Ransomware Protection with Veritas NetBackup and Hitachi Content Platform for Cloud Scale

Solution Whitepaper

This paper describes how to integrate Veritas NetBackup and Hitachi Content Platform for cloud scale to provide cyber protection against prescient ransomware threats.

Hitachi Vantara LLC

May 2022

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

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

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

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

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

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

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

Table of Contents

Preface 4

About this document.. 4

Document conventions.. 4

Intended audience.. 4

Revision history.. 4

Accessing product downloads.. 5

Getting help.. 5

Executive summary.. 6

Veritas NetBackup.. 6

Hitachi Content Platform for cloud scale.. 7

Amazon S3 Object Lock.. 7

Hardware and software components.. 7

Solution diagram.. 8

Test methodology.. 9

Prepare the environment.. 10

Validation tests.. 11

Create an MSDP cloud immutable storage volume.. 11

Validate the bucket using HCP for cloud scale.. 12

Configure the cloud scale MSDP-C server.. 12

Back up to the HCP for cloud scale bucket and test Object Lock immutability.. 15

Verify the security of the object lock.. 16

Observe deduplication and ingested details during a backup.. 17

Malware scan.. 19

Additional details.. 22

Conclusion.. 23

Further reading.. 23

Preface

About this document

This paper describes how to integrate Veritas NetBackup 10.x and Hitachi Content Platform for cloud scale with Amazon S3 Object Lock to provide cyber protection and resiliency against prescient ransomware threats. This integration enables oversight and accountability for cyber data protection to combat ransomware challenges.

The data captured in this paper is specific to the Veritas NetBackup[1] and Hitachi Vantara test plans, selected configurations, test methodology, and processes used to measure results. Actual user experience might vary based on the solution design and environment. Consult your Veritas NetBackup and Hitachi Vantara technical representatives before you implement this solution.

Document conventions

This paper uses the following typographic convention:

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`

Intended audience

This paper is intended for Veritas NetBackup and Hitachi Vantara customers, partners, and solution architects who evaluate modern and adaptive object storage technologies for their applications.

Revision history

Version	**Description**	Date
1.0	Initial version	05/04/2022

[1] https://www.veritas.com/protection/netbackup

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: https://support.hitachivantara.com/.

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

Getting help

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

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

Executive summary

Continued exponential growth of data in the industry has led to an increased demand on storage capacity and optimization of business-critical processes, such as backup and recovery. According to IDC's Worldwide Future of Digital Infrastructure 2022 predictions, by the year 2023, executive leaders will implement business critical key performance indicators (KPIs) that are tied to data availability, recovery, and cyber protection. This is because of the rising levels of cyberattacks that expose their company's data to risk.

To help customers optimize their cloud data infrastructure, Veritas and Hitachi Vantara offer a joint, prescient protection solution against ransomware for both hardware and software. This solution integrates the following approaches to protect data from ransomware attacks:

- **Govern**
  Veritas provides tools and applications to manage data. Using these tools, you can learn about your organization's data, identify any infrastructural risk of attack, and report data security compliance.

- **Protect**
  Hitachi Vantara makes data immutable by using Amazon S3 Object Lock[2], where the data is fixed, unchangeable, and can never be deleted. Hitachi Vantara creates a powerful defense against malicious code with several layers and tools to protect data and applications.

- **Detect**
  Hitachi Vantara and Veritas provide tools for accurate detection of ransomware on multiple levels. These tools report on the backup environment and send alerts if any suspicious activity is detected, for example, when large amounts of files are modified in a short period.

- **Respond/Recover**
  Veritas provides the last point of defense by making data more resilient in the face of attacks. Veritas' near 100% data recovery rate ensures that the backup stores are clean and recoverable.

Veritas NetBackup

Veritas NetBackup provides enterprise data management to organizations. Veritas NetBackup ensures resiliency and on-demand access from any location and reduces the risk and cost of storing an ever-increasing amount of data across the globe.

Safeguard your data with a unified platform approach that is designed to extend beyond data protection. Veritas NetBackup provides a multi-layered, proactive solution that ensures resiliency against ransomware.

For more information about Veritas NetBackup, see https://www.veritas.com/protection/netbackup.

[2] https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html

Hitachi Content Platform for cloud scale

Hitachi Content Platform (HCP) for cloud scale is a software-defined object storage solution that is based on a massively parallel microservice architecture. HCP for cloud scale is compatible with the Amazon S3 application programming interface (API). HCP for cloud scale is well suited to service applications that require high bandwidth and compatibility with S3 APIs. With Amazon Immutable S3 Object Lock, HCP for cloud scale forms a strong wall of protection.

For more information about HCP for cloud scale, see *Hitachi Content Platform (HCP) for Cloud Scale – Whitepaper* at https://www.hitachivantara.com.

Amazon S3 Object Lock

Amazon Simple Storage Service (S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. With S3 Object Lock, you can store objects using a write-once-read-many (WORM) model. S3 Object Lock helps prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely.

Use S3 Object Lock to meet regulatory requirements that require WORM storage, or to simply add another layer of protection against object changes and deletion.

S3 Object Lock has been assessed by Cohasset Associates for use in environments that are subject to SEC 17a-4, CFTC, and FINR. See the *Cohasset Associates Compliance Assessment* at https://d1.awsstatic.com/r2018/b/S3-Object-Lock/Amazon-S3-Compliance-Assessment.pdf.

For more information about using S3 Object Lock, see *Amazon Simple Storage Service User Guide* at https://docs.aws.amazon.com.

Hardware and software components

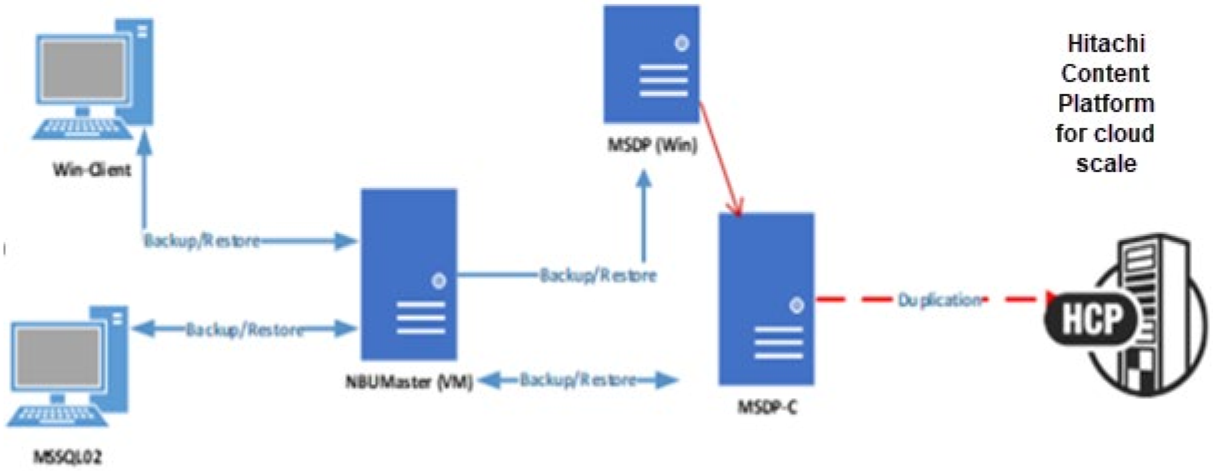
The following hardware and software components were used for the test environment:

- **Veritas NetBackup Master Server:**
  - Microsoft Windows Server 2016 DataCenter, Build 143893
    - 4 virtual cores, 64 GB virtual memory,
    - Disk 1: 200 GB virtual storage (Thin Provision)
    - Disk 2: 200 GB virtual storage (Thick Provision)
  - Veritas NetBackup v10
- **Veritas Media Server (Media Server Deduplication Pool (MSDP):**
  - Microsoft Windows Server 2016 DataCenter, Build 143893
    - 4 virtual cores**,** 64 GB virtual memory**,**

        - Disk 1: 200 GB virtual storage (Thin Provision)
        - Disk 2: 500 GB virtual storage (Thick Provision)
    - Veritas NetBackup v10
- **Veritas Media Server (Media Server Deduplication Pool for Cloud (MSDP-C):**
    - RedHat Enterprise Linux, v7.7
        - 4 virtual cores, 32 GB virtual memory
        - Disk 1: 200 GB virtual storage (Thin Provision)
        - Disk 2: 4 TB virtual storage (Thin Provision)
    - Veritas NetBackup v10
- **Microsoft SQL Server:**
        - 4 virtual cores, 32 GB virtual memory
        - 200 GB virtual storage (SSD)
- **Hitachi Content Platform for cloud scale**
        - 4 virtual storage nodes
        - 8 virtual cores – 64 GB virtual memory
        - HCP for cloud scale software v2.3

Solution diagram

The following diagram illustrates the architecture used for this solution:



Test methodology

The purpose of the testing is to validate integration, functionality, and highlight the importance of the protection strategy provided by Veritas NetBackup and Hitachi Content Platform for cloud scale.

The test suite is developed and provided by Veritas as part of Veritas NetBackup 10.x test validation. Configuration selection is at Hitachi Vantara's discretion. Veritas NetBackup can create an S3 Object Lock bucket on HCP for cloud scale and write backups to them.

The following tests are defined in the test plans for Veritas NetBackup 10.x and HCP for cloud scale validation:

Test	**Description**	**Pass/ Fail**
Create MSDP-C immutable storage volume from Veritas NetBackup	Creates an HCP for cloud scale bucket from Veritas NetBackup.	Pass
Validate the bucket created using Veritas NetBackup from the HCP for cloud scale interface.	Validates the bucket created with the default object lock.	Pass
Create and configure cloud scale MSDP server offload resiliency	Demonstrates step-by-step configuration of the MSDP disk pool using the Veritas NetBackup wizard and adds the HCP for cloud scale volume. An object lock bucket is created that is validated by Veritas NetBackup.	Pass
Perform a backup to the HCP for cloud scale bucket and test object lock and immutability	Demonstrates the retention set for the backup object, which is created from Veritas NetBackup and HCP for cloud scale.	Pass
Delete data for the backup object where the S3 Object Lock is set to expire.	Demonstrates that the data cannot be deleted until the Veritas NetBackup retention for the object expires.	Pass
Observe the deduplication and ingest details during backups	Demonstrates the deduplication achieved using MSDP-C and the ingest rate during the backup.	Pass
Malware scan[3] on demand service	Configure Microsoft Defender Antivirus software to verify backup images.	Pass

[3] https://www.veritas.com/content/dam/www/en_us/documents/technical-documents/TB_netbackup_10_malware_scanning_V1507.pdf

Prepare the environment

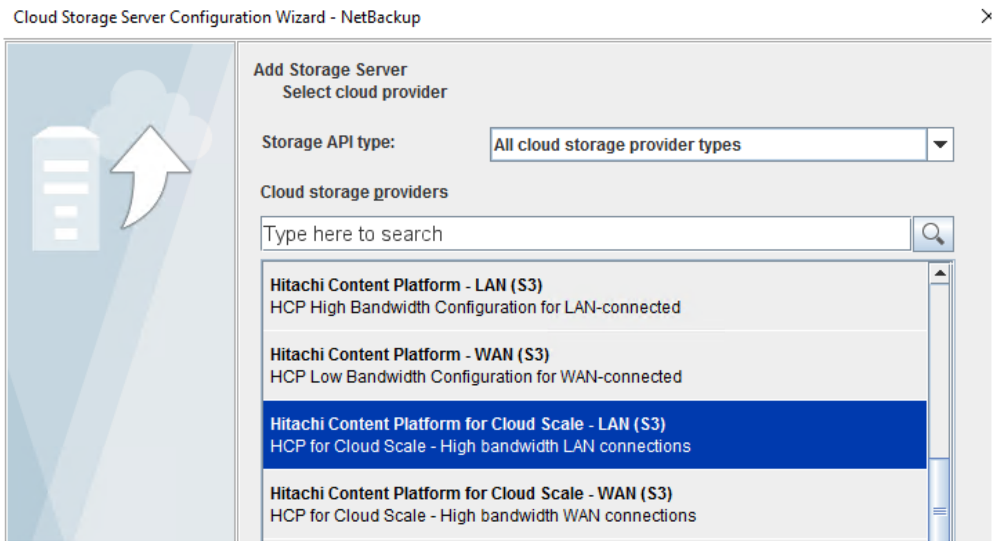
The environment was prepared by:

- Creating an immutable storage volume from Veritas NetBackup, which in turn creates a bucket in HCP for cloud scale.
- Verifying that HCP for cloud scale has a valid SSL certificate.
- Setting the following environment variables on the MSDP-C server to enable users to perform the system and the admin tasks:

```
export MSDPC_ACCESS_KEY=xxxx
export MSDPC_SECRET_KEY=yyyy
export MSDPC_REGION=us-west-2
export MSDPC_PROVIDER= Hitachi-csl
export MSDPC_ENDPOINT=hcpcloudscale.hostname
```

- Verifying 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 Configuration Wizard - NetBackup

Add Storage Server
Select cloud provider

Storage API type: All cloud storage provider types

Cloud storage providers

Type here to search

Hitachi Content Platform - LAN (S3)
HCP High Bandwidth Configuration for LAN-connected

Hitachi Content Platform - WAN (S3)
HCP Low Bandwidth Configuration for WAN-connected

Hitachi Content Platform for Cloud Scale - LAN (S3)
HCP for Cloud Scale - High bandwidth LAN connections

Hitachi Content Platform for Cloud Scale - WAN (S3)
HCP for Cloud Scale - High bandwidth WAN connections

Validation tests

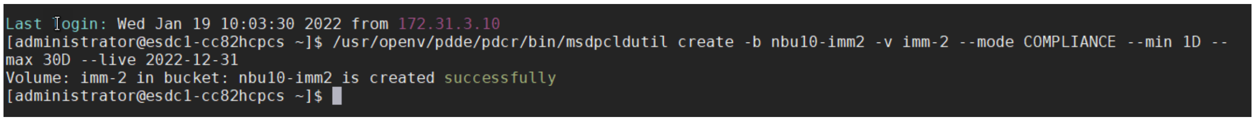
The following tests were performed to validate the Veritas NetBackup and HCP for cloud scale solution.

Create an MSDP cloud immutable storage volume

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

1. Create a cloud immutable storage volume using the `msdpclutil` tool. Enter:

   ```
   /usr/openv/pdde/pdcr/bin/msdpcldutil
   ```

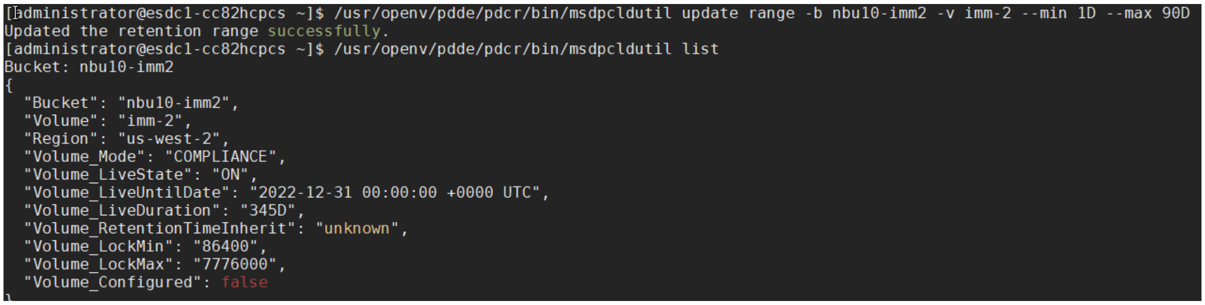
   ```
   Last login: Wed Jan 19 10:03:30 2022 from 172.31.3.10
   [administrator@esdc1-cc82hcpcs ~]$ /usr/openv/pdde/pdcr/bin/msdpcldutil create -b nbu10-imm2 -v imm-2 --mode COMPLIANCE --min 1D --
   max 30D --live 2022-12-31
   Volume: imm-2 in bucket: nbu10-imm2 is created successfully
   [administrator@esdc1-cc82hcpcs ~]$
   ```

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

   ```
   /usr/openv/pdde/pdcr/bin/msdpcldutil update range -b nbu10b6-imm1 -v
   b6-imm-1 --min 5D --max 30D
   ```

3. List the immutable bucket that was created using Veritas NetBackup when setting up the environment to view the defined storage parameters. Enter:

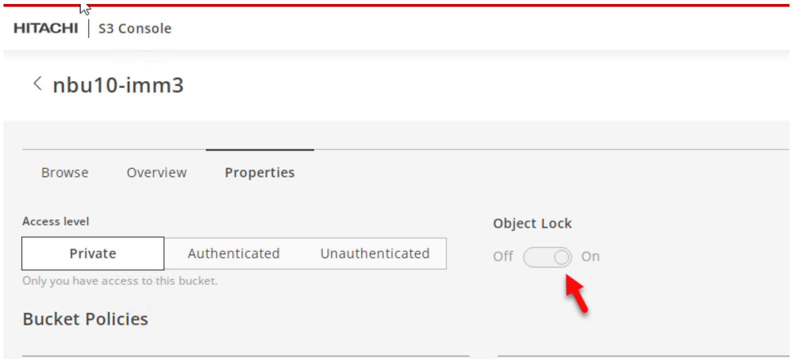
   ```
   /usr/openv/pdde/pdcr/bin/msdpcldutil list bucket
   ```

   ```
   [administrator@esdc1-cc82hcpcs ~]$ /usr/openv/pdde/pdcr/bin/msdpcldutil update range -b nbu10-imm2 -v imm-2 --min 1D --max 90D
   Updated the retention range successfully.
   [administrator@esdc1-cc82hcpcs ~]$ /usr/openv/pdde/pdcr/bin/msdpcldutil list
   Bucket: nbu10-imm2
   {
     "Bucket": "nbu10-imm2",
     "Volume": "imm-2",
     "Region": "us-west-2",
     "Volume_Mode": "COMPLIANCE",
     "Volume_LiveState": "ON",
     "Volume_LiveUntilDate": "2022-12-31 00:00:00 +0000 UTC",
     "Volume_LiveDuration": "345D",
     "Volume_RetentionTimeInherit": "unknown",
     "Volume_LockMin": "86400",
     "Volume_LockMax": "7776000",
     "Volume_Configured": false
   }
   ```

Validate the bucket using HCP for cloud scale

Log in to the HCP for cloud scale user interface and validate the immutable bucket that was created using Veritas NetBackup. You will notice that the S3 object lock for the immutable bucket is enabled as shown in the following figure:



Only you have access to this bucket.

This indicates that Veritas NetBackup can create an object lock bucket on HCP for cloud scale.

Configure the cloud scale MSDP-C server

Configure the cloud scale MSDP-C server to add the immutable storage volume that was created earlier using the Veritas NetBackup `msdpcutil` tool.

> Note: The difference between NetBackup cloud direct and MSDP-C is the deduplication. Only MSDP-C supports WORM immutability backups and server offload resiliency.

1. In NetBackup, create the MSDP-C storage server.

    a. Log in to NetBackup.

    b. In the left pane, select **Storage > Storage configuration** and click **Add**.

    c. Select **Media Server Deduplication Pool (MSDP-C)**.

    d. In the **Basic properties** window, enter the required information and click **Next**.

    e. Select a media server. You can use the Search option to search the available media servers.

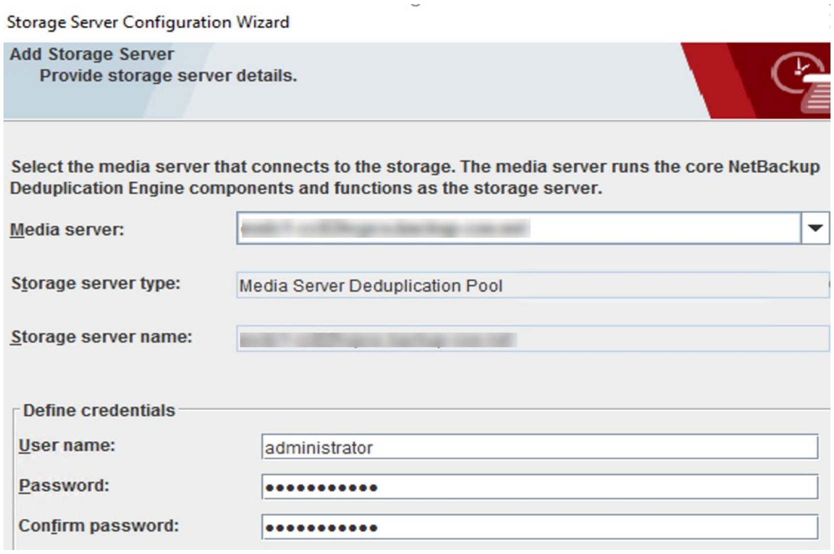
    f. Enter the storage server information and click **Next**.

    g. (Optional) In the **Media servers** window, click **Add** to add any additional media servers.

    h. Click **Next**.

    i. On the **Review** page, verify the selected options and click **Save**.

For more information, see the *Veritas NetBackup Deduplication Guide* at: https://www.veritas.com/content/support/



Storage Server Configuration Wizard

Add Storage Server
Provide storage server details.

Select the media server that connects to the storage. The media server runs the core NetBackup Deduplication Engine components and functions as the storage server.

Media server: [redacted]

Storage server type: Media Server Deduplication Pool

Storage server name: [redacted]

Define credentials

User name: administrator

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

2. Configure the MSDP server to use cloud storage. You can either select an existing disk pool or create a new disk pool. Optionally, you can create a cloud logical storage unit and disk pool with replication.

    a. Click **Create disk pool**.

    b. Enter the required information.

    c. Select and add the required cloud volume.

    d. Select the cloud storage provider as **Hitachi Content Platform for cloud scale**.

    e. Select the required details for the cloud storage provider.

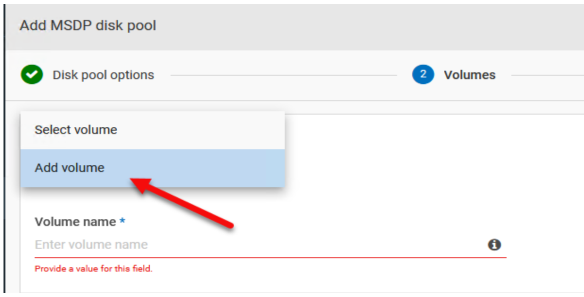
    f. Enter the login credentials to access the cloud storage provider.

    g. Enter the details for the **Advance** settings.

    h. Enter a name for the storage server and the disk pool.

3. Add the MSDP disk pool and the HCP for cloud scale volume.

    a. Click **Add Volume**.



Add MSDP disk pool

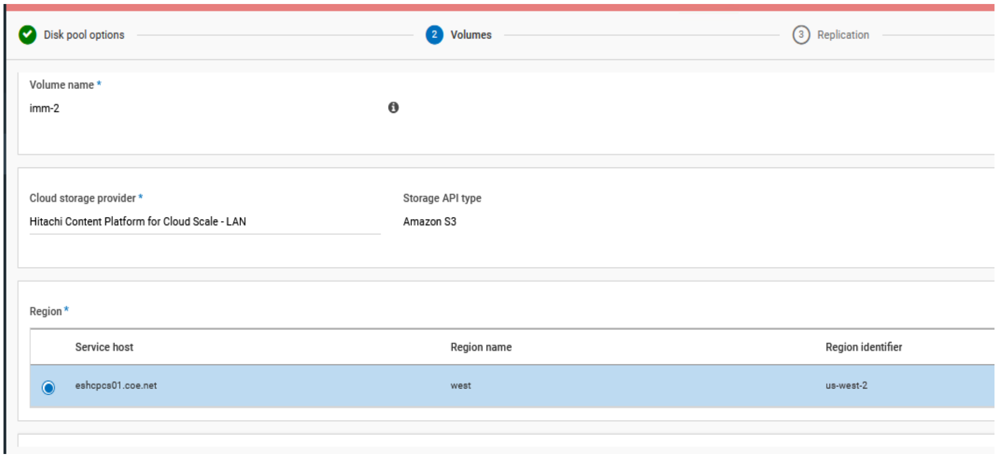
Volume name *

Enter volume name

Provide a value for this field.

b. Enter the volume name and click **Next**.

4. Enter the HCP for cloud scale bucket credentials and click **Next.**



Volume name *

imm-2

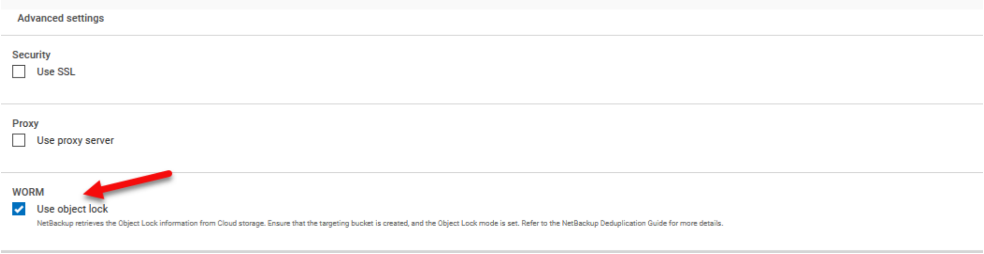
Cloud storage provider * Hitachi Content Platform for Cloud Scale - LAN

Storage API type Amazon S3

Region *

	Service host	Region name	Region identifier
●	eshcpcs01.coe.net	west	us-west-2

5. Select the **WORM Use object lock** option and click **Next**.



Advanced settings

Security

□ Use SSL

Proxy

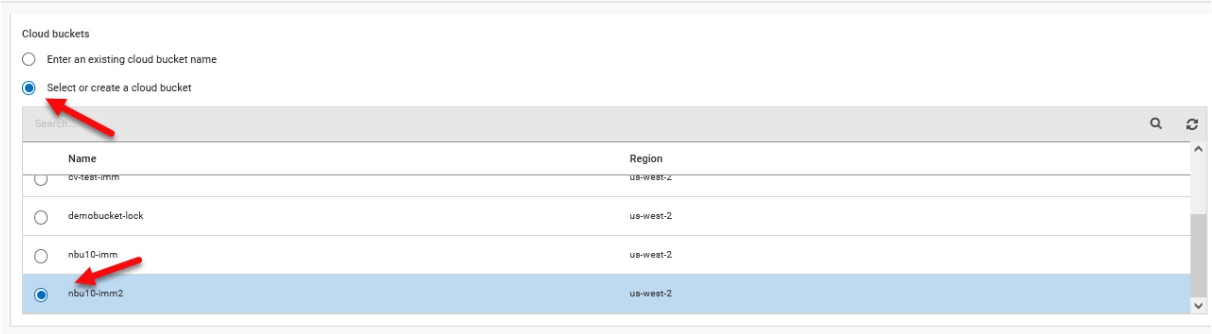
□ Use proxy server

WORM

☑ 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 details.

6. Select the **Select or create a cloud bucket** option and select the cloud bucket.



Cloud buckets

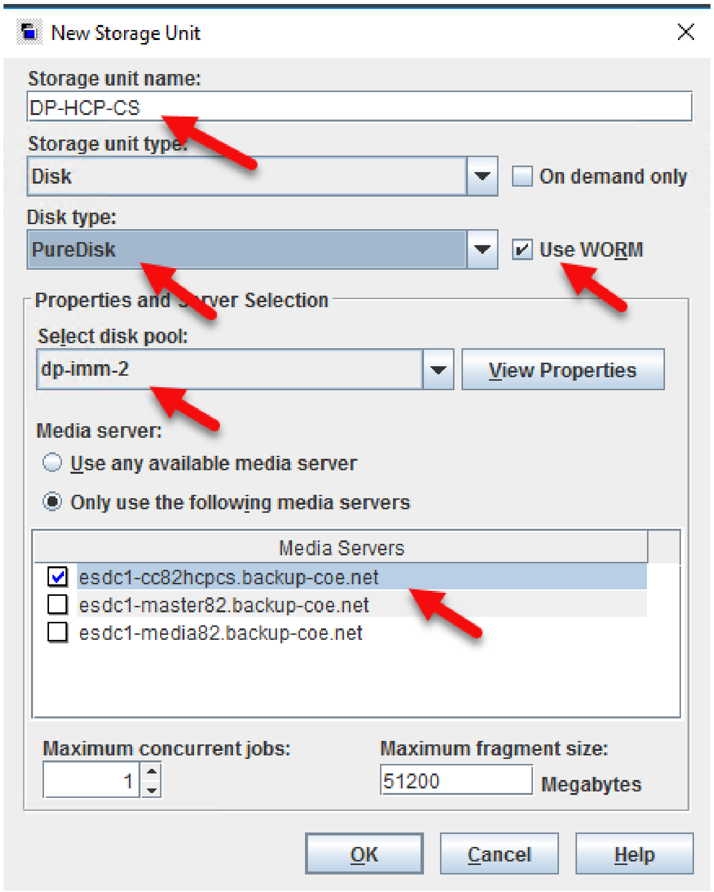
○ Enter an existing cloud bucket name

● Select or create a cloud bucket

	Name	Region
○	cv-test-imm	us-west-2
○	demobucket-lock	us-west-2
○	nbu10-imm	us-west-2
●	nbu10-imm2	us-west-2

7. Verify the following Veritas NetBackup storage unit parameters and click **OK.**

   - Storage unit name
   - Disk type
   - Disk pool
   - Media Servers
   - Use WORM (selected)



New Storage Unit

Storage unit name: DP-HCP-CS

Storage unit type: Disk

□ On demand only

Disk type: PureDisk

☑ Use WORM

Properties and Server Selection

Select disk pool: dp-imm-2

Media server:

○ Use any available media server

● Only use the following media servers

Media Servers
☑ esdc1-cc82hcpcs.backup-coe.net
□ esdc1-master82.backup-coe.net
□ esdc1-media82.backup-coe.net

Maximum concurrent jobs: 1

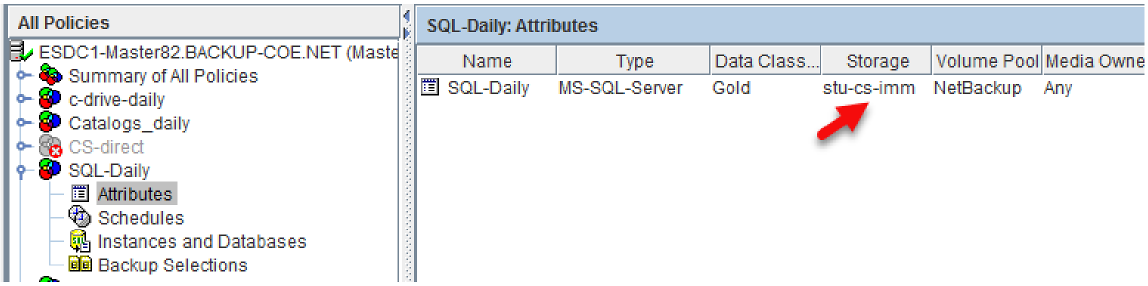
Maximum fragment size: 51200 Megabytes

Back up to the HCP for cloud scale bucket and test Object Lock immutability

After you configure the immutable storage volume, you can back up the data to the HCP for cloud scale bucket using Veritas NetBackup policies. You can also test object lock immutability.

1. Using the Veritas NetBackup wizard, configure the backup job.

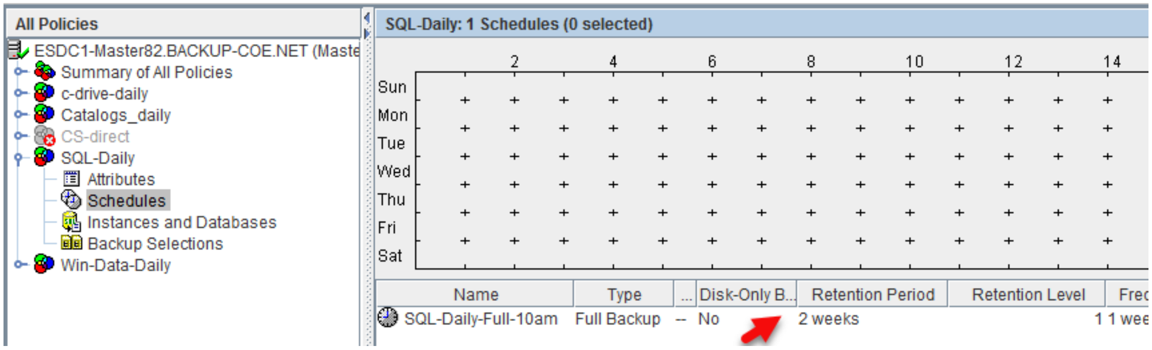
2. Create an SQL-daily job routing to storage unit `stu-cs-imm` that points to the HCP for cloud scale bucket.



SQL-Daily: Attributes

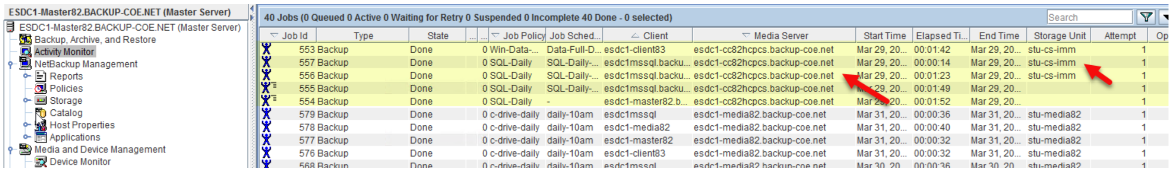
Name	Type	Data Class...	Storage	Volume Pool	Media Owne
SQL-Daily	MS-SQL-Server	Gold	stu-cs-imm	NetBackup	Any

The following image shows the retention set from the Veritas Netbackup policy:



Name	Type	...	Disk-Only B...	Retention Period	Retention Level	Frec
SQL-Daily-Full-10am	Full Backup	--	No	2 weeks	1	1 wee

3. View the completed backup jobs from the Activity monitor, based on the schedule and retention.


ESDC1-Master82.BACKUP-COE.NET (Master Server)
ESDC1-Master82.BACKUP-COE.NET (Master Server)
Backup, Archive, and Restore
Activity Monitor
NetBackup Management
Reports
Policies
Storage
Catalog
Host Properties
Applications
Media and Device Management
Device Monitor
Search

40 Jobs (0 Queued 0 Active 0 Waiting for Retry 0 Suspended 0 Incomplete 40 Done - 0 selected)

Job Id	Type	State	...	...	Job Policy	Job Sched...	Client	Media Server	Start Time	Elapsed Ti...	End Time	Storage Unit	Attempt	Op
553	Backup	Done		0	Win-Data-...	Data-Full-D...	esdc1-client83	esdc1-cc82hcpcs.backup-coe.net	Mar 29, 20...	00:01:42	Mar 29, 20...	stu-cs-imm	1	
557	Backup	Done		0	SQL-Daily	SQL-Daily-...	esdc1mssql.backu...	esdc1-cc82hcpcs.backup-coe.net	Mar 29, 20...	00:00:14	Mar 29, 20...	stu-cs-imm	1	
556	Backup	Done		0	SQL-Daily	SQL-Daily-...	esdc1mssql.backu...	esdc1-cc82hcpcs.backup-coe.net	Mar 29, 20...	00:01:23	Mar 29, 20...	stu-cs-imm	1	
555	Backup	Done		0	SQL-Daily	SQL-Daily-...	esdc1mssql.backu...	esdc1-cc82hcpcs.backup-coe.net	Mar 29, 20...	00:01:49	Mar 29, 20...		1	
554	Backup	Done		0	SQL-Daily	-	esdc1-master82.b...	esdc1-cc82hcpcs.backup-coe.net	Mar 29, 20...	00:01:52	Mar 29, 20...		1	
579	Backup	Done		0	c-drive-daily	daily-10am	esdc1mssql	esdc1-media82.backup-coe.net	Mar 31, 20...	00:00:36	Mar 31, 20...	stu-media82	1	
578	Backup	Done		0	c-drive-daily	daily-10am	esdc1-media82	esdc1-media82.backup-coe.net	Mar 31, 20...	00:00:40	Mar 31, 20...	stu-media82	1	
577	Backup	Done		0	c-drive-daily	daily-10am	esdc1-master82	esdc1-media82.backup-coe.net	Mar 31, 20...	00:00:32	Mar 31, 20...	stu-media82	1	
576	Backup	Done		0	c-drive-daily	daily-10am	esdc1-client83	esdc1-media82.backup-coe.net	Mar 31, 20...	00:00:32	Mar 31, 20...	stu-media82	1	
568	Backup	Done		0	c-drive-daily	daily-10am	esdc1mssql	esdc1-media82.backup-coe.net	Mar 30, 20...	00:00:36	Mar 30, 20...	stu-media82	1	

Verify the security of the object lock

Verify the security of the object lock by attempting to delete an object.

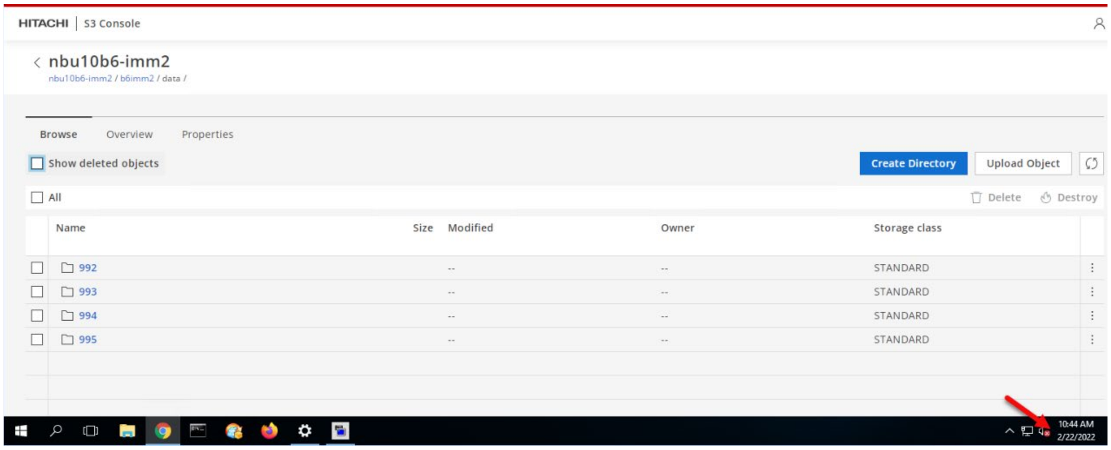
1. Log in to HCP for cloud scale**.**

2. Delete the S3 Object Lock data that was created using Veritas NetBackup backup policy.

   Note: Locked objects cannot be deleted. Object locks implement write once, read many (WORM) behavior, which protects objects from accidental or malicious changes.

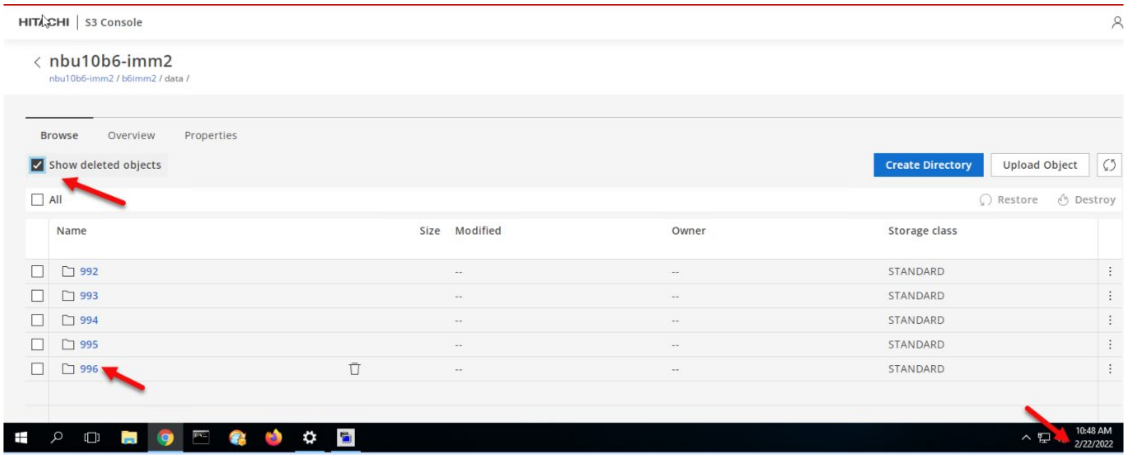
   When you delete an object or a version of an object, it is removed from the object list. However, a delete marker is created, allowing the data associated with it to be restored to full functionality at any point. HCP for cloud scale sets the delete marker.

   In the following example, object 996 was deleted. However, it was only moved to the object list, which is visible under deleted objects.



	Name	Size	Modified	Owner	Storage class
☐	992		--	--	STANDARD
☐	993		--	--	STANDARD
☐	994		--	--	STANDARD
☐	995		--	--	STANDARD

The deleted object remains visible until the Veritas NetBackup retention period expires.

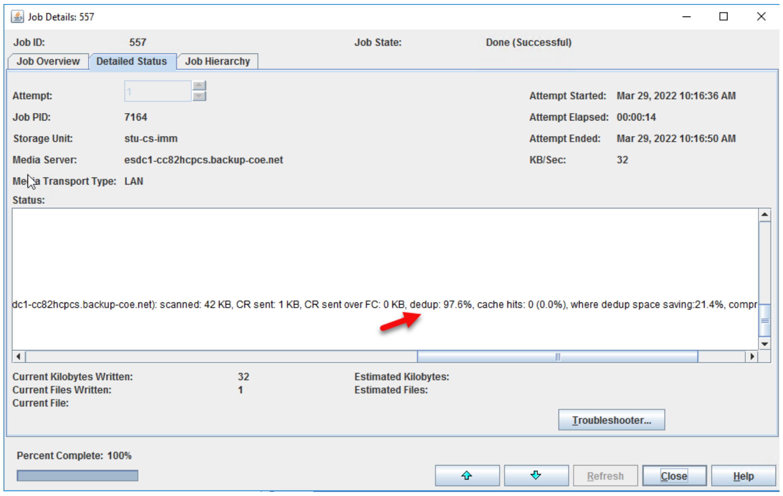


	Name	Size	Modified	Owner	Storage class
☐	992		--	--	STANDARD
☐	993		--	--	STANDARD
☐	994		--	--	STANDARD
☐	995		--	--	STANDARD
☐	996		--	--	STANDARD

Observe deduplication and ingested details during a backup

This test demonstrates the log validation of the deduplication and the ingested information during a backup job.

The Veritas NetBackup Job Details screen shows the job status with the source-side deduplication from the Veritas NetBackup MSDP-C.



Job ID: 557 Job State: Done (Successful)

Attempt: 1 Attempt Started: Mar 29, 2022 10:16:36 AM
Job PID: 7164 Attempt Elapsed: 00:00:14
Storage Unit: stu-cs-imm Attempt Ended: Mar 29, 2022 10:16:50 AM
Media Server: esdc1-cc82hcpcs.backup-coe.net KB/Sec: 32
Media Transport Type: LAN
Status:

```
dc1-cc82hcpcs.backup-coe.net): scanned: 42 KB, CR sent: 1 KB, CR sent over FC: 0 KB, dedup: 97.6%, cache hits: 0 (0.0%), where dedup space saving:21.4%, compr
```

Current Kilobytes Written: 32 Estimated Kilobytes:
Current Files Written: 1 Estimated Files:
Current File:

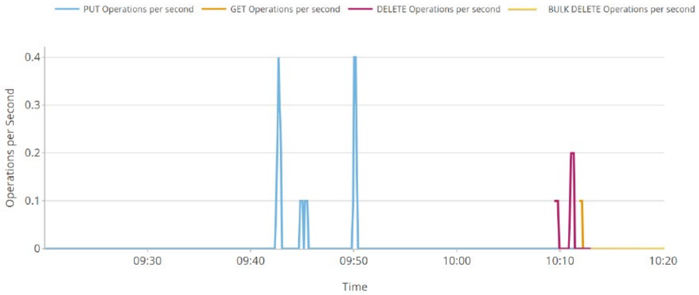
Percent Complete: 100%

The HCP for cloud scale S3 user interface provides the following metrics:

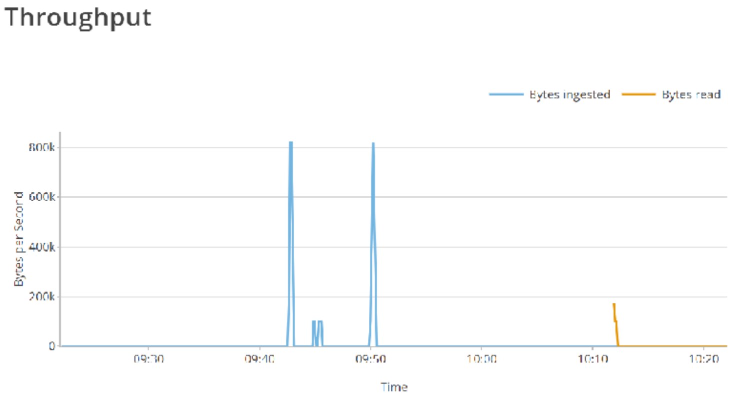
- Input/output operations
- Loading of objects (ingest)
- Number of object stores
- Disk usage of stored objects

For more information about Metrics and Monitoring, see the *Hitachi Content Platform for Cloud Scale Administration Guide* at https://knowledge.hitachivantara.com/Documents/Storage/HCP_for_Cloud_Scale

HCP for cloud scale tracks the input/output operations per second (IOPS) during the backup progress. The following dashboard displays the IOPS. You can hover your pointer over the graph for detailed information about PUT, GET, DELETE, and BULK DELETE operations per second.



The **Throughput** dashboard displays the throughput of the files that are being backed up in bytes. You can hover your pointer over the graph for detailed information about specific data points.



Malware scan

NetBackup malware detection defends against undesirable data propagating in your environment. With the Anomaly Detection engine working automatically, you can add malware detection workflows. Malware detection offers a powerful point of insight into backup images as a response to an alert or on-demand scan of a backup image.

Configure a malware scan and test the last known scan with Veritas NetBackup. Microsoft Defender Antivirus software was used for this test. For more information about AI-Driven Anomaly Detection and Automated Malware Scanning, see the *NetBackup Malware Detection* technical document at: https://www.veritas.com.

Perform the following steps using the NetBackup wizard:

1. Log in to the Windows media server.

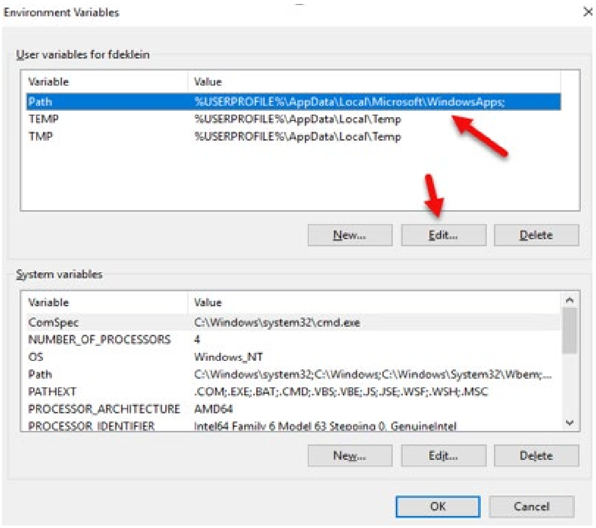
2. Set the executable path in the `PATH` environment variable:

    a. Navigate to Control Panel>All Control Panel Items>System Properties>Environment Variables.

    b. Click **Edit** and create a new user variable for Windows Defender.

    c. Set the variable value to the default installation location of Windows Defender. For example, C:\Program Files\Windows Defender.

    d. Click **OK** and click **Apply**.



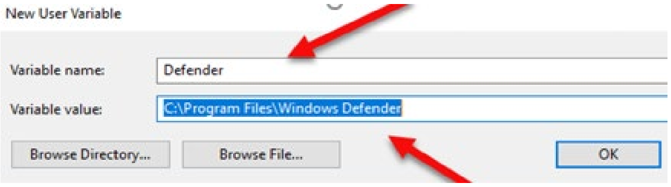
Environment Variables

User variables for fdeklein

Variable	Value
Path	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
NUMBER_OF_PROCESSORS	4
OS	Windows_NT
Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 63 Stepping 0, GenuineIntel



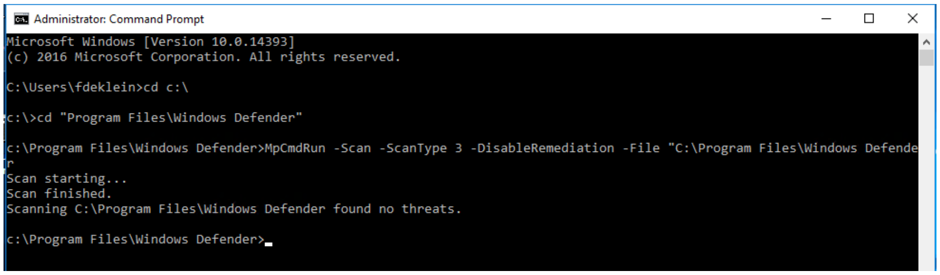
New User Variable

Variable name: Defender

Variable value: C:\Program Files\Windows Defender

3. Run the malware scan. Open a command prompt and enter:

```
C:\Program Files\Windows Defender>MpCmdRun -Scan -ScanType 3 -
DisableRemediation -File "C:\Program Files\Windows Defender
```



Administrator: Command Prompt

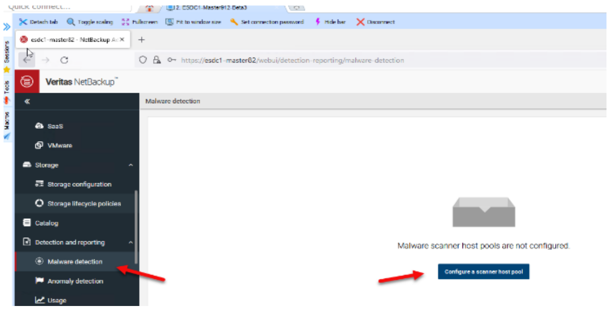
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\fdeklein>cd c:\

c:\>cd "Program Files\Windows Defender"

c:\Program Files\Windows Defender>MpCmdRun -Scan -ScanType 3 -DisableRemediation -File "C:\Program Files\Windows Defende
r
Scan starting...
Scan finished.
Scanning C:\Program Files\Windows Defender found no threats.

c:\Program Files\Windows Defender>_
```

4. Use the preconfigured malware application to create a malware scan host. Microsoft Defender Antivirus software was used to scan results in this test case.

   a. Log in to the Veritas NetBackup user interface.

   b. In the left pane, click **Detection and reporting**, and then click **Malware detection**.

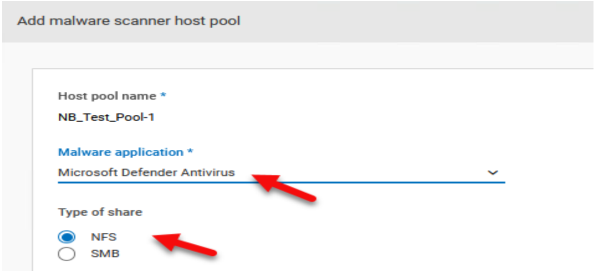
   c. On the **Malware detection** page, click **Configure a scanner host pool** to go to the **Host pools list** page.



Malware scanner host pools are not configured.

d. In the **Malware scanner host pools** page, click **Add** to add a new host pool.

e. In the **Add malware scanner host pools** page, enter the host pool name, the malware application, and the type of share.


Add malware scanner host pool

Host pool name *
NB_Test_Pool-1

Malware application *
Microsoft Defender Antivirus

Type of share
● NFS
○ SMB

f. Click **Save** to add the hosts.

4. Start the malware scanning to detect the malware:

   a. Navigate to the home page.

   b. Click **Detection and reporting**, and then click **Malware detection**.

   c. In the **Malware detection** window, click **Scan now**.

   d. Select **Standard Policy** or **Windows Policy**.

   e. From the client table, select a client to scan, and then click **Next**.

   f. In the **Select the timeframe of backups** window, verify and update the date and the time range.

   g. In the **Select a malware scanner host pool** window, select the appropriate host pool name.

   h. From the **Select the malware scan result status for images to be scanned** window, select one of the following options, and then click **Scan now**:

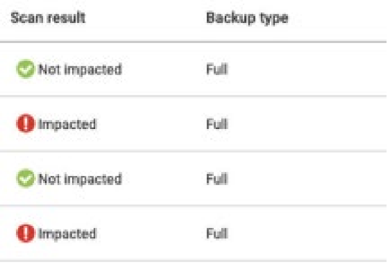
      - Not scanned
      - Not impacted
      - Impacted

- All

After the scan is initiated, you can see the malware scan progress in the **Malware Detection** window. The following fields are displayed:

- Not scanned
- Not impacted
- Impacted
- Failed

You can hover your pointer on the failed status to display the reason for the failed scan.

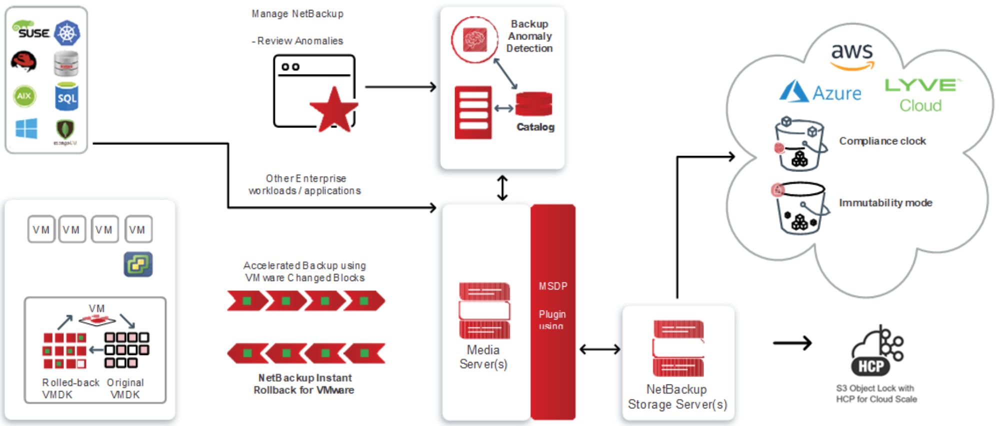


Scan result	Backup type
✓ Not impacted	Full
! Impacted	Full
✓ Not impacted	Full
! Impacted	Full

Additional details

- During backup, Veritas NetBackup divides the backup image data into chunks called objects.
- PUT requests are made for each object to move them to HCP for cloud scale. You can set a custom object size to control the number of PUT and GET requests that are sent to and from the cloud storage.
- With HCP for cloud scale, you can configure the maximum file size for a single PUT object through the management API. The maximum and default file size are 5 GB.
- HCP for cloud scale uses Prometheus and Grafana, third-party open-source tools for the graph and dashboard design. You can monitor various operations of different use cases. See the HCP for cloud scale documentation or the customer support site for more information.

  For more information about Prometheus, see https://prometheus.io/docs/prometheus/latest/querying/examples. For more information about Grafana, see https://grafana.com/grafana/dashboards.
- The following image shows end-to-end ransomware protection by Veritas NetBackup and Hitachi Vantara.


Manage NetBackup
- Review Anomalies
Backup Anomaly Detection
Catalog
Other Enterprise workloads / applications
VM
VM
VM
VM
VM
Rolled-back VMDK
Original VMDK
Accelerated Backup using VMware Changed Blocks
NetBackup Instant Rollback for VMware
Media Server(s)
MSDP
Plugin using
NetBackup Storage Server(s)
aws
Azure
LYVE Cloud
Compliance clock
Immutability mode
HCP
S3 Object Lock with HCP for Cloud Scale

Conclusion

Together, Veritas and Hitachi Vantara provide a multilayered approach to tackle ransomware throughout all threat stages. This was successfully demonstrated by performing the validation tests mentioned in this document. Veritas and Hitachi Vantara are focused on proactive infrastructure protection, rather than reactive defense. Hitachi Vantara builds strong walls between attackers and crucial data. Veritas provides rapid and accurate data recovery as the last line of defense if any attacks penetrate the defense mechanism.

Further reading

Visit the following links to learn more about Hitachi Content Platform:

- HCP for cloud scale product documentation (login required): https://knowledge.hitachivantara.com/Documents/Storage/HCP_for_Cloud_Scale/
- Hitachi support documentation (login required): https://support.hitachivantara.com/en/user/home.html
- Hitachi Product Compatibility Guide (login required): https://compatibility.hitachivantara.com/products/hcp-cloud

See the *Veritas NetBackup Deduplication Guide* and *Veritas NetBackup Administrator's Guide* at: https://sort.veritas.com/documents

Hitachi Vantara

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

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