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

v2.0

Implementation Guide

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

Table of Contents ................................................................. 3
Preface ...................................................................................... 5
   About this document .......................................................... 5
   Document conventions ....................................................... 5
   Intended audience ............................................................. 5
   Revision History ............................................................... 6
   Accessing product downloads ........................................... 6
   Getting Help ....................................................................... 6
   Comments ........................................................................... 6
Solution Overview ............................................................... 7
   Solution Diagram ............................................................. 9
   Solution Components ....................................................... 9
      Backup System ............................................................ 9
      Storage System .......................................................... 10
System Requirements ......................................................... 11
Configuring and Installing Hitachi Components .................... 12
   Installing the DNS and CM-REST Servers ......................... 13
      Configuring the DNS server ......................................... 13
      Configuring the CM-REST server ................................. 13
Configuring and Installing Veritas NetBackup Components ...... 15
   Installing the Master server .............................................. 15
   Installing NetBackup Media Server .................................. 15
   Installing NetBackup Client ............................................ 15
   Configuring MSDP-C Storage ......................................... 16
      Prepare the environment .............................................. 16
      Create an MSDP cloud immutable storage volume ........... 17
      Add a Disk pool from the NetBackup WEB UI ................ 20
      Create a Storage Unit using WORM Lock feature .......... 23
   Configuring Storage Life Cycle Policy ............................... 24
   Installing and Configuring the CloudPoint Server to use Snapshot Manager ................. 28
      Preparing for CloudPoint Installation ............................ 28
      Installing CloudPoint using Docker .............................. 28
Configuring CloudPoint plug-ins .......................................................................................................... 29
Configuring a Policy for using Snapshot Manager .............................................................................. 30
Installing NetBackup Malware Scanner ........................................................................................... 34
Preparing the Scan Host ..................................................................................................................... 34
Installing the Malware scanner ............................................................................................................ 34
Configuring Anomaly Detection ........................................................................................................ 34

NetBackup Backup and Restore Operations .................................................................................... 35
Running a Snapshot Backup Job using a CloudPoint server for VSP 5600 storage system and HCP for Cloud Scale ........................................................................................................................ 35
Restoring a Snapshot Backup Job .................................................................................................... 40
  Description before restoration ............................................................................................................. 40
  Preparation before Restore ............................................................................................................... 40
Restoring from a VSP 5600 storage system ....................................................................................... 41
Restoring from HCP for Cloud Scale ................................................................................................... 45
Point in time restore ............................................................................................................................. 47

NetBackup and Hitachi Cyber Security Capabilities .................................................................. 51
Verifying Anomaly Detection during Backup .................................................................................... 51
Verifying Malware detection after Backup and before Restore Manually ...................................... 53
  NetBackup Malware Scanner Test with Non-affected files ............................................................ 53
  NetBackup Malware Scanner Test with Virus affected files ............................................................ 58
Data Protection Within the Retention Period ...................................................................................... 63
  Verify WORM lock Feature from NetBackup End ........................................................................ 63

Limitations and Troubleshooting .................................................................................................... 65
Limitations ........................................................................................................................................ 65
Troubleshooting ................................................................................................................................. 65

Conclusion ......................................................................................................................................... 68
Preface

About this document

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

Document conventions

This document uses the following typographic convention:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 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

<table>
<thead>
<tr>
<th>Revision</th>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0</td>
<td>Initial release</td>
<td>April 2023</td>
</tr>
<tr>
<td>v2.0</td>
<td>Added x509 error solution and secured the connection for data transferring in HCP for Cloud Scale</td>
<td>October 2023</td>
</tr>
</tbody>
</table>

Accessing product downloads


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

Getting Help

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

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

Comments

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

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

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

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

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

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

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.

Figure 1: Data recovery framework
**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:

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

Table 1: Hardware and software requirements

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

<table>
<thead>
<tr>
<th>Server</th>
<th>Operating System version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td></td>
</tr>
<tr>
<td>Client</td>
<td>RHEL 7.8</td>
</tr>
<tr>
<td>CPE</td>
<td></td>
</tr>
<tr>
<td>CMREST server</td>
<td></td>
</tr>
<tr>
<td>Scan host</td>
<td>RHEL 8.2</td>
</tr>
<tr>
<td>DNS server</td>
<td>Windows 2019</td>
</tr>
</tbody>
</table>

Table 2: Operating systems
Configuring and Installing Hitachi Components

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

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

Configuring a Hitachi VSP 5600 storage system

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

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

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

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

For detailed information, see: Configuring iSCSI ports - Hitachi Vantara Knowledge

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

Configuring HCP for Cloud Scale

This section describes how to configure HCP for Cloud Scale Version 2.3.1 for a NetBackup end-to-end solution. This process consists of the following high-level steps:
1. Create an HCP for Cloud Scale S3 Bucket.

![HCP Console](image)

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

![Generate S3 Credentials](image)

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

## 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](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
   ![CPE file content]
   ```

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

   ```
   [root@cmrest tmp]# curl -k
   https://cmrest.ransomware.net:23451/ConfigurationManager/v1/objects/storages
   ```
Configuring and Installing Veritas NetBackup Components

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

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

Installing the Master server

To install the NetBackup master server, see the NetBackup Install Guide.

Installing NetBackup Media Server

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

Installing NetBackup Client

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

For more information, see the NBU installation Guide.

Configuring MSDP Storage

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

Configuring MSDP-C Storage

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

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

Prepare the environment

Before you begin, prepare the environment as follows:

1. Create an immutable storage volume from Veritas NetBackup, which creates a bucket in HCP for cloud scale.

2. Verify that HCP for cloud scale has a valid SSL certificate.

3. To perform the system and admin tasks, set up the following environment variables on the MSDP-C server:

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

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

   - hitachi-csw (HCP for cloud scale, WAN)
   - hitachi-csl (HCP for cloud scale, LAN)
Create an MSDP cloud immutable storage volume

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

Note: To skip SSL, use “—disablessl”. For more details, see the Troubleshooting section.

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

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

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

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

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

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

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

4. From master server properties, select Cloud Storage.

```
5. Add the Media server to the cloud provider Hitachi Content Platform for cloud scale LAN.
```
Add a Disk pool from the NetBackup WEB UI

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

1. Select a media server.
2. Enter a pool name.
3. Select the WORM lock feature.

4. Select an existing cloud bucket name.

5. Click **Next**.

6. Without adding replication, click **Next**.
7. Ensure that the use object lock feature is enabled.

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

```
[root@NBU MEDIA goodies]# /usr/openv/pdde/pdcr/bin/msdpclldutil list --disablesll
Bucket: veritas-ransomware
{
  "Bucket": "veritas-ransomware",
  "Volume": "veritas_vol",
  "Region": "us-west-2",
  "Volume Mode": "COMPLIANCE",
  "Volume LiveState": "ON",
  "Volume LiveUntilDate": "2025-08-25 00:00:00 +0000 UTC",
  "Volume LiveDuration": "2Y346D",
  "Volume RetentionTimeInherit": "unknown",
  "Volume LockMin": "86400",
  "Volume LockMax": "2592000",
  "Volume Configured": "true"
}
```

8. Verify the bucket and volume from HCP for Cloud Scale tab.
Create a Storage Unit using WORM Lock feature

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

1. Click Add Storage Unit.
2. Select the storage type.
3. Click Start.
4. Verify that WORM capable is checked.
5. Verify that a storage unit is created.

Configuring Storage Life Cycle Policy

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

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.
3. Select an operation.
   - First operation - Snapshot is created on a Hitachi VSP 5600 storage system.
   - Second operation - Backup of snapshot is stored on NetBackup media server (Hitachi VSP 5600 storage system).
   - Third operation - Backup of snapshot is stored on HCP for cloud scale.

4. Select **Destination Storage**.

5. Select an image expiry retention type and period.
Installing and Configuring the CloudPoint Server to use Snapshot Manager

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

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

Preparing for CloudPoint Installation

To install the container Platform Docker, complete the described in the following location:
https://www.veritas.com/content/support/en_US/doc/14079355-151836558-0/v140790360-151836558

Installing CloudPoint using Docker

To install CloudPoint using docker, complete the following steps:

1. Download the file from Veritas download center.

   ```
   docker load -i Veritas_CloudPoint_10.0.0.9818.img.gz
   docker run -it -rm -v /cloudpoint:/cloudpoint -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-cloudpoint:10.0.0.9818 install
   ```

2. From the NetBackup UI, click **Snapshot Manager**.
3. Enter a CloudPoint server name, user name, and password (which you created during installation).

Configuring CloudPoint plug-ins

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

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

To configure a policy, complete the following steps:

1. Right-click on **Summary of all policies**.
2. Click **New Policy**.

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

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

13. Select the backup path.
Installing NetBackup Malware Scanner

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

- Preparing the scan host
- Installing the malware scanner

Preparing the Scan Host

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

2. Before using the Malware scanner, review the following workflow:
   
   https://www.veritas.com/content/support/en_US/doc/21733320-149123528-0/v152646970-149123528

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

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

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

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

Installing the Malware scanner

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

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

Configuring Anomaly Detection

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

https://www.veritas.com/content/support/en_US/doc/21733320-149123528-0/v152007140-149123528
NetBackup Backup and Restore Operations

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

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

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

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

In this scenario, we are taking backup of a text file in the ‘/file_system’ path.
According to SLP, Snapshot job (Copy 1) has been completed successfully.

<table>
<thead>
<tr>
<th>Job ID</th>
<th>Type</th>
<th>State</th>
<th>Status</th>
<th>Job Policy</th>
<th>Job Schedule</th>
<th>Client</th>
<th>Media Seq</th>
<th>Start</th>
</tr>
</thead>
<tbody>
<tr>
<td>766 SnapShot</td>
<td>SnapShot</td>
<td>Active</td>
<td>Status</td>
<td>standard_nb_client</td>
<td>full</td>
<td>nbuora.ransomware.net</td>
<td>NBAMEC0</td>
<td>Oct 28, 2022</td>
</tr>
</tbody>
</table>

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:
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.

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

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

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:
6. Verify the backups from HCP for cloud scale.

Folders 10 and 11 are created in HCP for cloud scale after backup completion:
Folder 10 contains the backup data:

![Image of folder 10 containing backup data]

**Restoring a Snapshot Backup Job**

**Description before restoration**

According to SLP-cloud configuration:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Storage</th>
<th>Target Mail</th>
<th>Window</th>
<th>Volume Pool</th>
<th>Media Ow...</th>
<th>Retention</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot</td>
<td>MSDP-media</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Fixed</td>
<td>2 weeks</td>
<td></td>
</tr>
<tr>
<td>Backup From Snapshot</td>
<td>MSDP-media</td>
<td>--</td>
<td>Default</td>
<td>--</td>
<td>Fixed</td>
<td>2 weeks</td>
<td></td>
</tr>
<tr>
<td>Backup From Snapshot</td>
<td>MSDP-stu</td>
<td>--</td>
<td>Default</td>
<td>--</td>
<td>Fixed</td>
<td>2 weeks</td>
<td></td>
</tr>
</tbody>
</table>

**Preparation before Restore**

1. Before restoring any files, validate whether the backup images are infected or not. Follow the procedure in the [Malware detection before recovery](#) section.

2. To verify whether the deleted file is restored or not, manually remove the file from the client machine that was backed up.

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

**Restoring from a VSP 5600 storage system**

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

Complete the following steps:

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

2. Set Primary Copy to Yes.
3. Select the source and destination client for restoring
4. Select **Restore everything to its original location**.
5. Verify that the restoration is happening from copy 2.

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

2. Select **Restore everything to a different location** and then select the destination location.
Restoration is completed successfully from copy 3.

After the file is restored, it is visible from the client or destination server end.
Point in time restore

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

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

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

   All eligible snapshots are included in the list:
3. Select the correct image.

4. Click **OK**.

5. Select **Skip verification and force rollback**.

6. Select **Force rollback even if it destroys later snapshots**.
7. Verify that the restoration is happening from copy 1.

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
[root@nbuora linux_FS]# 
```
NetBackup and Hitachi Cyber Security Capabilities

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

Testing consists of the following high-level steps:

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

Verifying Anomaly Detection during Backup

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

Complete the following steps:

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

   ![Backup Jobs Table]

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

- **Mark as ignore:**

```
> 763 nbusran.. Standard 4 11.36 Medium Anomaly I.. Oct 26, 2022 Ignore test_malw.. full FULL
```

- **Confirm as anomaly:**

```
> 762 nbusran.. Standard 4 11.36 Medium Anomaly I.. Oct 26, 2022 Not review.. test_malw.. full FULL
```
• Report as false positive:

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

Verifying Malware detection after Backup and before Restore Manually

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

NetBackup Malware Scanner Test with Non-affected files

1. Set the backup image as the primary copy to scan.
2. Set copy 2 as the primary copy.
No malware is detected.

3. Click **Scan now**.

4. Select the client name for scanning the backup images.
5. Select the backup timeframe, Malware scanner host pool, and malware scan result status.

Scan task starts.

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

The **Create-Mount** operation is taking place.
### Job Details: 75534HBU390mware.net

**Job ID:** 75534

**File List:**
- SPWS_MOUNT_ID=55_16689502685
- SPWS_JOB_ID=39_16689502685

### Attempt Details:

- **Attempt Started:** Oct 31, 2022 4:25:46 AM
- **Attempt Elapsed:** 00:04:37
- **Attempt Ended:**
- **KB/sec:**

#### Storage Unit:
- **NBUMedia: ransomware.net**

#### Media Transport Type:
- **LAN**

**Status:**

### Malware Detection

**Last 48 hours**

- **0** Impacted
- **0** Not impacted
- **0** Pending
- **1** In progress
- **0** Failed
Instant Access completed.

Scan results:

After scanning, the scan result is not impacted.

The delete-mount task was started after scanning and completed successfully.
NetBackup Malware Scanner Test with Virus affected files

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

The following tests verify whether the file is affected or not.
1. Select the backup for the affected files (assumption) and take a full backup.

2. Perform malware scanning of the backup image.
Scanning is in progress.

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

3. To check the infected files, click **View infected files**.
It shows the virus affected files that have been manually created for the test.

![Infected files]

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.**

![Expire all copies]

Backup image is successfully expired.
After expiring the impacted files, they are removed from the catalog as well.

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

After expiration, the image is removed.

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.

2. Expire the image.

After you expire the image, the following error shows up:
WORM is working and is not giving permission to expire the image.

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

  **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:**
  
  ```bash
  # 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.

While adding cloud storage in NetBackup, add http and https ports.
2. After creating volumes from CLI, you can modify cloud storage settings from the NetBackup UI.

3. To secure the data transfer process, enable the SSL setting for Data Transfer and save the setting.

The data is safe in this solution.
Conclusion

In conclusion, we've effectively demonstrated the full utilization of the NIST framework in a comprehensive end-to-end cyber protection solution by 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.