

Hitachi Vantara-Veritas NetBackup Endto-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 maynot make anyother 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 onlyunder 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:

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
 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 Licenseeshall 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, BCPiiTM 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	
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	

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

Convention	Description
Bold	 Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK.
	 Indicates emphasized words in list items.
Italic	Indicates a document title or emphasized words in text.
Monospace	Indicates text that is displayed on screen or entered by the user. Example: pairdisplay -g oradb

This document uses the following typographic convention:

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: <u>https://support.hitachivantara.com/</u> and Veritas download center: <u>https://www.veritas.com/support/en_US/downloads</u>

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

<u>Hitachi Vantara Support Connect</u> 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: <u>https://support.hitachivantara.com/en_us/contact-us.html</u>.

<u>Hitachi Vantara Community</u> 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 <u>community.hitachivantara.com</u>, register, and complete your profile.

Comments

Send us any comments on this document to <u>GPSE-Docs-Feedback@hitachivantara.com</u>. 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
\/Mwara	VMware ESXi	VMware ESXi, 6.7.0, 10302608
Viviware	VMware vCenter Server	vSphere Client Version 6.7.0.20000
	Veritas NetBackup (Master, Media, Client) server	NetBackup 10.0
Veritas NetBackup	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	
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 usein 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	Chatur	Pool Type	Drive Tupe/RPM	Number of	Number of	Number of	RAID	Capacity			
ľ		Status	Poor type	Dive type/kem	Pool VOLs	V-VOLs	Root VOLs	Level	Total	Reserved	Used	Used (
Ī	DP0	Normal	DP	SSD,FMD/-	32	30	0	6(6D+2P)	84474.9	0.00 GB	2223.21 GB	
I	lexsnap pool	Normal	ті	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-toend solution. This process consists of the following high-level steps: 1. Create an HCP for Cloud Scale S3 Bucket.

HITACHI S3 Console					8
Buckets				Last updated 1 min	ute ago
Total Bytes	Total Objects	Total buckets			
169.96 MB [↑] 169.75 MB	1283 1283	× 1			
Search	Q		+ Create	Generate credent	ials
 Bucket name 	Objects	Size	Access level	Created	
veritas-ransomware	1283	169.96 MB STANDARD	Private	07/08/2022 19:20:51	:

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

HITACHI S3 Console	
< Generate S3 Credentials	Generate Cancel
Access key	
	Сору
Secret key	
	Сору

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
{
    "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 <u>NetBackup™ Installation</u> <u>Guide (veritas.com)</u>.

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)

Cloud Storage Server Configura	ation Wizard - NetBackup		×
	Add Storage Server Select cloud provider		
$\Box \land$	Storage API type:	All cloud storage provider types	•
	Cloud storage providers		
	Type here to search		Q
	Hitachi Content Platform HCP High Bandwidth Con	- LAN (S3) figuration for LAN-connected	
	Hitachi Content Platform HCP Low Bandwidth Cont	- WAN (S3) figuration for WAN-connected	
	Hitachi Content Platform HCP for Cloud Scale - Hig	for Cloud Scale - LAN (S3) Ih bandwidth LAN connections	_
	Hitachi Content Platform HCP for Cloud Scale - Hig	for Cloud Scale - WAN (S3) Ih bandwidth WAN connections	=

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/msdpcldutil

```
/usr/openv/pdde/pdcr/bin/msdpcldutil 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/msdpcldutil create -b veritas-ransomware -v veritas_vol --mode COMPLIANCE --min 1D --max 30D --live 2025-08-25 --disabless1

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

/usr/openv/pdde/pdcr/bin/msdpcldutil update range -b veritas-ransomware -v veritas vol --min 5D --max 30D

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



4. From master server properties, select Cloud Storage.

Applications Places Master Server Properties: NBU.rans	omware.net								Wed	07:43	(0)
		Master Server F	roperties: NBU.ransom	ware.net			×				
⑧ Veritas NetBackup™	- 12: Fibre Transport	Cloud Storage				<u>D</u> efaults	ŀ			<mark>ر ک</mark>	lav
Elle Edit View Actions Help NBU-ransomware.net (Master Server) HBU-ransomware.net (Master Server) HBU-ransomware.net (Master Server) HBU-ransomware.net (Master Server) HBU-ransomware.net (Master Server) Activity Nontor Activity Nontor HBU-ransomware.net (Master Server) Host Bracouts HBU-ransomware.net HBU-ransomwa	Restore Fallover General Server Ort Ranges Media Gineral Attributes Distributed Appl Firewall Inerouts Clean-up NoMP Access Control UNIX Server Backup Host Por NoMP Access Control UNIX Server Rackup Host Por NoMP Control UNIX Server Resource Limit Throtte Bandwic Preferred Netwo Resource Limit Suprameters Suprameters Codustorage Count Suprameters Codustorage Control Suprameters	Service Hostname / Auth Associated Cloud Storage Storage Server Nan	Service Endpoint	Service Type	Provider	Add Change Bemove		Status onnected	Off	Login Activi	ty T
	🕱 Loading Cloud Instan	ces		<u>o</u> k (Cancel	Apply <u>H</u> elp			Alert Notific	ation	-

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

Cloud Storage Defaults Servers Cloud Storage: Servers Cloud Storage: Servers Cloud Storage: General Server General Server Media Change Timeouts General Settings Provider type: Service host: Service endpoint: Region Settings Provider type: Service host: Service endpoint: HITP port: HITP port: HITPs port: Storage server name: Hitachi Content Platform for Clot • NutanixAHV Access Fordential Acces O Faults Banner (Content Platform for Clot • Change Preferred Network Ok Cancel Help Change Ok Cancel Help
Servers Bandwidth General Server O Port Ranges Media Timeouts Clear Attributer Distributed App Firewall Logging Clear-up NDMP Access Control UNX Server Backup Host Pc Mware Access Provider type: Service endpoint: HITP port: HITP port: HITP port: HITP port: Backup Host Pc Mware Access Provider type: Service endpoint: HITP port: HITP port: HITPS port: Storage server name: Endpoint access style: Path Style Change Change Bemove Clear-up Content of the style Change change Clear-up Content of the style Clear-up Change change Clear-up Change change Clear-up Change change Clear-up Change change Clear-up Change change Clear-up Change change Clear-up Change change Clear-up Change change Clear-up Service Hot Storage server name: Endpoint access style: Path Style Change change Clear-up Change change Clear-up Change change Change change Change change Change change Change change Change change Change change change change change Change change change change change change change change Change change
Bandwidth Service Hostname / Auth Service Endpoint Service Provider O Port Ranges Media Timeouts Client Attribute Distributed App Frewall Logging Clean-up MutanixAHV Access Control UNIX Server Backup Host Po NutanixAHV Access Hot Rey Cancel Help Credential Acce Default job Prio Endpoint access style: Path Style Change Change Change
Restore Failover Service Hostname / Auth Service Endpoint Service Provider Add Port Ranges Media Media Timeouts Client Attributer Distributed App Firewall Logging Clean-up Provider type: Service endpoint: HTP port: HTTPS port: Storage server name: HITPS port: Storage server name: Path Style Change Change
Overt Ranges Media Media Media Change Media Distributed App Firewall Logging Clean-up Service endpoint: HTP port: HTPS port: Storage server name: Endpoint access style: Path Style Change Change Change Change
Media Timeouts Client Attributer Distributed App Firewall Logging Clean-up NDMP Access Control UNIX Server Backup Host Po MittanixAHV Access RHV Access Host Storage server name: Hitachi Content Platform for Clou NutanixAHV Acc NutanixAHV Acc NutanixAHV Acc Default Job Prio Change Change Change Server Name: Enterprise Vault Resource Limit Throttle Bandwi Preferred Networ Cloud Storage Cloud Storage
General Settings Region Settings Client Attribute Distributed App Firewall Logging Clean-up NUMP Access Control UNIX Server Backup Host Po MWare Access RHV Access Hot NutanixAHV Acc NutanixAHV Acc Resource Limit Credential Access style: Path Style Change Ok Cancel Help Provider type: Service endpoint: HTTPS port: Storage server name: Endpoint access style: Path Style Change
Client Attributes Distributed App Firewall Clean-up NDMP Access Control UNIX Server Backup Host Po VMware Access MutanixAHV Acc NutanixAHV Acc NutanixAHV Acc NutanixAHV Acc Default Job Prio Credential Acce Default Job Prio Enterprise Vault Resource Limit Throttle Bandwi Preferred Netwoi Resilient Netwoir SLP Parameters Cloud Storage
Frewall Service host: Service endpoint: Access Control UNIX Server HTTP port: UNIX Server HTTPS port: Storage server name: Endpoint access style: Path Style Change Change
Service host: Clean-up Clean-up Clean-up Clean-up Clean-up Clean-up Clean-up Clean-up Clean-up Service endpoint: HTTP port: HTTPS port: Storage server name: Hitachi Content Platform for clou Storage server name: Endpoint access style: Path Style Change Change Change Change
Service endpoint: WNDMP Access Control UNIX Server Backup Host Po Storage server name: HITTPS port: Storage server name: Hitachi Content Platform for Clou • Storage server name: Endpoint access style: Path Style Change Change Change Change Change
Image: NDMP Image: NDMP <
Image: Second Secon
Backup Host Po Whware Access RHV Access Hot NutanixAHV Acc NutanixAHV Acc NutanixAHV Acc Network Setting Credential Acce Default Job Prio Enterprise Vault Resource Limit Throttle Bandwi Preferred Networ SLP Parameters Cloud Storage
Storage server name: BrHV Access Hos NutanixAHV Acc NutanixAHV Acc Network Setting Credential Acce Default Job Prio Enterprise Vault Enterprise Vault Enterprise Vault Resource Limit Throttle Bandwi Preferred Networ SLP Parameters Cloud Storage
Control Revealed and the second
Wetwork Setting Change Credential Acce Default Job Prio Enterprise Vault Change Clogin Banner Co Change Resource Limit Qk Preferred Networ SLP Parameters Cloud Storage Image: Cloud Storage
Image: Credential Acce Image: Change: Ch
Default Job Priol Enterprise Vault Ent
Charles Cancel Help Cancel Help Cancel Concel
Image: Control Control Image: Control Control Image: Control Control Image: Control Image: Control Control Image: Control Control Image: Control Control Image: Control Control Image: Control Control Image: Control Image: Control Control Image: Control Control Image: Control Im
Image: Control of the second storage Image: Control of the second storage
Image: Step Parameters Image: Step Parameters Image: Step Parameters Image: Step Parameters
Gar Resilient Networ
Re Cloud Storage
Master Server Properties: NBU ransomware.net
Defaults
Bandwidth Cloud Storage:
- Mestore Failover Service Hostname / Auth Service Endpoint Service Provider Add
Add Cloud Storage x Change
Port Ranges Remove
Timeouts
General Settings Region Settings
Distributed App Provider type: Hitachi Content Platform for
Bervice host: bcpcs-shared.gpsecontent.local
NDMP Service endpoint:
Access Control HITP port: 80
Backup Host Po HTTPS port: 443
-B VMware Access Storage server name: NRUMEDIA ransomware net
- RHV Access Hos
NutanixAHV Acc Endpoint access style: Path Style
- % Credential Acce
Default Job Prior
- Senterprise Vault
I Datis Dospor Ed
- B Resource Limit - B Throttle Bandwi - Cancel Help
Cancel Help Preferred Netwo
Image: Comparison of the compar
Courte Limit Ok Cancel Help School Storage Courte Storage

Hitachi Vantara-Veritas NetBackup End-to-End Cyber Protection Solution Page 19

6. Add region settings.

General Setting	s Region Sett	ings	
Regions: <u>R</u> egion name	Location const	traint <u>S</u> ervice host	
			米 <u>A</u> dd
us-west-2	us-west-2	hcpcs_shared.gps	X <u>D</u> el

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.

Disk neel entione	(2) Malumaa	(2) Deplication	
Disk pool options	Volumes	Replication	G Re
Storage server name *	Features		
NBUMEDIA.ransomware.net	Accelerator, A	A.I.R., Instant access, WORM capable	Change
Disk pool name *			
	0		
MSDPC-pool			
MSDPC-pool Description			
MSDPC-pool Description Enter description			

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

1	Veritas NetBackup [™]			2	?	٥	R
«		Add MSDP disk pool					×
0	😹 Microsoft SQL Server	Disk pool options Volumes Replication				4	Review
:	× Nutanix AHV	WUKM					
:	OpenStack	Use object lock NetBackup retrieves the Object Lock information from Cloud storage. Ensure that the targeting bucket is created, and the Object Lock mode is set. Refer to the NetBackup Deduplication Guide for more de	etails.				
	Se Oracle						
	🛎 RHV	Cloud buckets Enter an existing cloud bucket name					
	SaaS	Cloud bucket name					
c	ф VMware	veritas-ransomware					
-	Storage ^	Select or create a cloud bucket					
ł	Storage configuration	Community and Franchise					
	Storage lifecycle policies	MSDP compression is automatically enabled					
	Catalog	X MSDP KMS encryption is not enabled					
ا ھ	Detection and reporting		Activ	ate Win	dows		-
	Anomaly detection	Ca	ncel	Previo	octiva je d	Nex	ĸt

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

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

O	Disk pool options	Volumes	Replication	- 4 Review
	General settings			•
	X Use SSL		X Check certificate revocation	
	Proxy settings			
	X Use proxy server			
	WORM settings			
	✓ Use object lock			
C	 Origination Configuring the disk volume. Configuring the disk pool. 			
				Close

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



Γ		Name	Available space	Total size	Encryption	Replication	Bucket name	WORM capable	Minimum lock duratio	Maximum lock duration
()	PureDiskVolume	1.34 TB	1.34 TB	Yes	None				
0)	veritas_vol	8.00 PB	8.00 PB	No	None	veritas-ransomware	•	1 day	30 days

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

Verifias-ransonware/verifias_vol/ Browse Overview Properties Show deleted objects All Name Size Mame Size Mame Size Mame Size Mame Size Mane Size Mane Size Mane Size Mane Size Modified Owner StanDaRD StanDaRD StanDaRD	۶						CHI S3 Console	HITAC
Browse Overview Properties Show deleted objects Create Directory Upload Objects All							veritas-ransomware veritas-ransomware / veritas_vol /	< \
All Image: Delete of the	ct 💭	te Directory Upload Objec	Create Directory				trowse Overview Properties	Br
Name Size Modified Owner Storage class data databases lockdown-mode.conf 23 B 09/3/2022.04:42:59 Mousumi Ghosh STANDARD	Destroy	🗍 Delete 🖑					All	
Image: Constraint of the state of the st		age class	Storage class	Owner	Modified	s	Name	
Image:	:	NDARD	STANDARD				🗋 data	
Dickdown-mode.conf 23 B 09/13/2022 04:42:59 Mousumi Ghosh STANDARD	:	NDARD	STANDARD				🗋 databases	
	:	NDARD	STANDARD	Mousumi Ghosh	09/13/2022 04:42:59	2:	Dickdown-mode.conf	
Li Isu-worm.conf 72 B 09/13/2022 04:42:59 Mousumi Ghosh STANDARD	:	NDARD	STANDARD	Mousumi Ghosh	09/13/2022 04:42:59	7.	🖹 Isu-worm.conf	

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.

		🛇 Disk poo	successfully created.	Add storage u	nit					3
Storage servers	Disk pools	Storage units	Universal shares							
+ Add Search							Q T	C		1≣ ~
Name	Add storage unit			×	Low water ma Us	se WORN	On demand	Maxi	mum	
adv-stu-stu	Select the type of storag	e that you want to configur	e				Ø	1		:
basic-stu	AdvancedDisk Media server local storage							10		:
MSDP-me	Cloud storage Direct backup to cloud							100		:
	Media Server Dedup Deduplication to local store	plication Pool (MSDP) ge and cloud								
	OpenStorage									
			Ca	ncel Start						

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

ē	Veritas NetBackup [™]									P	?	٥	R
«		Add N				Disk pool successf	fully created. Add s	storage unit					×
>	Nutanix AHV	В	asic properties			Disk pool		🕑 Media se	rver			4	Review
8	OpenStack									1		-	
°,	Oracle		Name	Available space	Raw size	Replication	Volumes	WORM capable	Minimum	ock durat Maxin	num lock d	ura	
4	RHV		MSDPC-pool			None	veritas_vol	٢	1 day	30 day	s		
e	SaaS		Showing 1-1 of 1										
đ	Ĵ ∨Mware												
🚔 s	torage ^	Me	dia server									/	、
	Storage configuration								Q			_	
(Storage lifecycle policies		Name			NetBackup version		OS platform					- 11
E c	atalog		NBUMEDIA.rans	somware.net		10.0		Linux					
D D	etection and reporting ^		1 Records										
•	Anomaly detection									Activate Win	dows		Ŧ
0	Malware detection									Go to Settings to Cancel	Previo	ndows Js	Save

5. Verify that a storage unit is created.

Sto	rage servers	Disk po	ols	Storage units	Unive	rsal shares								
Ado	Bearch									Q	т	C	□~	t≣ v
	Name	Media server:	Category	Disk pool u	Fragment :	Disk pool	High water m	Low water ma	Use WORN	On den	nanc	Maxir	num	
	adv-stu-stu	Any available	AdvancedDisk	44.02 MB of	512 GB	adv-stu				C		1		;
	basic-stu	NBUMEDIA.r	Basic disk	586.12 MB (512 GB							10		:
	MSDP-me	NBUMEDIA.r	MSDP	586.12 MB (50 GB	MSDP-media						100		•
7	MSDPC-stu	NBUMEDIA.r	MSDP	0.00 KB	50 GB	MSDPC-pool			0	C		100		:

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.

```
Conflict Statement
While configuring a NetBackup policy with the
Veritas snapshot option (VSO) FIM, you must select
an SLP as Policy storage destination.
```

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.

New Storage Lifecycle Policy@NBU.ransomware.net	x
Storage Lifecycle Policy Validation Report	
Storage lifecycle policy name: Data classifi	ecation: Priority for secondary operations: ass • •
Operation Storage Target Ma Window Volur	ne Pool Media Ow Retention Retention Alternate Preserve
↑ ↓ ↓ Add Change <u>R</u> emove	
State of secondary operation processing Active Postponed Until Nov 21, 2022 10:56:15	To find impact on Policies associated with this SLP due to change in configuration click here. Check <u>for Conflicts with Backup Policies</u>
	<u>O</u> K <u>C</u> ancel <u>H</u> elp

- 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.

New Operation@NI	3U.ransomware.net	x
Properties		
Source storage:		
Operatio <u>n</u> :	Backup	▼
Destination Sto De <u>s</u> tination sto	Backup Snapshot Import	pn
MSDP-media-s	tu 🔻	Retention type:
<u>V</u> olume pool:		Fixed
NetBackup	-	Retention period:
Media owner:		2 weeks (Retention Level 1) 👻
Any	~	

<u>File Edit View Actions Help</u>	Change Storage Lifecycle P	olicy@NBU.ranson	nware.net						x
	Storage Lifecycle Polic	v Validation	Report						
NBU.ransomware.net (Master Se 🚦 4 Storage L	ecycle					-			
NBU.ransomware.net (Master Server	<u>Storage lifecycle policy</u>	/ name:	<u>D</u> ata classi	ification:	<u>P</u> riority	for second	lary operati	ons:	
Backup, Archive, and Restore	SLP-Cloud		<no data<="" td=""><td></td><td></td><td>0 * (high</td><td>er number i</td><td>s greater p</td><td>riority)</td></no>			0 * (high	er number i	s greater p	riority)
NetBackup Management			and data	and some					
Intersection of the section of t	Operation	Storage	Target Ma	Window	Volume Poo	Media Ow	Retention	Retention	Alterna
- 🖪 Policies 🛛 🖉 SLP_test	Spanshot	MSDP-media	Target Main	WINGOW		i nicula own	Fived	2 weeks	ALGING
🕈 🥅 Storage	Backup From Spansho	MSDP-media	-	Default 2	a		Fixed	2 weeks	
Storage Units	Backup From Snapsho	MSDPC.etu		Default 2			Fived	2 weeks	
Storage Unit Groups	Backap Hom Shapsho	11001 0-010		Deradit_2			10004	2 10000	
Gotolog									
• We Host Properties									
- And Master Servers									
- 🗐 Media Servers									
- 🗐 Clients									
🔶 📰 Applications									
🕈 🖺 Media and Device Management									
- Device Monitor				-					
Y 🔤 Media									
Volume Pools									
- Solume Groups									
Standalone	Add Change	Remove	7						
🗢 🥃 Devices									
🕈 😪 Credentials	State of secondary op	eration proce	ssina						
— 📑 Disk Array Hosts				To find	impact on P	olicies ass	ociated with	n this SLP	
NDMP Hosts	Active			due to	change in c	onfiguratio	n click here.		
Storage Servers	Postponed			Chas	k for Conflic	to with Bay	kup Belisio		
Sponshot Monogement Sel				cnec	K IOI COIIIIC	LS WILLI Day	Kup Policies	>	
WebSocket Servers	Until Nov 6, 2022	12:37:58 PN							
- Security Management									
- 🥵 Security Events									
- 🛃 Host Management						9	<u>o</u> k <u>c</u>	ancel	Help
🗢 💽 Certificate Management									

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: <u>https://www.veritas.com/content/support/en_US/doc/140789355-151836558-0/v140790360-151836558</u>

Installing CloudPoint using Docker

To install CloudPoint using docker, complete the following steps:

1. Download the file from Veritas download center.



2. From the NetBackup UI, click Snapshot Manager.

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

NBU.ransomware.net (Master Se	1 Snapshot Management Servers (1 selected) Search		Y
BU.ransomware.net (Master Server	Host Name		
Backup, Archive, and Restore	CPE ransomware local	443	
	Change Spanshot Management Server@NDU ranser	awara pot	Y
NetBackup Management		iware.net	
Policies	CloudPoint Host Name:		
Storage			
Storage Unit Groups	CPE.ransomware.local		
Storage Lifecycle Policies			
SLP Windows	Connect using Port number		
- Scatalog			
- M Host Properties	443		
- A Master Servers			
- Bu Media Servers	Valid	ate Serve	r
- Clients			
- Applications			
🕈 🗒 Media and Device Management			
🗍 🔄 🖳 Device Monitor	Enter credentials for added CloudPoint H	ost Name	:
🖓 🏧 Media	liser name:		
🗠 🐙 Volume Pools			
🗢 🍓 Volume Groups	USER_CPE		
🗢 📴 Robots	Password:		
🔄 🗗 Standalone			
🗠 🥃 Devices			
🕈 😪 Credentials			
– 🎼 Disk Array Hosts	<u>O</u> K <u>C</u> ancel	Hel	p
NDMP Hosts			
Storage Servers	671		
Virtual Machine Servers			100
Snapsnot Management Se			
- es websocket Servers	<u> </u>		

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.

Configure Plugin	×
CloudPoint Server: NBUCPE.ransomware.local	
Selected Plugin: Hitachi Storage Array	
Credentials	
Enter Plugin ID:	
VSP5600H	
Hitachi Configuration Manager Server IP:	
Hitachi Configuration Manager Server Port:	
Array Username:	
Array Password:	
Array storage Device Id:	
T	
<u>O</u> K <u>C</u> an	cel <u>H</u> elp

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.

All Policies		4	2 Policies (0 sel
🛃 NBU.ransomware.n	et (Master Server)	1000	Name
Summary of All F standard	🎒 New Policy		
- R windows backup	W New Schedul	e	
- 1	New Client		
	\min New Backup 🤅	Se	lection
	Insert		Insert
	X Delete		Delete
	🔎 Change		
	🕼 Copy To New.		
	X Cut		Ctrl-X
	🖻 <u>С</u> ору		Alt-C
	🖺 Paste		Ctrl-V
	🗘 <u>R</u> efresh		F5
	Activate		
	D <u>e</u> activate		
	Manual Backı	ıp	
	Upgrade Hos	t	
		12	

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.

Attributes Schedules Clients Backup Selections Policy type: Standard Standard The following selections are optional. If no snapshot method is selected, NetBackup will select a snapshot method at the time of backup. Snapshot Method at the time of backup. Snapshot method of this policy: Image: SLP-Cloud	Server: NBU.rans	omware.net					
Policy type: Standard Destination: Who data classification> Data classification: No data classification> Policy storage: SLP-Cloud Policy golume pool: FietBackup Take checkpoints every: 0 minutes Limit jobs per policy: 0 finigher number is greater priority) Media Ownger: Invy Snapshot Client and Replication Director Perform Block level incremental backups Perform Block level incremental backups Options Perform off-host backup Options Perform off-host backup Options Preform off-host backup Options Machine: Machine: Image of the streaming tributes Allow Oynamic Streaming Maximum number of files in a batch 300 °	🛾 Attributes 🖉 S	Schedules	🖲 Clients 🎽 靤 Backup Selection	ns	Spanshot Options - Policy standard physiont@NR	Il ransomware net	-
Detaination: Data classification: Vio data classification> Policy storage: SLP-Cloud Policy volume pool: NetBackup NetBackup Policy volume pool: NetBackup NetBackup VSO Snapshot method for this policy: VSO The following parameters can be set for backups performed in this policy: VSO The following parameters can be set for backups performed in this policy: Snapshot method: Configuration Parameters Value Snapshot Clent and Replication Director Perform snapshot backups Options Perform snapshot for instant Recovery or SLP management Hyper-V server: Perform off-host backup Use: Machine: Perform off-host backup Machine: Wathin: Ortions: Options: Machine: Options: Options	Policy type:	Standard	1	•	The following selections are optional. If	no snapshot method is selected,	
Policy storage: SLP-Cloud VSO Policy golume pool: NetBackup The following parameters can be set for backups performed in this policy tau use this snapshot method: Take checkpoints every: O,************************************	Destination: Data classificatio	in:	<no classification="" data=""></no>	•	Snapshot method for this policy:	o at the time of backup.	
Policy golume pool: ItelBackup Policy golume pool: Itake checkpoints every: Itake checkpoints every:<	Policy storage:		SLP-Cloud	-	VSO	•	
Limit jobs per policy: Parameter Value Job priority: O (higher number is greater priority) Snapshot Type Cow Media Owner: Any Snapshot Client and Replication Director Snapshot Lient and Replication Director Snapshot Super Value Perform block level incremental backups Options OK Cancel Perform snapshot backups Options OK Cancel Perform off-host backup Preferred server list (Exchange DAG only) Use: Machine: Value	Policy volume poo	ol: ts every:	NetBackup	s	The following parameters can be set for that use this snapshot method: Configuration Parameters	backups performed in this policy	
Limit jobs per policy: Lob priority: O Iob priority: O Any Snapshot Client and Replication Director Perform block level incremental backups O Berform snapshot backups Options Perform snapshot for instant Recovery or SLP management Hyper-V server: Perform off-host backup Use: Machine: Other and the server list (Exchange DAG only) Database backup source: Preform off-host backup Use: Machine: Allow Dynamic Data Streaming Maximum number of files in a batch		- 11			Parameter	Value	
Iob priority: 0 : (higher number is greater priority) Media Owner: Any Snapshot Client and Replication Director Perform block level incremental backups Use Replication Director Enable vendor change tracking for incremental backups Ø Perform snapshot backups Ø Perform snapshot backups Ø Perform off-host backup Use: Perform off-host backup Use: Berior off-host backup Ø Snapshot for Instant Recovery or SLP management Hyper-V server: Perform off-host backup Ø Snapshot for Instant Recovery or SLP management Huyper-V server: Perform off-host backup Ø Snapshot for Instant Recovery or SLP management Huyper-V server: Perform off-host backup Ø Snapshot Database backup source: Preferred server list (Exchange DAG only) Ø Snapshot Database backup source:	<u> </u>	uncy:			Snapshot Type	Cow	
Media Owner: Any Snapshot Client and Replication Director Perform block level incremental backups Use Replication Director Enable vendor change tracking for incremental backups Ø Perform snapshot backups Ø Perform snapshot backups Ø Perform off-host backup Use: Perform off-host backup Use: Maximum Off-host backup Use: Machine: Ø Dynamic Data Streaming Attributes Allow Dynamic Streaming Maximum number of files in a batch 300 t	lob priority:	0 🛟 (hig	her number is greater priority)		Snapshot Host	CPE.ransomware.local	
Snapshot Client and Replication Director Perform block level incremental backups Use Replication Director Enable vendor change tracking for incremental backups Perform snapshot backups Retain snapshot for Instant Recovery or SLP management Hyper-V server: Perform off-host backup Use: Nachine: Value Machine: Value Maximum number of streams per volume 4 Maximum number of files in a batch	Media Ow <u>n</u> er:	Any		~	Maximum Snapshots (Instant Recovery only)	200	
Database backup source: Derform off-host backup Use: Machine: Dynamic Data Streaming Attributes Dynamic Streaming Maximum number of files in a batch 300 c	Perform block le Use Replication Enable vendor Perform snapsh Retain snapsh	evel incremen Director change tracki hot backups	ntal backups	Option <u>s</u>		<u>OK</u> <u>C</u> ancel <u>H</u> elp	
Perform off-host backup Use: Machine: Image: I	Hyper-V serve		It Recovery of SLP management		Database backup source:	T	
Use: Image: Constraining and the second	Perform off-h	ost backup			Preferred server list	Truck and a DAC and A	
Machine: Image: Dynamic Data Streaming Attributes Machine: Image: Dynamic Data Streaming Attributes Maximum number of streams per volume 4 Image: Dynamic Data Streaming Maximum number of files in a batch Maximum number of files in a batch 300 Image: Dynamic Data Streaming Maximum number of files in a batch	Use:			-		(Exchange DAG only)	
Allow Dynamic Streaming Maximum number of files in a batch	Machine:				Dynamic Data Streaming Attributes		
Maximum number of streams per volume 4	. Autiliter				Allow Dynamic Streaming		
Maximum number of files in a batch					Maximum number of streams per volum	4 ‡	
					Maximum number of files in a batch		

11. Add schedules.

	📑 Se	erver: N	VBU.r	ransom	ware.	net																				
\square	🔳 At	tribute	s	🚯 Sche	dules	; 🖣	Clien	ts 💼	Backu	p Selec	tions															
				2		4		6		8		10		12		14		16		18		20		22		24
S	Sun [+		+ +	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
N T	10n	+		+ +		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-
l v	Ved	+		+ +		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	1
Ť	hu	+		+ +	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	1
F	ri [+		+ +	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+]
S	at L								_		_															
[١	Vame		Туре	Syn	thetic	B Di	sk-Only E	3 Ret	ention P	Ret	ention L	F	requency	Med	ia Multi	S	torage	Volur	ne Pool	Pc	licy	Media	Owner /	Accelei	rator
	🕘 fu	III	Full	Backup	No		No		Dete	ermined.			01 W	veek		1					standa	ard_n		ľ	10	

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

Server: NBU.ransomware.net			
🛅 Attributes 🕲 Schedules 📲 Client	s 📴 Backup Selections		
Client Name	Hardware	Operating System	Resiliency
📕 nbuora.ransomware.net	Linux	RedHat3.10.0	

13. Select the backup path.

[🛢 Server: NBU.ransomware.net
	🗉 Attributes 🏽 🤀 Schedules 🖉 🖷 Clients 🗋 📾 Backup Selections
	Backup Selection List
	lie_yfile_system/
l	

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 desribed 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**.

File Edit View Actions Help X 10 10 [7] 📑 🗢 🗉 🖬 🔛 📇 🖨 😒 🖻 🚔 🗛 🍸 🗶 🖑 📓 🔛 🗎 🛪 🌮 Login Activity mware.net (Master Se... All Policies standard_nbuclient Type Data Clas... -- SLP-Cloud NBU.ransormvare.net (Master Server)
 NBU.ransormvare.net (Master Server)
 Standard.nbuclinex
 Atributes
 Atributes
 Atributes
 Atributes
 Mew Policy...
 Schedules
 Mew Schedule...
 Backup Selec
 Mew Backup Selec
 New Backup Selec U.ransomware.net (Master Sen Backup, Archive, and Restore Name Volume P... Media Ow... Checkpoi... Jobs/Policy Priority NetBackup Any 0 --Storage standard_nbucli... Standard JetBackup Management EF ports Status of Backups Client Backups Problems All Log Entries Images on Media Media Logs Tape Reports 💾 New Backup Selection... Media Lu Media Lu Tape Reports Disk Reports Vault Report X Delete Delete A Change Copy To New... Image: Store
 Image: Store ∦ Cut ⊫ <u>C</u>opy Storage Storage Units Storage Unit Groups Storage Lifecycle Policies SLP Windows At-C I Paste 🔹 <u>R</u>efresh Catalog Host Properties Master Servers Media Servers Manual Backup...

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

Manual Backup@NBU.ransomware.net		×
Server: NBU.ransomware.net		
Start backup of policy: standard_nbuclient	<u>0</u> K	
Select the schedule you want to use:	<u>C</u> afficel	
full	Help	
Select one or more clients you want to back up. If you select no clients, all clients are backed up: nbuora.ransomware.net		

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

🗢 Job Id	🛆 Туре	🛆 State	Stat	Status	Job Policy	Job Schedule	Client	Media Se	Start
😚 769 Snapsh	ot	Active			standard_nbuclient	full	nbuora.ransomware.net	NBUMEDI	Oct 28, 2022 5
≂ Job Id	🛆 Туре	∠ State	Stat	Status	Job Policy	Job Schedule	Client	Media Se	Start

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:

Job ID:	76	9	Job State:	Done (Successful)		
Job Overview Det	ailed Status	Job Hierarchy				_
Attempt:				Attempt Started:	Oct 28, 2022 5:56:24 AM	
Job PID:				Attempt Elapsed:	00:06:12	
Storage Unit:	MSDP-me	dia		Attempt Ended:	Oct 28, 2022 6:02:36 AM	
Media Server:	NBUMEDI	A.ransomware.n	t	KB/Sec:		
Media Transport Ty	e: LAN					
Status:						
Oct 28, 2022 5:56:42 Oct 28, 2022 5:56:51 Oct 28, 2022 5:57:19 Oct 28, 2022 5:57:19 Oct 28, 2022 5:57:28 Oct 28, 2022 5:57:72 Oct 28, 2022 5:57:73 Oct 28, 2022 5:57:72 Oct 28, 2022 5:57:72 Oct 28, 2022 5:57:73 Oct 28, 2022 5:57:75 Oct 28, 2022 6:00:45 Oct 28, 2022 6:00:45 Oct 28, 2022 6:00:55 Operation Status: 0 Operation Status: 0	AM - started pr AM - Info bpbrm AM - Info bpfis (AM - end SLP M AM - Info bpfis (AM - end writing	ocess bpbrm (pid= n (pid=23591) The n (pid=23591) read n (pid=23591) read n (pid=23591) start n (pid=23591) Start (pid=23591) Start (pid=23591) valid (pid=31252) done, g	3591) at-in-transit encryption (DTE) is disabled for the client (nbuor a.ransomware.net is the host to backup data from gig file list for client pg create snapshot processing started reate Snapshot: elapsed time 0:03:21 ting image for client nbuora.ransomware.net tatus: 0: the requested operation was successfully completed	ra.ransomware.net) as the global	DTE mode is set to 'Preferred Off' and the	
oct 28, 2022 6:00:55 oct 28, 2022 6:00:55 ott 28, 2022 6:00:55 oct 28, 2022 6:00:55 oct 28, 2022 6:01:03 oct 28, 2022 6:01:03 oct 28, 2022 6:01:04 oct 28, 2022 6:01:05 oct 28, 2022 6:01:05 oct 28, 2022 6:02:08 oct 28, 2022 6:02:05 oct 28, 2022 6:02:35	AM - end Paren AM - Info nbjm (AM - begin SLP AM - started pr AM - Info bpbrm AM - Info bpbrm AM - Info bpfis (AM - Info bpfis (AM - Info bpfis (AM - end writing	t Job; elapsed time (pld=2557) snapsh occess bptrm (pld= n (pld=24117) The n (pld=24117) Start (pld=832) Backup s (pld=832) done. st. anaged Snapshot:1 (pld=832) done. st. 9	1:04:31 Itd=nburgaransomware.net_1666950984 Delete Snapshot 41.77 ata-in-transit encryption (DTE) is disabled for the client (nbuor og delete snapshot processing arted us: 0 elete Snapshot; elapsed time 0:01:40 us: 0: the requested operation was successfully completed	ra.ransomware.net) as the global	DTE mode is set to 'Preferred Off' and the	
Operation Status: 0 Operation Status: 0 The requested operat	ion was succes	ssfully completed.()			-

3. 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.

SI	Pairs TI Root	Volumes C	onsistency (Groups Snapshot G	roups								
	reate TI Pairs	Operate TI Pa	irs View Pai	ir Synchronization Rate	More Actions 🔻						Select	ed: 0 d	of 1
1	Filter ON OFF	Select All P	ages Column	Settings						Options 👻 🔣	€ 1	/1	>))
	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			

TI Pairs							TOX
\$ TI Pairs				_			
\$Filter ON OFF S	Select All Pages				Opti	ions 🔻 Ѥ 🗲 1 🛛 / 1	⇒ ⋺
		Secondary \	/olume				
Snapshot Date	Snapshot SLU ID	LDEV ID	LDEV Name	Port ID	Host Group Name / iSCSI Target Alias	iSCSI Target Name	LUN I
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)	146	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 JD	NB16660763710544598844	CL1-A	1A-G00 (00)	•	7

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

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

4. 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:

 Job Details: 771@NBU.rar	somware.net				_	•	x
Job ID:	771	Job State:	Done (Successful)				
Job Overview Detai	led Status Job Hierarchy						
Attempt:	1		Attempt Started:	Oct 28, 2022 6:03:41	AM		
Job PID:			Attempt Elapsed:	00:19:09			
Storage Unit:	MSDP-media		Attempt Ended:	Oct 28, 2022 6:22:50	AM		
Media Server:	NBUMEDIA.ransomware.net		KB/Sec:				
Media Transport Type	: LAN						
Status:							
Current Kilobytes Writ Current Kilobytes Writ	 Info nbjm (pid=2557) starting backup job (Info nbjm (pid=2557) requesting STANDAR, requesting resource NBU-ransomware.net NE granted resource NBU-ransomware.net NE granted resource NBU-ransomware.net NE granted resource MSDP-media eganated resource MSDP-media estimated 0 kbytes needed begin Parent job begin SnapDupe Mount:Read File List end SnapDupe Mount:Read File List, elapse begin SnapDupe Mount:Read File List, Info RUNCMD (pid=25355) started end SnapDupe Mount:Deferred Resource d end SnapDupe Mount:Deferred Resource d end SnapDupe Mount:Deferred Resource info RUNCMD (pid=25375) The data-in-transit begin SnapDupe Mount:Deferred Resource d end SnapDupe Mount:Deferred Resource info RUNCMD (pid=2577) The data-in-transit linfo bybrm (pid=24752) The data-in-transit linfo bybrm (pid=24752) rhouar.ansorwa linfo bybrm (pid=24752) rhouar.ansorwa 	obid=771) for client nbuora.ransomware.net, policy sta D_RESOURCE resources from RB for backup job (jobid=7: N.BU_CLIENT.MAX/08S.nbuora.ransomware.net IU_CLIENT.MAX/00S.nbuora.ransomware.net IU_CLIENT.MAX/00S.nbuora.ransomware.net Iu/CLIENT.MAX/00S.nbuora.ransomware.net Iu/CLIENT.MAX/00S.nbuora.ransomware.net Iu/CLIENT.Max/00S.nbuora.ransomware.net iu/client.Max/00S.nbuora.ransomware.net iu/client.max ed time 0:00:00 er :CPE.ransomware.local upsed time 0:03:24 elapsed time 0:00:00 ransomware.net_1666950984 encryption (DTE) is disabled for the client (nbuora.rans re.net is the host to backup data from	ndard_nbuclient, schedule f 71, request id: {CC8D8EA2-5 reDiskVolume;StorageServer onware.net) as the global (0 1	uli 16A7-11ED-AEDC-843E4 r=NBUMEDIA.ransomwa DTE mode is set to 'Pre	DOAE373	۲) ediaSer ۴ and tl	ver •
Current File:			-				
			Trouble	eshooter			

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

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

5. 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:		<u>m</u>		Attempt Started:	Oct 28, 2022 6:37:41 AM
Job PID:				Attempt Elapsed:	00:14:03
Storage Unit:	MSDPC-stu			Attempt Ended:	Oct 28, 2022 6:51:44 AM
Media Server:	NBUMEDIA.r	ransomware.net		KB/Sec:	
Media Transport	Type: LAN				
Status:					
Oct 28, 2022 6:37 Oct 28, 2022 6:38 Operation Status: Oct 28, 2022 6:38 Oct 28, 2022 6:38	41 AM - Info nbjm (pid 41 AM - Info nbjm (pid 41 AM - requesting re 41 AM - requesting re 41 AM - requesting re 41 AM - granted reso 41 AM - granted reso 41 AM - granted reso 41 AM - begin SnapDu 41 AM - begin SnapDu 41 AM - hedgin SnapDu 41 AM - end SnapDup 41 AM - end SnapDup 66 AM - end SnapDup 00 AM - hedgin SnapDu 00 AM - end SnapDup 66 AM - end SnapDup 66 AM - begin SnapDu 66 AM - begin SnapDu 00 AM - hedgin SnapDu 66 AM - end SnapDup 66 AM - begin SnapDu 00 AM - hito bab/m (pid 24 AM - started proce 33 AM - Info bab/m (pid 24 AM - started proce 33 AM - Info bab/m (pid AM - Info bab/m	d=2557) starting backup job (jol d=2557) requesting STANDARD_ esource NBDrC-stu esource NBDrC-stu uncre NBU-ransornware.net.NBU uncre NBU-ransornware.net.NBU uncre MediaID=@aaaaw,DiskVol uncre MsDrC-stu kbytes needed ;job upe Mount:Read File List pe Mount:Read File List pe Mount:Read File List (pid=8732) started (pid=8732) started (pid=8732) exiting pe Mount:Infport Snapshot; elap; upe Mount:Deferred Resource; els upe Mount:Resource; els upe Moun	id=775) for client nbuora.ransomware.net, ESOURCE resources from RB for backup job BU_CLIENT.MAXJOBS.nbuora.ransomware.net CLIENT.MAXJOBS.nbuora.ransomware.net ime=veritas_vol:DiskPool=MSDPC-pool;Path time 0:00:00 sed time 0:00:25 upsed time 0:00:25 upsed time 0:00:00 isomware.net_1666950984 net js the host to backup data from ent shot processin Estimated Kilobytes: Estimated Files:	policy standard_nbuclient, schedule f (jobid=775, request id: {8CB7CEDC-5 : =veritas_vol;StorageServer=NBUMEDI buora.ransomware.net) as the global [0 1	ull 6AC-11ED-9640-FF62F119ED6A}) A.ransomware.net:MediaServer=NBUMEDL DTE mode is set to 'Preferred Off' and the
				Trouble	eshooter

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				8		
< veritas-ransomware veritas-ransomware / veritas_vol / data /						
Browse Overview Properties			Create Directory Upload Object	S		
	All Delete & Destroy					
Name	Size Modified	Owner	Storage class			
□ □ 1 <u>9</u>	**		STANDARD	:		
			STANDARD	3		
			STANDARD	1		
		(***)	STANDARD	1		
			STANDARD	:		
			STANDARD	:		
		**	STANDARD	:		

Folder 10 contains the backup data:

HITACHI S3 Console			R
< veritas-ransomware veritas-ransomware / veritas_vol / data / 10 / 211106232533010 / 2161727821138	302240.sobhd /		
Browse Overview Properties			Contro Directory I Helend Object
			Delete
Name	Size Modified	Owner	Storage class
	172 B 10/28/2022 10:29:38	Mousumi Ghosh	STANDARD :

Restoring a Snapshot Backup Job

Description before restoration

According to SLP-cloud configuration:

Storage lifecycle policy na	ime:	<u>D</u> ata cla	Data classification:		Priority for secondary operations:					
	<no da<="" th=""><th colspan="2"><no class="" data="" th="" 🔻<=""><th colspan="5">0 🕻 (higher number is greater pric</th></no></th></no>	<no class="" data="" th="" 🔻<=""><th colspan="5">0 🕻 (higher number is greater pric</th></no>		0 🕻 (higher number is greater pric						
		Chausan	Torget Mo	Window	Volume Pool	Madia Ow	Retention	Retentio		
Operation		Storage	Taryet Man	WIIIGOW	volume room	Media Owin	THOSE OF THE OF THE THE	1.000011010		
Operation Snapshot	MSDP	media		■			Fixed	2 weeks		
Operation Snapshot Backup From Snapshot	MSDP- MSDP-	media media		 Default 			Fixed Fixed	2 weeks 2 weeks		

				· · · · · · · · · · · · · · · · · · ·	4			
 X	1381 Backup From Snapshot	Done	0 SLF	SLP-Cloud	MSDPC-stu	full	1006	520,128 nbuora.ransomware.net
X∃	1380 Backup From Snapshot	Done	0 SLF	SLP-Cloud	MSDPC-stu	-		nbuora.ransomware.net
 X	1378 Backup From Snapshot	Done	0 SLF	SLP-Cloud	MSDP-media	full	1006	520,128 nbuora.ransomware.net
X≞	1377 Backup From Snapshot	Done	0 SLF	SLP-Cloud	MSDP-media	-		nbuora.ransomware.net
 X	1376 Snapshot	Done	0 sta	ndard 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 <u>Malware detection before recovery</u> section.
- 2. To verify whether the deleted file is restored or not, manually remove the file from the client machine that was backed up.



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.

NULransomware.net (Master Server Backup, Archive, and Restors Actint: Verify Search Results NULransomware.net (Master Server Actin: Verify Actin: Verify Metda kup Mangement Problems Metda host: Copres: Copy 2 Copres: Copy 2 Copres: Copy 2 Problems Metda log: Metda Log Entries Metda host: Problems Obik Type: Disk pol: Pape Reports Problems Call Medda Hosts> Call Policites> Policy type: Call Media Hosts> Call Media Hosts> Policy type: Call Media Hosts> Call Media Hosts> Call Media Hosts> Call Media Hosts> Call Media Hosts> Call Media Hosts> Call Media Hosts> Call Media Hosts> Call Media Hosts> Call Media Hosts Call Media Hosts Call Media Hosts Call Media Hosts Call Media Hosts Call Medi					_		
Rebut cansonware, net (Master Server) Activity Montor Baskcoby, Active, and Restore Activity Montor Media Activity Montor Media host: Copies: Copies: Copies: Copies: Media ID: Media host: Copies: Copies: All Log Entries Disk Poper Disk Poperts Copies: Media ID: Copies: Oisk Type: Disk pool: Disk Poperts Oisk Type: Disk Poperts Call Media host: Oisk Type: Disk pool: Disk Reports Call Media host: Oisk Type: Disk pool: Disk Reports Call Media host: Oisk Type: Disk pool: Disk Reports Call Media host: Oisk Type: Disk pool: Disk Type: Call Media host: Oisk Type: Disk pool: Disk Type: Call Media host: Oisk Type: Call Media host: Oisk Type: Call Media host: Oisk Type: Call Media host: Disk Type: Call Media host: <th>NBU.ransomware.net (Master Se</th> <th>Search Results</th> <th></th> <th></th> <th></th> <th></th> <th></th>	NBU.ransomware.net (Master Se	Search Results					
Backup, Archwe, and Restore Activity Mentior Nettactup Management Propertis Case Maximum Problems Case Maximum Problems Case Maximum Problems Case Maximum	BU.ransomware.net (Master Server	Action:					
Addwig weiling P Reports Copy 2	Backup, Archive, and Restore	Verify					
Media Copres: Copres: Copres: Co	NetBackup Management	[,					
Status of Backups Media ID: Media host: Copy 2 Policy Traine: All> Copy 2 Policy Traine: All Policides Policy Type: Disk pool: Disk Pool: Policy Type: Call Policies Policy Type: Call Policies Policy Type: Policy Type: Call Policy Type: <td></td> <td>Media</td> <td></td> <td></td> <td></td> <td>Copies:</td> <td></td>		Media				Copies:	
All> All> Policy name: All Log Entries Disk Type: Disk pool: Disk Type: Disk pool: Policy runne: All Log Entries Disk Type: Disk pool: Disk Reports All> All> All Redia Hosts> All> All> Disk Reports All> All> All Redia Hosts> All> All> Policy Type: All> All> All Redia Hosts> All> All> All Redia Hosts> All> All> Policy Type: All Policy Types> All All Redia Hosts> All> Duplicate Policy Type: All Media Hosts> All> Biolicies All Media Hosts Duplicate Biolicies Distroperial Distroperial Distroperial Biolicies Distroperial Distroperial Distro	🗌 🕤 Status of Backups	Media ID:	Media host:			Сору 2	-
All Policies A	- 🚨 Client Backups		- All Media Hector			Policy name:	
I log Entries Disk Type: Disk pool: Policy type: I log Entries I log Entries I log Entries I log Entries Policy type: I log Entries I log Entries I log Entries I log Entries Policy type: I log Entries Policy type: </td <td>- A Problems</td> <td>SAIL></td> <td>CAIL MEDIA HOSES</td> <td></td> <td>1</td> <td><all policies=""></all></td> <td></td>	- A Problems	SAIL>	CAIL MEDIA HOSES		1	<all policies=""></all>	
Point Probasical Storage Life Storage L	All Log Entries	🔾 🔾 Disk Type:	Disk pool:			Dellas har as	
Image Regists Image Regists<	Media Logs	Dasichiek			1_	Policy Lype:	
I bick Reports Image: Path: Image: Pa	- 🖬 Tape Reports				-	<all policy="" types=""></all>	
Columns C	🕶 🛄 Disk Reports	Media server:	Path:	🛃 Verify		Type of backup:	
Bolicies	🗢 🞯 Vault Reports	<all hosts="" media=""></all>	<all></all>	Duplicate		<all backup="" types=""></all>	
Sudrage Units Storage	- OI Policies			M Expire Delete	e	Client (host name):	
	Storage Linits			🖉 Initiate Import		nbuora.ransomware.net	-
Image: Storage Lifecycle Policies From: Oct 27, 2022 11:21:02 From: Oct 27, 2022 11:20:02 From: Oct 27, 2022 11:20:02 From: Oct 27, 2022 11:59:59 From: Oct 27, 202 Oct 28, 202	🗢 🌚 Storage Unit Groups 🗧	Date/Time Range		# Import		Job Priority	
Image: Start Mindows Image: Start Mindows Image: Start Mindows Ima	- 🐻 Storage Lifecycle Policies	From: Oct 27, 2022 11:21:02 P		Set Drimary Conv		Override default priority	
Catalog 100. Uct 30. 2022 11:9959 m m m Ub Sopy To Clipboard Cetc Ioo Priority 2300 m Matter Servers Columns Columns (higher number is greater priority) Ioo Priority Matter Servers Search Results: 1 backup image(s) found (1 selector) Filter Cut Pilter Cut Pilter Deck Moxing Backup ID Search Results: 1 backup image(s) found (1 selector) If clear Filter Policy Schedule Name	SLP Windows	To: Out on anonal second		M get rimary copy			
Image: Search Results: 1 backup image(s) found (1 selected) Image: Search Results: 1 backup image(s) found (1 selected	Catalog	Oct 30, 2022 11:59:59 P		Copy To Clipboard Ctri-C		Job Priority	
Bendela Storers Spart Bendela Storers Spart Bendela Storers Spart Bendela and Derke Management Search Results: 1 backup image(s) found (1 selector) Policy Schedule Name Work (and the second s	A Moster Servers			Columns	•	(higher number is greater priority)	
Applications Search Results: 1 backup image(s) found (1 selected) Search Results: 1 backup image(s) found (1 selected) Chart Search Results: 1 backup image(s) found (1 selected) Chart Chart Search Results: 1 backup image(s) found (1 selected) Chart Chart Search Results: 1 backup image(s) found (1 selected) Chart Chart Search Results: 1 backup image(s) found (1 selected) Chart Search Results: 1 backup image(s) found (1 selected) Chart Search Results: 1 backup image(s) found (1 selected) Chart Search Results: 1 backup image(s) found (1 selected) Chart Search Results: 1 backup image(s) found (1 selected) Search Results: 1 backup i	-Bit Media Servers			2 Sort			Holp Coarde Now
Clear Filter Standard obucient full Search Results: 1 backup image(s) found (1 selected) Y Filter Crist Search Results: 1 backup image(s) found (1 selected) Y Filter Crist Search Results: 1 backup image(s) found (1 selected) Y Filter Crist Search Results: 1 backup image(s) found (1 selected) Y Filter Crist Search Results: 1 backup image(s) found (1 selected) Y Filter Crist Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Filter Search Results: 1 backup image(s) found (1 selected) Y Fi	🗳 Clients			Find Ctrl-F			Teh Zearch Mow
Media and Device Management Backup ID Primer: Const Policy Schedule Name WORM Unlock Time Primary Copy Clear Filter const standard phyclent full No	- Applications	Search Results: 1 backup ima	ne(s) found (1 selected)				D.
Clear Filter Chu Schedule Value Schedule Value Volume Value Volue Volume Value	Media and Device Management Device Management	Backup ID		The Filter		Poliny Schedule Name	WORM Unlock Time Primary Com
	Media	nbuora ransorrware net 1666950	0985 Oct 28, 20	X Clear Filter Ctrl-U		standard nbuclient full	No.

2. Set Primary Copy to Yes.

NBU ransomware net (Master Se	Search Posults					
BNBU ransomware net (Master Server*	A diam					
Backup, Archive, and Restore	ACLION					
- 🖪 Activity Monitor	Verity					
🕈 🛄 NetBackup Management	Media		Conies:			
Status of Backups	Media ID: Media	host.	Copy 2			
- Client Backups	· Ficula ID.	ilost.	Delley name:			
- A Problems	<all></all>	edia Hosts>	Policy name:			
- 🐚 All Log Entries	O plate Turner		<all policies=""></all>			•
- 🔐 Images on Media	Uisk Type: Disk pi	001:	Policy type:			
- 😼 Media Logs	BasicDisk 👻 <all></all>		<all policy="" types=""></all>			-
🗠 📾 Tape Reports	Media server: Path:		Type of backup:			
 Disk Reports 			туре от васкар.			
 We vault Reports Relision 	<all hosts="" media=""> <a <="" a="" href="mailto:selic"></all>	*	«All Backup Types»			×
Storage			Client (host name):			
Storage Units			nbuora.ransomware.net			-
Storage Unit Groups =	Date/Time Range		lob Priority			
- R Storage Lifecycle Policies	From: Oct 27 2022 11:21:02 P		Override default priority			
- 🔁 SLP Windows			ogernde deradit priority			
- 🍋 Catalog	To: Oct 30, 2022 11:59:59 P		Job Priority			
Host Properties	k .		(higher number is greater p	(iority)		
- Master Servers						
Hedia Servers					Help	Search Now
Clients						
- Madia and Device Management	Search Results: 1 backup image(s) found	(0 selected)				Ø
Device Monitor	Backup ID	Date	Policy	Schedule Name	WORM Unlock Tim	Primary Copy
Media	nbuora,ransomware.net 1666950985	Oct 28, 2022 5:56:25 AM	standard nbuclient	full		Yes
- Devices			- wooneric			

3. Select the source and destination client for restoring

Specify NetBackup	Machines and Policy Typ	e@NBU.ransomware.net		x
Server to use fo	r backups and res	tores:		
NBU.ransomwa	re.net	-	Edit Server List	
Source client for	r restores:			
nbuora.ransom	ware.net	-	Edit Client List	Re <u>f</u> resh
			Search <u>V</u> M Clients	
Destination clie	nt for restores:			
nbuora.ransom	ware.net	~		
Policy type for r	estores:			
Standard		-		
			•	
			<u></u>	<u>Cancel</u> <u>H</u> elp
ile Edit View Actions Help	a			Login Activity
NBU.ransomware.net (Master Se NBU.ransomware.net (Master Server	NetBackup server: NBU.ransomware.net	Source client: nbuora.ransomware.net	Destination client: nbuora.ransomware.net	Policy type: Standard
Sackup, Archive, and Restore	Backup Files Restore Files	Task Progress		
	Normal Backups			
Client Backups Problems All Log Entries	<none></none>	4	Star Oct 2	28, 2022 5:56:25 AM Oct 28, 2022 5:56:25 AM
Images on Media	/ Directory Structure			
← Tape Reports Disk Reports	⊷ ₩ h	Name Backup Date	Size(Bytes) Modified Schedule Type	Policy Image Format Data Move
 ♥ Vault Reports ♥ Policies ♥ ■ Storage 		Inux_FS Oct 28, 2022 5:56:25 AM	Oct 28, 2022 Full Backup	standard_nbuclient Snapshot VSO

							A C A
Content	s of selected directory					Se	arch
Name	Backup Date	Size(Bytes)	Modified	Schedule Type	Policy	Image Format	Data Mover
Inux	FS Oct 28, 2022 5:56:25 AM	0.20(0)(00)	Oct 28, 2022	Full Backup	standard_nbuclient	Snapshot	VSO
•							•
						Preview	Restore

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

neral estination			
Restore everything to its original Restore everything to a different	t location (maintaining existin	ng structure).	
vestination:			
Restore individual directories an	d files to different locations.		
Source	Destination	Backup Date	Modified
Source	Destination	Backup Date Oct 28, 2022 5:56:25 AM	Modified Oct 28, 2022 6:39:50 AM
Source	Destination	Backup Date Oct 28, 2022 5:56:25 AM	Modified Oct 28, 2022 6:39:50 AM
Source	Destination	Backup Date Oct 28, 2022 5:56:25 AM	Modified Oct 28, 2022 6:39:50 AM

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

Backup Files Restore Files Tas Tasks Performed Job Id e 614 615 e 618 782	k Progress Task Restore Restore Restore Restore Restore	Date Oct 13, 2022 12:17:27 AM Oct 13, 2022 12:24:52 AM Oct 13, 2022 11:39:48 AM Oct 30, 2022 11:24:32 PM	Search Successful Successful Successful
Job Id Ø 614 Ø 615 Ø 618 Ø 782	Task Restore Restore Restore Restore	Date Oct 13, 2022 12:17:27 AM Oct 13, 2022 12:24:52 AM Oct 13, 2022 11:39:48 AM Oct 30, 2022 11:24:32 PM	Search Successful Successful Successful
jobid 2 614 2 615 2 618 - 782	Task Restore Restore Restore Restore	Date Oct 13, 2022 12:17:27 AM Oct 13, 2022 12:24:52 AM Oct 13, 2022 11:39:48 AM Oct 30, 2022 11:24:32 PM	Successful Successful Successful Successful
 ☑ 614 ☑ 615 ☑ 618 ☑ 782 	Restore Restore Restore Restore	Oct 13, 2022 12:17:27 AM Oct 13, 2022 12:24:52 AM Oct 13, 2022 11:39:48 AM Oct 30, 2022 11:39:48 AM	Successful Successful Successful
 ✓ 615 ✓ 618 ✓ 782 	Restore Restore Restore	Oct 13, 2022 12:24:52 AM Oct 13, 2022 11:39:48 AM Oct 30, 2022 11:24:32 PM	Successful Successful
 € 618 ☐ 782 	Restore Restore	Oct 13, 2022 11:39:48 AM Oct 30, 2022 11:24:32 PM	Successful
782	Restore	Oct 30, 2022 11:24:32 PM	
			In Progress
•	III:		
Results of the Task Selected Above			
🕼 🗹 Auto Refresh Rate (second	ds): 10 🕻		
Progress log filename : /usr/openv/netba Restore started 10/30/2022 23:23:38	ckup/logs/user_ops/root/logs/jbp-254406	67186618712799000000014-CKqi6k.log Restore	Job Id=782
23:25:07 (782.xxx) Found (2) files in (1) i 23:25:34 (782.xxx) Searched (2) files of (mages for Restore Job ID 782.xxx (2) files for Restore Job ID 782.xxx		
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 Select	ed Above		
Auto Refresh Rat	te (seconds): 10 👙		
Progress log filename : /usr/o	penv/netbackup/logs/user_ops/root/logs/jbp-25440	667186618712799000000014-CKqi6k.log Restore Job Id=7	82
23:28:03 (782.001) Ignoring F	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/f	file_text.txt		
23:29:14 (782.001) INF - TAR I	RESTORED 1 OF 2 FILES SUCCESSFULLY		
23:29:14 (782.001) INF - TAR 23:29:14 (782.001) INF - TAR	KEPT 1 EXISTING FILES PARTIALLY RESTORED 0 FILES		× .
00.00.14 (700.001) Chatura af	restore from some 2 of import overhead 5rd 20 Oct 20		k
23:29:14 (782.001) Status of	restore from copy 2 of image created Fri 28 Oct 20	122 UD:D0:20 AM EDT = the requested operation was succe	ssiully 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-rr 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.



1. Set the copy 3 image as primary copy.

Backup ID

Date

nbuora.ransomware.net_1666950985 Oct 28, 2022 5:56:25 AM standard_nbuclient full

Action: Verify Media O Media host: Copy 3 Copy 3 Copy 3 Copy 3 Verify Copy 3 Verify Coll Policy types Verify Coll Policy types Verify Coll Policy types Verify Coll Policy types Verify Ver	Search Results				
Verify • • Media D: Media host: Copies: • Media ID: Media host: Copy 3 • • All Media Hosts> • Policy name: < • All Policy name: < • • Disk Type: Disk pool: • Policy name: • • Policy type: • Policy type: <td< th=""><th>Action:</th><th></th><th></th><th></th><th></th></td<>	Action:				
Media Disk Media ID: Media host: CAll Media Hosts> CAll Media Hosts> O Disk Type: Disk pool: PureDisk Valume: CAll Policy Types> Valume: CAll Policies> Media Hosts> Valume: Call Policies> Valume: Valume: </td <td>Verify</td> <td></td> <td></td> <td></td> <td></td>	Verify				
○ Media ID: Media host: Copy 3 ▼ CAII> CAII Media Hosts> Policy name: CAII Policies> ▼ PureDisk ✓ cAII> ✓ cAII> Policy Types> ▼ Media server: Volume: ✓ Verify packup: ▼ CAII Media Hosts> ✓ cAII> ✓ Duplicate packup: ▼ CAII Media Hosts> ✓ cAII> ✓ Duplicate packup: ▼ CAII Media Hosts> ✓ cAII> ✓ Duplicate packup: ▼ Cot 20, 2022 11:59:59 F ✓ Se Primary Copy ride default priority ▼ To: Oct 29, 2022 11:59:59 F ✓ ✓ Figure 10 Cot 28, 2022 5:56:25 AM standard_robucilent Tuli Cot 11, 2022 5:50:02 AM No NBUMEDIA Nov 11, 2022 4:5 Yes @ aaaaw	Media			Copies:	:
CAll> Call Media Hosts> • Disk Type: Disk pool: PureDisk PureDisk • Call Policies>	🔾 Media ID:	Media host:		Сору З	· · · · · · · · · · · · · · · · · · ·
• Disk Type: • Disk pool: • Disk pool: • Policites> • Oligot type: • Oligot typ	<all></all>	All Media Hosts>	*	Policy n	name:
Point Type: Point Type: PureDisk PureDisk All> All Media Hosts> Backup Io Columns K End Cut+f Columns K End Cut+f Backup ID Date Date P Clear Filter Cut+f Nov	Disk Type:	Disk pool:		<all pol<="" td=""><td>licies></td></all>	licies>
Pure tooks < <all> < <all policy="" types=""> < <</all></all>	Burspiel			Policy ty	ype:
Media server: Volume: P Vgrly packup: c.All Media Hosts> v <all> buplicate buplicate for Types> Date/Time Range Imitiate Import ransomware.net v v From: Oct 26, 2022 4:20:06 AM Se Primary Copy ride default priority v Imit Ort Tity ride default priority v Columns mumber is greater priority) mumber is greater priority) Search Results: 1 backup image(s) found (1 selected) V Filter CHF Backup ID Date P Clear Filter Column CHF Help Search Results: 1 backup image(s) fourd (1 selected) V Filter CHF Backup ID Date P Clear Filter CHF Help Search Now Nov 11, 2022 5:50:02 AM No NBUMEDIA Nov 11, 2022 4:5 Yes @aaaaw</all>	Purebisk	<all></all>	A	<all po<="" td=""><td>licy Types></td></all>	licy Types>
Image: Second Results: 1 backup image(s) found (1 selected) V Filter Celer Ce	Media server:	volume:	Puplicato		packup:
Date/Time Range Initiate Import ransomware.net Import From: Oct 26, 2022 4:20:06 Ab Import rity To: Oct 29, 2022 11:59:59 F Import Import Search Results: 1 backup image(s) found (1 selected) V Filter CtH Backup ID Date V Filter CtH Backup ID Date V Clear Filter CtH Novular.aransomware.net 1666950985 Oct 28, 2022 5:56:25 AM standard_nouclient Tull Nov 11, 2022 5:50:02 AM No NBUMEDIA Nov 11, 2022 4:5, Yes	<all hosts="" media=""></all>	<all></all>	Evpire	Delete	kup types>
Date/Time Range Import rity From: Oct 26, 2022 4:20:06 Ah See Primary Copy ride default priority To: Oct 29, 2022 11:59:59 P See Originary Copy ride default priority Search Results: 1 backup image(s) found (1 selected) Y Filter Celum Ctrice Backup ID Date P Clear Filter Chear Filter Chear Filter Chear Filter Backup ID Date P Clear Filter Chear Filter Chear Filter Chear Filter Chear Filter Backup ID Date P Clear Filter Chear Filter <td></td> <td></td> <td>Dinitiate Import.</td> <td></td> <td>ransonware net</td>			Dinitiate Import.		ransonware net
From: Oct 26, 2022 4:20:06 AN Image: See Primary Copy ride default priority To: Oct 29, 2022 11:59:59 P Image: See Primary Copy ride default priority Columns Image: See Primary Copy Image: See Primary Copy ride default priority See characterization Image: See Primary Copy Image: See Primary Copy Image: See Primary Copy See characterization Image: See Primary Copy Image: See Primary Copy Image: See Primary Copy See characterization Image: See Primary Copy Image: See Primary Copy Image: See Primary Copy See characterization Image: See Primary Copy Image: See Primary Copy Image: See Primary Copy See characterization Image: See Primary Copy Image: See Primary Copy Image: See Primary Copy See characterization Image: See Primary Copy Image: See Primary Copy Image: See Primary Copy See characterization Image: See Primary Copy Image: See Primary Copy Image: See Primary Copy Backup ID Date P Clear Filter Chi-U Image: See Primary Copy Inbuora.ransormware.net_1666950965 Oct 28, 2022 5:56:25 AM standard_nouclient Tull Nov 11, 2022 5:50:02 AM No NBUMEDIA Nov 11, 2	Date/Time Range		Ja Import	21	rity
To: Oct 29, 2022 11:59:59 F	From: Oct 26, 2022 4:20:06 AN	3	Set Primary Cop	У	ride default priority
Columns number is greater priority) Line Line Search Results: 1 backup image(s) found (1 selected) Filter Backup ID Date P Citer Filter Char Filter Ctrlu VORM Unlock Time Primary Copy/Media Server Expiration Date P ORM Unlock Time Primary Copy/Media Server Expiration Date P ORM Unlock Time Nov 11, 2022 5:50:02 AM No NBUMEDIA Nov 11, 2022 4:5 Yes	To: Oct 29, 2022 11:59:59 P	3	Copy To Clipboa	rd Ctrl-C	rity75000 ^
Search Results: 1 backup image(s) found (1 selected) ▼ Filter Ctri-F Backup ID Date P ✓ Clear Filter Ctri-U Nbuora.ransomware.net_1666950985 Oct 8, 2022 5:56:25 AM standard_nbuclient Tull Nov 11, 2022 5:50:02 AM No NBUMEDIA Nov 11, 2022 4:5 Yes			Columns		number is greater priority)
Search Results: 1 backup image(s) found (1 selected) Y Filter Ctrl-T Backup ID Date P Y Clear Filter Ctrl-U Nov 11, 2022 5:50:02 AM No NBUMEDIA Nov 11, 2022 4:5 Yes			2: S <u>o</u> rt		
Search Results: 1 backup image(s) found (1 selected) Y Filter Ctrl-T Ctrl			🙀 <u>E</u> ind	Ctrl-F	<u>H</u> elp <u>S</u> earch Now
Backup ID Date P Clear Filter Ctrlu ORM Unlock Time Primary Copy Media Server Expiration Date Immutable nbuora.ransomware.net_1666950985 Oct 82, 2022 5:56:25 AM standard_nbucilent Tull Nov 11, 2022 5:50:02 AM No NBUMEDIA Nov 11, 2022 4:5 Yes @aaaaw	Search Results: 1 backup image(s) found (1 selected)	🝸 Filter	Ctrl-T	<u>م</u>
nbuora.ransorrware.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 @aaaaw	Backup ID	Date	P 🛒 Clea <u>r</u> Filter	Ctrl-U	ORM Unlock Time Primary Copy Media Server Expiration Date Immutable
	nbuora.ransomware.net_1666950985	0ct 28, 2022 5:56:25 AM	standard_nbuclient_full	Nov	/11, 2022 5:50:02 AM No NBUMEDIA, Nov 11, 2022 4:5 Yes @aaaaw
		16 170 1 1 1			

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

Policy

 Schedule Name
 WORM Unlock Time
 Primary Copy
 Media Server
 Expiration Date
 Immutable

 nt full
 Nov 11, 2022 5:50:02 AM Yes
 NBUMEDIA... Nov 11, 2022 4:5... Yes

Destination			
O Restore everything to its origin	al location.		
Restore everything to a differer	nt location (maintaining existi	ng structure).	
Destination: /linux_ES/HCPCS/			
 Restore individual directories and 	nd files to different locations.		
Source	Destination	Backup Date	Modified
/		Oct 28, 2022 5:56:25 AM	Oct 28, 2022 6:39:50 AM
Channe Selecte	d Destination(s)	Chan	ne All Destinations
C <u>h</u> ange Selecte Add Des	d Destination(s)	Chang	ge All <u>D</u> estinations Selected Destination(s)
Change Selecte Add Des O Create and restore to a new v	d Destination(s) stination virtual hard disk file.	Chang Remove	ge All <u>D</u> estinations Selected Destination(s)
Change Selecte Add Des Create and restore to a new v	d Destination(s) stination virtual hard disk file.	Chang Remove	ge All <u>D</u> estinations Selected Destination{s}
Change Selecte Add Des O Create and restore to a new v	d Destination{s} stination virtual hard disk file.	Chang Remove	ge All <u>D</u> estinations Selected Destination{s} Se Se
Change Selecte Add Des Create and restore to a new v Options Overwrite existing files	d Destination(s) stination virtual hard disk file.	Chang Remove Media (Def	ge All <u>D</u> estinations Selected Destination(s) Seaserver ault)
Change Selecte Add Des Create and restore to a new v Coptions Overwrite existing files	d Destination(s) stination virtual hard disk file.	Chang Remove : Media (Def	ge All <u>D</u> estinations Selected Destination(s) Selected Destination(s) Selected Destination(s)
Change Selecte Add Des Create and restore to a new v Create and restore to a new v Options Overwrite existing files Restore directories without cross Restore without access-control	d Destination(s) stination virtual hard disk file. ssing mount points attributes (Windows clients o	Chang Remove : Media (Def	ge All <u>D</u> estinations Selected Destination(s) Selected Destination(s) Selected Destinations Selected Destinations
Change Selecte Add Des Create and restore to a new v Create and restore to a new v Options Overwrite existing files Restore directories without cross Restore without access-control Rename hard links	d Destination(s) stination virtual hard disk file. ssing mount points attributes (Windows clients o	Chang Remove : Media (Def	ge All Destinations Selected Destination(s) Selected Destination(s) Server a Server ault) erride default priority

Restoration is completed successfully from copy 3.

783	Restore	Oct 31, 2022 12:36:44 AM	Successful
	III		
Results of the Task Selected Above			
🖉 🗆 Auto Refresh Rate (seconds)	: 10 🗘		
Progress log filename : /usr/openv/netback	up/logs/user_ops/root/logs/jbp-:	11857667190949820536000000027-FgNfBV.log Restore Job Id=783	
Restore started 10/31/2022 00:35:49			
00:42:36 (783.001) Changed /linux FS/ to /l	inux ES/HCPCS/linux ES/		
00:42:36 (783.001) /linux FS/file text.txt			
00:42:36 (783.001) Changed /linux_FS/file_t	ext.txt to /linux_FS/HCPCS/linux_	FS/file_text.txt	
00:42:36 (783.001) INF - TAR EXITING WITH 9	STATUS = 0		
00:42:36 (783.001) INF - TAR RESTORED 2 0	F 2 FILES SUCCESSFULLY		
00:42:36 (783.001) INF - TAR KEPT 0 EXISTIN	IG FILES		
00:42:36 (783.001) INF - TAR PARTIALLY RES	TORED 0 FILES		
	and the set of the set		with a second state of
00:42:36 (783.001) Status of restore from (copy 3 of image created Fri 28	Oct 2022 05:56:25 AM EDT = the requested operation was successf	ully completed

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.

NBU.ransomware.net (Master Se	Search Results								
BU.ransomware.net (Master Server	Action:								
Backup, Archive, and Restore	Verify								
Activity Monitor	verny								
P B Deperts	Media				Copie	s:			
Status of Baskups	Modia ID:	Madia bost			Conv	1			
Client Backups	e Media ID.	media nost.			copy	1			
A Problems	<all></all>	<all hosts="" media=""></all>			Policy	/ name:			
All Log Entries					<all f<="" td=""><td>Policies></td><td></td><td></td><td>-</td></all>	Policies>			-
Images on Media	Disk Type:	Disk pool:			Policy	type:			
- Media Logs	Residuek	-Alls			Foncy	rype.			
- E Tape Reports		-section			<all f<="" td=""><td>Policy Types></td><td></td><td>,</td><td>•</td></all>	Policy Types>		,	•
Disk Reports	Media server:	Path:			Туре	of backup:	Verify		
- 🚱 Vault Reports	<all hosts="" media=""></all>	<all></all>		*	<all e<="" td=""><td>Backup Types></td><td>P Duplicate</td><td></td><td>*</td></all>	Backup Types>	P Duplicate		*
- 💁 Policies					Client	(host name)	El Cumiro	Delate	
🕈 📼 Storage					Chern	t (nost nume).	Fail Expire	Develue	
- 🔤 Storage Units	L				nbuo	ra.ransomware.net	Initiate Import		`
🗢 🥸 Storage Unit Groups 👘	Date/Time Range				Job	Priority	Import		
Storage Lifecycle Policies	From: Oct 27, 2022 11:21:02 P				0	verride default priority	Set Primary Conv		
SLP Windows									
- 🎦 Catalog	OCT 30, 2022 11:59:59 P				JOD P	riority	Copy To Clipboard	Ctrl-C	
9 3 Host Properties					(high	ner number is greater p	Columns	•	
- J Master Servers							** Sort		
- Call Media Servers									Help Search Now
							A Eind	Ctrl-F	
Applications	Search Results: 1 backup image(s)) found (1 selected)					V Filter	Ctrl-T	D.
Device Monitor	Backup ID	Date	Policy	Schedule	Name	WORM Unlock Time	T Class Filter	Chilli	r Media ID
- Media	nbuora ransorrware net 1666950985	Oct 28, 2022 5:56:25 AM	standard nhuclient	full			∦r clea <u>r</u> Filter	CUPO	net /linux ES
Bouters	industrial office_1000000000	000 201 2022 0100120 AM	Standard Indenent				insubianal		and a second second

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

NetBackup server: NBU.ransomware.net	Source client nbuora.rans	Source client: Destination client: Policy type: nbuora.ransomware.net nbuora.ransomware.net Standard			R			
Backup Files Restore Files	Task Progress							
Restore type: Point in Time Rollback					Star Oct 2	t date: 28, 2022 5:56:25 AM	End date: Oct 28, 2022 5:5	6:25 AM 🔳 🔳
Browse directory:	4							13 I m
Directory Structure	Contents of se	lected directory					Sear	ch 🍸
	Name	Backup Date	Size(Bytes)	Modified	Schedule Type	Policy	Image Format	Data Mover

All eligible snapshots are included in the list:

NetBackup	server:	Source cli	ent:		Destination client:	
NBU.rans	Date Range@NBU.ransomw	are.net				X
Backup F						
Restore to	Point in Time Rollback	Backup Image	es			
Point in T	Backup Date	Expires	Files	Size(KB) Compress	s Schedul Policy Inte	llige Keyword
FOILT	Oct 28, 2022 5:56:25 AM	Nov 11, 2	2	32 No	Full Back standard No	A
Keyword	Oct 18, 2022 2:59:32 AM	Nov 1, 2022	2	32 No	Full Back standard No	
<none></none>	Oct 18, 2022 1:12:51 AM	Nov 1, 2022	2	32 No	Full Back test_malw No	
Browse d	Oct 17, 2022 6:44:46 AM	Oct 31, 2	2	32 No	Full Back test_malw No	
/	Sep 29, 2022 4:42:34 AM	Dec 31, 3	1	32996 No	Full Back standard No	=
Director	Sep 29, 2022 4:36:26 AM	Dec 31, 3	1	32996 No	Full Back standard No	
∽□/>/	Sep 23, 2022 1:49:00 PM	Dec 31, 3	2	25275836 No	Full Back Linux No	
	Sep 23, 2022 1:20:56 PM	Dec 31, 3	2	25275648 No	Different Linux No	
	Sep 23, 2022 1:09:41 PM	Dec 31, 3	2	25275640 No	Full Back Linux No	
	Sep 23, 2022 12:11:55 PM	Dec 31, 3	2	25275600 No	Full Back Linux No	
	Sep 23, 2022 4:46:12 AM	Dec 31, 3	1	14448976 No	Full Back Linux No	
	Sep 23, 2022 4:39:39 AM	Dec 31, 3	1	14448924 No	Full Back Linux No	
	Sep 23, 2022 4:09:40 AM	Dec 31, 3	1	14448860 No	Full Back Linux No	
	Sep 22, 2022 6:00:00 PM	Dec 31, 3	1	14415508 No	Different Linux No	
	Sep 22, 2022 7:07:15 AM	Dec 31, 3	1	14393568 No	Different Linux No	
	Sep 21, 2022 6:44:21 PM	Dec 31, 3	1	33000 No	Different Linux No	
	Sep 20, 2022 11:05:42 PM	Dec 31, 3	1	60752 No	Full Back Linux No	
	500 20 2022 12:40-12 DM	Dao 11 1	1	COTED No.	Different Linux No	·

- 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.

estination				
Restore everything to its origina	l location.			
Restore everything to a different	t location (maintaining existin	g structure}.		
Destination:				
Restore individual directories an	d files to different locations.			
Source	Destination	Backup D	ate	Modified
/linux_FS/		Oct 28, 2022 5:56:25 /	AM	Oct 28, 2022 5:43:59 AM
C <u>h</u> ange Selected	Destination(s)		Change All	I <u>D</u> estinations
C <u>h</u> ange Selected <u>A</u> dd Dest	I Destination(s)		Change All	I <u>D</u> estinations cted Destination{s}
C <u>h</u> ange Selected <u>A</u> dd Dest ○ Create and restore to a new vi	I Destination(s) ination irtual hard disk file.	[Change All	I <u>D</u> estinations cted Destination{s}
C <u>h</u> ange Selected <u>A</u> dd Dest O Create and restore to a new vi	l Destination(s) ination irtual hard disk file.		Change Al emove Selec	I <u>D</u> estinations cted Destination(s) Settin
C <u>h</u> ange Selected <u>A</u> dd Dest O Create and restore to a new vi	l Destination(s) tination irtual hard disk file.		Change All emove Selec	l <u>D</u> estinations cted Destination{s} Settin
Change Selected Add Dest O Create and restore to a new vi Create and restore to a new vi Skip verification and force rollba	l Destination(s) tination irtual hard disk file. ck		Change All emove Selec	I <u>D</u> estinations cted Destination{s} Settin ver
Change Selected Add Dest Create and restore to a new vi Create and restore to a new vi Skip verification and force rollba Restore directories without cros	l Destination(s) tination irtual hard disk file. ck sing mount points	[Change All emove Selec Media Sen (Default)	I <u>D</u> estinations cted Destination{s} Settin
Change Selected Add Dest Create and restore to a new vi Create and restore to a new vi Skip verification and force rollbar Skip verification and force rollbar Restore directories without cros Restore without access-control a	l Destination(s) ination irtual hard disk file. ck sing mount points attributes (Windows clients of	<u></u>	Change All emove Selec Media Sen (Default)	I <u>D</u> estinations cted Destination{s} Settin
Change Selected Add Dest Create and restore to a new vi Create and restore to a new vi Skip verification and force rollbar Restore directories without cros Restore without access-control a Rename hard links	l Destination(s) tination irtual hard disk file. ck sing mount points attributes (Windows clients or	nły)	Change All emove Selec Media Sen (Default)	I <u>D</u> estinations cted Destination{s} Settin
Change Selected Add Dest O Create and restore to a new vi otions Skip verification and force rollbar Restore directories without cros Restore without access-control a Rename hard links Rename soft links	l Destination(s) ination irtual hard disk file. ck sing mount points attributes (Windows clients or	nły)	Change All emove Select Media Sen (Default)	I Destinations cted Destination(s) Settin ver default priority
Change Selected Add Dest O Create and restore to a new vi otions Skip verification and force rollbar Restore directories without cros Restore without access-control a Rename hard links Rename soft links	I Destination(s) ination irtual hard disk file. ck sing mount points attributes (Windows clients or	nly)	Change All emove Select Media Sen (Default) Job Priorit	I Destinations cted Destination(s) Settin ver default priority Settin Setti

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 A	bove		
🖉 🗆 Auto Refresh Rate (se	econds): 10 🗘		
Progress log filename : /usr/openv/	netbackup/logs/user_ops/root/logs/jbp-1185	7667194609388164000000120-CHx6uu.log Restore Job Id	=784
Restore started 10/31/2022 01:36:	49		
01:42:18 (784.xxx) Found (2) files if	n (1) Images for Restore Job ID 784.xxx		
01:42:27 (764.00) Searched (2) Int	convil of image created Fri 29 Oct 2022 05	56-25 AM EDT from policy standard polyclight	
01:43:25 (784.001) INF - Selected I	Path /linux ES. Copy 1. Fragment 1	30.25 AM EDT from policy standard_fibidelient	
01:43:25 (784.001) INF - Connect t	o hostname=NBU.ransomware.net. port=0.	IPC="/usr/openy/var/tmp/vnet-2347666719494758282700	0000004-aPvP7K".
01:43:25 (784.001) INF - Data sock	et to NBU.ransomware.net is connected, fd	4	
01:43:25 (784.001) INF - BPPFI EXIT	ING WITH STATUS = 0		
01:46:40 (784.001) INF - ROLLED BA	ACK /linux_FS SUCCESSFULLY		
01:46:58 (784.001) Status of resto	re from copy 1 of image created Fri 28 Oct 2	022 05:56:25 AM EDT = the requested operation was suc	cessfully 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:

30 Jo	bs (0 Queued 0 A	ctive 0 Waiting for Rel	try 0 Suspended 0 Incon	nplete	30 Done -	20 selected)			Search	7 -
🔽 Jo	b Id	🛆 Туре	State	Stat	Status	Job Policy	Job Schedule	Client	Media Se	Start Tir
X	722 Backup		Done		(test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	721 Backup		Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	720 Backup		Done		C	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	719 Backup		Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	718 Backup		Done		(test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	717 Backup		Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	716 Backup		Done		C	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	715 Backup		Done		C	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	714 Backup		Done		C	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	713 Backup		Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	712 Backup		Done		C	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	711 Backup		Done		C	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	710 Backup		Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	709 Backup		Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	708 Backup		Done		(test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	707 Backup		Done		C	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	706 Backup		Done		0	test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	705 Backup		Done		(test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	704 Backup		Done		(test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11
X	703 Backup		Done		(test_malware	full	nbuora.ransomware.net	NBUMEDI	Oct 25, 2022 11

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

- 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.

											_		
											Q 1	r C	±
	Job ID	Client na	Policy ty	Count	Score	Anomaly	Anomaly su	Received 🕹	Review s	Policy na	Schedule	Schedu	le i
>	731	nbuora.ran	Standard	1	4.7	Low	Backup fil	Oct 26, 2022	Not review	test_malw	full	FULL	1
>	733	nbuora.ran	Standard	1	4.7	Low	Backup fil	Oct 26, 2022	Not review	test_malw	full	FULL	1
>	732	nbuora.ran	Standard	1	4.7	Low	Backup fil	Oct 26, 2022	Not review	test_malw	full	FULL	:
>	734	nbuora.ran	Standard	1	4.7	Low	Backup fil	Oct 26, 2022	Not review	test_malw	full	FULL	:
>	736	nbuora.ran	Standard	1	4.7	Low	Backup fil	Oct 26, 2022	Not review	test_malw	full	FULL	:
>	735	nbuora.ran	Standard	1	4.7	Low	Backup fil	Oct 26, 2022	Not review	test_malw	full	FULL	1
>	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:

Anon	aly dete	ection											Ar	nomaly de	tectior	n settings
Sea												Q	T	2	Ł	□~
		Job ID	Client na	Policy ty	Count	Score	Anomaly	Anomaly su	Receiver 🕹	Review s	Policy na	Schedule		Schedul		-
~		762	nbuora.ran	Standard	4	11.36	Medium	Anomaly i	Oct 26, 2022	Not review	test_malw	full	I	FULL		:
	Anom	aly detected or	i job 762													1
	Job 762	ID		Client nbuora	name a.ransomware.r	iet	Policy nan test_malw	ie are		Policy type Standard						
	Sch full	edule name		Sched FULL	ule type		Review sta Not review	tus ed		Backup ID nbuora.ransor 275	mware.net_166	6762				
	And 762	maly ID _1666762275		Anoma Mediu	aly severity m											
	Anom	aly details						Mark a	as ignore	Confirm as	anomaly	Report a	as fals	se positiv	e	
	And 800	o <mark>maly: Backup</mark> 02 (Usual: 1 - 2	files count ?)	Anoma 195.34 0.031	a ly: Data transf 14 MB (Usual: 0 MB)	erred .031 MB -	Anomaly: 195.344 M 0.031 MB)	mage size B (Usual: 0.031	MB -	Anomaly: Tota 1177 Seconds - 1144 Second	al time s (Usual: 70 Sec is)	conds				

- 4. To respond to a particular alert, select from the following options:
 - Mark as ignore:

> 763 nbuora.ran Standard 4 11.36 Medium Anomaly i Oct 26, 2022 Ignore test_malw full FUL	.L 🚦
---	------

• Confirm as anomaly:

	Job ID	Client na	Policy ty	Count	Score	Anomaly	Anomaly su	Receiver 🕹	Review status	Policy na	Schedul	Sche	
>	762	nbuora.ran	Standard	4	11.36	Medium	Anomaly i	Oct 26, 2022	Anomaly	test_malw	full	FULL	:

• Report as false positive:

>	763	nbuora ran	Standard	4	11.36	Medium	Anomaly i	Oct 26, 202	2 Ignore	test_malw	full	FULL	
~	751	Report as fals	e positive					× 202	2 Not review	test_malw	full	FULL	
	Anomaly detecte	Report this ano	maly as a fals	e positive an	d do not show	similar anom	alies in the futu	re.					
	Job ID 751						Cancel	eport	Policy type Standard				
	Schedule name		Sched	ule type		Review s	tatus		Backup ID				
	full		FULL			Not revie	wed		nbuora.ransor 375	nware.net_166	6761		
	Anomaly ID		Anom	aly severity									
	751_16667613	75	Mediu	m									
	Anomaly details	S					Mark	as ignore	Confirm as	anomaly	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.

NBU.ransomware.net (Master Se	Search Results								
NBU.ransomware.net (Master Server) Stackup, Archive, and Restore Activity Monitor	Action: Verify								
P Reports	Media			Co	pies:				
- 🖪 Policies	Media ID:	Media host:		Co	ру 2				-
- Storage	<all></all>	<all hosts="" media=""></all>		- Pol	licy name:				
- Se Host Properties				<a< td=""><td>II Policies></td><td></td><td></td><td></td><td></td></a<>	II Policies>				
- 🖻 Applications	O Disk Type:	Disk pool:		Pol	licy type:				
- Media and Device Management	PureDisk 👻			< <a< td=""><td>Il Policy Types></td><td></td><td></td><td></td><td></td></a<>	Il Policy Types>				
- Media	Media server:	Path:		TVE	pe of backup:				
🗢 屢 Devices	<all hosts="" media=""></all>	<all></all>			II Backup Types>				
🗢 🚼 Credentials				Clie	ent (host name):				
Security Management				nb	uora.ransomware.net				
- Host Management	Date/Time Range			10	b Priority				
🗢 幊 Certificate Management	From: Oct 27, 2022 4:20:06 AN				Override default priorit	v			
- Recurity Settings					· · · ·				
Access Management Deployment Management	Oct 31, 2022 11:59:59 P			Jo	b Priority				
Deployment Policies	L			(h	igher number is greater	priority)			
🗢 🛞 Vault Management								Hein	Search Now
🗢 🔞 Bare Metal Restore Management								Пеф	Tegrounda
- We Logging Assistant	Search Results: 1 backup image(s) found (0 selected)							Ø
	Backup ID	Date	Policy	Schedule Nam	work Unlock Time	Primary Copy	Media Server		Media ID
	nbuora.ransomware.net_1666950985	Oct 28, 2022 5:56:25 AM	standard_nbuclient fu	ell		No NE	BUMEDIA.ransomwa	re.net @aaa	ai

Search Results						
Action:						
Verify						
Media		Copies:				
Media ID: Media host:		Сору 2				
<all></all>	*	Policy name:				
O Diek Tures		<all policies=""></all>				
Disk type: Disk pool:		Policy type:				
PureDisk - All>	7	<all policy="" th="" typ<=""><th>ies></th><th></th><th></th><th>-</th></all>	ies>			-
Media server: Path:	Verify		:			
<all hosts="" media=""> 💌 <all></all></all>	<u>Duplicate</u>	a	pes>			×
	🖼 Expire	Delete	me):			
	🗕 🛃 I <u>n</u> itiate Ir	nport	hware.net			•
Date/Time Range	Import					
11011. Oct 27, 2022 4:20:06 AM	🐴 <u>S</u> et Prima	ary Copy	stault priority	·		
To: Oct 31, 2022 11:59:59 P	Copy To	Clipboard Ctrl-C				
	Columns	•	r is greater	priority)		
	2 Sort				[Help Search Now
	👬 Eind	Ctrl-F			-	2-if 2-iiiiiii
Search Results: 1 backup image(s) found (1 selected)	Filter	Ctrl-T			-	Ø
Backup ID Date Policy	Clear Filt	er Ctrl-U	Unlock Time	Primary Copy	Media Server	Media ID
nbuora.ransomware.net_1666950985_Oct 28, 2022 5:56:25 AM_standard_nbuc	clie			No	NBUMEDIA.ransomware	a.net @aaaai

No malware is detected.



3. Click Scan now.

Veritas NetBackup [™]									₽	?	٠	R
«	Malware detec	tion							N	lalware dete	ection se	ettings
🚍 Storage	◆ Scap now	Search							Q	τ 2	; 🗆]~
Storage configuration	Client	Backup time	Scan result	Backup type	Date of scan 🕹	Malware scann	Number of files	Backup ID	Scan I	nost name		1
O Storage lifecycle policies	nbuora.ransom	w October 18, 2022 2:	Solution Not impacted	Full	October 18, 2022 4:	NetBackup Malware	0	nbuora.ransomware	scanho	ost.ransomv	N :	£
E Catalog	nbuora.ransom	w October 18, 2022 1:	S Failed	Full	October 18, 2022 2:	NetBackup Malware	0	nbuora.ransomware	scanho	ost.ransomv	» :	1
Detection and reporting	nbuora.ransom	w October 18, 2022 1:	E Failed	Full	October 18, 2022 2:	NetBackup Malware	0	nbuora.ransomware	scanho	os <mark>t.ransomv</mark>	N 1	1
🍽 Anomaly detection	nbuora.ransom	w October 18, 2022 1:	Solution Not impacted	Full	October 18, 2022 2:	NetBackup Malware	0	nbuora.ransomware	scanh	ost.ransomv	N 1	ł
Malware detection	nbuora.ransom	w October 17, 2022 6:	🛇 Not impacted	Full	October 18, 2022 12	NetBackup Malware	0	nbuora.ransomware	scanho	ost.ransomv	» :	1
🛃 Usage	nbuora.ransom	w October 17, 2022 6:	📀 Not impacted	Full	October 18, 2022 1:	NetBackup Malware	0	nbuora.ransomware	scanho	ost.ransomv	~ <mark> </mark>	1
🔩 Credential management	nbuora.ransom	w October 17, 2022 6:	Not impacted	Full	October 17, 2022 7:	NetBackup Malware	0	nbuora.ransomware	scanh	ost.ransomv	N 1	

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

Malware scan						×
Select a client to scan ()						
Search			Q	T	0	□~
Client	Platform	Policy type				
(h) nbuora.ransomware.net	Linux	Standard				

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

Malware scan			
Select the timeframe of	backups		
Start date and time:			
10/27/2022		04:22:17 AM	0
End date and time:			
10/31/2022	Ê	11:59:59 PM	O
Select a malware scanne	er host po	ool *	
Malware_scanner		Q	
Select the malware scan	result st	tatus for images to be	e scanned
Not scanned			
Not impacted			
O Impacted			
All			

Scan task starts.

Client	Backup time	<u>,S</u> çan result	Backup type	Date of scan 🕹	Malware scann	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 Back		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				-	•	x
Job ID: Job Overview	785 Detailed Status Job H	lierarchy	Job State:	Active			
Job Type: Backup Type:	Instant Access Create-Mount	File List:					
Client:	k	SPWS_MOUNT_ID=55_1666950985 SPWS_JOB_ID=55_1666950985					
Master Server:	NBU.ransomware.net						
Job Policy: Policy Type: Job Schedule: Schedule Type	Standard						
Priority: Owner: Group: Compression: Off-Host:							
Start Time: Elapsed Time: End Time: Retention:	Oct 31, 2022 4:25:46 AM 00:04:37						
		Status:					

Job ID: Job Overview	785 Detailed Status Job Hierarchy	Job State:	Active
Attempt: Job PID:	1		Attempt Started: Oct 31, 2022 4:25:46 AM Attempt Elapsed: 00:04:37 Attempt Ended:
Media Server: Media Transpor	NBUMEDIA.ransomware.net rt Type: LAN		KB/Sec:
Oct 31, 2022 4:2 Oct 31, 2022 4:2 Oct 31, 2022 4:2 Oct 31, 2022 4:2 Oct 31, 2022 4:2	5:46 AM - Info NBWMC (pid=1401) Creating instant a 5:46 AM - Info NBWMC (pid=1401) Storage server NB 5:46 AM - Info NBWMC (pid=1401) The SPWS ID 55_1 5:46 AM - Info NBWMC (pid=1401) The NetBackup re 5:46 AM - Info NBWMC (pid=1401) Mount clients sca	iccess mount from Standard Image nbuora.ransomware.net JUMEDIA.ransomware.net. 666950985. isource ID 8d7e4c75-ef05-4896-9d83-e6caf567ff7d. nhost.ransomware.local.	_1666950985 and copy number 2.



Instant Access completed.

Job ID:	785		Job State:	Done (Successful)	
Job Overview	Detailed Status Job	Hierarchy			
Job Type: Backup Type:	Instant Access Create-Mount	File List:			
Client:		SPWS_MOUNT_ID=55_1666950985 SPWS_JOB_ID=55_1666950985			
Master Server:	NBU.ransomware.net				
Job Policy: Policy Type: Job Schedule: Schedule Type	Standard				
Priority: Owner: Group: Compression: Off-Host:					
Start Time: Elapsed Time: End Time: Retention:	Oct 31, 2022 4:25:46 AM 00:21:46 Oct 31, 2022 4:47:32 AM	1			
		Status:			
		1: (0) The requested operation was succe	essfully completed.		

Scan results:

After scanning, the scan result is not impacted.

Client	t 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 Malware	0	nbuora.ransomware.net_1666950985	scanhost.r;	:



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

<i>i</i> Job Details: 7860	NBU.ransomware.net				-	•	x
Job ID:	786		Job State:	Done (Successful)			
Job Overview	Detailed Status Job H	ierarchy					
Job Type: Backup Type:	Instant Access Delete-Mount	File List:					
Client:		SPWS_MOUNT_ID=55_1666950985 SPWS_IOB_ID=55_1666950985					
Master Server:	NBU.ransomware.net						
Job Policy: Policy Type: Job Schedule: Schedule Type:	Standard						
Priority: Owner: Group: Compression: Off-Host:							
Start Time: Elapsed Time: End Time: Retention:	Oct 31, 2022 4:59:25 AM 00:00:07 Oct 31, 2022 4:59:32 AM						
		Status:					
		1: (0) The requested operation was succes	sfully completed.				

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.

	^				
,? M:∖	Name	Date modified	Туре	Size	
test	L KB4	11/16/2022 11:52	File folder		
This PC	PerfLogs	5/19/2021 4:05 PM	File folder		
3D Objects	Program Files	11/14/2022 3:33 A	File folder		
Desktop	Program Files (x86)	11/14/2022 3:35 A	File folder		
Documents	📜 temp	12/22/2022 12:01	File folder		
Documents	Users	9/30/2020 4:27 PM	File folder		
Downloads	WCLauncher	11/15/2022 1:44 PM	File folder		
Music	Windows	11/14/2022 3:41 A	File folder		
Pictures	👔 eicar_com	12/22/2022 7:51 PM	Compressed (zipp	1 KB	
Videos	5				
Local Disk (C:)					

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



2. Perform malware scanning of the backup image.

Ì	Veritas NetBackup [™]		 0	?	٠	R
«		Malware scan				×
	■ RHV SaaS	Select the timeframe of backups Start date and time: 12/23/2022				
(Storage ^	End date and time: 12/23/2022				
	Storage lifecycle policies	Select a malware scanner host pool * Malware_scanner Q				
	Catalog	Select the malware scan result status for images to be scanned				
ا ھ	Detection and reporting	Not scanned				
	Malware detection	Not impacted Impacted All				
1 - C - L	✓ Usage					

1	Malware detectio	on	ß					Malw	are detect	ion setting
1	Scan now							Q 1	r c	□~
	Client	Backup time	Scan result	Backup type	Date of scan 🕹	Malware scann	Number of files	Backup ID	Scan ho	05
	Win_client.ransor	December 23, 2022 1:40 AM	Pending	Full	December 23, 2022	NetBackup Malware	0	Win_client.ransomv	scanhos	t I

Scanning is in progress.

Malware detection							Ма	lware	detectio	on setting
Scan now Searce	Scan now Search						Q	T	C	
Client	Backup time	Scan result	Backup	Date of scan 🕹	Malware scanner	Number of files	Backup ID)	Scan h	
Win_client.ransomware.	December 23, 2022 1:40 AM	In progress	Full	December 23, 202	NetBackup Malware Scanner	0	Win_client	.rar	scanho	:
Win_client.ransomware.	December 22, 2022 10:58 PM	Impacted	Full	December 22, 202	NetBackup Malware Scanner	1	Win_client	.rar	scanho	

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

Malware detection							Ma	alware	detectio	on setti	ngs
Scan now Sear	Scan now Search					Q	T	C	□~		
Client	Backup time	Scan result	Backup	Date of scan 🕹	Malware scanner	Number of files	Backup II	D	Sran h		-
Win_client.ransomware	e. December 23, 2022 1:40 AM	Impacted	Full	December 23, 202	NetBackup Malware Scanner	1	Win_client	t.rar	scanho	ł	
Win_client.ransomware	. December 22, 2022 10:58 PM	Impacted	Full	December 22, 202	NetBackup Malware Scanner	1	Win_client	t.rar	scanho	:	

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

alware detection	Ilware detection										
Scan now Sea							Q	T	C	□~	
Client	Backup time	Scan result	Backup	Date of scan 🕹	Malware scanner	Number of files	Backup II	D Sc	an hos	3	*
Win_client.ransomwar	e. December 23, 2022 1:40 AM	Impacted	Full	December 23, 202	NetBackup Malware Scanner	1	Win_client	t.r sc	anhost.		
Win_client.ransomwar	e. December 22, 2022 10:58 PM	Impacted	Full	December 22, 202	NetBackup Malware Scanner	1	Win_cli I	Expire	all cop	ies	
Win_client.ransomwar	re. December 22, 2022 10:56 PM	✓ Not impacted	Full	December 22, 202	NetBackup Malware Scanner	0	Win_di	View ir	fected	l files	

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

ected files	×
	ß
/C/eicar_com.zip	

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

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

Scan now Search							Q T 2
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	View infected files
Are you	sure you war	nt to expi	re all (copies?			
					С	ancel	Expire

Backup image is successfully expired.

							₽	? 40	R
Nalware detection			Succ	essfully expired all c	opies.		Mai	ware dotech	ion settings
Scan now Search	1						Q	T C	
Client	Backup time	Scan result	Backup	Date of scan 🕹	Malware scanner	Number of files	Backup ID	Scan ho	s
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.	scanhost	

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:

Scan not	w Search					Q	T	C	□~
Client	Backup ID	Backup time	Scan result	Backup type	Date of scan 🕹	Malware scann	Numbe	r of file	: :
Win_client.	Win_client.ransomware.local_1671777634	December 23, 2022 1:40 AM	Impacted	Full	December 23, 2022	NetBackup Malware	1		:
Win_client.	Win_client.ransomware.local_1671767888	December 22, 2022 10:58 PM	Impacted	Full	December 22, 2022	NetBackup Malware	1		:

After expiration, the image is removed.

<u>File Edit View Actions Help</u>												
😑 🗢 > 🔁 🖬 🖨 💐 🗞 🖀	a 7 7	🔊 🖉 🖬 🎥 🖉 📉 🗙 3	- 🔊 😨								Login Ac	tivity 🔻
NBU.ransomware.net (Master Se	Search	Results										
NBU.ransomware.net (Master Server)	Action:											
Backup, Archive, and Restore	Vorify	-										
Activity Monitor	verny											
B Reports	Media					Copies:						
Policies	Media	a ID: M	edia host:			Primary	Сору					-
- E Storage			All Media Hostss		1.1	Policy na	ame:					
Gatalog Host Properties						<all poli<="" td=""><td>cies></td><td></td><td></td><td></td><td></td><td>-</td></all>	cies>					-
Master Servers	🔾 Disk 1	Type: Di	isk pool:			Policy ty	ne:					
- Bin Media Servers	BasicDis	;k ▼ <			+	<all poli<="" td=""><td>cv Types></td><td></td><td></td><td></td><td></td><td>-</td></all>	cv Types>					-
- Elients	Media se	erver: Pa	ath:			Type of t	backup:					
P Media and Device Management	<all mer<="" td=""><td>tia Hostss</td><td>All></td><td></td><td>-</td><td><all bad<="" td=""><td>kup Types</td><td>></td><td></td><td></td><td></td><td>-</td></all></td></all>	tia Hostss	All>		-	<all bad<="" td=""><td>kup Types</td><td>></td><td></td><td></td><td></td><td>-</td></all>	kup Types	>				-
- Device Monitor					_	Client (h	ost name)					
- Media						Win die	nt.ransom	ware.local				-
~ Credentials	Date/Tin	ne Range				Inh Prin	rity					
🗣 🖵 Security Management	From: De	22 2022 2:00:21 AM				Over	rido dofau	lt priority				
- 🧱 Security Events	_	C 22, 2022 2.00.21 A				- Ofer	nue uerau	it priority				
- 🖳 Host Management	TO: De	ec 23, 2022 11:59:59 🖶 🔝				Job Prio	rity					
Clobal Security Settings						(higher	number is	greater pr	iority)			
- Access Management											Liste Course	h Marine
🕈 🔽 Deployment Management											Help Searc	nNow
Deployment Policies	Search R	tesults: 2 backup image(s) f	ound (1 selected)	<u></u>								Z
- Bare Metal Restore Management		Backup ID	Date	Policy	Sch	nedule N	WORM U	nlack Time	Primary (Copy Media Serve	er Expiration	Date
Logging Assistant	Vin client.	ransomware.local 1671777634	Dec 23, 2022 1:40:34 AM	vindows backup	Full				Yes	MSDPC.ranso.	Jan 6, 2023 1:40:34 AM	1
	Vin client.	ransomware.local 1671767789	Dec 22, 2022 10:56:29 PM	vindows_backup	Full				Yes	MSDPC.ranso.	Jan 5, 2023 10:56:29 F	M
								-				
Backup ID		Date	Policy	Schedule N	WO	RM Unlo	ck Time	Primary	Сору М	edia Server	Expiration	Date
Win_client.ransomware.local_1671	777634	Dec 23, 2022 1:40:34 AM	windows_backup	Full				Yes	MSE	DPC.ranso Ja	in 6, 2023 1:40:34 AM	И
Win_client.ransomware.local_1671	767789	Dec 22, 2022 10:56:29 P	M windows_backup	Full				Yes	MSE)PC.rans <mark>o</mark> Ja	n 5, 2023 10:56:29 F	Mc

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.

Action: Verify										
Media				Cor	pies:					
🔾 Media ID:	Media host:			Co	ру З					-
<all></all>	<all hosts="" media=""></all>			Pol	icy name:					
				<a< td=""><td>ll Policies></td><td></td><td></td><td></td><td></td><td>-</td></a<>	ll Policies>					-
• Disk Type:	Disk pool:			Pol	icy type:					
PureDisk	<all></all>		-	<a>	ll Policy Types>					-
Media server:	Volume:			Тур	e of backup:					
<all hosts="" media=""></all>	<all></all>		-	<a< th=""><th>ll Backup Types></th><th></th><th></th><th></th><th></th><th>~</th></a<>	ll Backup Types>					~
				Clie	ent (host name):					
				nb	uora.ransomware.net					-
Date/Time Range				Jo	b Priority					
From: Oct 27, 2022 4:20:06 AN					Override default prior	ity				
To: Oct 28, 2022 11:59:59 P				Job	b <u>Priority</u>					
				(hi	igher number is greate	r priority)				
								Hel	p <u>S</u> earc	h Now
Search Results: 1 backup image(s) found (1 selected)									Ø
Backup ID	Date	Policy	Schedule	Name	WORM Unlock Time	Primary Copy	Media Server	Expiration Date	e Immutable	1
nbuora.ransomware.net_1666950985	Oct 28, 2022 5:56:25 AM	standard_nbuclient	full		Nov 11, 2022 5:50:02 AM	4 No	NBUMEDIA	Nov 11, 2022 4:5	Yes	@aaaaw

2. Expire the image.

Action: Verify						
Media				Copies:		
🔾 Media ID:	Media host:			Сору З		-
<all></all>	All Media Hosts>		*	Policy name:		
0.000				<all policies=""></all>		-
Disk Type:	Disk pool:			Policy type:		
PureDisk	▼ <all></all>		-	<all policy="" types=""></all>		-
Media server:	Volume:			Verify		
<all hosts="" media=""></all>	<all></all>		-	Duplicate		
-				M Expire	Delete	
				🐉 I <u>n</u> itiate Import		•
Date/Time Range				🖉 Import		
From: Oct 27, 2022 4:20:06 AN				🐁 Set Primary Copy		
To: Oct 28, 2022 11:59:59 P +	15			Copy To Clipboar	d Ctrl-C	75000 📮
				Columns	•	priority)
				2 S <u>o</u> rt		Help Search Now
				🛱 Eind	Ctrl-F	
Search Results: 1 backup imag	e(s) found (1 selected)			Filter	Ctrl-T	Ø
Backup ID	Date	Policy	Schedule	🗶 Clear Filter	Ctrl-U	rimary Copy Media Server Expiration Date Immutable
nbuora.ransomware.net_16669509	35 Oct 28, 2022 5:56:25 AM	standard_nbuclient	full	NOV 11, 2022 0.0	0.02 APT	NBUMEDIA Nov 11, 2022 4:5 Yes @aaaaw

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

Action: Verify									
Media			Cop	ies:					
O Media ID:	Media host:		Cop	ру З					-
<all></all>	Expire Images@NBU.ransomwa	are.net		x					
Dick Type:									-
PureDisk Media server: <all hosts="" media=""> Date/Time Range From: Oct 27, 2022 4:20:06 AM To: Oct 28, 2022 11:59:59 P</all>	The expiration Any searches p could be invalid. The number of seen on the stat For the selecte collectively form volume will also Would you like t	of images is irrevo serformed while es remaining images us bar below. ed image, all assoc a distinct recovery expire. to expire the select	ocable. cpiration is in pr to be expired of clated images th point of a give ted images?	rogress an be nat n NAS	> : ure.net ult priori	ty 75000 -			•
Search Results: 1 hackun ima	ne(s) found (1 selected)	Yek <u>N</u> o					<u>H</u> elp	<u>S</u> earch N	low 2
Backup ID	Date	Policy	Schedule Name	WORM Unio	ock Time	Primary Copy Media Server	Expiration Date	Immutable	
nbuora.ransomware.net_1666950	985 Oct 28, 2022 5:56:25 AM	standard_nbuclient	full	Nov 11, 2022 5	5:50:02 AM	No NBUMEDIA	Nov 11, 2022 4:5	Yes @a	aaaaw

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

		ISAIL PHILLIPS2
📱 Image Expire Error@NBU.ransomware.net		x
Backup ID	Copy Number	Error Message
nbuora.ransomware.net_1666950985	3	Expiration for Open Storage WORM cannot be shortened. (2530)
•		
		Οκ

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.

3	Veritas NetBackup [™]									58	? 4	> R)
«		Malware detection	on							Ma	Iware detect	tion settings	5
	D SaaS	Scan now								Q	T 2	□~	
C	9 VMware	Client	Backup time 🕹	Scan result	Backup type	Date of scan	Malware scann	Number of files	Backup ID	Scan ho	ist name	Â	l
a s	Storage ^	nbu.ransomware	August 25, 2022 4:4	Failed to conr	ect to the scan host.	August 25, 2022 5:3	NetBackup Malware	0	nbu.ransomware.ne	scanhos	t.ransomw	:	
ł	🔹 Storage configuration	nbu.ransomware	August 25, 2022 4:4	🙁 Failed	Full	August 25, 2022 4:4	NetBackup Malware	0	nbu.ransomware.ne	scanhos	t.ransomw	-	
(Storage lifecycle policies	nbu.ransomware	August 24, 2022 11	🙁 Failed	Full	August 25, 2022 4:4	NetBackup Malware	0	nbu.ransomware.ne	scanhos	t.ransomw	-	
	Catalog	nbu.ransomware	August 24, 2022 11	😢 Failed	Full	August 25, 2022 5:5	NetBackup Malware	0	nbu.ransomware.ne	scanhos	t.ransomw		
6	Detection and reporting ^	nbu.ransomware	August 23, 2022 12	😢 Failed	Full	August 23, 2022 12	NetBackup Malware	0	nbu.ransomware.ne	scanhos	t.ransomw	-	
)	Anomaly detection	nbuora.ransomw	August 19, 2022 12	🙁 Failed	Full	August 19, 2022 12	NetBackup Malware	0	nbuora.ransomware	scanhos	t.ransomw		
(Malware detection	nbuora.ransomw	August 16, 2022 9:4	😢 Failed	Full	August 16, 2022 11	NetBackup Malware	0	nbuora.ransomware	scanhos	t.ransomw	;	
Ŀ	🛃 Usage	nbuora.ransomw	August 16, 2022 9:4	😢 Failed	Full	August 16, 2022 9:4	NetBackup Malware	0	nbuora.ransomware	scanhos	t.ransomw		
۹ (Credential management	nbuora.ransomw	July 28, 2022 9:16 F	😢 Failed	Full	August 8, 2022 3:05	NetBackup Malware	0	nbuora.ransomware	scanhos	t.ransomw	ı	
	inete ^	nbuora ransomw	July 28, 2022 9:16 F	R Failed	Full	August 11, 2022 12	NetBackun Malwarr	0	nhuora ransomwäre	tesòànnos	†ráňsomw_	• •	

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 "—disablessl" from the NetBackup media server.

Master Serv	er Properties: NBU.ransomware.net	×
Fibre Transport Servers Gloud Storage Cloud Storage:		<u>D</u> efaults
Service Hostname / Auth	Service Endpoint Service Provider	Add
General Server Port Panges	Add Cloud Storage ×	Change
Media		Remove
Timeouts General Settings Regi	ion Settings	
	Hitachi Content Platform for 💌	
Image: Comparison of the second se	hcpcs-shared.gpsecontent.local	
- the service endpoint:	80	
- Ⅲ UNIX Server - 酚 Backup Host Po HTTPS port:	443	
- B VMware Access - B RHV Access Hos	NBUMEDIA.ransomware.net	
By NutanixAHV Acc Endpoint <u>a</u> ccess style: By Network Setting	Path Style	
- 12 Credential Acce	4	Change
- Senterprise Vault		
Resource Limit	Ok Cancel Help	
Preferred Netwo		
- BSLP Parameters		
Cloud Storage		-

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.

Master Server Properties: NBU ransomware.net	×
Properties Cloud Storage	Defaults
- Oliversal String	
Retention Period	
- 🖄 Data Classif 🗣 Cloud Storage Server Configuration@NBU.ransomware.net 🛛 🗙	<u>A</u> dd
- 🙀 Fibre Transi	Change
Servers Advanced Server Configuration	Remove
Sandwidth	1 mar 1 m
General Ser	
O Port Range: Use SSL	
- 🍘 Media	
Timeouts O Authentication Only	
- 4 Client Attrib	
Distributed	
Firewall Check Certificate Revocation	
Clean un HTTP Headers:	
Cleaning	
Header Value	
- III UNIX Server	
Backup Hos	
- B VMware Acc	
-B RHV Access	
- B Nutanb AHV	Change
- 월 Network Set	
- 18 Credential A	
- Contraction -	
S Later Pare	
- Throttle Bar	
Preferred N QK Cancel Help	
- 😹 Resilient Network	
- Leg SLP Parameters	
Cloud Storane	

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 combing 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 <u>www.HitachiVantara.com</u> <u>community.HitachiVantara.com</u>

Regional Contact Information Americas: +1 866 374 5822 or <u>info@hitachivantara.com</u> Europe, Middle East and Africa: +44 (0) 1753 618000 or <u>info.emea@hitachivantara.com</u> Asia Pacific: +852 3189 7900 or <u>info.marketing.apac@hitachivantara.com</u>

