nbuclient	MSDP-media	full	-	53,072	nbuora.ransomware.net

Copy 1 - Snapshot operation and snapshot image stored on a Hitachi VSP 5600 storage system having point in time restore feature.

Copy 2 - Backup of snapshot stored in MSDP-media that is created using a Hitachi VSP 5600 storage system. To reduce the time taken to complete, backup happens in multiple streams.

Copy 3 - Another backup of snapshot stored in MSDP-stu that is created using HCP for cloud scale (object storage). To reduce the time taken to complete, backup happens in multiple streams.

Preparation before Restore

1. Before restoring any files, validate whether the backup images are infected or not. Follow the procedure in the [Malware detection before recovery](#) section.
2. To verify whether the deleted file is restored or not, manually remove the file from the client machine that was backed up.

```
[root@nbuora linux_FS]# ls
file_text.txt
[root@nbuora linux_FS]# date
Sun Oct 30 20:14:25 PDT 2022
[root@nbuora linux_FS]# pwd
/linux_FS
[root@nbuora linux_FS]#
```

```
[root@nbuora linux_FS]# ls -lrt
total 4
-rw-r--r--. 1 root root 45 Oct 28 02:43 file_text.txt
[root@nbuora linux_FS]#
[root@nbuora linux_FS]# rm -rf file_text.txt
[root@nbuora linux_FS]# ls -lrt
total 0
[root@nbuora linux_FS]#
```

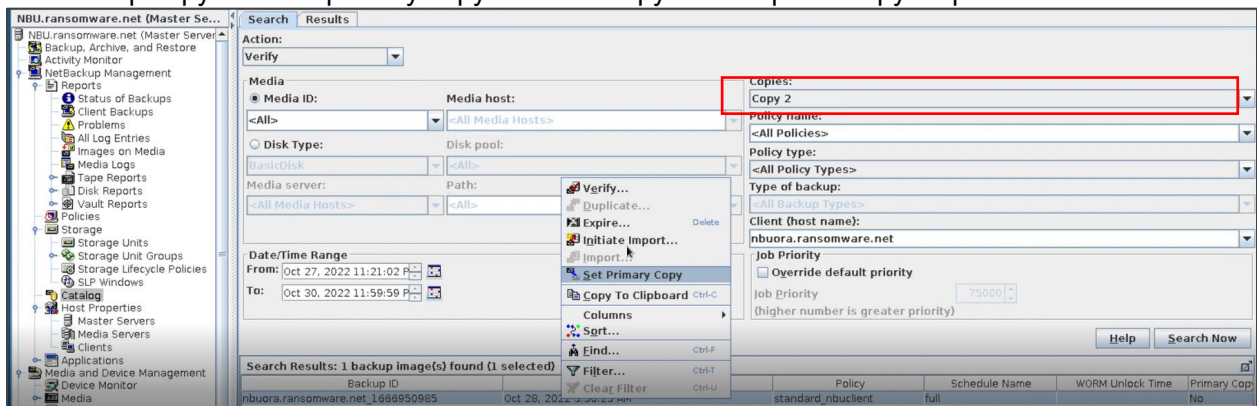
There is no file in client or destination server before restoring.

Restoring from a VSP 5600 storage system

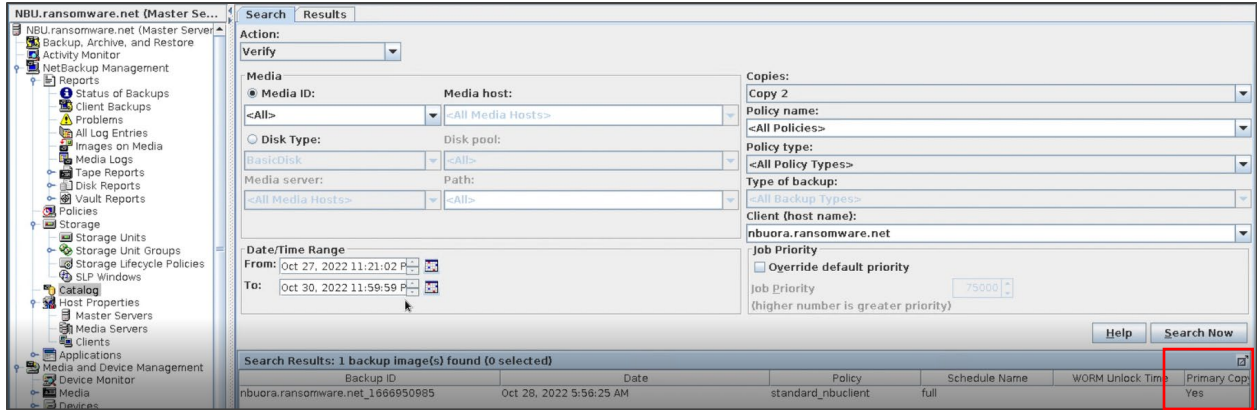
If you want a normal file-level restore, you must restore from the backup images stored in the VSP 5600 storage system. Ensure that the backup image is disinfected.

Complete the following steps:

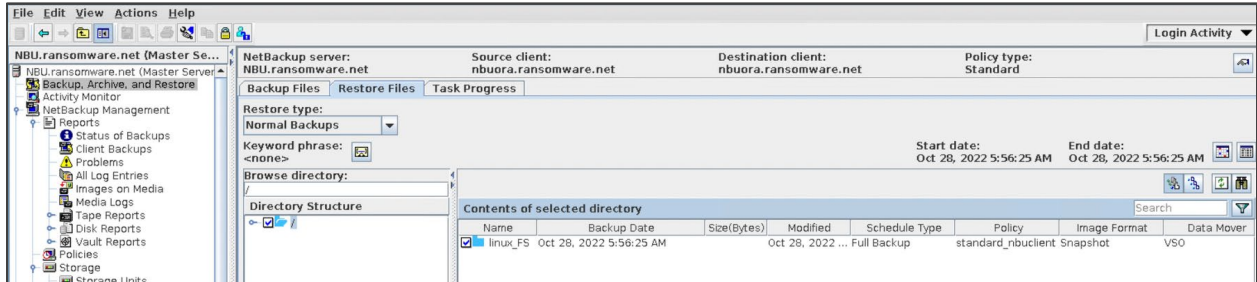
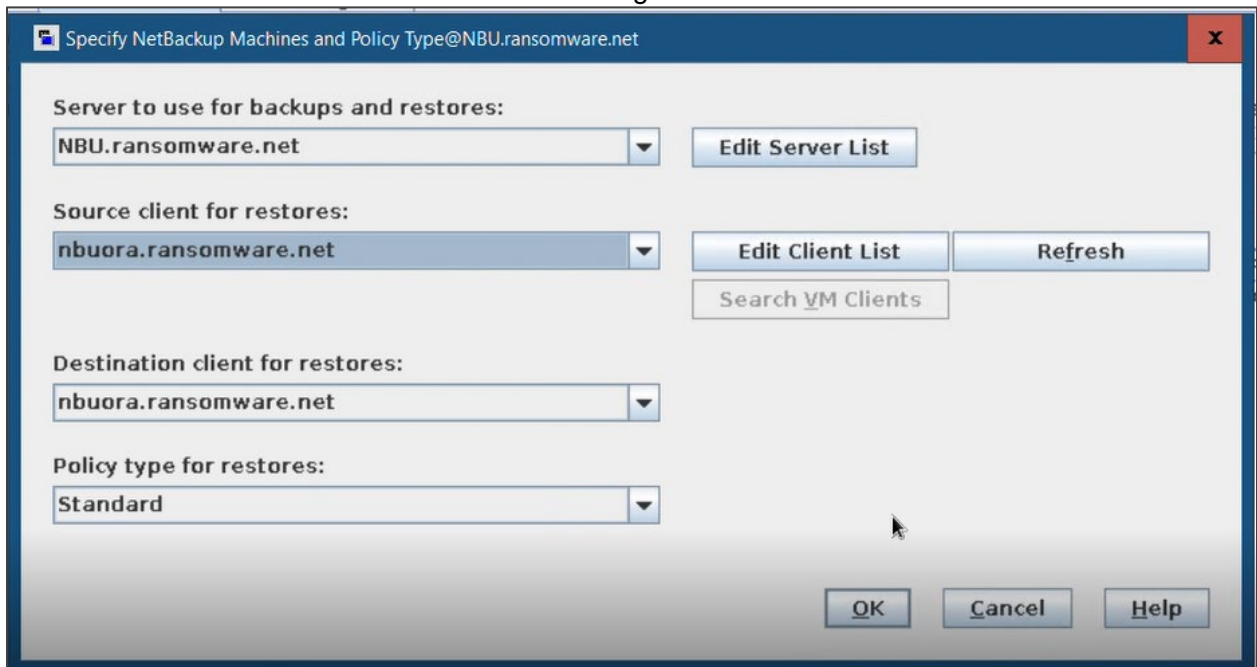
1. Set backup copy 2 as the primary copy because copy 2 is snapshot copy as per SLP.

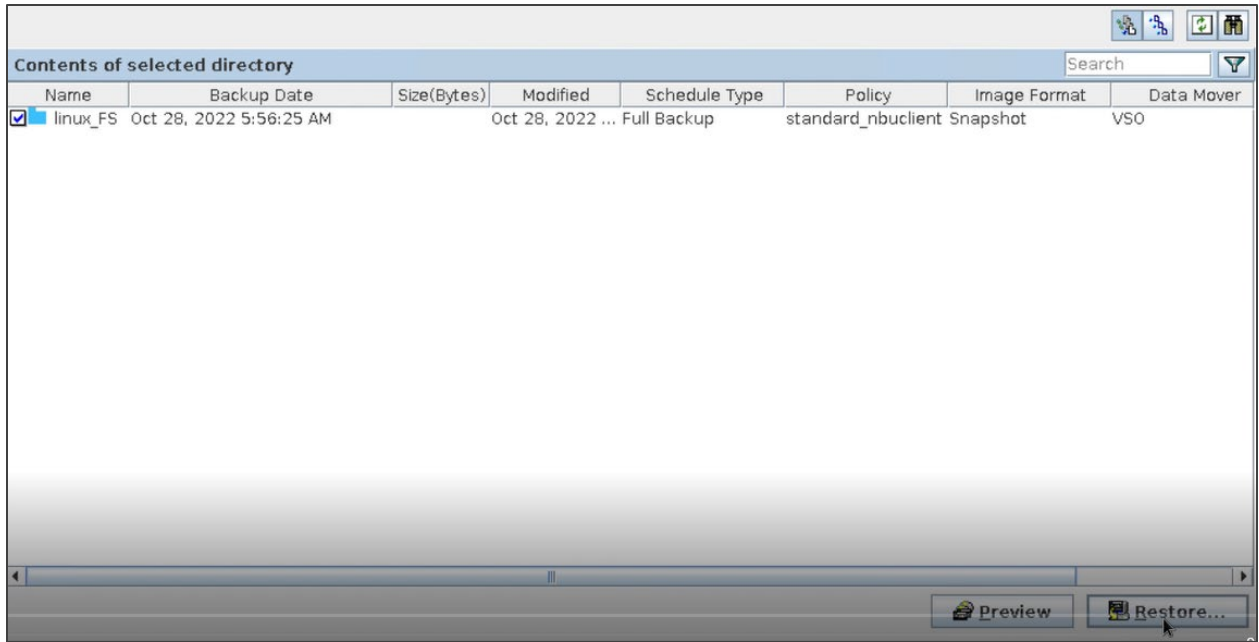


2. Set Primary Copy to Yes.

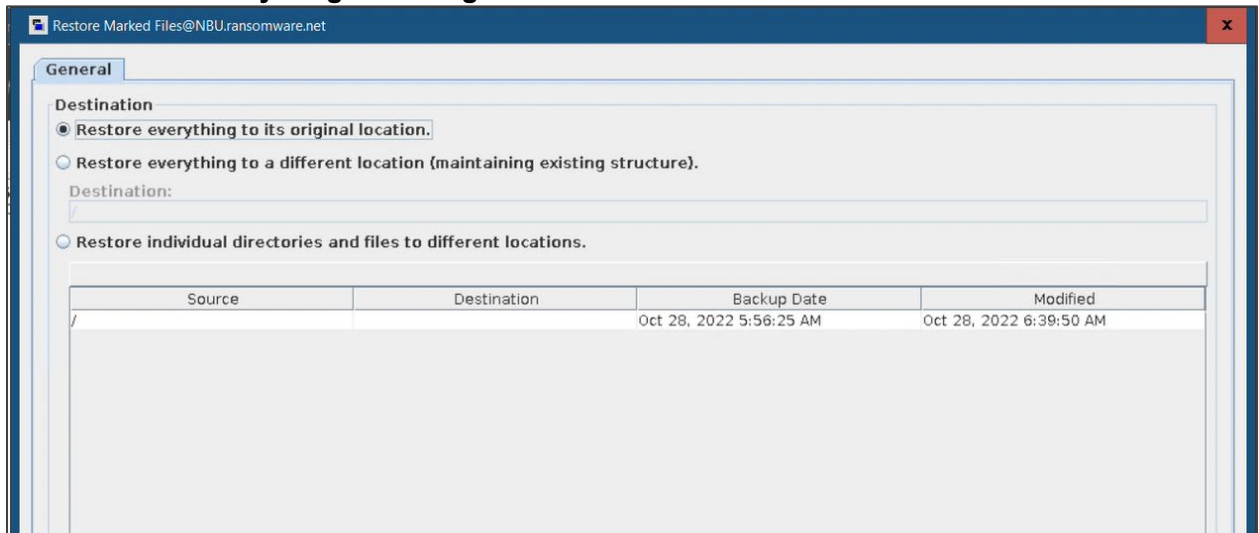


3. Select the source and destination client for restoring





4. Select **Restore everything to its original location.**



5. Verify that the restoration is happening from copy 2.

NetBackup server: NBU.ransomware.net Source client: nbuora.ransomware.net Destination client: nbuora.ransomware.net Policy type: Standard

Backup Files Restore Files **Task Progress**

Tasks Performed

Job id	Task	Date	Status
614	Restore	Oct 13, 2022 12:17:27 AM	Successful
615	Restore	Oct 13, 2022 12:24:52 AM	Successful
618	Restore	Oct 13, 2022 11:39:48 AM	Successful
782	Restore	Oct 30, 2022 11:24:32 PM	In Progress

Results of the Task Selected Above

Auto Refresh Rate (seconds): 10

Progress log filename : /usr/opensv/netbackup/logs/user_ops/root/logs/jbp-25440667186618712799000000014-CKqj6k.log Restore Job Id=782
Restore started 10/30/2022 23:23:38

```
23:25:07 (782.000) Found (2) files in (1) images for Restore Job ID 782.000
23:25:34 (782.000) Searched (2) files of (2) files for Restore Job ID 782.000
23:25:34 (782.001) Restoring from copy 2 of image created Fri 28 Oct 2022 05:56:25 AM EDT from policy standard_nbuclient
```

782 Restore Oct 30, 2022 11:24:32 PM Successful

Results of the Task Selected Above

Auto Refresh Rate (seconds): 10

Progress log filename : /usr/opensv/netbackup/logs/user_ops/root/logs/jbp-25440667186618712799000000014-CKqj6k.log Restore Job Id=782
Restore started 10/30/2022 23:23:38

```
23:28:03 (782.001) Ignoring RESTORE_FIFO_ABORT for restore operation
23:29:14 (782.001) /linux_FS/
23:29:14 (782.001) Directory /linux_FS/ exists. Keeping it.
23:29:14 (782.001) /linux_FS/file_text.txt
23:29:14 (782.001) INF - TAR EXITING WITH STATUS = 0
23:29:14 (782.001) INF - TAR RESTORED 1 OF 2 FILES SUCCESSFULLY
23:29:14 (782.001) INF - TAR KEPT 1 EXISTING FILES
23:29:14 (782.001) INF - TAR PARTIALLY RESTORED 0 FILES
23:29:14 (782.001) Status of restore from copy 2 of image created Fri 28 Oct 2022 05:56:25 AM EDT = the requested operation was successfully completed
```

After restoration, file_text.txt is restored on the destination server.

```
[root@nbuora linux_FS]# ls -lrt
total 0
[root@nbuora linux_FS]# ls -lrt
total 4
-rw-r--r--. 1 root root 45 Oct 28 02:43 file_text.txt
[root@nbuora linux_FS]# date
Sun Oct 30 20:29:42 PDT 2022
[root@nbuora linux_FS]#
```


Restoring from HCP for Cloud Scale

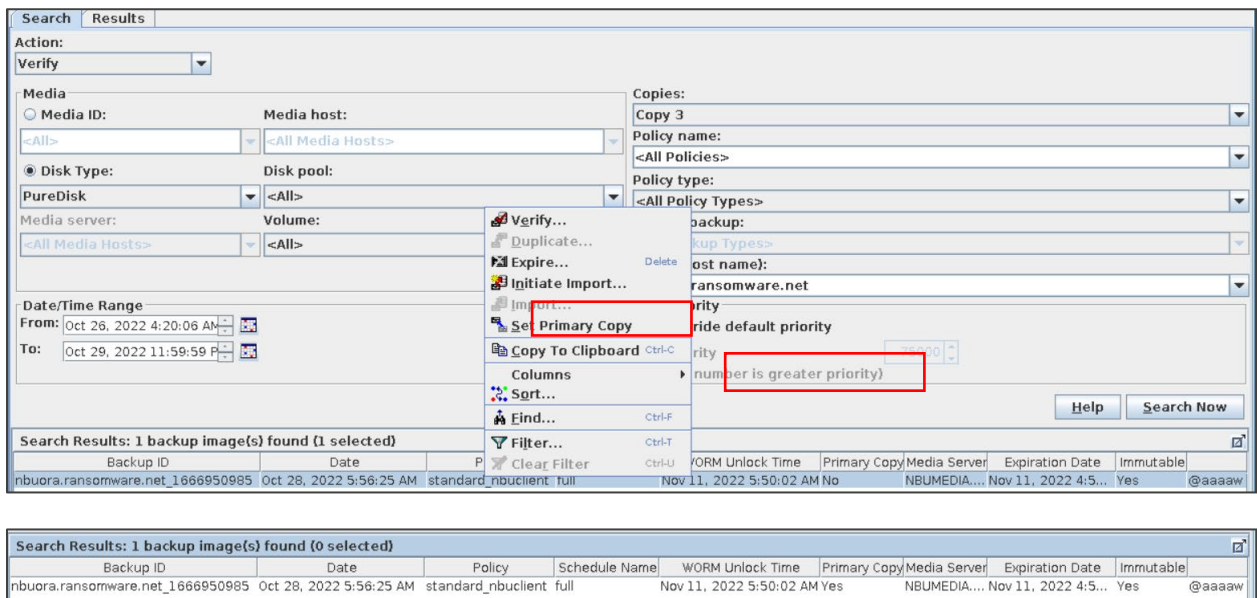
Even if a file is deleted or corrupted from the MSDP pool by cyber criminals, you can still restore it from the MSDP-C pool because of WORM feature. However, the file cannot be deleted from HCP for Cloud Scale if it is within the retention period.

To recover the destroyed file from the immutable bucket, complete the following steps:

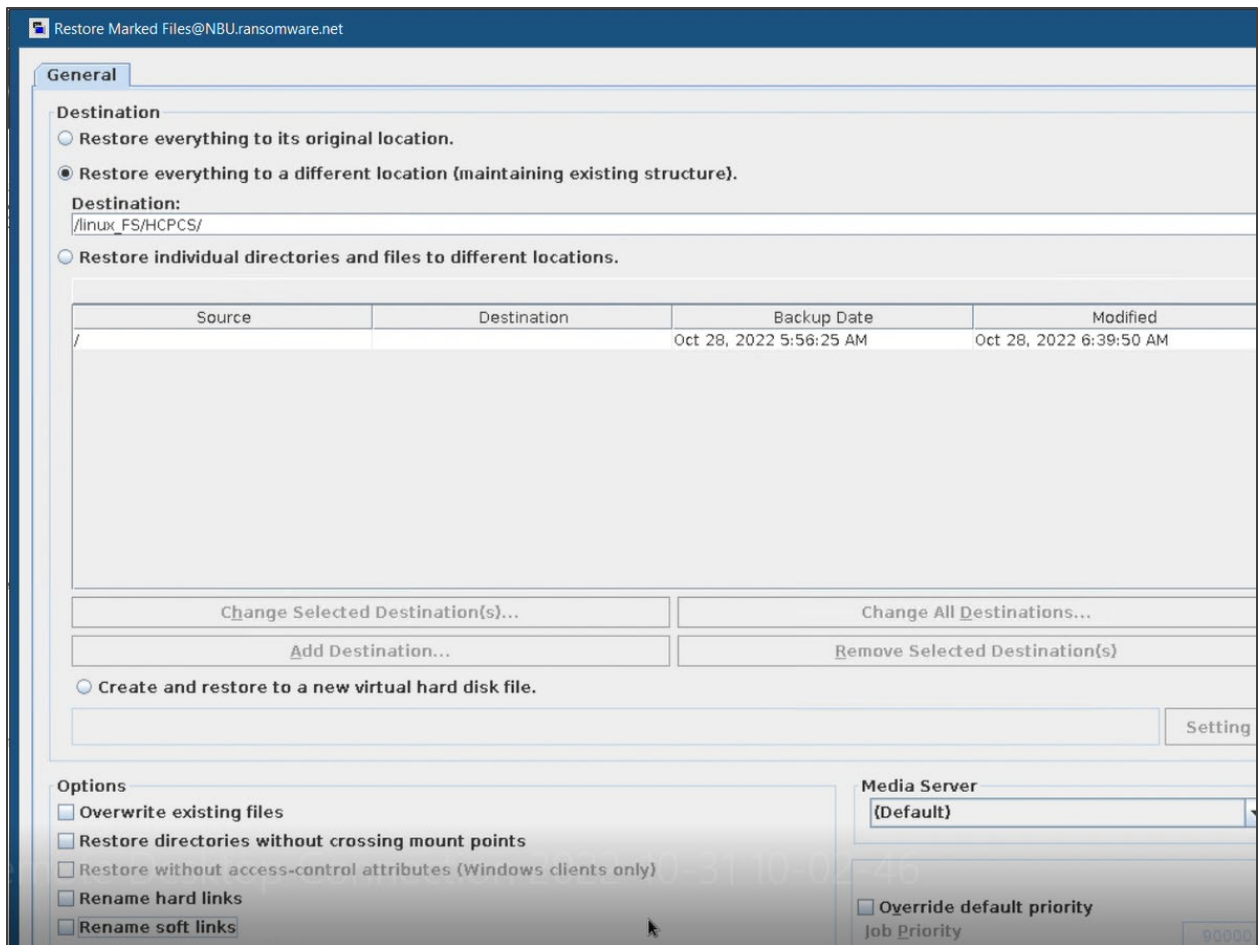
There is no file in the client or destination server before restoration.

```
[root@nbuora HCPCS]# ls -lrt
total 0
[root@nbuora HCPCS]# pwd
/linux_FS/HCPCS
[root@nbuora HCPCS]#
```

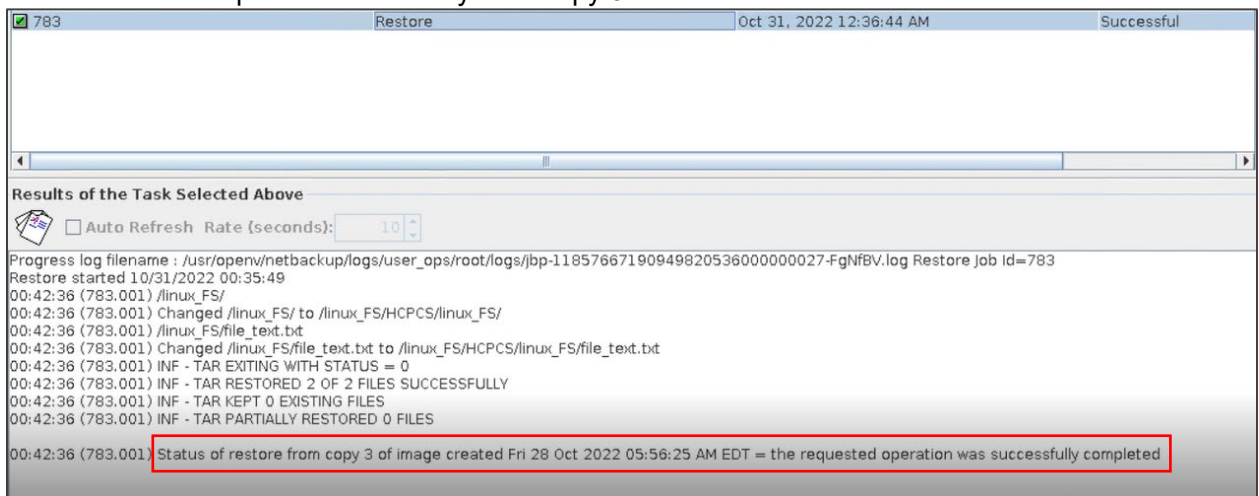
1. Set the copy 3 image as primary copy.



2. Select **Restore everything to a different location** and then select the destination location.



Restoration is completed successfully from copy 3.



After the file is restored, it is visible from the client or destination server end.

```

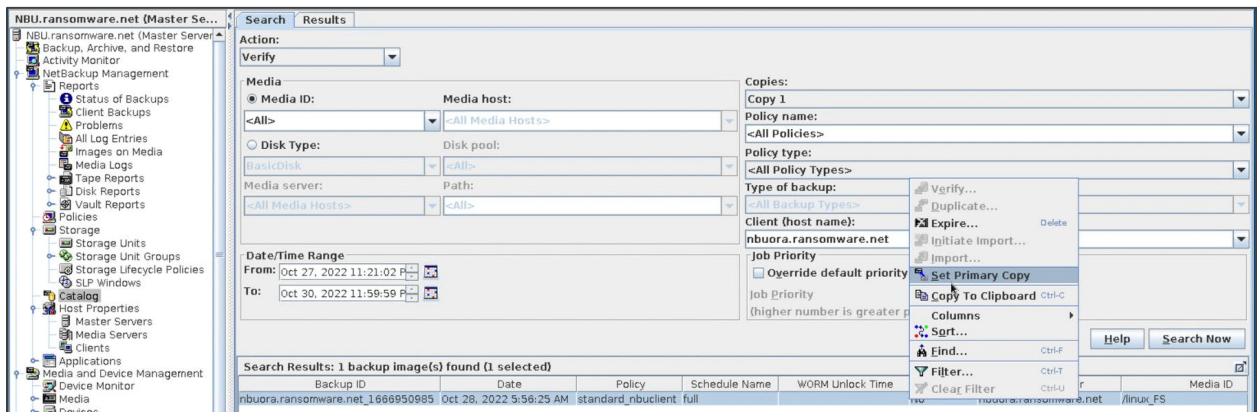
[root@nbuora HCPCS]# pwd
/linux_FS/HCPCS
[root@nbuora HCPCS]# ls -lrt
total 0
drwxr-xr-x. 2 root root 27 Oct 28 02:43 linux_FS
[root@nbuora HCPCS]# cd linux_FS
[root@nbuora linux_FS]# ls
file_text.txt
[root@nbuora linux_FS]# pwd
/linux_FS/HCPCS/linux_FS
[root@nbuora linux_FS]#

```

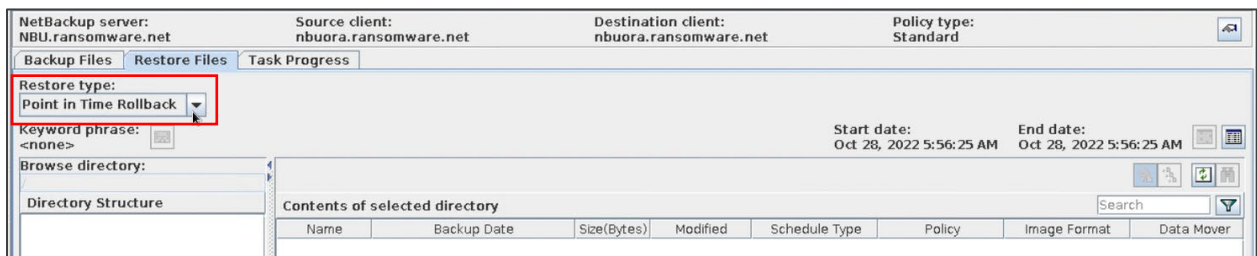
Point in time restore

To perform a point-in-time restore, complete the following steps:

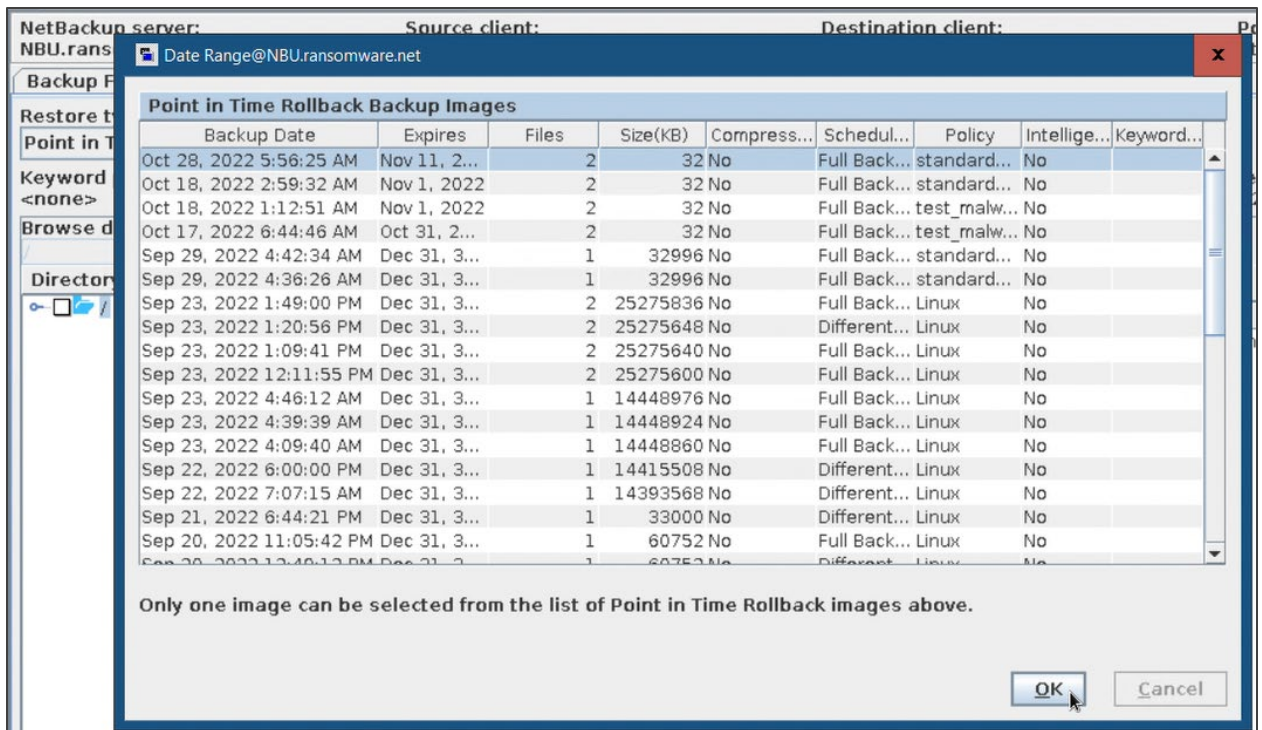
1. Set the copy 1 image as the primary copy. According to SLP, copy 1 is snapshot copy.



2. Select the policy type as **Point in Time Rollback**.



All eligible snapshots are included in the list:



3. Select the correct image.
4. Click **OK**.
5. Select **Skip verification and force rollback**.
6. Select **Force rollback even if it destroys later snapshots**.

General

Destination

Restore everything to its original location.

Restore everything to a different location (maintaining existing structure).

Destination:
/linux_FS/

Restore individual directories and files to different locations.

Source	Destination	Backup Date	Modified
/linux_FS/		Oct 28, 2022 5:56:25 AM	Oct 28, 2022 5:43:59 AM

Change Selected Destination(s)... Change All Destinations...

Add Destination... Remove Selected Destination(s)

Create and restore to a new virtual hard disk file.

Setting

Options

Skip verification and force rollback

Restore directories without crossing mount points

Restore without access-control attributes (Windows clients only)

Rename hard links

Rename soft links

Force rollback even if it destroys later snapshots

Force rollback even if it destroys the consistency group's state on the storage array

Media Server

(Default)

Override default priority

Job Priority: 90000
(higher number is greater priority)

7. Verify that the restoration is happening from copy 1.

784 Restore Oct 31, 2022 1:37:50 AM Successful

Results of the Task Selected Above

Auto Refresh Rate (seconds): 10

Progress log filename : /usr/openw/netbackup/logs/user_ops/root/logs/jbp-1185766719460938816400000120-CHx6uu.log Restore Job id=784

Restore started 10/31/2022 01:36:49

01:42:18 (784.xxx) Found (2) files in (1) images for Restore Job ID 784.xxx

01:42:27 (784.xxx) Searched (2) files of (2) files for Restore Job ID 784.xxx

01:42:27 (784.00) Restoring from copy 1 of image created Fri 28 Oct 2022 05:56:25 AM EDT from policy standard_nbuclient

01:43:25 (784.001) INF - Selected Path /linux_FS, Copy 1, Fragment 1

01:43:25 (784.001) INF - Connect to hostname=NBU.ransomware.net, port=0, IPC="/usr/openw/var/tmp/net-2347666719494758282700000004-qPvP7K".

01:43:25 (784.001) INF - Data socket to NBU.ransomware.net is connected, fd 4

01:43:25 (784.001) INF - BPPFI EXITING WITH STATUS = 0

01:46:40 (784.001) INF - ROLLED BACK /linux_FS SUCCESSFULLY

01:46:58 (784.001) Status of restore from copy 1 of image created Fri 28 Oct 2022 05:56:25 AM EDT = the requested operation was successfully completed

After restoration, the server is recovered by the snapshot.

```
[root@nbuora ~]# cd /linux_FS/
[root@nbuora linux_FS]# ls
file_text.txt
[root@nbuora linux_FS]# ls -lrt
total 4
-rw-r--r--. 1 root root 45 Oct 28 02:43 file_text.txt
[root@nbuora linux_FS]# date
Sun Oct 30 22:48:25 PDT 2022
[root@nbuora linux_FS]# █
```


NetBackup and Hitachi Cyber Security Capabilities

This section describes cyber security in every stage of the solution and how every engine follows the five pillars (Identify, Protect, Detect, Respond, and Recover) of NIST cyber security framework.

Testing consists of the following high-level steps:

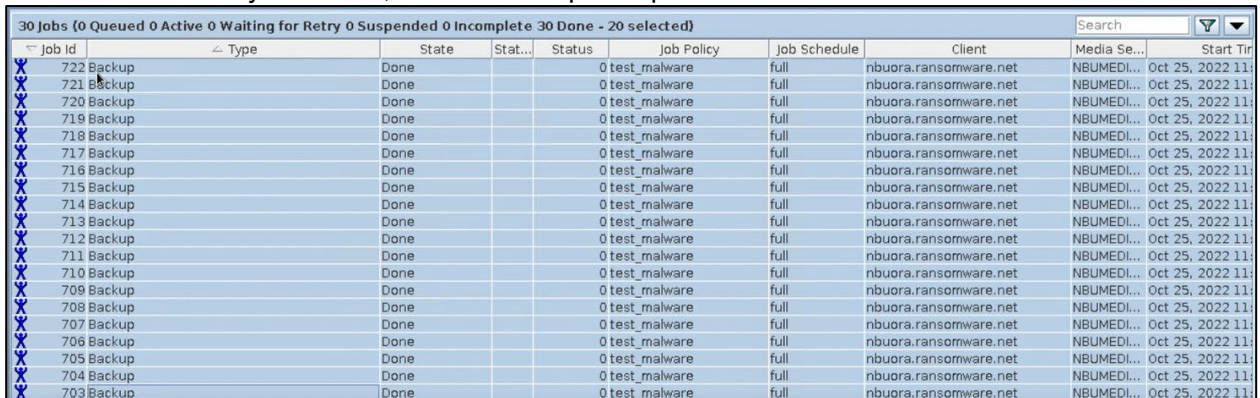
- Verifying Anomaly Detection during Backup
- Verifying Malware detection after Backup and before Restore Manually
- Data Protection Within Retention Period

Verifying Anomaly Detection during Backup

The Veritas NetBackup Anomaly Detection Engine helps to identify any unusual patterns during backup. For instance, Anomaly Detection starts if you schedule backups of one folder or directory every day or a particular folder or directory gets affected by size or file count or some unexpected changes are happening in NetBackup.

Complete the following steps:

1. To train the Anomaly detection, run the backup multiple times.



Job Id	Type	State	Stat...	Status	Job Policy	Job Schedule	Client	Media Se...	Start Tir
722	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
721	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
720	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
718	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
718	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
717	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
716	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
715	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
714	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
713	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
712	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
711	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
710	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
708	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
708	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
707	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
706	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
705	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
704	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:
703	Backup	Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI...	Oct 25, 2022 11:

2. To make changes and take multiple backups again, increase the file size and file counts.
3. Wait for 15 minutes to gather the data.

Anomaly detection matches the new data with the previous data for the same location. Based on the differences, it shows an alert.

Anomaly detection Anomaly detection settings

Search...

<input type="checkbox"/>	Job ID	Client name	Policy type	Count	Score	Anomaly	Anomaly su	Receiver ↓	Review s	Policy name	Schedule	Schedule
> <input type="checkbox"/>	731	nbuora.ran...	Standard	1	4.7	Low	Backup fil...	Oct 26, 2022	Not review...	test_malw...	full	FULL
> <input type="checkbox"/>	733	nbuora.ran...	Standard	1	4.7	Low	Backup fil...	Oct 26, 2022	Not review...	test_malw...	full	FULL
> <input type="checkbox"/>	732	nbuora.ran...	Standard	1	4.7	Low	Backup fil...	Oct 26, 2022	Not review...	test_malw...	full	FULL
> <input type="checkbox"/>	734	nbuora.ran...	Standard	1	4.7	Low	Backup fil...	Oct 26, 2022	Not review...	test_malw...	full	FULL
> <input type="checkbox"/>	736	nbuora.ran...	Standard	1	4.7	Low	Backup fil...	Oct 26, 2022	Not review...	test_malw...	full	FULL
> <input type="checkbox"/>	735	nbuora.ran...	Standard	1	4.7	Low	Backup fil...	Oct 26, 2022	Not review...	test_malw...	full	FULL
> <input type="checkbox"/>	737	nbuora.ran...	Standard	1	4.7	Low	Backup fil...	Oct 26, 2022	Not review...	test_malw...	full	FULL

The following image shows the job details and provides the Anomaly severity:

Anomaly detection Anomaly detection settings

Search...

<input type="checkbox"/>	Job ID	Client name	Policy type	Count	Score	Anomaly	Anomaly su	Receiver ↓	Review s	Policy name	Schedule	Schedule
▼ <input type="checkbox"/>	762	nbuora.ran...	Standard	4	11.36	Medium	Anomaly l...	Oct 26, 2022	Not review...	test_malw...	full	FULL

Anomaly detected on job 762

Job ID 762	Client name nbuora.ransomware.net	Policy name test_malware	Policy type Standard
Schedule name full	Schedule type FULL	Review status Not reviewed	Backup ID nbuora.ransomware.net_1666762 275
Anomaly ID 762_1666762275	Anomaly severity Medium		

Anomaly details

Mark as ignore
Confirm as anomaly
Report as false positive

Anomaly: Backup files count 80002 (Usual: 1 - 2)	Anomaly: Data transferred 195.344 MB (Usual: 0.031 MB - 0.031 MB)	Anomaly: Image size 195.344 MB (Usual: 0.031 MB - 0.031 MB)	Anomaly: Total time 1177 Seconds (Usual: 70 Seconds - 1144 Seconds)
---	--	--	--

4. To respond to a particular alert, select from the following options:

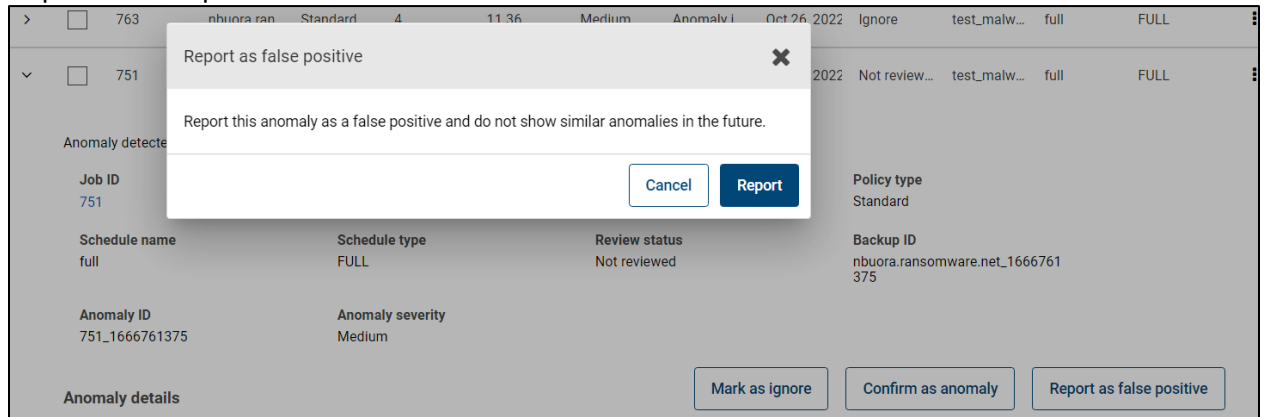
- Mark as ignore:

> <input type="checkbox"/>	763	nbuora.ran...	Standard	4	11.36	Medium	Anomaly l...	Oct 26, 2022	Ignore	test_malw...	full	FULL
----------------------------	-----	---------------	----------	---	-------	--------	--------------	--------------	--------	--------------	------	------

- Confirm as anomaly:

<input type="checkbox"/>	Job ID	Client name	Policy type	Count	Score	Anomaly	Anomaly su	Receiver ↓	Review status	Policy name	Schedule	Schedule
> <input type="checkbox"/>	762	nbuora.ran...	Standard	4	11.36	Medium	Anomaly l...	Oct 26, 2022	Anomaly	test_malw...	full	FULL

- Report as false positive:



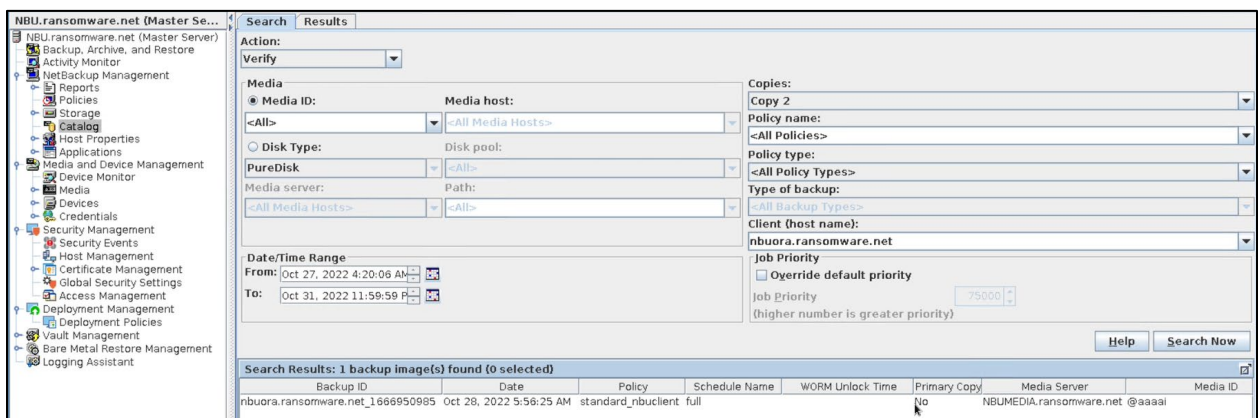
Note: Anomaly Detection is working for backups and not for snapshots.

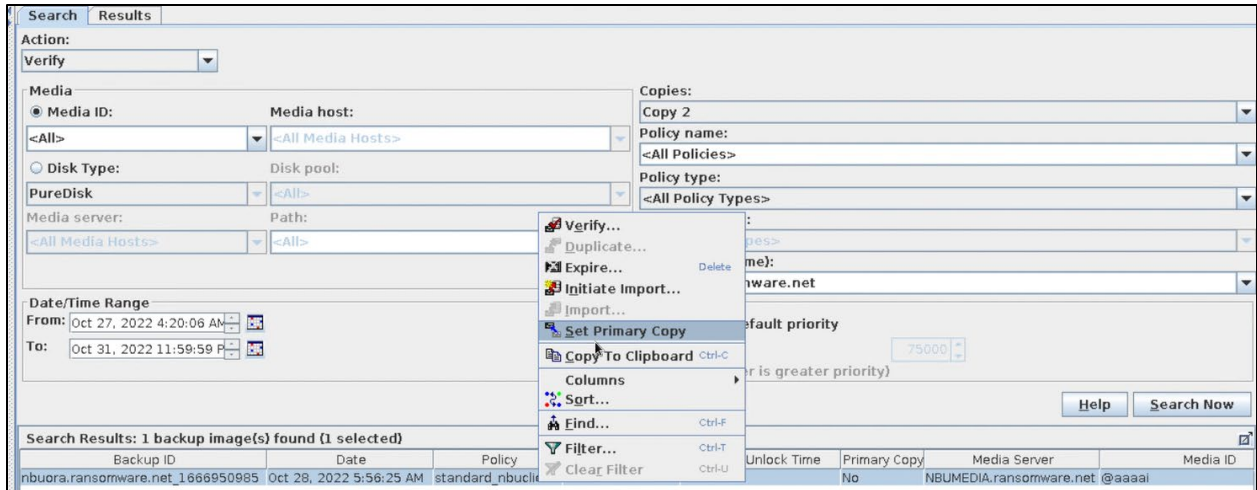
Verifying Malware detection after Backup and before Restore Manually

NetBackup Malware scanner detects virus-infected files after Backup and before recovery. You can schedule a particular time after the scheduled backup completion or scan manually at any point of time for all backup images or any images before recovery.

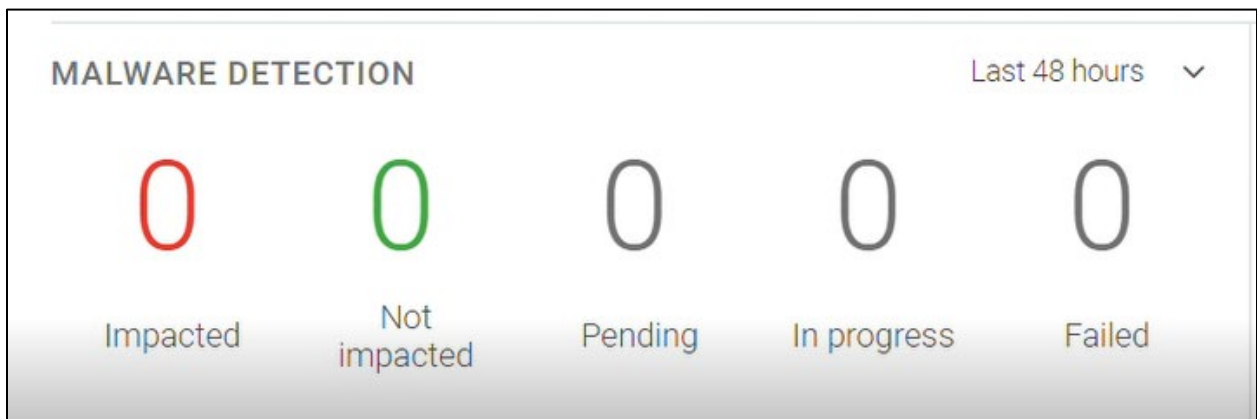
NetBackup Malware Scanner Test with Non-affected files

1. Set the backup image as the primary copy to scan.
2. Set copy 2 as the primary copy.

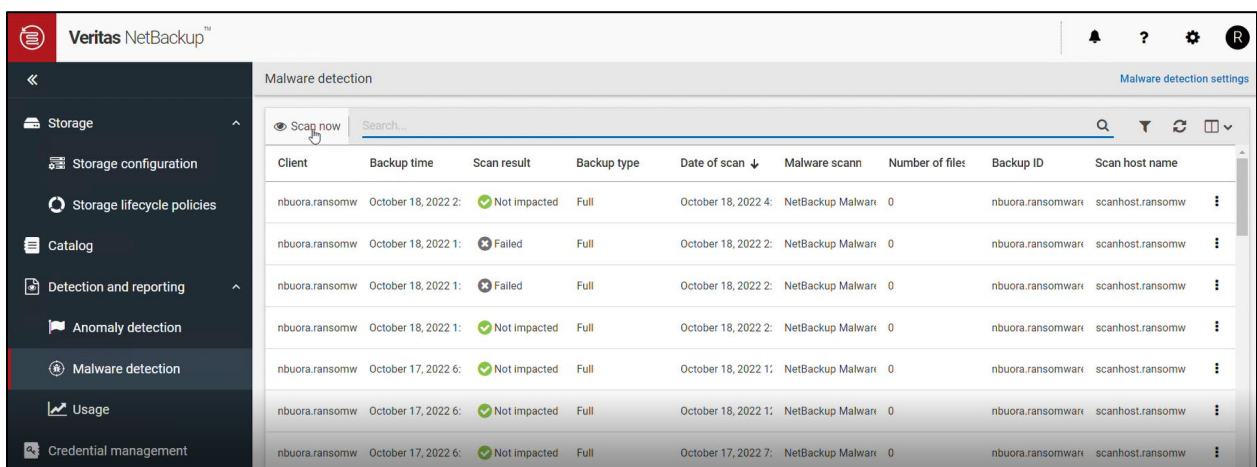




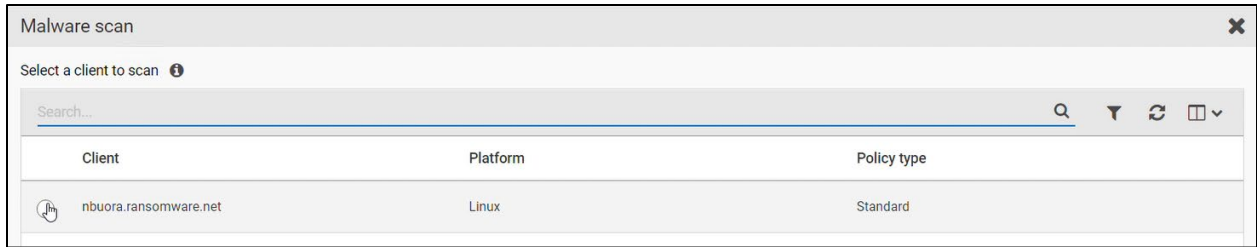
No malware is detected.



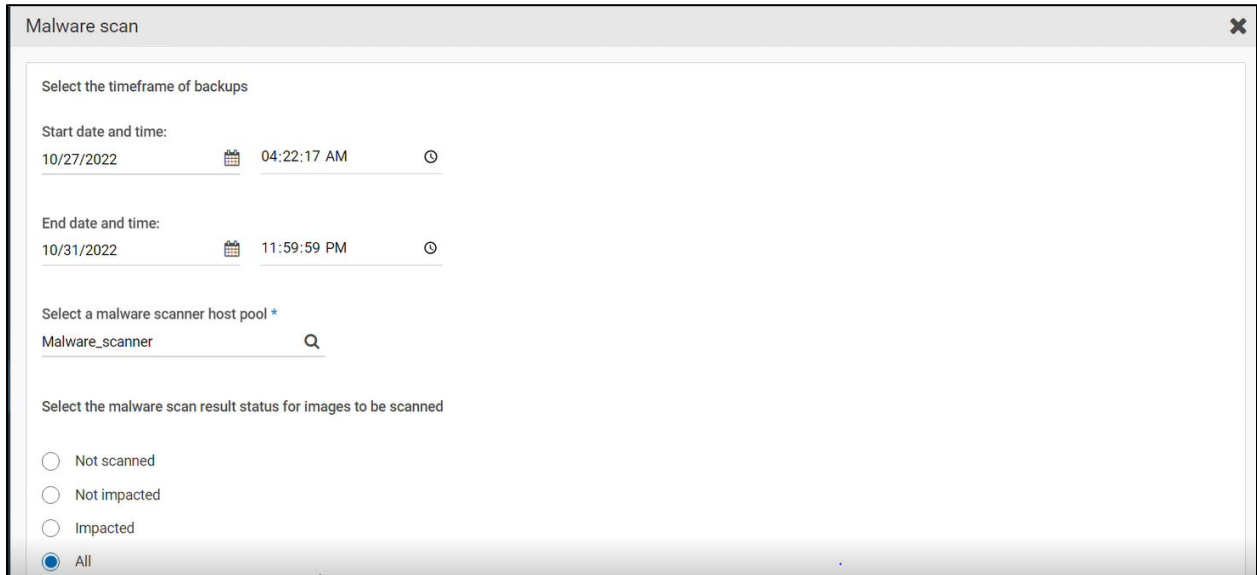
3. Click **Scan now**.



4. Select the client name for scanning the backup images.



5. Select the backup timeframe, Malware scanner host pool, and malware scan result status.



Scan task starts.

Client	Backup time	Scan result	Backup type	Date of scan ↓	Malware scanner	Number of files	Backup ID	Scan host name
nbuora.ransomw	October 28, 2022 5:	Pending	Full	October 31, 2022 4:	NetBackup Malware	0	nbuora.ransomware	scanhost.ransomw

6. Verify the backup ID and backup time for the selected backup image.

Client	Backup time	Scan result	Backup	Date of scan ↓	Malware scanner	Number of	Backup ID	Scan host
nbuora.ransomware	October 28, 2022	In progress	Full	October 31, 2022 4:	NetBackup Malware Sc	0	nbuora.ransomware.net_1666950985	scanhost.ra

The **Create-Mount** operation is taking place.

Job Details: 785@NBU.ransomware.net

Job ID: 785 Job State: Active

Job Overview Detailed Status Job Hierarchy

Job Type: Instant Access File List:

Backup Type: Create-Mount

Client: SPWS_MOUNT_ID=55_1666950985
SPWS_JOB_ID=55_1666950985

Master Server: NBU.ransomware.net

Job Policy:

Policy Type: Standard

Job Schedule:

Schedule Type:

Priority:

Owner:

Group:

Compression:

Off-Host:

Start Time: Oct 31, 2022 4:25:46 AM

Elapsed Time: 00:04:37

End Time:

Retention:

Status:

Job ID: 785 Job State: Active

Job Overview Detailed Status Job Hierarchy

Attempt: 1 Attempt Started: Oct 31, 2022 4:25:46 AM

Job PID: Attempt Elapsed: 00:04:37

Storage Unit: Attempt Ended:

Media Server: NBUMEDIA.ransomware.net KB/Sec:

Media Transport Type: LAN

Status:

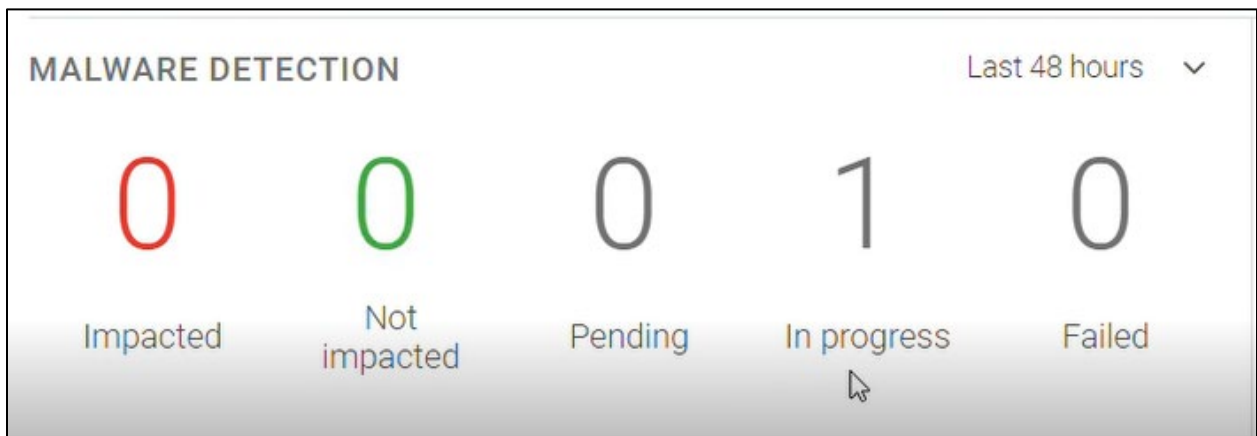
Oct 31, 2022 4:25:46 AM - Info NBWMC (pid=1401) Creating instant access mount from Standard image nbuora.ransomware.net_1666950985 and copy number 2.

Oct 31, 2022 4:25:46 AM - Info NBWMC (pid=1401) Storage server NBUMEDIA.ransomware.net.

Oct 31, 2022 4:25:46 AM - Info NBWMC (pid=1401) The SPWS ID 55_1666950985.

Oct 31, 2022 4:25:46 AM - Info NBWMC (pid=1401) The NetBackup resource ID 6d7e4c75-ef05-4896-9d83-e6caf567ff7d.

Oct 31, 2022 4:25:46 AM - Info NBWMC (pid=1401) Mount clients scanhost.ransomware.local.



Instant Access completed.

Job ID: 785 Job State: Done (Successful)

Job Overview Detailed Status Job Hierarchy

Job Type: Instant Access Backup Type: Create-Mount File List:

Client: SPWS_MOUNT_ID=55_1666950985
SPWS_JOB_ID=55_1666950985

Master Server: NBU.ransomware.net

Job Policy: Policy Type: Standard Job Schedule: Schedule Type: Priority: Owner: Group: Compression: Off-Host:

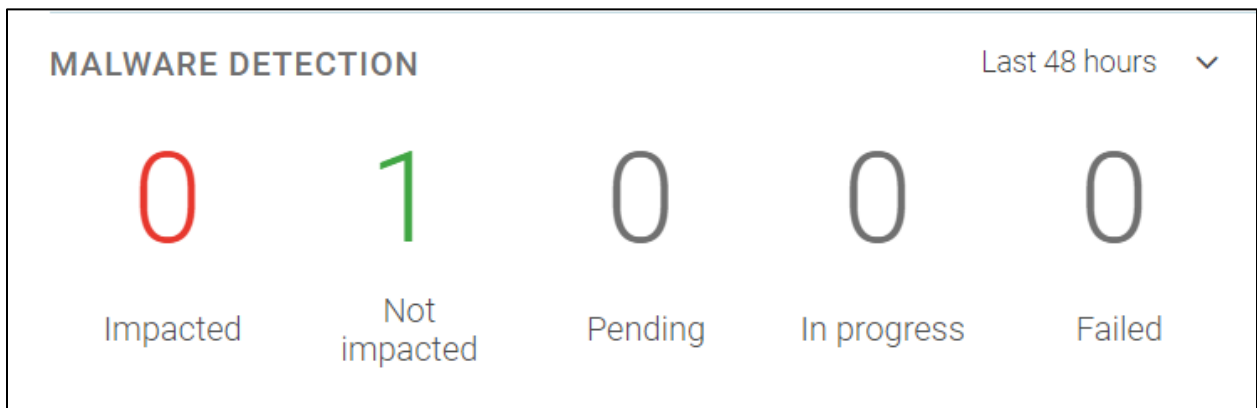
Start Time: Oct 31, 2022 4:25:46 AM Elapsed Time: 00:21:46 End Time: Oct 31, 2022 4:47:32 AM Retention:

Status:
1: (0) The requested operation was successfully completed.

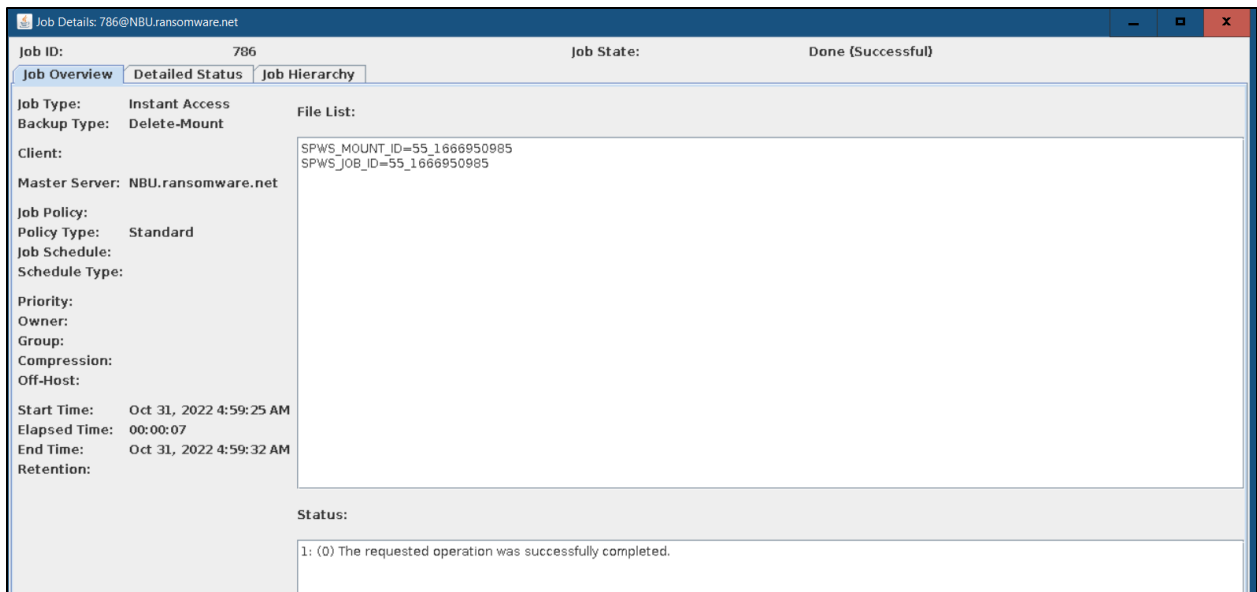
Scan results:

After scanning, the scan result is not impacted.

Client	Backup time	Scan result	Backup	Date of scan ↓	Malware scann	Number of files	Backup ID	Scan host
nbuora.ransomw	October 28, 2022 5:	✔ Not impacted	Full	October 31, 2022 4:	NetBackup Malwar	0	nbuora.ransomware.net_1666950985	scanhost.r



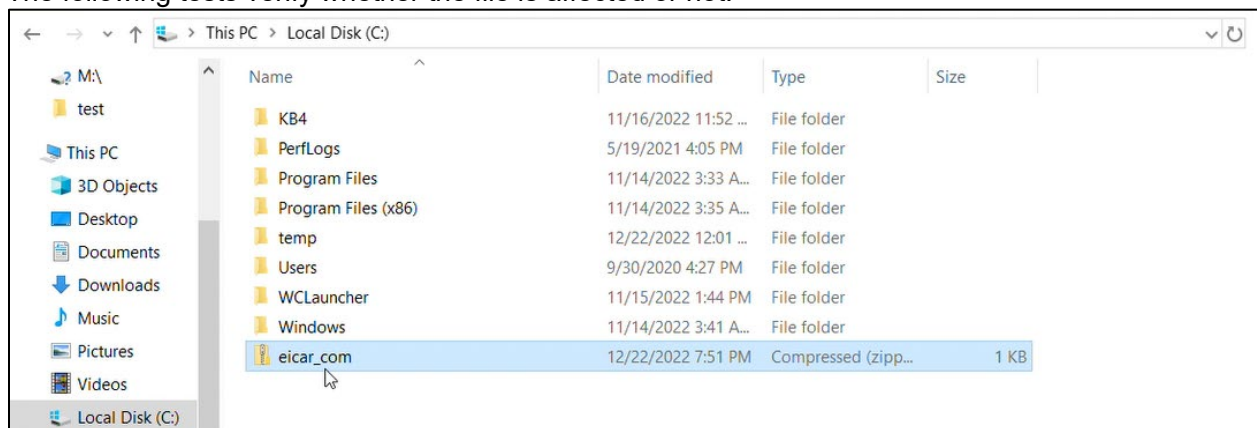
The delete-mount task was started after scanning and completed successfully.



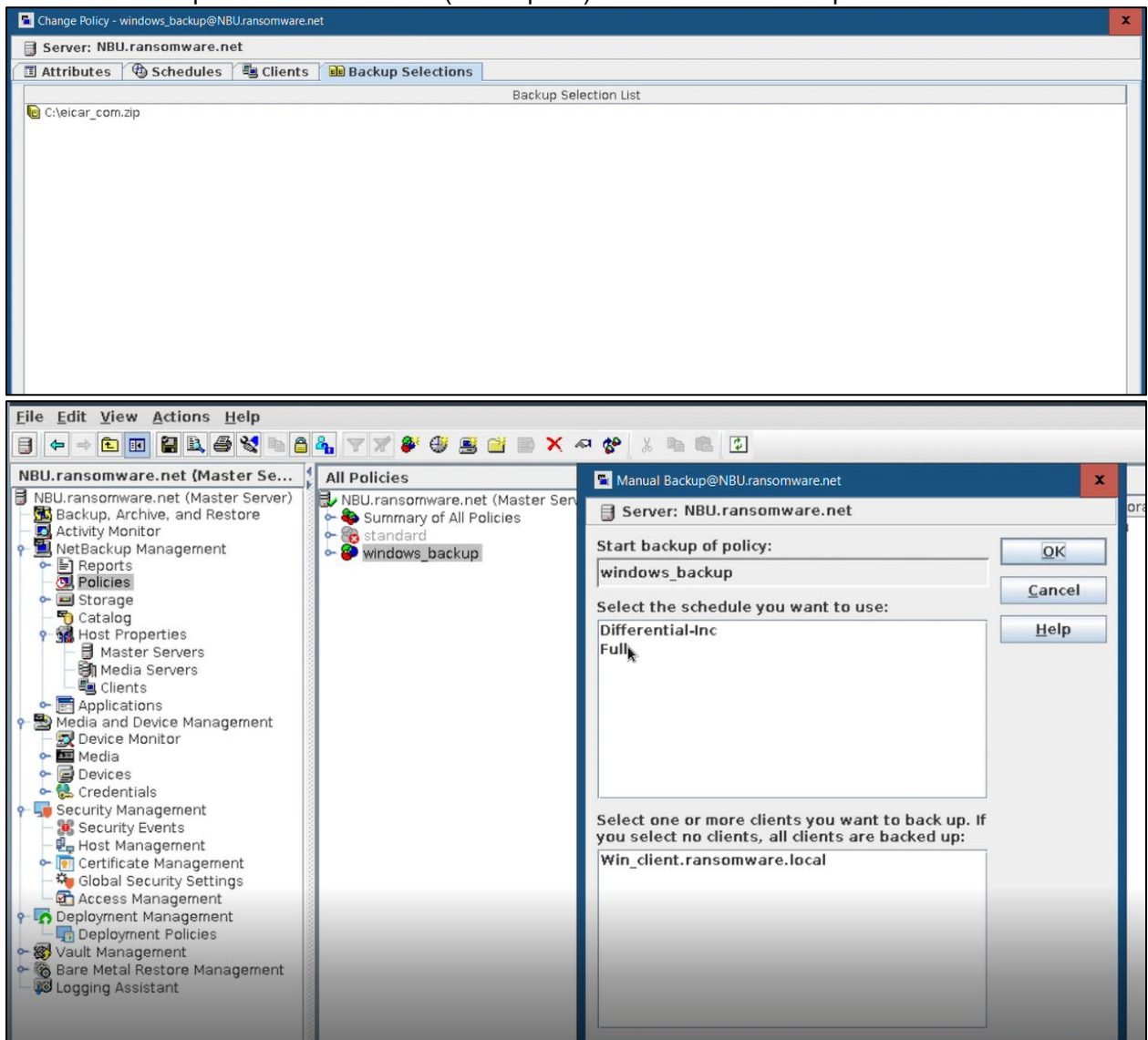
NetBackup Malware Scanner Test with Virus affected files

We used the following virus affected files in this test case:

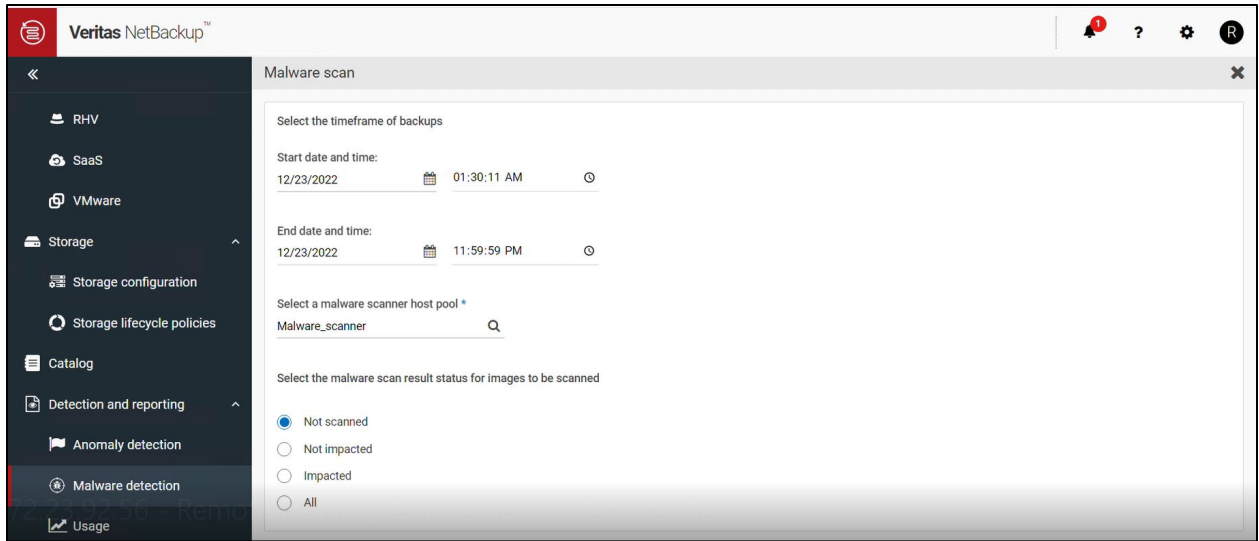
The following tests verify whether the file is affected or not.



1. Select the backup for the affected files (assumption) and take a full backup.



2. Perform malware scanning of the backup image.



Malware detection Malware detection settings

Scan now | Search...

Client	Backup time	Scan result	Backup type	Date of scan ↓	Malware scanner	Number of files	Backup ID	Scan host
Win_client.ransom	December 23, 2022 1:40 AM	⏸ Pending	Full	December 23, 2022	NetBackup Malware	0	Win_client.ransomv	scanhost

Scanning is in progress.

Malware detection Malware detection settings

Scan now | Search...

Client	Backup time	Scan result	Backup	Date of scan ↓	Malware scanner	Number of files	Backup ID	Scan host
Win_client.ransomware.	December 23, 2022 1:40 AM	⏸ In progress	Full	December 23, 2022	NetBackup Malware Scanner	0	Win_client.rar	scanho
Win_client.ransomware.	December 22, 2022 10:58 PM	! Impacted	Full	December 22, 2022	NetBackup Malware Scanner	1	Win_client.rar	scanho

After the task is completed, the scan result shows “impacted” for both backup images.

Malware detection Malware detection settings

Scan now | Search...

Client	Backup time	Scan result	Backup	Date of scan ↓	Malware scanner	Number of files	Backup ID	Scan host
Win_client.ransomware.	December 23, 2022 1:40 AM	! Impacted	Full	December 23, 2022	NetBackup Malware Scanner	1	Win_client.rar	scanho
Win_client.ransomware.	December 22, 2022 10:58 PM	! Impacted	Full	December 22, 2022	NetBackup Malware Scanner	1	Win_client.rar	scanho

3. To check the infected files, click **View infected files**.

Malware detection Malware detection settings

Scan now | Search...

Client	Backup time	Scan result	Backup	Date of scan ↓	Malware scanner	Number of files	Backup ID	Scan hos
Win_client.ransomware.	December 23, 2022 1:40 AM	Impacted	Full	December 23, 202	NetBackup Malware Scanner	1	Win_client.r	scanhost. ⋮
Win_client.ransomware.	December 22, 2022 10:58 PM	Impacted	Full	December 22, 202	NetBackup Malware Scanner	1	Win_cl	Expire all copies
Win_client.ransomware.	December 22, 2022 10:56 PM	Not impacted	Full	December 22, 202	NetBackup Malware Scanner	0	Win_cl	View infected files

It shows the virus affected files that have been manually created for the test.

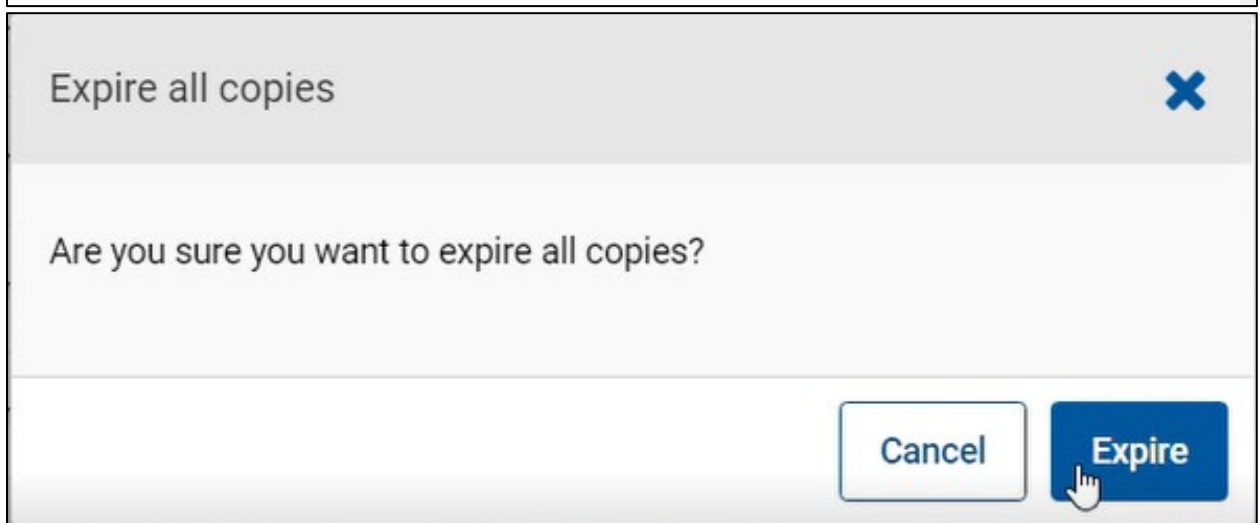


You must expire the backup image copies manually when the scan result is impacted.

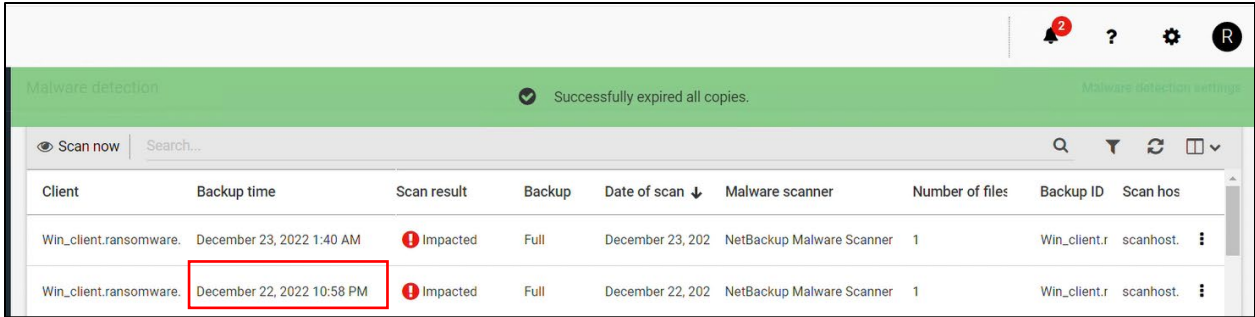
- To expire the backup image copies manually, click **Expire all copies**.

Scan now | Search...

Client	Backup time	Scan result	Backup	Date of scan ↓	Malware scanner	Number of files	Backup ID	Scan hos
Win_client.ransomware.	December 23, 2022 1:40 AM	Impacted	Full	December 23, 202	NetBackup Malware Scanner	1	Win_client.r	scanhost. ⋮
Win_client.ransomware.	December 22, 2022 10:58 PM	Impacted	Full	December 22, 202	NetBackup Malware Scanner	1	Win_client.r	scanhost. ⋮
Win_client.ransomware.	December 22, 2022 10:56 PM	Not impacted	Full	December 22, 202	NetBackup Malware Scanner	0	Win_cl	Expire all copies
Win_client.ransomware.	December 12, 2022 6:00 PM	Not impacted	Differential	December 12, 202	NetBackup Malware Scanner	0	Win_cl	View infected files

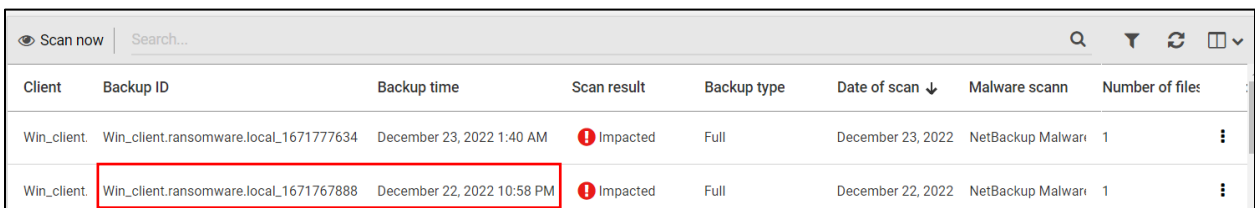


Backup image is successfully expired.

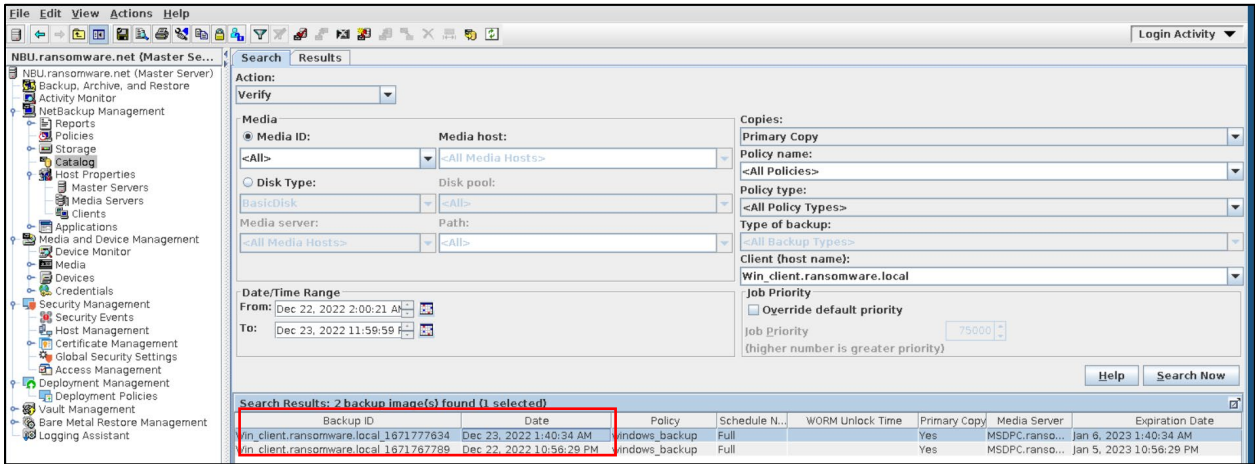


After expiring the impacted files, they are removed from the catalog as well.

The following image shows the backup ID and backup time of the impacted files that are expired:



After expiration, the image is removed.



Backup ID	Date	Policy	Schedule N..	WORM Unlock Time	Primary Copy	Media Server	Expiration Date
Win_client.ransomware.local_1671777634	Dec 23, 2022 1:40:34 AM	windows_backup	Full		Yes	MSDPC.ranso...	Jan 6, 2023 1:40:34 AM
Win_client.ransomware.local_1671767789	Dec 22, 2022 10:56:29 PM	windows_backup	Full		Yes	MSDPC.ranso...	Jan 5, 2023 10:56:29 PM

Impacted files are removed and the remaining data is safe.

Data Protection Within the Retention Period

This feature protects the backup data in HCP for Cloud Scale environments. Attackers cannot modify or delete the backup data from an immutable bucket because it has an object locking feature adding WORM (Write Once Read Many) properties to the protected data. In essence, nobody can delete or change the backup images within the retention period.

Verify WORM lock Feature from NetBackup End

From Veritas NetBackup, set an expiration date for the backup image by completing the following steps:

1. Verify the image with the WORM lock feature.

The screenshot shows the NetBackup console interface. The 'Action' dropdown is set to 'Verify'. The 'Media' section is configured with 'Disk Type' set to 'PureDisk' and 'Disk pool' set to '<All>'. The 'Date/Time Range' is set from 'Oct 27, 2022 4:20:06 AM' to 'Oct 28, 2022 11:59:59 PM'. The 'Copies' section is set to 'Copy 3'. The 'Policy name' is '<All Policies>' and the 'Policy type' is '<All Policy Types>'. The 'Type of backup' is '<All Backup Types>'. The 'Client (host name)' is 'nbuora.ransomware.net'. The 'Job Priority' is set to '75000'. The 'Search Results' table shows one backup image found:

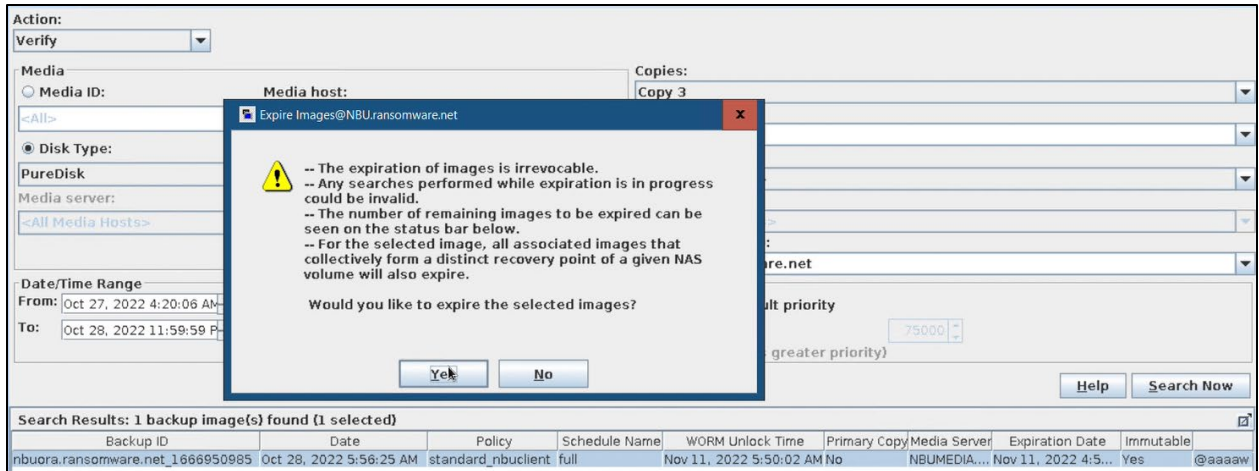
Backup ID	Date	Policy	Schedule Name	WORM Unlock Time	Primary Copy	Media Server	Expiration Date	Immutable
nbuora.ransomware.net_1666950985	Oct 28, 2022 5:56:25 AM	standard_nbuclient	full	Nov 11, 2022 5:50:02 AM	No	NBUMEDIA...	Nov 11, 2022 4:5...	Yes

2. Expire the image.

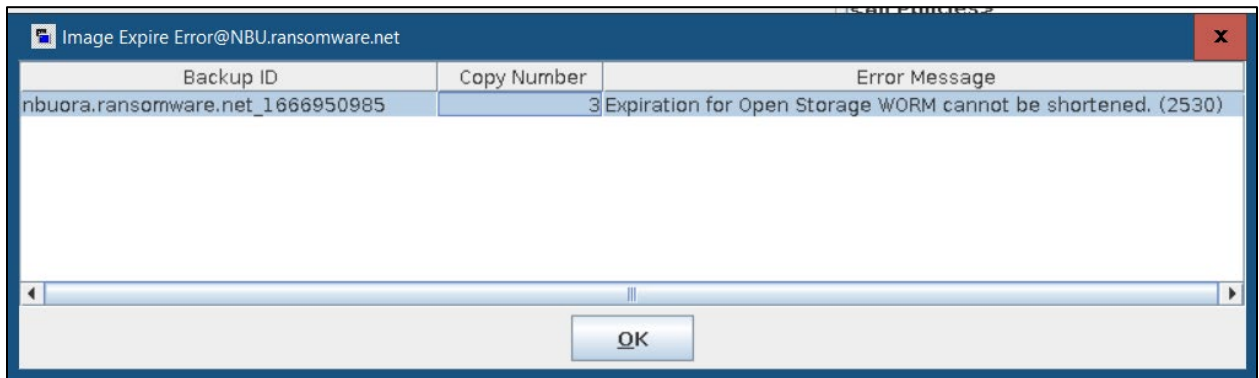
The screenshot shows the NetBackup console interface. The 'Action' dropdown is set to 'Verify'. The 'Media' section is configured with 'Disk Type' set to 'PureDisk' and 'Disk pool' set to '<All>'. The 'Date/Time Range' is set from 'Oct 27, 2022 4:20:06 AM' to 'Oct 28, 2022 11:59:59 PM'. The 'Copies' section is set to 'Copy 3'. The 'Policy name' is '<All Policies>' and the 'Policy type' is '<All Policy Types>'. The 'Type of backup' is '<All Backup Types>'. The 'Client (host name)' is 'nbuora.ransomware.net'. The 'Job Priority' is set to '75000'. The 'Search Results' table shows one backup image found:

Backup ID	Date	Policy	Schedule	Primary Copy	Media Server	Expiration Date	Immutable
nbuora.ransomware.net_1666950985	Oct 28, 2022 5:56:25 AM	standard_nbuclient	full		NBUMEDIA...	Nov 11, 2022 4:5...	Yes

After you expire the image, the following error shows up:



WORM is working and is not giving permission to expire the image.



Data is safe in HCP for Cloud Scale. No one can delete the backup data within the retention period, and you can recover the data without any trouble.

Backup ID	Date	Policy	Schedule N...	WORM Unlock Time	Primary Copy	Media Server	Expiration Date	Immutable	
nbuora.ransomware.net_1666950985	Oct 28, 2022 5:56:25 AM	standard_nbuclient	full	Nov 11, 2022 5:50:02 AM	Yes	NBUMEDIA.ran...	Nov 11, 2022 4:5...	Yes	@aaaaw

Limitations and Troubleshooting

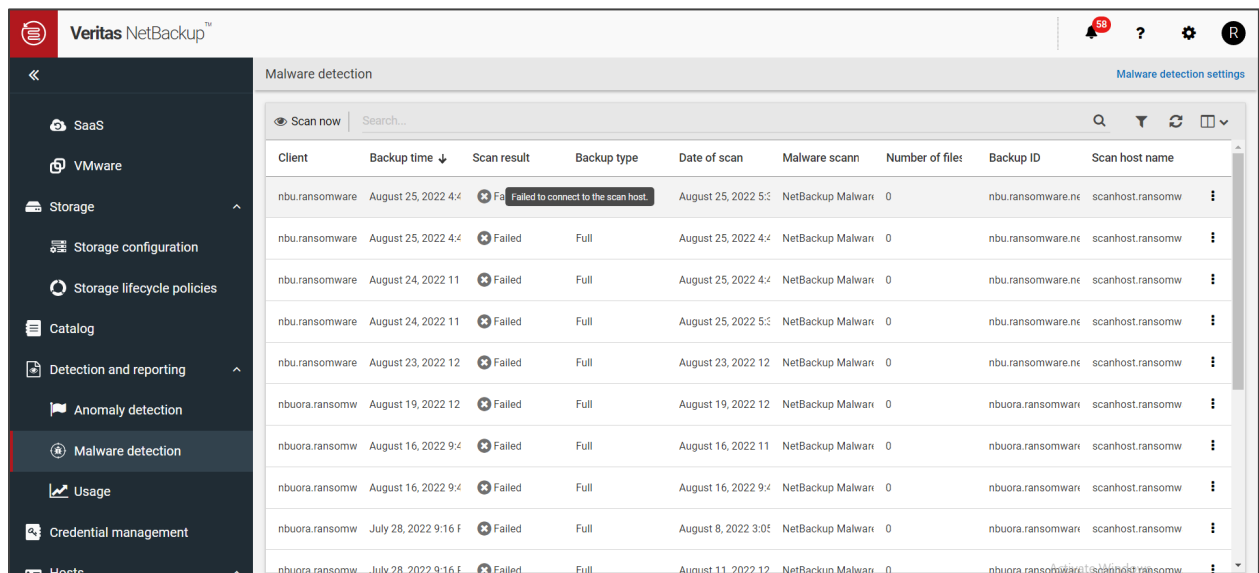
Limitations

The following lists the limitations of NetBackup malware scanner:

- NetBackup Malware scanner (version 10.0) has no access to MSDP-C backup images.
- NetBackup Malware scanner can only scan standard and MS Windows policy types and is not applicable for any other policy type.

Troubleshooting

- **Error:** Failed to connect to the scan host.



The screenshot shows the Veritas NetBackup Malware detection interface. The left sidebar contains navigation options: SaaS, VMware, Storage, Storage configuration, Storage lifecycle policies, Catalog, Detection and reporting, Anomaly detection, Malware detection (selected), Usage, and Credential management. The main panel displays a table of scan results. The first row is highlighted with a red background and contains the error message 'Failed to connect to the scan host'.

Client	Backup time ↓	Scan result	Backup type	Date of scan	Malware scann	Number of files	Backup ID	Scan host name
nbu.ransomware	August 25, 2022 4:4	Failed to connect to the scan host.		August 25, 2022 5:0	NetBackup Malwar	0	nbu.ransomware.ne	scanhost.ransomw
nbu.ransomware	August 25, 2022 4:4	Failed	Full	August 25, 2022 4:4	NetBackup Malwar	0	nbu.ransomware.ne	scanhost.ransomw
nbu.ransomware	August 24, 2022 11	Failed	Full	August 25, 2022 4:4	NetBackup Malwar	0	nbu.ransomware.ne	scanhost.ransomw
nbu.ransomware	August 24, 2022 11	Failed	Full	August 25, 2022 5:0	NetBackup Malwar	0	nbu.ransomware.ne	scanhost.ransomw
nbu.ransomware	August 23, 2022 12	Failed	Full	August 23, 2022 12	NetBackup Malwar	0	nbu.ransomware.ne	scanhost.ransomw
nbuora.ransomw	August 19, 2022 12	Failed	Full	August 19, 2022 12	NetBackup Malwar	0	nbuora.ransomwar	scanhost.ransomw
nbuora.ransomw	August 16, 2022 9:4	Failed	Full	August 16, 2022 11	NetBackup Malwar	0	nbuora.ransomwar	scanhost.ransomw
nbuora.ransomw	August 16, 2022 9:4	Failed	Full	August 16, 2022 9:4	NetBackup Malwar	0	nbuora.ransomwar	scanhost.ransomw
nbuora.ransomw	July 28, 2022 9:16 f	Failed	Full	August 8, 2022 3:00	NetBackup Malwar	0	nbuora.ransomwar	scanhost.ransomw
nbuora.ransomw	July 28, 2022 9:16 f	Failed	Full	August 11, 2022 12	NetBackup Malwar	0	nbuora.ransomwar	scanhost.ransomw

Cause:

libnsl.so.1 was missing from the scan host.

Solution:

To allow the NetBackup malware detection utility to run on scan host, install the libnsl.so.1 library on the scan host.

If the latest version of the libnsl library file is available (for example: /usr/lib64/libnsl.so.2), then, as a workaround, you can create a softlink file /usr/lib64/libnsl.so.1 that points to /usr/lib64/libnsl.so.2.

Example of creating a softlink file:

```
# cd /usr/lib64
```

```
# ln -sf libnsl.so.2 libnsl.so.1
```

For reference, see:

https://www.veritas.com/content/support/en_US/article.100053050

- **Error:** x509: certificate relies on legacy Common Name field, use SANs instead.

During HCP CS bucket creation from the NetBackup Media server, we received the following error:

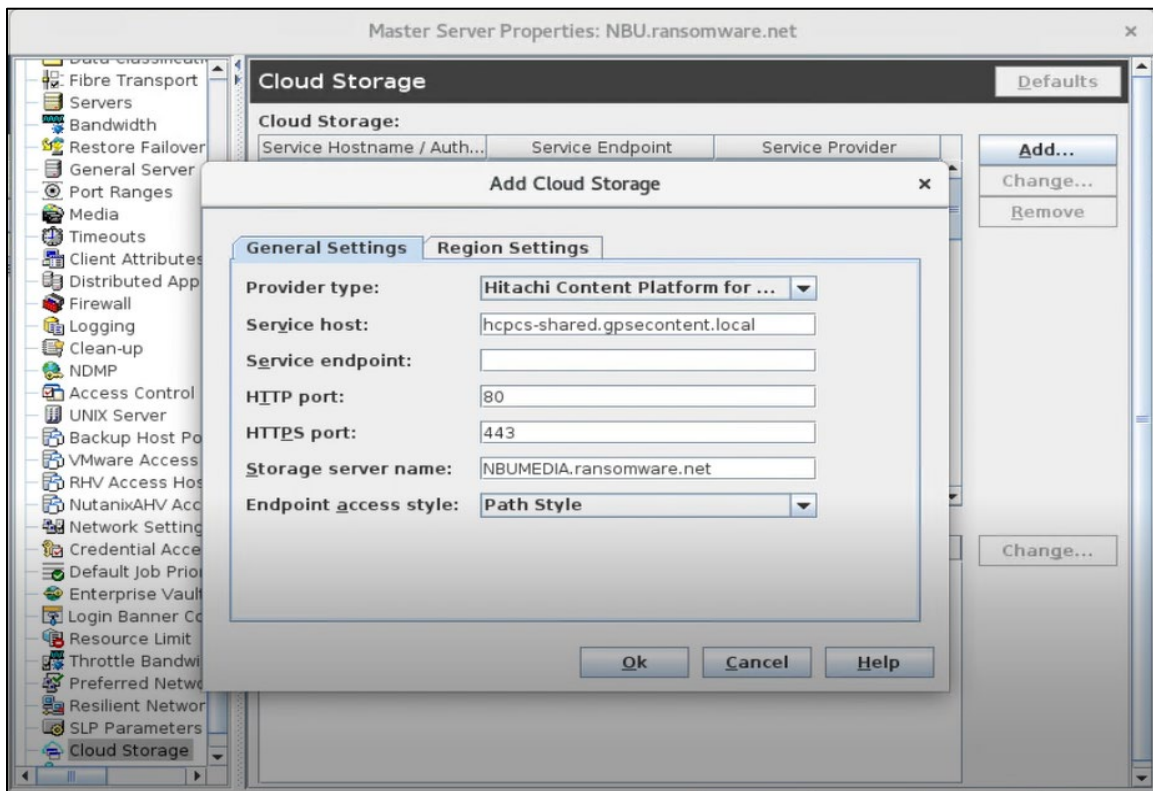
```
CreateS3Bucket: RequestError: send request failed
caused by: Put https://***/** x509: certificate relies on legacy Common Name field, use SANs
instead
createVolume: fail to create bucket: xzsb1
Error: cannot create volume: failed to create bucket
```

Cause:

Certificate issue between Veritas NetBackup and the cloud provider. NetBackup is unable to create a bucket through SSL.

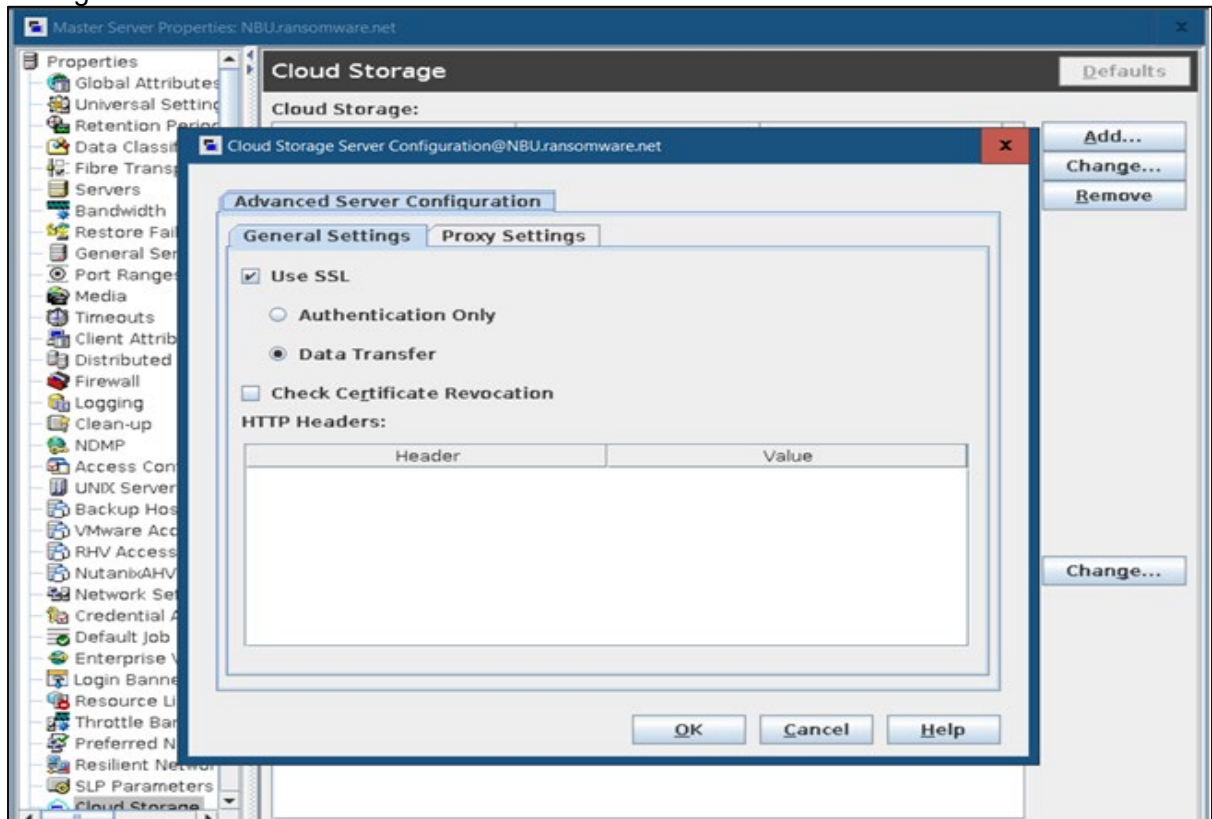
Solution:

1. While creating volumes in HCP for cloud scale, use “—disablesl!” from the NetBackup media server.



While adding cloud storage in NetBackup, add http and https ports.

2. After creating volumes from CLI, you can modify cloud storage settings from the NetBackup UI.
3. To secure the data transfer process, enable the SSL setting for Data Transfer and save the setting.



The data is safe in this solution.

Conclusion

In conclusion, we've effectively demonstrated the full utilization of the NIST framework in a comprehensive end-to-end cyber protection solution by combining the powerful technologies provided in NetBackup, HCP for Cloud Scale, and VSP storage systems.

The integration of these technologies provides a robust and reliable data protection and management system, ensuring the availability, confidentiality, and integrity of critical information assets.

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information

Americas: +1 866 374 5822 or info@hitachivantara.com

Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com

Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com

