

HITACHI

Double Immutability in Backup Targets using Ansible-Orchestrated Thin Image Advanced Snapshots and Hitachi Data Protection Suite

Implementation Guide

MK-SL-422-00

January 2026

Table of Contents

Notices and Disclaimer	3
About This Document	4
Introduction	4
Key Components.....	4
Intended Audience.....	4
Value Proposition	4
Document Revisions	5
Comments.....	5
Architecture Diagram.....	5
Core Components:	6
Test Scenario:	7
Prerequisites:	7
Ansible Configuration:.....	8
Implementation Steps.....	9
Test Scenario 1:.....	9
Test Scenario 2:.....	11
Test Scenario 3:.....	12
Test Scenario 4:.....	15
Summary	16
Appendix	16

Notices and Disclaimer

© 2026 Hitachi Vantara LLC. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara (collectively, "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" means text, data, photographs, graphics, audio, video and documents.

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

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

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

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

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

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

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

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

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

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

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

About This Document

Introduction

This document outlines the implementation of Double Immutability, leveraging the Hitachi Virtual Storage Platform One Block 26 (VSP One B20 series) with Thin Image Advanced (TIA) Safe Snap to deliver hardware-enforced immutability - a cornerstone of modern data protection and cyber-resilience strategies.

By integrating VSP's hardware-based immutable snapshots with Hitachi Data Protection Suite (HDPS), organizations can ensure their backup data remain secure, tamper-proof, and fully recoverable, even in the face of ransomware or insider threats. This solution provides an automated, verifiable, and policy-driven data protection workflow that unites software-defined immutability with hardware-level safeguards.

Key Components

The following components constitute the core of the validated solution:

- Storage Systems: Hitachi VSP E Series (storage source) and VSP One Block 20 series (storage target with QLC drives)
- Backup Software: Hitachi Data Protection Suite (HDPS) with immutable repository.
- Hitachi Thin Image Advanced (TIA) Automation Framework: TIA is the core snapshot technology that delivers rapid, space-efficient point-in-time copies on Hitachi Virtual Storage Platform VSP One Block 20 series storage systems. The automation framework leverages Ansible playbooks to trigger TIA Safe Snap creation and enforce immutability policies post-backup window.
- Network Infrastructure: Cisco Nexus 9000 Series switch for LAN connectivity and 25 Gb iSCSI fabric between Media Agent and storage
- Media Agent Server: Hitachi Advanced Server HA820 G2 configured as the HDPS Media Agent and backup controller

This guide is a blueprint to design, deploy, and automate a Double Immutability framework that protects backup data from ransomware, accidental deletion, and malicious modification.

Intended Audience

This document is designed for IT and infrastructure professionals responsible for data protection, cyber resilience, and operational recovery. It provides targeted insights for:

- Cybersecurity Analysts -> Understanding how double immutability mitigates ransomware risks and prevents reinfection by ensuring all recovery points are clean and tamper-proof.
- Backup & Recovery Administrators -> Learning how to manage HDPS immutable repositories, restore from Safe Snaps, and validate data integrity across backup and storage layers.
- Storage Administrators -> Configuring and maintaining Hitachi VSP E Series and VSP One Block 20 series storage systems, implementing TIA Safe Snap policies, and integrating with HDPS through Ansible workflows.
- Automation and DevOps Engineers -> Developing and maintaining Ansible playbooks that automate post-backup Safe Snap creation, recovery orchestration, and repository validation tasks.

Value Proposition

This solution's core strength is its ability to establish hardware-level immutability at the backup target. It achieves this robust defense through Double Immutability, uniting two distinct, robust layers of protection:

- Hardware-Level Immutability at the storage tier via TIA Safe Snap.
- Software Immutability at the backup layer via HDPS immutable repositories.

This combined approach delivers end-to-end protection against ransomware and unauthorized modification by making the entire backup target verifiably secure and unchangeable.

- Automated, policy-based protection through Ansible orchestration
- Defense-in-depth against ransomware, malicious deletions
- Simplified recovery operations with minimal administrative effort

Document Revisions

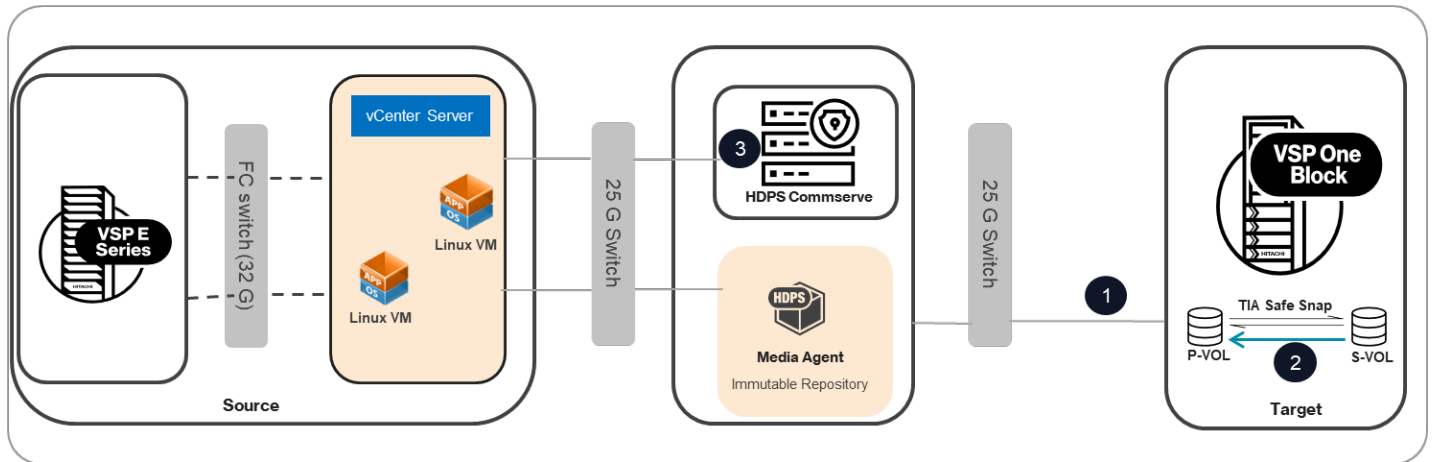
Revision Number	Date	Details
v1.0	1/2026	Initial release

Comments

Send any comments regarding this document to Docs-Feedback@hitachivantara.com. Include the document title, including the revision level, and refer to specific sections and paragraphs whenever possible. All comments are the property of Hitachi Vantara LLC.

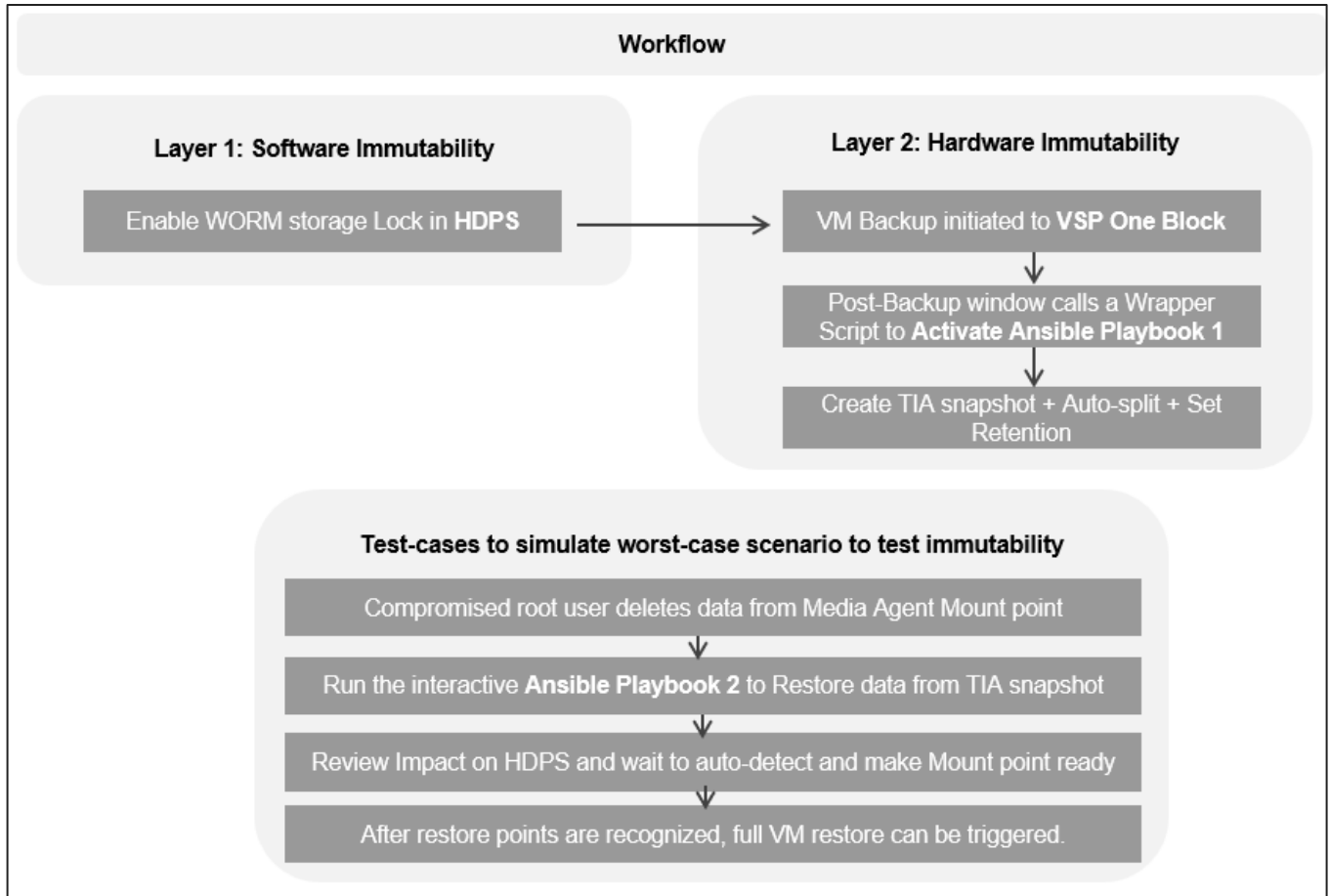
Thank you.

Architecture Diagram



- 1 VM backups are sent to VSP One Block via HDPS, followed by scheduled TIA snapshot post backup window (Ansible triggered to create TIA snapshot + set retention period + Auto Split)
- 2 In case of accidental deletion second Ansible playbook restores S-Vol data to P-VOL, replenishing the Media Agent mount point with untampered data
- 3 Commserve detects this renewed Immutable Repository, thus restoring recovery points.

The following section provides a comprehensive overview of the basic flow, detailing each step involved in the process:



Core Components:

Commserve and Media Agent	Storage
Version – 11.38 Compute: 2 x Hitachi Advanced Server HA820 G2 <ul style="list-style-type: none"> Operating System: RHEL 9.4 Processor: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz Network: HPE SN1600Q 32Gb 2p FC HBA Memory: 64GB, 2400 MHz Operating frequency 	Storage System: 1 x VSP One Block 26 <ul style="list-style-type: none"> Microcode: SVOS 10.4.1 Host Connectivity: FC Volume Type: DP and DRS Storage System: 1 x VSP E series <ul style="list-style-type: none"> Microcode: SVOS 9.8.7 Host Connectivity: FC Volume Type: DP
Production Hosts	Ansible
Compute: 8 x Hitachi Advanced Server HA810 G2 <ul style="list-style-type: none"> Operating System: RHEL 9.4 Processor: Intel® Xeon® Silver 4110 CPU @ 2.10GHz Network: HPE SN1600Q 32Gb 2p FC HBA Memory: 64GB, 2400 MHz Operating frequency 	Ansible Version: <ul style="list-style-type: none"> Ansible Core version: 2.14.18 Ansible Adapter version: 4.0 Compute: 1 x Hitachi Advanced Server HA810 G2 <ul style="list-style-type: none"> Operating System: RHEL 9.4 Processor: Intel® Xeon® Silver 4110 CPU @ 2.10GHz

Non-reducible and non-deduped data have been loaded using open-source tool VDBench.

Workload Details:

Random Block size: 2616 KB, Sequential Block size: 1639 KB, write ratio: 100%, Random ratio: 38%, Random write hit ratio: 4%

- Network: HPE SN1600Q
32Gb 2p FC HBA
- Memory: 64GB, 2400 MHz
Operating frequency

Test Scenario:

	Scenario	Action
1	Verify successful completion of VM backups to the HDPS Immutable Repository and enforcement of immutability within HDPS	Configure a virtualization client and run a backup job targeting the HDPS Immutable Repository with set retention and immutability policies. Confirm job completion. Attempt to delete backup data from the HDPS console. The backup should be completed successfully, and all deletion attempts must fail, validating software-defined immutability and retention lock.
2	Verify successful creation of TIA Safe Snap on VSP One B26 storage system for volumes hosting the HDPS Immutable Repository.	Execute an Ansible playbook from the HDPS Media Agent or proxy server to trigger a TIA Safe Snap on the target volume. Confirm that the snapshot is created successfully with the correct retention settings and immutable attributes, validating hardware-level immutability enforcement.
3	Validate protection of backup data against deletion or modification by a compromised root user and confirm successful restoration of the HDPS Immutable Repository using Safe Snap immutable snapshots on VSP One B26 storage system.	As root, attempt to modify or delete data from the HDPS Immutable Repository to simulate data loss. Use an Ansible plugin to restore the affected volume from the latest Safe Snap on VSP One B26 storage system (within the retention period). After restoration, perform an HDPS rescan to confirm all backup data is recovered and available, validating recovery through hardware-level immutability.
4	Validate end-to-end data recovery by restoring a client VM from the HDPS Immutable Repository.	From the HDPS console, initiate a full VM restore for a client backed up to the Immutable Repository. Select the desired restore point and destination, configure restore options, and execute the job. Verify that the VM is restored, and operational, confirming successful recovery from double-immutable protection.

Prerequisites:

- Deploy and configure virtual machines for the client (source VMs), HDPS CommServe, and Media Agent/VSA Proxy, ensuring all HDPS components (CommServe, Media Agent, VSA) are properly installed and connected.
- Provision and map LDEVs on the target storage system (VSP One B26 storage system), and mount HDPS disk libraries (immutable repositories) on the Media Agent using the XFS file system. Configure these libraries with WORM policies to enforce software-defined immutability.
- Create an HDPS administrative user with the required roles and permissions for backup, restore, and snapshot operations.

Ansible Configuration:

1. Download the Ansible Installation package (ansible-galaxy collection install hitachivantara.vspone_block) from [Ansible Galaxy – hitachivantara.vspone_block](#) and install it on a separate server to use it as the Ansible control node.
2. Once installed, the Ansible Control node is ready to access VSP One Block 26.
3. Access the path for getting the playbooks
/root/.ansible/collections/ansible_collections/hitachivantara/vspone_block/playbooks.
4. Navigate to the ansible_vault_vars directory and modify the ansible_vault_storage_var.yml file to adjust the following variables.
 - storage_serial
 - storage_address
 - vault_storage_username
 - vault_storage_secret

```
[root@SISHA820G3-46 ansible_vault_vars]# cat ansible_vault_storage_var.yml
---
# User will use Ansible Vault to encrypt this file.
# Ansible will decrypt this file when it executes the playbook.

# storage_serial and secondary_storage_serial are optional fields, they are kept for backward compatibility.
# You can remove these fields if you don't need them.

# Hitachi Vantara VSP One Block Storage Modules use REST API to communicate with the storage.
# For the storage_address and secondary_storage_address fields use the IP address or FQDN of the REST API server of the corresponding storage.
# For system configuration of the REST API for different Hitachi Storage Models, please refer to the following link:
# https://docs.hitachivantara.com/r/en-us/virtual-storage-platform-g130-g/f350-g/f370-g/f700-g/f900/93-07-2x/mk-23vspib003/overview-of-the-rest-api

storage_serial: 810020 # Example: 810018
storage_address: 172.23.68.56 # Example: storaget.company.com or sds1.company.com or 10.10.10.10
vault_storage_username: [REDACTED]
vault_storage_secret: [REDACTED]

secondary_storage_serial: <your_secondary_storage_serial_number>
secondary_storage_address: <your_storage_ip_address_or_fqdn> # Example: storaget.company.com or sds1.company.com or 10.10.10.10
vault_secondary_storage_username: <your_storage_user_name>
vault_secondary_storage_secret: <your_storage_password>
[root@SISHA820G3-46 ansible_vault_vars]#
```

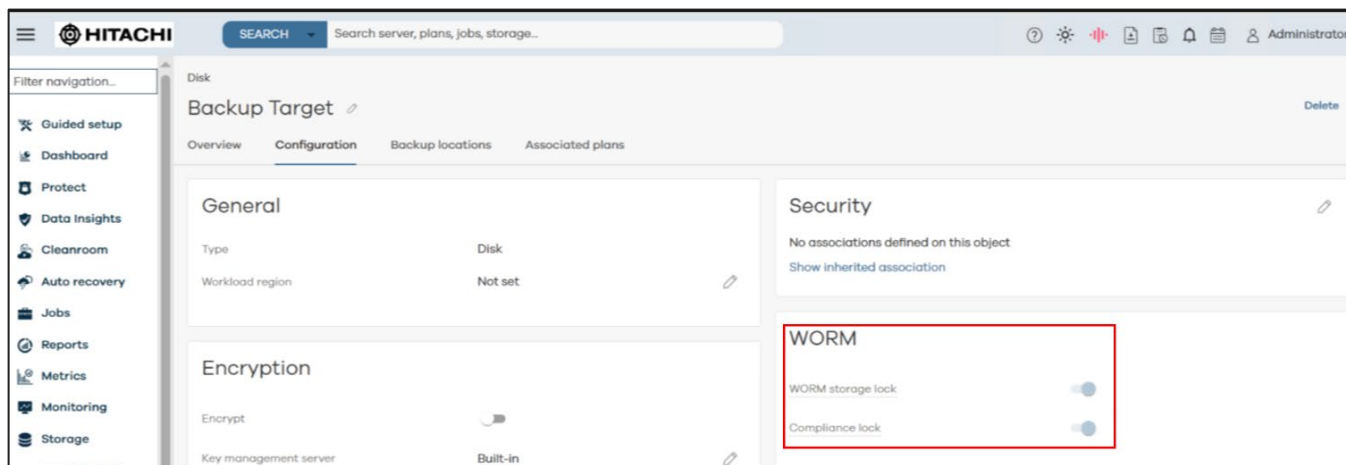
5. Then access the path
/root/.ansible/collections/ansible_collections/hitachivantara/vspone_block/playbooks/vsp_direct and get all the playbooks for managing VSP storage.
6. Get the playbook from the GitHub link and follow the instructions in the README.md file.
[hv-playbooks-vspone-block/HTIA_snapshotrestore](#) at main · hitachi-vantara/hv-playbooks-vspone-block
7. Keep the playbook snapshot_restore.yml on path
/root/.ansible/collections/ansible_collections/hitachivantara/vspone_block/playbooks/vsp_direct for point-in-time snapshot restore.

```
[root@SISHA820G3-46 vsp_direct]# pwd
/root/.ansible/collections/ansible_collections/hitachivantara/vspone_block/playbooks/vsp_direct
[root@SISHA820G3-46 vsp_direct]# ls | grep snapshot_restore.yml
snapshot_restore.yml
```

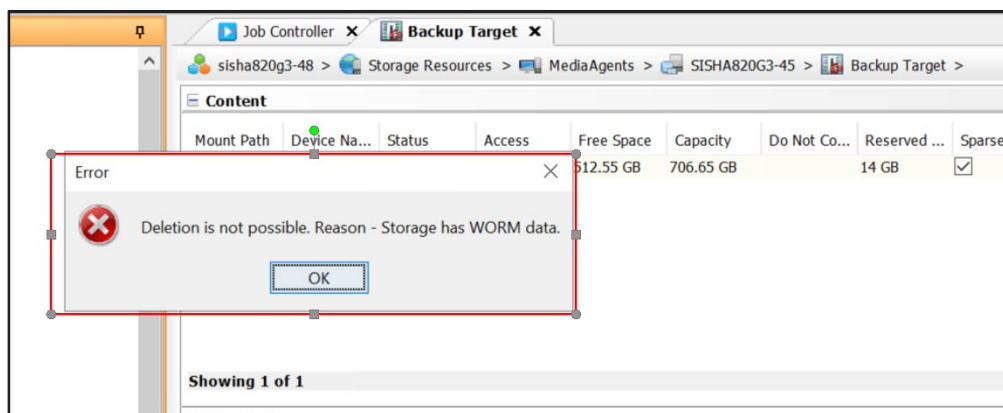
Implementation Steps

Test Scenario 1:

1. Activate software immutability by enabling WORM storage lock in HDPS



Once enabled, the associated library can't be deleted within the retention period.



2. Initiate Full Backup of the required VM group from HDPS console to the Immutable Repository. Verify that the backup location is available and healthy.

The screenshot displays the 'Job 22739 - [VM Admin Job(Backup)]' page in the Hitachi Vantara interface. A green notification banner at the top right states 'Job 22739 completed successfully'. The page is divided into several sections:

- Overview:** Shows tabs for Overview, VM list, Attempts, and Events.
- General:**
 - Type: VM Admin Job(Backup)
 - Backup type: Full
 - Status: Completed
 - Job started by: admin (Started interactively)
 - Encryption enabled: No
 - Storage Accelerator: No
- Progress:**
 - Start time: Oct 16, 2025, 7:58:42 AM
 - Elapsed time: 6 minutes 7 seconds
 - End time: Oct 16, 2025, 8:05:00 AM
 - Duration: 6 minutes 18 seconds
 - Average throughput: 2.04 TB/hr
 - Load: (Read: 92.38%, Write: 5.71%, Network: 1.91%)
 - Network throttle level: None
- Associations:**
 - Agent: Virtual Server
 - Source client computer: vCenterpod2C
 - Instance: VMware
 - Subclient: DoubleimmutabilityVMgroup
 - Plan: Backuptarget plan
- Item status:**
 - Failures: 0 Folders, 0 Files
 - Data transferred on network: 6.55 GB
 - Size of application: 202.04 GB
 - Estimated media size: 189.04 GB

The screenshot displays the 'Backup Target' configuration page in the Hitachi Vantara interface. The page includes the following sections:

- Overview:** Shows tabs for Overview, Configuration, Backup locations, and Associated plans.
- Associated MediaAgents:** A table listing the associated media agents.

MediaAgents	Roles	Actions
SSH-AE0003-45	Storage (Read/Write)	
- Backup locations:** A table listing the backup locations.

Name	Status	Actions
[SSH-AE0003-45]doubleimmutability	Ready	

Test Scenario 2:

1. Enforce Hardware-Level Immutability at the Backup Target using Hitachi TIA Safe Snap. Safe Snap is the essential technology, creating immutable snapshots on VSP One B26. This hardware-level defense locks the data against any modification or deletion.

To do this, start by configuring a “dummy” subclient in Commvault with a post-backup wrapper script to automatically trigger the Hitachi TIA Safe Snap process after the main backup window ends. This can be scheduled or run manually as needed.

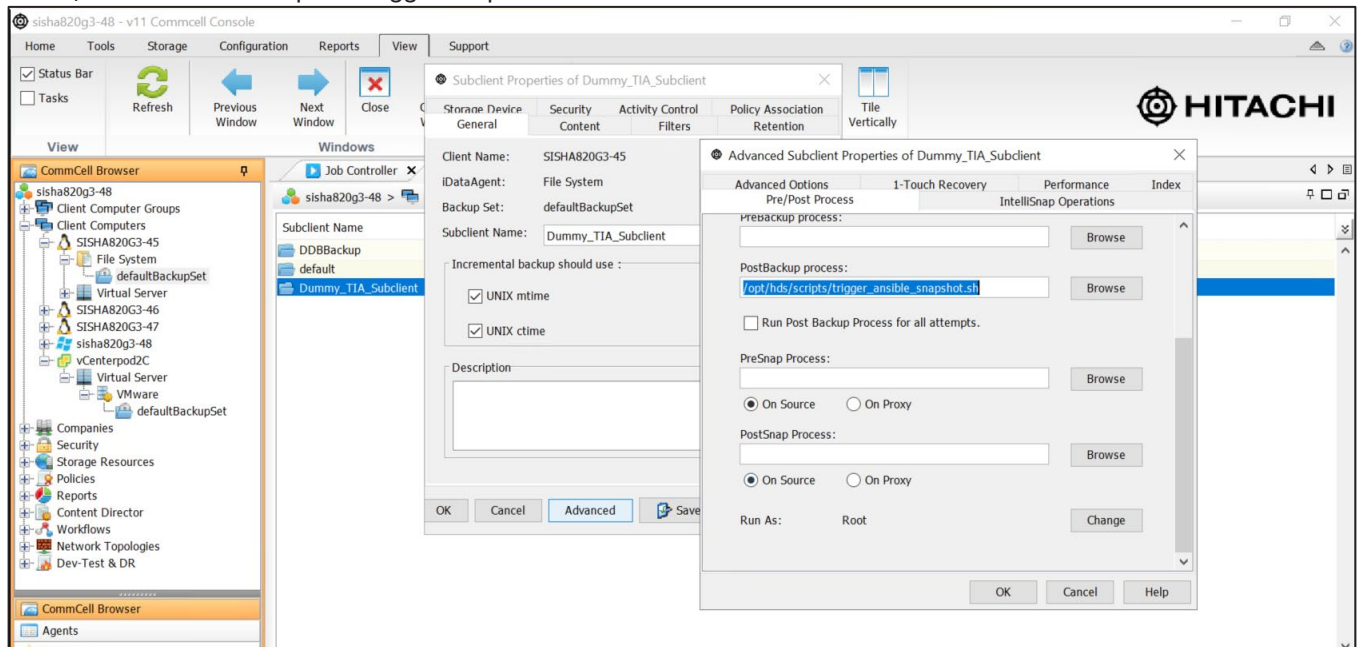
- **Step 1** – Prepare Trigger Script: Create and tag the wrapper script under:
`/opt/hds/scripts/trigger_ansible_snapshot.sh` on the Media Agent to invoke the Ansible playbook for snapshot creation. (Shared in Appendix: `trigger_ansible_snapshot.sh`)
- **Step 2** – Create Dummy Subclient: In the CommCell Console → Client Computers → [Media Agent] → New Subclient.
 - Configure:
 - Name: TIA_Trigger_Subclient
 - Content: /root/Dummy
 - Storage Policy: any valid policy
- **Step 3** – Assign Post-Backup Script: Open the subclient → Properties → Pre/Post Process tab → set Post Backup Process to `/opt/hds/scripts/trigger_ansible_snapshot.sh`.

NOTE: Disable secure install to save changes using: `cvpkgchg -sip N`.

Refer to Commvault documentation for disabling secure UNIX access permissions: [Disabling Secure UNIX Access Permissions for Existing Clients](#)

This is required to save the changes to the subclient after feeding the postscript in the media agent.

2. Schedule Trigger: Schedule or manually run the dummy subclient after the main backup window (for example, post 10 PM) to execute the snapshot trigger script.



Decoupling the TIA snapshot execution from active backup jobs was required to prevent I/O contention and ensure reliable scheduling. This method was essential due to the following constraints:

- There is no native Commvault trigger to schedule external scripts after all backup jobs finish.

- IntelliSnap integration is limited to source side, doesn't extend to Target side
 - Requirement to orchestrate snapshots via Ansible playbooks
3. Perform TIA Snapshot Creation: The wrapper script from the previous step, calls the Ansible Playbook 1 (Shared in Appendix: Ansible Playbook 1) to create a TIA Safe Snap on VSP One B26, capturing an immutable hardware-level snapshot of the backup volume.

```
[root@SISHA820G3-45 ~]#
[root@SISHA820G3-45 ~]# date
Thu Oct 16 08:21:41 AM UTC 2025
[root@SISHA820G3-45 ~]#
[root@SISHA820G3-45 ~]#
[root@SISHA820G3-45 ~]#
[root@SISHA820G3-45 ~]# raidcom get snapshot -snapshotgroup TIA_SNAP_12 -I001 -key details
SnapShot_name      P/S  STAT  Serial# LDEV#  MU#  P-LDEV#  PID  %  MODE      SPLT-TIME      SLU  C_LDEV#  P  R  D  STAT  RETENTION(H)
TIA_SNAP_12        P-VOL PSUS  810020  12    5    19    0    -  ---ARS----- 68f0a9d4      -   -  N  D  PSUS  1
[root@SISHA820G3-45 ~]#
[root@SISHA820G3-45 ~]#
[root@SISHA820G3-45 ~]#
[root@SISHA820G3-45 ~]# date
Thu Oct 16 08:21:46 AM UTC 2025
[root@SISHA820G3-45 ~]#
```

4. (Optional) Verify using the command shown above. Here, the user can confirm that the TIA snapshot has been created with a 1-hour retention period and a PSUS (Pair Suspended) state. Immutable snapshot cannot be deleted from VSP One Block 26 storage within the retention period.

Test Scenario 3:

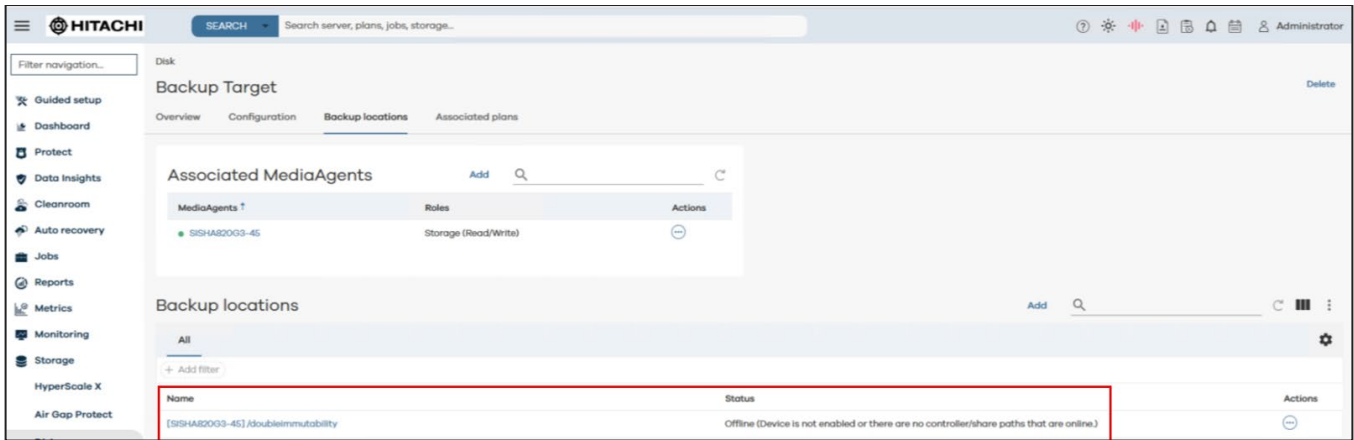
1. Simulate Data Deletion and Execute Restore: Data within the Immutable Repository is deleted inside the immutable repository by a compromised super user from the Media Agent.

Before deletion:

```
[root@SISHA820G3-45 doubleimmutability]# date
Thu Oct 16 08:22:21 AM UTC 2025
[root@SISHA820G3-45 doubleimmutability]# df -kh
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0  4.0M   0% /dev
tmpfs           63G   12K  63G   1% /dev/shm
tmpfs           26G   214M  25G   1% /run
efivarfs        496K  372K  120K  76% /sys/firmware/efi/efivars
/dev/mapper/rhel-root  70G   14G   57G  20% /
/dev/mapper/rhel-home 1.1T   7.3G  1.1T   1% /home
/dev/sdb2        960M  328M  633M  35% /boot
/dev/sdb1        599M   7.1M  592M   2% /boot/efi
tmpfs           13G   52K   13G   1% /run/user/42
tmpfs           13G   36K   13G   1% /run/user/0
/dev/mapper/vg_DIM-lv_DIM 450G   3.2G  447G   1% /DIM_DDB
/dev/mapper/mpathat 527G   3.8G  524G   1% /DIM_IC
/dev/mapper/mpathau 707G  195G  513G  28% /doubleimmutability
[root@SISHA820G3-45 doubleimmutability]#
[root@SISHA820G3-45 doubleimmutability]#
[root@SISHA820G3-45 doubleimmutability]# ll
total 4
-rw-rw---- 1 root root 38 Oct  7 04:15 DEVICE_LABEL
dwxrwxr-x 2 root root  6 Oct 15 04:25 LPQXH7_10.15.2025_04.22
dwxrwxr-x 3 root root 25 Oct 15 04:26 OSXJEI_10.15.2025_04.23
[root@SISHA820G3-45 doubleimmutability]#
[root@SISHA820G3-45 doubleimmutability]#
```

After data deletion:

```
[root@SISHA820G3-45 doubleimmutability]#
[root@SISHA820G3-45 doubleimmutability]# rm -rf DEVICE_LABEL LPQXH7_10.15.2025_04.22/ OSXJEI_10.15.2025_04.23/
[root@SISHA820G3-45 doubleimmutability]#
[root@SISHA820G3-45 doubleimmutability]#
[root@SISHA820G3-45 doubleimmutability]# ll
total 0
[root@SISHA820G3-45 doubleimmutability]#
[root@SISHA820G3-45 doubleimmutability]# date
Thu Oct 16 08:23:12 AM UTC 2025
```



Post Data Deletion: After the snapshot backup data is deleted from the Media Agent, the backup location status changes to Offline in the HDP console, indicating that the repository is no longer accessible.

2. Execute the `snapshot_restore.yml` playbook for data replenishment to the P-VOL.
3. Provide Primary Volume ID to fetch snapshot details. Recommended to use the snapshot that has a retention period set.
 - Identify the relevant `<mirror_unit_id>` for the desired point-in-time restore.

```
[root@SISHA820G3-46 vsp_direct]# ansible-playbook snapshot_restore.yml
[WARNING]: Collection hitachivantara.vspone_block does not support Ansible version 2.14.18
[WARNING]: running playbook inside collection hitachivantara.vspone_block
[WARNING]: Collection ansible.posix does not support Ansible version 2.14.18
Please enter the Primary_volume_id (e.g., convert from Hex[00:00:22] to Decimal[34]): 12

PLAY [Snapshot Pair Facts] *****
TASK [Get snapshot pairs with same primary_volume_id] *****
ok: [localhost]

TASK [Debug the result variable] *****
ok: [localhost] => {
  "result": {
    "ansible_facts": {
      "snapshots": [
        {
          "can_cascade": true,
          "concordance_rate": -1,
          "copy_pace_track_size": "",
          "copy_rate": -1,
          "is_clone": false,
          "is_cloned": false,
          "is_consistency_group": false,
          "is_data_reduction_force_copy": true,
          "is_redirect_on_write": true,
          "is_snapshot_data_read_only": null,
          "is_written_in_svol": false,
          "mirror_unit_id": 5,
          "pool_id": 0,
          "primary_hex_volume_id": "00:00:0C",
          "primary_volume_id": 12,
          "reconcile_rate": -1
        }
      ]
    }
  }
}
```

4. Get the details from all snapshots by scrolling up the tab. Again, a prompt will appear to provide the required details for restoration. User needs to provide `<Primary_volume_id>` and `<mirror_unit_id>` to continue the restoration task.

```
TASK [debug] *****
ok: [localhost] => {
  "msg": "Please check the all Snapshot Pairs and get the mirror_unit_id of required snapshot pair for restore"
}
Please enter the Primary Volume id (e.g., convert from Hex[00:00:22] to Decimal[34]): 12
Please enter the mirror_unit id: 5

PLAY [Snapshot Pair Module] *****
TASK [Restore snapshot pair] *****
changed: [localhost]
```

Restoration is completed, and data is recovered to its original location and remount to the directory is needed to view the recovered data.

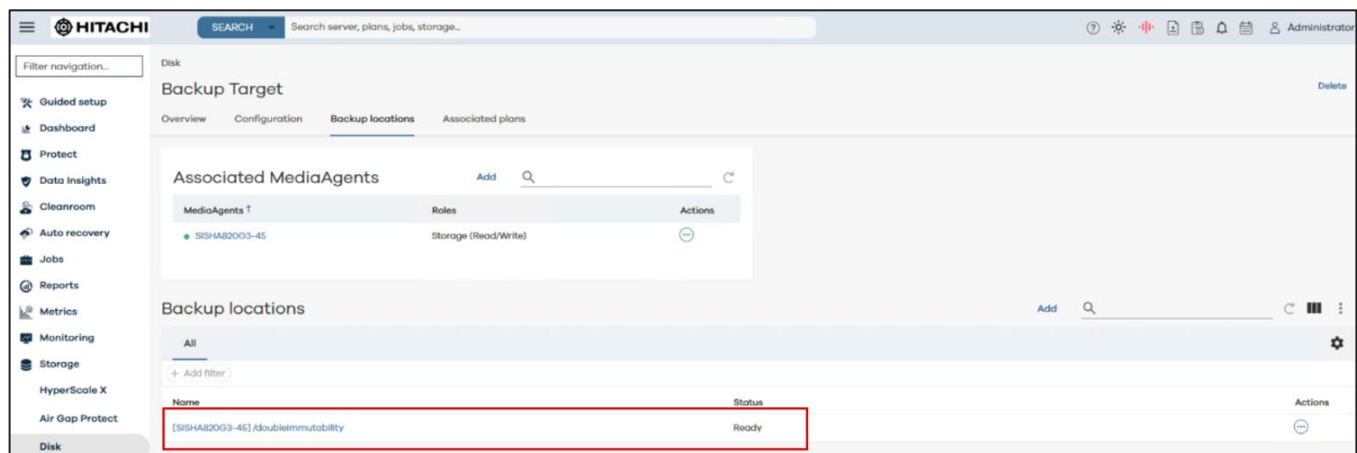
- Remount and Validate Restored Data: After restoration, provide the production server IP, mount path, and device path when prompted. The playbook automatically performs unmount, filesystem repair, and mount operations, after which data restoration is verified – confirming that the recovered data is visible and accessible from the production host.

```
TASK [debug] *****
ok: [localhost] => (
  "msg": "Your data has been restored to its original spot. Now, remount the directory to access the recovered files"
)
Please enter the production server IP for restore: 172.23.93.174
Please enter the mount path of your XFS volume (e.g., /directory): /doubleimmutability
Please enter the device path of your XFS volume (e.g., /dev/sdX or /dev/mapper/volume_group-logical_volume: /dev/mapper/mpathau)
PLAY [Unmount, XFS Repair, and Remount Volume] *****
TASK [Gathering Facts] *****
ok: [172.23.93.174]
TASK [Ensure no processes are using the mount point (optional but recommended)] *****
ok: [172.23.93.174]
TASK [Forcefully unmount the XFS volume] *****
changed: [172.23.93.174]
TASK [Perform XFS repair on the volume] *****
ok: [172.23.93.174]
TASK [Remount the XFS volume] *****
changed: [172.23.93.174]
PLAY RECAP *****
172.23.93.174      : ok=5   changed=2  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
localhost        : ok=6   changed=1  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
[root@SISHA820G3-46 vsp_direct]#
[root@SISHA820G3-46 vsp_direct]# date
Thu Oct 16 08:31:57 AM UTC 2025
```

- Data deleted from the Immutable Repository is fully recovered from the TIA Safe Snap, confirming end-to-end double immutability and seamless restoration through Ansible-driven orchestration.

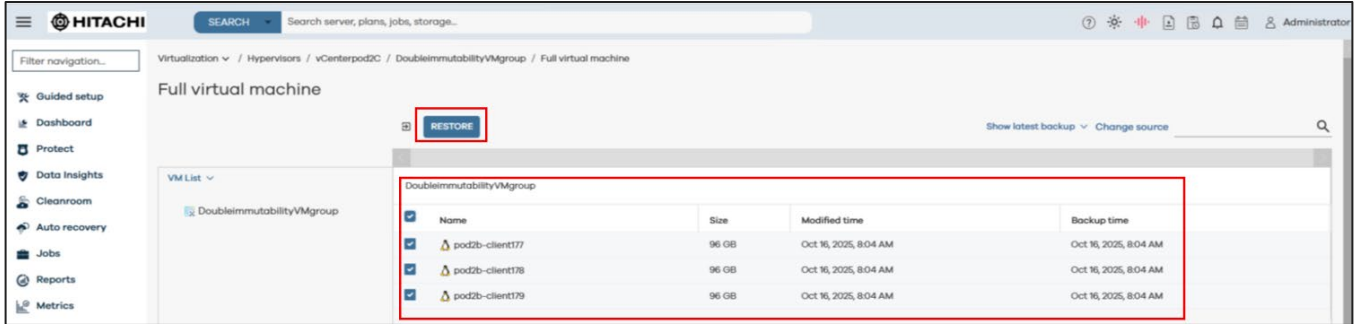
```
[root@SISHA820G3-45 ~]#
[root@SISHA820G3-45 ~]#
[root@SISHA820G3-45 ~]# cd /doubleimmutability
[root@SISHA820G3-45 doubleimmutability]# ll
total 4
-rw-rw---- 1 root root 38 Oct  7 04:15 DEVICE_LABEL
drwxrwxr-x 2 root root  6 Oct 15 04:25 LPQXH7_10.15.2025_04.22
drwxrwxr-x 3 root root 25 Oct 15 04:26 OSXJEI_10.15.2025_04.23
[root@SISHA820G3-45 doubleimmutability]#
[root@SISHA820G3-45 doubleimmutability]#
[root@SISHA820G3-45 doubleimmutability]# date
Thu Oct 16 08:32:14 AM UTC 2025
[root@SISHA820G3-45 doubleimmutability]#
```

Data is visible from the production host as seen above. From the HDPS, after waiting a few minutes, the mount point for the backup target comes back in ready status.

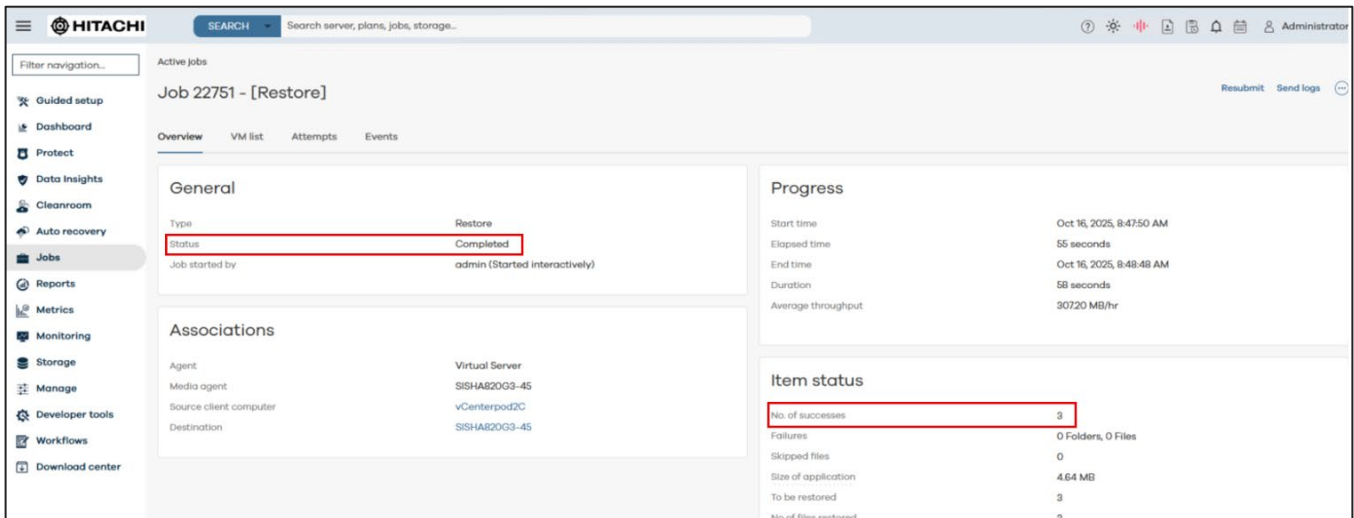
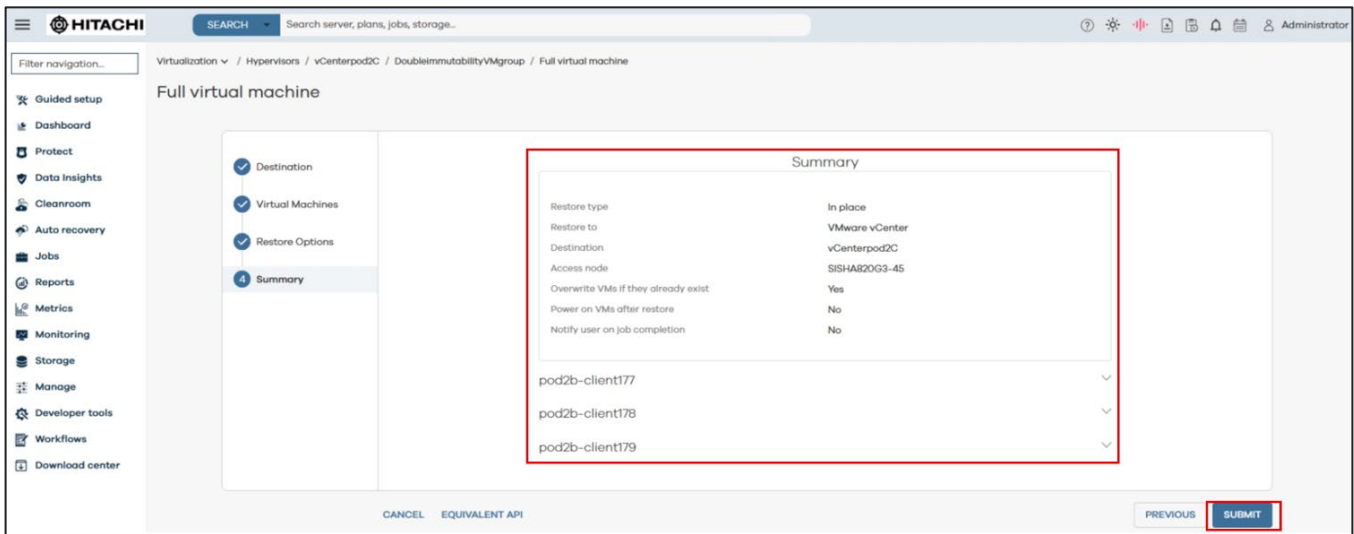


Test Scenario 4:

1. Restore from Immutable Repository: Initiate a full VM restore from the HDPS Immutable Repository using the CommCell Console (or Command Center). Select the required virtualization client and choose the desired restore point from the immutable backup.



Summary section gives a glimpse of the options selected as shown below:



After the job status displays Completed with successful item count, verify that the restored virtual machine is operational and accessible on the target ESXi host. This confirms successful end-to-end recovery and validates the Double immutability architecture – ensuring data protected through HDPS and Hitachi TIA Safe Snap can be fully recovered without integrity loss.

Summary

The integration of Hitachi Data Protection Suite (HDPS), Thin Image Advanced (TIA) Safe Snap, and Ansible automation delivers a resilient, double-immutability framework that ensures verified data integrity and dependable recovery against ransomware and insider threats.

Software-defined immutability in HDPS secures backup repositories, while hardware-level immutability via TIA Safe Snap on VSP One B20 series provides tamper-proof recovery points.

Furthermore, the TIA snapshots are now configured to execute automatically after the backup window, utilizing Commvault scheduling to eliminate I/O contention and ensure clean separation between backup and snapshot operations, simplifying operations and strengthening overall data protection.

The combination of hardware-enforced immutability and precise automation dramatically strengthens the cyber-resilience posture, guaranteeing that organizations maintain business continuity and can execute seamless recovery from any compromise.

Appendix

1. Wrapper Script:

- a. Name: trigger_ansible_snapshot.sh
- b. Use: Executes Ansible playbook 1 to trigger Hitachi TIA snapshot creation, invoked during Post-Backup Process via post-script
- c. Code:

```
#!/bin/bash

# --- CONFIGURATION VARIABLES ---
ANSIBLE_SERVER="172.23.93.175"
ANSIBLE_USER="root"
PLAYBOOK_PATH="/root/.ansible/collections/ansible_collections/hitachivantara/vspone_block/playbooks/vsp_direct/D
Ksnapshot_multi.yml"
LOG_FILE="/opt/hds/log/ansible_snapshot_trigger.log"

# --- FUNCTIONS ---
log_message() {
    echo "$(date '+%Y-%m-%d %H:%M:%S') - $1" | tee -a "$LOG_FILE"
}

# --- MAIN SCRIPT EXECUTION ---
log_message "Starting remote Ansible playbook execution on $ANSIBLE_SERVER"

# Use SSH to run the Ansible playbook on the remote server
ssh "$ANSIBLE_USER@$ANSIBLE_SERVER" "ansible-playbook $PLAYBOOK_PATH" >> "$LOG_FILE" 2>&1

# Check the exit status of the SSH command
SSH_STATUS=$?
if [ $SSH_STATUS -eq 0 ]; then
    log_message "Ansible playbook completed successfully on $ANSIBLE_SERVER."
    exit 0
else
    log_message "ERROR: Ansible playbook failed on $ANSIBLE_SERVER. SSH exit status: $SSH_STATUS."
    exit 1
fi
~
```

2. Ansible Playbook 1:

- a. Name: DKsnapshot_multi.yml
- b. Use: Trigger Hitachi TIA snapshot creation, splits the Pair and creates a retention period of 1 hour
- c. Code:

```

---
#####
#####
# Example : Snapshot Playbook to process multiple P-VOLs
#####
#####
- name: Snapshot Pair Module - Multiple P-VOLs
  hosts: localhost
  gather_facts: false

  vars_files:
    - ../ansible_vault_vars/ansible_vault_storage_var.yml

  vars:
    # 1. Define the list of Primary Volume IDs (P-VOLs) to snapshot
    p_vols_to_snapshot:
      - 12
      - 22

    # Common connection info for all tasks
    connection_info:
      address: "{{ storage_address }}"
      username: "{{ vault_storage_username }}"
      password: "{{ vault_storage_secret }}"

  tasks:

#####
#####
    # Task 1: Create Thin Image Advanced snapshot pair for all P-VOLs

#####
#####
    - name: Create Thin Image Advanced snapshot pair
      hitachivantara.vspone_block.vsp.hv_snapshot:
        connection_info: "{{ connection_info }}"
        state: "present"
        spec:
          # Use a dynamic snapshot group name based on the P-VOL ID
          snapshot_group_name: "TIA_SNAP_{{ item }}"
          primary_volume_id: "{{ item }}"
          secondary_volume_id: # Leave blank for Thin Image Advanced (TIA)
          pool_id: 0
          is_data_reduction_force_copy: true
          can_cascade: true
          # Loop through the list of P-VOL IDs defined in vars
          loop: "{{ p_vols_to_snapshot }}"
          register: snapshot_creation_results

    - name: Debug the creation results

```

```

ansible.builtin.debug:
  var: snapshot_creation_results

#####
#####
# Task 2: Set retention period of snapshot pair with auto split

#####
#####
- name: Set retention period of snapshot pair with auto split
  hitachivantara.vspone_block.vsp.hv_snapshot:
    connection_info: "{{ connection_info }}"
    state: "split"
    spec:
      # Get IDs from the successful creation result
      primary_volume_id: "{{ item.snapshot_data.primary_volume_id }}"
      mirror_unit_id: "{{ item.snapshot_data.mirror_unit_id }}"
      retention_period: 1 # Setting retention to 1 day
      pool_id: 0
      # Use the snapshot group name from the previous task
      snapshot_group_name: "TIA_SNAP_{{ item.snapshot_data.primary_volume_id }}"
    # Loop through the results of the creation task
    loop: "{{ snapshot_creation_results.results }}"
    # Only run the split if the creation step for that volume was successful
    when: item.changed and item.snapshot_data is defined
    register: snapshot_split_results

- name: Debug the split results
  ansible.builtin.debug:
    var: snapshot_split_results

```

3. Ansible Playbook 2:

- a. Name: snapshot_restore.yml
- b. Use: Restore snapshot data and mount the snapshot to a host
- c. Code: Get the playbook from github link and follow the instruction of README.md file.
[hv-playbooks-vspone-block/HTIA_snapshotrestore at main · hitachi-vantara/hv-playbooks-vspone-block](https://github.com/hitachi-vantara/hv-playbooks-vspone-block)

References:

Thin Image Advanced: [About Thin Image Advanced](#) • [Thin Image Advanced User Guide](#) • [Reader](#) • [Hitachi Vantara Documentation Portal](#)

Safe Snap:

Hitachi Thin Image safe snaps are immutable snapshots with locks applied for specific retention periods that cannot be changed. The data is protected against host writes, array operations or any malicious attempts to change the data footprint. In case of a ransomware attack, Thin Image safe snaps are timelocked immutable snapshots required for recovery of clean data that provides true immutability as the volume locks cannot be removed prior to the specified retention period

These snapshots can be either floating (volumeless) or volume-based (S-VOL). The retention period can range from one hour to 12,288 hours (512 days). During this period, the data on the snapshot, snapshot group, or snapshot consistency group cannot be altered, including preventing changes by mounting the S-VOL to a host and writing to the volume, as well as resyncing or deleting the snapshot.