Hitachi Vantara Object Storage with Veeam Backup & Replication

Solutions Reference Architecture & Best Practices

Content Engineering

v1.0.2 – March 2024

Table of
Contents

Solution Introduction

Veeam Backup & Replication (VBR), part of the Veeam Data Platform, delivers fast, flexible, and reliable backup and recovery for virtual machine, physical server, cloud-based workloads, and unstructured data backup (e.g. NFS, S3) in addition to providing virtual machine replication. Combined with Hitachi Vantara's object storage offerings: Hitachi Content Platform (HCP) and Hitachi Content Platform for Cloud Scale (HCP CS), this solution provides enterprise grade data protection with massive scalability to meet customer data protection requirements.

This solution is currently supported with the following versions of Hitachi Vantara and Veeam offerings:

- Hitachi Content Platform 9.6
- Hitachi Content Platform for Cloud Scale 2.6
- Veeam Backup & Replication 12

You should ensure that your systems are on the latest released versions of each offering listed above.

Solution status

Veeam Backup & Replication 12 has been validated for **compatibility** with the Hitachi object storage offerings listed above.

No specific use cases (workloads) have been validated at this time. Performance tests were not part of the compatibility validation.

Partner certification program

Hitachi Vantara has completed validation for HCP and HCP CS through the Veeam Ready Program. There are two test suites in the Veeam Ready Program for object storage:

- Veeam Ready – Object
- Veeam Ready – Object Immutability

As of VBR 12, Object test suites are included in the Object Immutability test suites. Object storage with object locking capabilities now only need to run the Object Immutability test suites.

Veeam has a single web page for each product that has been validated Veeam Ready. Hitachi Vantara's Veeam Ready status for HCP and HCP CS can be found at:

- HCP: https://www.veeam.com/sys360
- HCP CS: https://www.veeam.com/sys268

> *Note: On these web pages, Veeam may list Veeam Backup for Microsoft 365 and Veeam Agent for Mac 2.0 – these are not validated or supported with HCP or HCP CS. We have initiated the request for Veeam to remove these products from the list.*

Prerequisites

This document assumes you have firm knowledge and understanding of:

- Features and functionality of the products and components in the solution
- How to install and configure the products and components in the solution for your specific use case(s)
- Any support infrastructure used as part of the solution

This is not a comprehensive document for VBR with HCP or HCP CS. It is important that you understand your use cases and how to configure each product in the solution correctly. Consult Hitachi Vantara and Veeam documentation for details on features, configuration, etc.

Executive Summary

The validation process for solution **compatibility** covers full lifecycle of VBR data residing on Hitachi Vantara object stores: HCP and HCP CS. Sources of the VBR data included virtual machines from VMWare ESXI hosts, Windows and Linux operating systems, and SQL Databases on Windows.

Full lifecycle testing includes backup, recovery, and deletion of data from all above-mentioned sources. Backup tests included VBR Scale-out Backup Repository (SOBR) and Direct to Object configurations. Deletion tests were performed via multiple methods (i.e. manual deletion of backups, allowing data to age out via retention policies).

Additional VBR features covered as part of the compatibility validation include Backup Storage Immutability, Stand Alone & Managed mode for Veeam Agent for Windows/Linux, entire machine recovery, instant machine recovery, and restore point-based retention policies.

Note: As of the publication date of this whitepaper, Hitachi is engaged with Veeam Support on an issue where SQL backups and restores are unable to leverage SQL transaction logs for these processes.

Reference Model

The reference implementation used to validate **compatibility** of the solution included the following components:

- Backup sources:
  - Microsoft SQL Server 2016 v18.8
  - Windows Server 2019
  - Centos 7
  - VMware ESXI 7
- Supporting infrastructure:
 - VMware ESXi Server 7
  - 25GbE network

Reference implementation diagram

VBR can leverage HCP or HCP CS with one, or both, of the following configurations:

- Scale-out Backup Repository (SOBR)
- Direct to Object (introduced in VBR 12)

Below VBR is configured for SOBR, HCP or HCP CS is configured as the Capacity Tier for long-term storage. Here, data is initially back up to a Performance Tier (i.e. Hitachi VSP) for short-term retention. Data is first backed up to the Performance Tier and then copied to the Capacity Tier.

This is the recommended configuration for VBR with HCP CS.
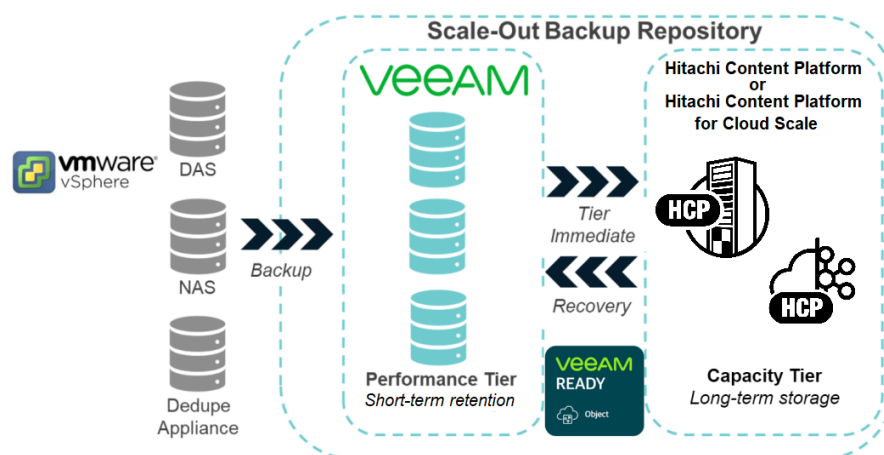
Below VBR is configured for Direct to Object, HCP or HCP CS is the primary storage used for the backups. In many cases, HCP or HCP CS is the only storage used in this solution.
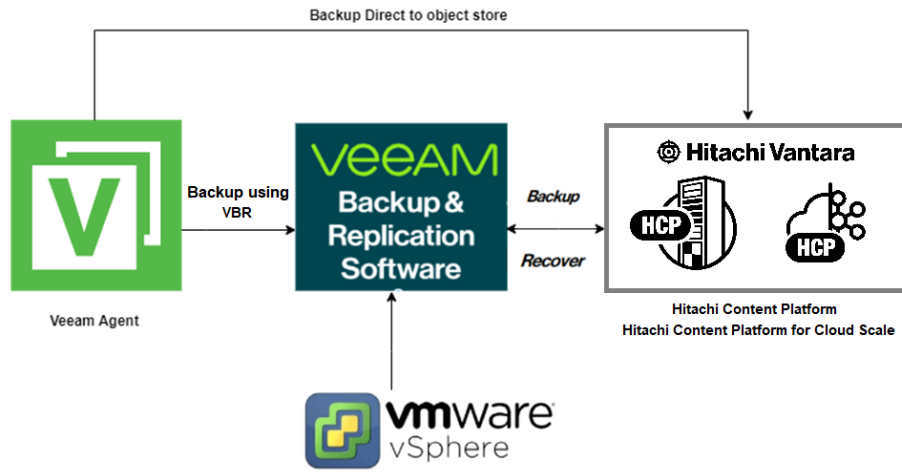
Overview of Best Practices for HCP and VBR

When using HCP with VBR ensure that you are following the best practices in this section for the solution to function and perform properly.

Important:

- *HCP namespace settings must be configured properly when the namespace is created. Many settings cannot be changed after a namespace has been created.*
- *The table below is not a full list of HCP settings to be configured.*
- *See HCP documentation for more information.*

HCP configurations

Setting	Value	Notes
Versioning	If VBR Immutability is disabled, for the HCP namespace: - disable Versioning - enable S3 Overwrite If VBR Immutability is enabled, for the HCP namespace: - enable Versioning - enable Object Lock	
Namespace Directory Usage	set to Unbalanced	See the "Protocol optimization and directory usage" topic of the HCP documentation.

Overview of Best Practices for HCP CS and VBR

When using HCP CS with VBR ensure that you are following the best practices in this section for the solution to function and perform properly.

Important:

- *VBR Immutability must be enabled when integrating with HCP CS.*
- *Disabling VBR Immutability with HCP CS is <u>not</u> supported by Veeam. Per Veeam documentation: "Data in object storage bucket/container must be managed solely by Veeam Backup & Replication, including retention and data management. Enabling lifecycle rules is not supported, and may result in backup and restore failures."*
- *The table below is <u>not</u> a full list of HCP CS settings to be configured.*
- *See HCP CS documentation for more information.*

VBR configurations

Setting	Value	Notes
Immutability	Enabled	Required for configuration with HCP CS.
Storage Optimization	4 MB	HCP CS is optimized for larger object sizes.
Storage Tier Type	set HCP CS as the Capacity Tier	When VBR is configured with SOBR.

HCP CS configurations

Setting	Value	Notes
Object Lock	Enabled	Object Lock must be enabled to function properly when VBR Immutability is enabled.
Partition Threshold	2 GB	Default is 1 GB; see instructions below to change this setting.

Setting Partition Threshold parameter on HCP CS

To set the partition threshold to 2 GB (default is 1 GB), run the following command on any HCP CS node or on any node that has the network connectivity to the Metadata Coordination Service (MCS) node:

```
curl -id "{'key':'splitPartition.thresholdSizeInBytes', 'value':'<partitionSize>'}" http://<cluster-name-or-MCS-IP>:9760/support/ext/config/set
```

Examples:

```
curl -id "{'key':'splitPartition.thresholdSizeInBytes', 'value':'2147483648'}"
http://myhcpcs.example.com:9760/support/ext/config/set
```

```
curl -id "{'key':'splitPartition.thresholdSizeInBytes', 'value':'2147483648'}"
http://172.18.48.23:9760/support/ext/config/set
```

- where 172.18.48.23 is the MCS IP address
- you can find the MCS IP address in System Management console > Services > Metadata-Coordination

To confirm that the new value is indeed set, run a similar (get) command:

```
curl -id "splitPartition.thresholdSizeInBytes" http://<cluster-name-or-MCS-
IP>:9760/support/ext/config/get
```

An output from this command will not include a value, if the threshold size is still the default (1GB), for example:

```
{"key":"splitPartition.thresholdSizeInBytes"}
```

Otherwise, if the threshold size was set to 2GB, the output would be:

```
{"key":"splitPartition.thresholdSizeInBytes","value":"2147483648"}
```

Overview of VBR Components and Configurations

This section summarizes the specific VBR components used as part of the **compatibility** validation with HCP and HCP CS.

This table is not a full list of all VBR components and is not intended to replace Veeam technical documentation. See Veeam documentation for more information.

VBR component	Description	Configuration used
Veeam Backup & Replication Backup Server	The backup server is the core component to the Veeam solution. The backup server stores information about backups, backup jobs, and other components. It is also where you create and run backup jobs as well as recover backups.	The backup server requires an MS SQL Server or PostgreSQL database to store data. Testing in this report was done with a MS SQL Server deployed locally on the same Windows Server.
Veeam Backup Proxy	A Veeam Backup Proxy is the component which processes data to be backed up. The proxy will retrieve data from sources and depending on the configuration, may compress, deduplicate, or encrypt the data before sending it to the appropriate backup repository.	Veeam Backup proxies can be configured to handle a certain number of concurrent tasks. A task is defined by backing up of a single disk of a machine. For the testing in this report this was set to 4.
Block Generation	When Veeam immutability is being used, Veeam will automatically add 10 days to the immutability expiration period. This is referred to as block generation.	The testing performed in this report was done with block generation disabled. This was done to expedite the testing process.
Veeam Backup Agents	Veeam Backup Agents are components that resides on a target machine's operating system (I.E. Windows/Linux). The backup agent creates backups of the machine and supports both full image backups, or specific files and folders.	Veeam Backup Agents can be configured as managed agents or standalone agents. Managed agents are managed by the Veeam Backup & Replication server while standalone agents are configured by the end user. Both have been tested for this solution.

Appendix A – Troubleshooting

This section summarizes some common issues along with advice provided by Veeam Support during compatibility validation of VBR with HCP and HCP CS.

Issue	Resolution or workaround
VM backup fails as free space in datastore is below 5%	Free up space in the datastore. A workaround is to lower or disable the thresholds in VBR; however, it may cause instability.
VM backup fails as maximum number of hypervisor snapshots has been met	Increase the number of snapshots allowed by the hypervisor.

Appendix B – Resources

Related Hitachi Vantara and Veeam resources.

Hitachi Vantara resources

Documentation (docs.hitachivantara.com)

- Hitachi Content Platform (HCP)
- Hitachi Content Platform for Cloud Scale (HCP CS)

Veeam resources

Technical documentation

- Veeam Backup & Replication product guides
- Veeam Alliance Technical Programs – Veeam Ready database

Appendix C – Document History

Revision history for this document.

Revision	Date	Summary
1.0.0	Dec 15, 2023	v1.0.0 of VBR + HCP & CS (Compatibility only)
1.0.1	Feb 9, 2024	v1.0.1 of VBR + HCP & CS (Compatibility only), changes: ▪ updated links to new Hitachi Vantara Documentation portal for HCP and HCP CS ▪ added best practices for HCP CS configurations: partition threshold and usage as a capacity tier
1.0.2	Mar 1, 2024	v1.0.2 of VBR + HCP & CS (Compatibility only), changes: ▪ added important notes – especially related to what Veeam supports/requires with HCP CS ▪ updated diagrams for accuracy ▪ general cleanup of document including clarify VBR (not general reference to Veeam as there are multiple Veeam products) ▪ removed list of test cases as they are not pertinent to the best practices for the solution