

Hitachi Storage Plug-in for Veeam[®] Backup & Replication[™]

v2.2.0

User Guide

This document provides information about the environment settings, operational restrictions, managing, and troubleshooting information that you need in order to introduce Hitachi Storage Plug-in for Veeam[®] Backup & Replication[™].

© 2025, 2026 Hitachi Vantara, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., Hitachi Vantara, Ltd., or Hitachi Vantara LLC (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" mean text, data, photographs, graphics, audio, video and documents.

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

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC 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 LLC.

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; and
2. Verifying that your 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.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, DB2, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, IntelliMagic, IntelliMagic Vision, OS/390, PowerHA, PowerPC, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z17, z/VM, 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, Microsoft Edge, the Microsoft corporate logo, the Microsoft Edge 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 website are properties of their respective owners.

The open source content used in Hitachi Vantara products may be found within the Product documentation or you may request a copy of such information (including source code and/or modifications to the extent the license for any open source requires Hitachi make it available) by sending an email to OSS_licensing@hitachivantara.com.

Contents

Preface	5
Product version.....	5
Release notes.....	5
Storage model abbreviations.....	5
Accessing product documentation.....	7
Chapter 1: Overview	8
What is Veeam Backup & Replication?.....	8
System requirements.....	9
Environment requirements.....	10
To back up a TrueCopy or global-active device volume by using synchronous replication.....	14
Restrictions on using Storage Plug-in.....	16
Chapter 2: Setting up the environment	17
Preparing the backup environment for the storage system.....	17
Example of a system configuration.....	26
Installing Storage Plug-in.....	28
Registering a storage system in Veeam Backup & Replication.....	29
Unregistering a storage system from Veeam Backup & Replication.....	30
Configuration file: For a Microsoft Windows-based backup server.....	32
Configuration file: For Veeam Software Appliance (Linux)	35
Chapter 3: Backing up and restoring virtual machines using Storage Plug-in	40
Restrictions on backup and restore using Storage Plug-in.....	40
Restrictions on backup of data reduction shared volumes.....	41
Running and checking backup jobs with the Snapshot Immutability function enabled.....	42
Backing up on a primary storage system.....	43
Backup from storage snapshots (primary storage system).....	43
Snapshot orchestration (primary storage system).....	44
Backup from storage snapshots with snapshot retention (primary storage system).....	45
Backing up on a secondary storage system.....	47
Backup from storage snapshots (secondary storage system).....	47

Snapshot orchestration (secondary storage system).....	49
Backup from storage snapshots with snapshot retention (secondary storage system).....	51
Restoring from storage snapshot.....	53
Instant recovery from storage snapshot.....	53
Chapter 4: Troubleshooting.....	55
What to check first.....	55
Handling failures.....	56
Message: The hostGroup used in the plugin does not exist.....	56
Message: There is no iSCSI target to register iSCSI name.....	56
Message: Unable to access file snapshot.....	57
Message: Cannot choose between the volume LUNs with the same ID / No synchronous replication relationship was detected for these volumes...	57
Message: Unexpected character encountered while parsing value.....	57
Message: The timeout (xx:xx:xx) occurred in the REST-API response. Try the operation again when the storage load is light.....	57
Message: Synchronous replication relationships not found.....	58
Message: The pre-check process before creating a snapshot/clone has timed out. Please check the status of the pairs created on the target production volume and try again after a while.....	58
Message: The error is occurred in REST API. Please contact storage system administrator to check the details in the log file. A message including KART40009-E is output to the log file.....	58
Message: The number of files in the gc folder exceeded the limit.....	59
Files remain in the gc folder after a storage system is unregistered.....	59
Storage Plug-in processing and storage system processing are slow.....	60
An error or warning event is logged in the event log of the backup proxy server.....	60
Information to be collected when a failure occurs.....	61
Collecting Storage Plug-in information.....	61
Collecting storage system information.....	61

Preface

This document provides information about the environment settings, operating restrictions, managing, and troubleshooting information that you need in order to introduce Hitachi Storage Plug-in for Veeam® Backup & Replication™.

Product version

This document supports Hitachi Storage Plug-in for Veeam® Backup & Replication™ v2.2.0. The *Quick Start Guide* (QSG) and the *Implementation Guide* (IG) have been consolidated into a single, comprehensive document, now titled the *Hitachi Storage Plug-in for Veeam® Backup & Replication™ v2.2.0 User Guide*. This update ensures that all essential setup and usage instructions are available in one place, enhancing accessibility and ease of use.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on the Hitachi Vantara documentation website: <https://docs.hitachivantara.com>.

Storage model abbreviations

This document uses the following abbreviations for storage models.

Abbreviation	Full name
VSP E series	Hitachi Virtual Storage Platform E series Collective name for the following storage models: <ul style="list-style-type: none">▪ Hitachi Virtual Storage Platform E590▪ Hitachi Virtual Storage Platform E790▪ Hitachi Virtual Storage Platform E990▪ Hitachi Virtual Storage Platform E1090

Abbreviation	Full name
	<ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform E590H ▪ Hitachi Virtual Storage Platform E790H ▪ Hitachi Virtual Storage Platform E1090H
VSP E590	Hitachi Virtual Storage Platform E590
VSP E790	Hitachi Virtual Storage Platform E790
VSP E990	Hitachi Virtual Storage Platform E990
VSP E1090	Hitachi Virtual Storage Platform E1090
VSP E590H	Hitachi Virtual Storage Platform E590H
VSP E790H	Hitachi Virtual Storage Platform E790H
VSP E1090H	Hitachi Virtual Storage Platform E1090H
VSP F350	Hitachi Virtual Storage Platform F350
VSP F370	Hitachi Virtual Storage Platform F370
VSP F700	Hitachi Virtual Storage Platform F700
VSP F900	Hitachi Virtual Storage Platform F900
VSP G350	Hitachi Virtual Storage Platform G350
VSP G370	Hitachi Virtual Storage Platform G370
VSP G700	Hitachi Virtual Storage Platform G700
VSP G900	Hitachi Virtual Storage Platform G900
VSP 5000 series	<p>Hitachi Virtual Storage Platform 5000 series</p> <p>Collective name for the following storage models:</p> <ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform 5100 ▪ Hitachi Virtual Storage Platform 5200 ▪ Hitachi Virtual Storage Platform 5500 ▪ Hitachi Virtual Storage Platform 5600 ▪ Hitachi Virtual Storage Platform 5100H ▪ Hitachi Virtual Storage Platform 5200H

Abbreviation	Full name
	<ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform 5500H ▪ Hitachi Virtual Storage Platform 5600H
VSP 5100	Hitachi Virtual Storage Platform 5100
VSP 5200	Hitachi Virtual Storage Platform 5200
VSP 5500	Hitachi Virtual Storage Platform 5500
VSP 5600	Hitachi Virtual Storage Platform 5600
VSP 5100H	Hitachi Virtual Storage Platform 5100H
VSP 5200H	Hitachi Virtual Storage Platform 5200H
VSP 5500H	Hitachi Virtual Storage Platform 5500H
VSP 5600H	Hitachi Virtual Storage Platform 5600H
VSP One B20 series	Hitachi Virtual Storage Platform One Block 20 series Collective name for the following storage models: <ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform One Block 24 ▪ Hitachi Virtual Storage Platform One Block 26 ▪ Hitachi Virtual Storage Platform One Block 28
VSP One B85	Hitachi Virtual Storage Platform One Block 85

Accessing product documentation

Product user documentation is available on: <https://docs.hitachivantara.com>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Chapter 1: Overview

Hitachi Storage Plug-in for Veeam® Backup & Replication™ is a plug-in that enables integration of Hitachi storage systems in Veeam® Backup & Replication™.

Hereinafter in this manual, Hitachi Storage Plug-in for Veeam® Backup & Replication™ is referred to as Storage Plug-in.

What is Veeam Backup & Replication?

Veeam Backup & Replication backs up virtual and physical environments, including virtual machines, physical servers, and cloud instances, and replication of virtual machines for orchestrated failover and failback.

If the virtual machine's VM snapshot retention time is long, it takes longer to commit the VM snapshot data after the backup is complete, which increases load on the machine. With Storage Plug-in, you can reduce the VM snapshot retention time, and prevent the performance degradation of the virtual machine.

You can use the following Veeam Backup & Replication functions: Backup from Storage Snapshots, Data Recovery from Storage Snapshots, and Snapshot Orchestration. For details, see the description of Storage System Snapshot Integration in the Veeam Backup & Replication documentation (<https://www.veeam.com/support/help-center-technical-documentation.html>).

In this document, a server assigned the role of a backup proxy, which is a component of Veeam Backup & Replication, is called a backup proxy server.

System requirements

The following describes the specific requirements for Storage Plug-in.

- The operations of the following versions of Veeam Backup & Replication are supported.

For details about Veeam Backup & Replication requirements, see the system requirements listed in the *Veeam Backup & Replication User Guide for VMware vSphere*.

- Veeam Backup & Replication V13.0.1
- Hitachi storage systems whose microcode versions are as follows are supported.

Storage system	Microcode version
VSP E series	93-03-01-60/00 or later
VSP F350, F370, F700, F900	88-07-01-x0/00 or later
VSP G350, G370, G700, G900	88-07-01-x0/00 or later
VSP 5100, 5500, 5100H, 5500H	90-05-01-00/00 or later
VSP 5200, 5600, 5200H, 5600H	90-08-01-00/00 or later
VSP One B20 series	A3-03-01-x0/01 or later
VSP One B85	A0-05-21-00/00 or later

- Licenses for the following program products are required.
 - Hitachi Storage Virtualization Operating System (SVOS)
 - Hitachi LUN Manager
 - Hitachi Dynamic Provisioning
 - Resource Partition Manager
 - If data reduction shared volumes are backed up
 - Hitachi Thin Image Advanced
 - If other volumes are backed up
 - Hitachi Thin Image
- Storage Plug-in uses port number 80 or 443 for the REST API connection to the storage system. Refer to this information when setting up a firewall.

Environment requirements

To use Storage Plug-in, your environment must meet the following requirements:

- You can use Veeam Backup & Replication to perform operations on the VMware ESXi host on which the virtual machine to be backed up is located.

For details on the components and system configuration of Veeam Backup & Replication, see the description of Deployment Scenarios in the Veeam Backup & Replication documentation.

- The datastore where the VMware ESXi host is to be backed up must be created from a volume on a supported Hitachi storage system.

The volume must meet the following conditions:

- The volumes are connected to some hosts by using a host group or iSCSI target.
- The host mode of the host group or iSCSI target is 01 [(Deprecated)VMware] or 21 [VMware Extension].

- Note the following about the volume to be backed up:
 - For the volume to be backed up, those volumes must have the Dynamic Provisioning attribute specified. Additionally, the following states are supported. If you specify settings other than the supported settings, you will no longer be able to operate the corresponding volumes with Veeam Backup & Replication.
 - In addition to the Dynamic Provisioning attribute, the Dynamic Tiering attribute is also specified.
 - The dedupe and compression function is enabled.



Note: When the volume to be backed up is a data reduction shared volume, Storage Plug-in uses Thin Image Advanced to back up the corresponding volume. When the volume to be backed up is a non-data reduction shared volume, Storage Plug-in uses Thin Image to back up the corresponding volume.

For the volumes to be backed up that are supported by each storage system

The volumes to be backed up that are supported by each storage system are as follows:

- For VSP E series or VSP 5000 series

For the following Hitachi storage systems, Storage Plug-in supports backup of both data reduction shared volumes and non-data reduction shared volumes. For VSP E series and VSP 5000 series storage systems and microcode versions that are not listed in the table, backup of data reduction shared volumes is not supported.

Storage system	Microcode version
VSP E series	93-07-25-x0/00 or later
VSP 5200, 5600, 5200H, 5600H	90-09-26-00/00 or later

- For VSP One B20 series and VSP One B85

Storage Plug-in only supports backup of data reduction shared volumes.

- For other storage models

Backup of data reduction shared volumes is not supported.

For Snapshot Immutability

To use backups using Snapshot Immutability, all of the following conditions must be met:

- The storage systems must have the following microcode versions:

Storage system	Microcode version
VSP E series	93-07-26-x0/00 or later
VSP 5200, 5600, 5200H, 5600H	90-09-27-00/00 or later
VSP One B20 series	A3-04-01-40/00 or later
VSP One B85	A0-05-21-00/00 or later

- The volume to be backed up must be a data reduction shared volume.
- The version of Veeam Backup & Replication must be the one that supports Snapshot Immutability.

**Note:**

- For details on the version requirements and other conditions for using Snapshot Immutability in Veeam Backup & Replication, see the Veeam Backup & Replication documentation.
- For details on the protection period for snapshots using the Snapshot Immutability function, also see [Running and checking backup jobs with the Snapshot Immutability function enabled \(on page 42\)](#).

**Tip:**

When considering which to build or operate as the volume to be backed up, a data reduction shared volume or a non-data reduction shared volume, consider the operational use and make a decision by referring to the respective storage documentation* for data reduction shared volumes, Thin Image Advanced, and Thin Image.

*You can refer to the following storage documents:

- *Provisioning Guide*
- *Hitachi Thin Image User Guide*
- *Hitachi Thin Image Advanced User Guide*

- The following table outlines the scope of support and required settings for copy-type program products related to the volume to be backed up. If you specify settings outside

of the scope of support, or do not specify the required settings, you will no longer be able to operate the corresponding volumes with Veeam Backup & Replication.

Copy-type program product	Volumes supported to be backed up	Required settings
Thin Image	Root volume	-
Thin Image Advanced	Root volume	-
TrueCopy	<ul style="list-style-type: none"> ▪ For backup using synchronous replication: Primary volume and secondary volume ▪ For backup that does not use synchronous replication: Primary volume 	<ul style="list-style-type: none"> ▪ The volume to be backed up must belong to a device group¹ ▪ Settings for such as copy groups must be configured if you are performing backup using synchronous replication.² ▪ Do not connect the secondary volumes to the VMware ESXi host used for restoration.
Universal Replicator	Primary volume on the primary site	<ul style="list-style-type: none"> ▪ The volume to be backed up must belong to a device group¹ ▪ Do not connect the secondary volumes to the VMware ESXi host used for restoration.
Global-active device	<ul style="list-style-type: none"> ▪ For backup using synchronous replication: Primary volume and secondary volume ▪ For backup that does not use synchronous replication: Primary volume³ 	<ul style="list-style-type: none"> ▪ The volume to be backed up must belong to a device group¹ ▪ Settings for such as copy groups must be configured if you are performing backup using synchronous replication.²

Copy-type program product	Volumes supported to be backed up	Required settings
		<ul style="list-style-type: none"> ▪ For backup that does not use synchronous replication, if the two volumes in a global-active device pair are registered as one datastore, register only one of the two storage systems that make up the pair in Veeam Backup & Replication.
ShadowImage	Volumes that have the ShadowImage attribute specified are not supported.	-
<p>Notes:</p> <ol style="list-style-type: none"> 1. This device group must belong to a copy group created by specifying the same MU number as the TrueCopy, Universal Replicator, or global-active device pair. To back up a global-active device volume, specify the copy group name in the following format: <i>VBR_<any-string-of-single-byte-characters></i>. 2. For details on how to backup TrueCopy or global-active device volumes using synchronous replication, see To back up a TrueCopy or global-active device volume by using synchronous replication (on page 14) and configure the settings in advance. 3. For backup that does not use synchronous replication, if the pair status of the global-active device is PSUS, PSUE, SSUS, or SSWS, and the volume I/O mode is Block, backup jobs will fail. 		

To back up a TrueCopy or global-active device volume by using synchronous replication

To back up a TrueCopy or global-active device volume by using synchronous replication, specify settings in advance to meet the following status:

- Both the volumes that belong to the target pair meet the following conditions:
 - The volumes are connected to some hosts by using a host group or iSCSI target.
 - The host mode of the host group or iSCSI target is 01 [(Deprecated)VMware] or 21 [VMware Extension].
- Both the storage systems that make up the target pair are registered on a Veeam backup server on which Storage Plug-in is installed.

- The status of the configured pair is PAIR.
- The following conditions must be met in order for Storage Plug-in to determine whether the volumes that belong to the target pair are ready for backup:
 - Each of the primary and secondary side volumes belonging to the target pair belongs to a device group. Each device group on the primary and secondary sides belongs to a copy group created by specifying the same MU number as the target pair. When the settings are specified by using Command Control Interface, the device name used to register the corresponding volume to the device group matches on the primary and secondary sides, and the copy group name to which the device group belongs matches on the primary and the secondary sides. The copy group name is in the following format: *VBR_<any-string-of-single-byte-characters>*.

Create new copy groups and device groups that meet the requirements. You need to create them regardless of whether the copy groups and device groups that manage the volumes to be backed up already exist. Also, do not make any changes to the existing copy groups and device groups. If a change is made, remote copy pairs might be interrupted or deleted.

For the preceding copy groups, we recommend that you use a configuration in which only a copy group that meets the requirements is created and the following pairs are managed by that copy group:

- All pairs of global-active device volumes to be backed up
- All pairs of global-active device volumes and TrueCopy volumes that are to be backed up by using synchronous replication

Note that if multiple combinations of storage systems are used to make up pairs to be backed up, you need to separately create a copy group for each combination of storage systems. At this time, the names of these copy groups must be different. If the names of these copy groups are the same, backup that uses synchronous replication might fail.

- Both the storage systems that make up the target pair are mutually registered as a remote storage system by the REST API. In addition, when the storage systems are registered by the REST API, they are registered with the IP address used for registering the storage systems on the Veeam backup server.
- The credentials (the username and password for the Veeam Backup & Replication dedicated user) registered in Veeam Backup & Replication are the same for both the storage systems that make up the target pair.

Restrictions on using Storage Plug-in

- In this document, descriptions related to the screen display and operation of Veeam Backup & Replication are based on the Veeam Backup & Replication Console. If you are using the Veeam Backup & Replication Web UI, and experience restrictions in screen display or operation, use the Veeam Backup & Replication Console instead.
- When you use storage system management software (such as Ops Center Protector, Device Manager - Storage Navigator or Command Control Interface) to perform operations involving resource locks on resource groups (meta_resource or business resource groups) to which LDEVs to be backed up are assigned or on resource groups for backup, the following operations on that storage system might fail or errors might occur:
 - Backup job
 - Rescan (Storage Discovery) Process
 - Creating and Deleting Snapshots Manually
 - Data Recovery from Storage Snapshots
 - On-Demand Sandbox for Storage Snapshots
 - Removing Storage Systems

For operations involving resource locks, see the documentation for each management software such as Ops Center Protector or Device Manager - Storage Navigator.

- If dedupe and compression is enabled for the secondary volume of a Thin Image pair or for a volume cloned by using Thin Image, you will not be able to delete snapshots of that volume by using Veeam Backup & Replication. Use the storage system's management software to delete the corresponding volume.

Chapter 2: Setting up the environment

Before introducing Storage Plug-in, the storage system administrator must prepare a backup environment for the storage systems that are in use. The storage system administrator must also use Veeam Backup & Replication to unregister storage systems when they are no longer needed.

Perform the following procedure to set up the environment:

1. [Preparing the backup environment for the storage system \(on page 17\)](#)
2. [Installing Storage Plug-in \(on page 28\)](#)
3. [Registering a storage system in Veeam Backup & Replication \(on page 29\)](#)

Preparing the backup environment for the storage system

Create backup storage resources for active storage systems, and then configure the settings so that backup operation users can access the backup storage resources and the volumes to be backed up.

Perform the following procedure by referring to the manuals (*Provisioning Guide*, *System Administrator Guide*, *Hitachi Thin Image User Guide* and *Hitachi Thin Image Advanced User Guide*) for each storage system.

Before you begin

- Do not use storage system management software such as Device Manager - Storage Navigator or Command Control Interface to perform operations on the following storage resources unless a procedure or other description explicitly instructs you to use such software:

- Snapshots and snapshot clones created using Veeam Backup & Replication

In storage systems, the terms snapshot and snapshot clone refer to the following resources:

- Snapshots: Secondary volumes of Thin Image or Thin Image Advanced pairs
- Snapshot clones: Volumes cloned using Thin Image

- Storage resources created by using the procedure described in this section

If you perform operations by using storage system management software, the following problems might occur:

- The data on the storage system and the data in Veeam Backup & Replication might become inconsistent, and you might not be able to perform operations on snapshots or snapshot clones by using Veeam Backup & Replication.
- The data in a snapshot or in its clone might change.
- You might not be able to delete volumes created by using Storage Plug-in.

- Configure the backup infrastructure that is required for Veeam Backup & Replication.

For details, see the description of Backup Infrastructure for Storage Integration in the Veeam Backup & Replication documentation. To register storage systems after you perform this procedure, see [Registering a storage system in Veeam Backup & Replication \(on page 29\)](#).

- For details about the prerequisite environment, see [Environment requirements \(on page 10\)](#).

- The system configuration varies depending on whether the LDEVs to be backed up are allocated to meta_resource or to a business resource group. For details, see [Example of a system configuration \(on page 26\)](#).

A host group or iSCSI target corresponding to the VMware ESXi host used for business must be allocated to meta_resource or to a business resource group.

- For storage systems that use Storage Plug-in, do not add `_DEL` to the end of LDEV names, because such LDEVs are periodically and automatically deleted according to certain conditions.
- Verify that `VBR_` has not been added to the beginning of the name for any of the following. If `VBR_` has been added, delete it. This is because Storage Plug-in identifies its storage resources based on whether `VBR_` is added to the beginning of the resource name.
 - All resource groups on the storage system
 - All Dynamic Provisioning pools on the storage system
 - Host groups or iSCSI targets to which meta_resource or business resource groups have been allocated

- When the volumes to be backed up are the data reduction shared volumes, the following condition applies to the pool volumes of the pool to which the volumes belong:
All LDEVs allocated as pool volumes to the pool must belong to the same resource group (meta_resource or business resource group) as that of the LDEVs to be backed up.
- Do not use the NVMe mode as the operating mode of ports connecting the backup proxy server or the VMware ESXi host used for restoration and the storage system.

Procedure

1. (Optional) Create a parity group for backups, and then create a volume with an LDEV in that parity group. This step separates the work area from the backup pool area. Although optional, this step helps reduce the impact in case of a failure.
2. Prepare the Dynamic Provisioning pool for backup.



Tip: If the volumes to be backed up are data reduction shared volumes, volumes of snapshots or snapshot clones will be created in the same pool as the volumes to be backed up. For this reason, if the volumes to be backed up are all data reduction shared volumes, you do not need to prepare a Dynamic Provisioning pool for backup.

The procedure varies depending on whether you create a new pool for backup or use an existing pool.

- **Creating a new pool for backup**

If you created an LDEV for backup in step 1, allocate it as a pool volume. If you create a new pool for backup from an existing LDEV, also allocate that LDEV as a pool volume.

Specify the pool name in the following format: *VBR_any-string-of-single-byte-characters*. Alternatively, create a configuration file by referring to [Configuration file: For a Microsoft Windows-based backup server \(on page 32\)](#) and [Configuration file: For Veeam Software Appliance \(Linux\) \(on page 35\)](#), and then specify the pool name.

- **Using an existing pool**

Change the pool name to the following format: *VBR_any-string-of-single-byte-characters*. Alternatively, create a configuration file by referring to [Configuration file: For a Microsoft Windows-based backup server \(on page 32\)](#) and [Configuration file: For Veeam Software Appliance \(Linux\) \(on page 35\)](#), and then specify the pool name.



Note: Although you can use a pool for business as a pool for backup, we recommend that keep the pool for backup and the pool for business separated to avoid potential impacts in case of a failure.

You can use only one Dynamic Provisioning pool shared as the pool for backup that can be used for snapshots or snapshot clones. Do not create more than one backup pool.

3. Create a host group or an iSCSI target for a backup proxy server. If the VMware ESXi host is used for restoration and the storage system are connected, create a host group or an iSCSI target for the VMware ESXi host.



Caution:

- When performing this procedure to create a host group or an iSCSI target, do not set LU paths (users manually setting LU paths themselves or setting LU paths by using other software) outside of Storage Plug-in.
- If the following changes are made to the backup proxy server or the VMware ESXi host used for restoration, you must change the host group or iSCSI target settings.
 - The number of machines
 - The ports to be used and the number of ports

Create the host group or iSCSI target by performing the following operations:

- Specify the host group name or iSCSI target name in the following format: *VBR_any-string-of-single-byte-characters*.
- For the host mode, specify **21 [VMware Extension]**.



Tip: Host mode: **21 [VMware Extension]** also supports backup proxy server operating systems such as Windows and Linux.

- For the host mode options, specify 2, 22, 25, 40, 54, 63, 68, 91, and 110.

- For Fibre Channel and iSCSI connections, note the following:

For a Fibre Channel connection

Register the WWNs of backup proxy servers and the VMware ESXi hosts used for restoration to the host groups. If you are using multipath configuration, create a host group for every storage port that is used to connect to a backup proxy server or a VMware ESXi host used for restoration.

When using backup proxy servers

Use one of the following methods to register the WWNs to host groups:

[1]

Register all of the WWNs of a backup proxy server to the same host group.

[2]

Register one WWN of a backup proxy server per a separate host group. (Create a different host group for each WWN.)



Note:

- If you are using a multipath configuration, use method [1] to register WWNs.
- If you use method [1] to register WWNs, you can reduce the total number of host groups and optimize the configuration for the backup.
- If you are using multiple backup proxy servers, do not register the WWNs of different backup proxy servers to the same host group.

When using VMware ESXi hosts used for restoration

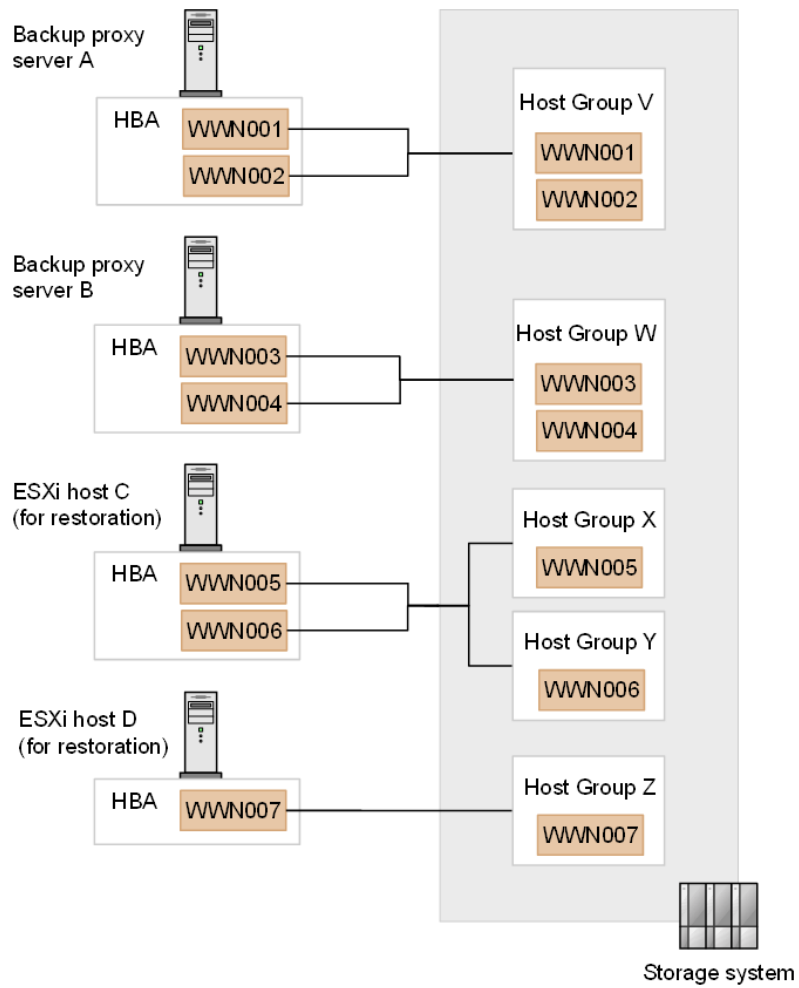
Register one WWN of a VMware ESXi host used for restoration per a separate host group. (Create a different host group for each WWN.)



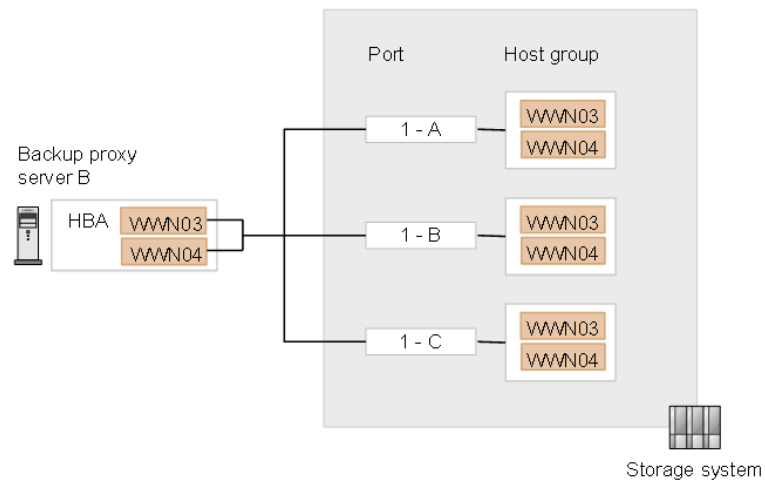
Note: If you are using multiple VMware ESXi hosts used for restoration, do not register the WWNs of different VMware ESXi hosts used for restoration to the same host group.

An example of registering the WWNs of backup proxy servers and VMware ESXi hosts for restoration in a host group.

The following shows an example of registering the WWNs of backup proxy servers and VMware ESXi hosts for restoration in a host group.



In addition, the following shows an example of using backup proxy server B in the preceding figure to create a multipath configuration.



Note:

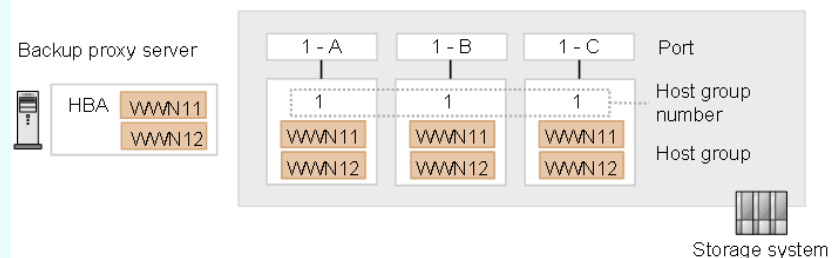
When creating multiple host groups on multiple ports for a single backup proxy server and registering that backup proxy server's

WWNs in each host group, if you set in advance a configuration that satisfies all of the following conditions, the execution time of backup jobs in Backup from storage snapshots will be shorter than with configurations that do not satisfy these conditions:

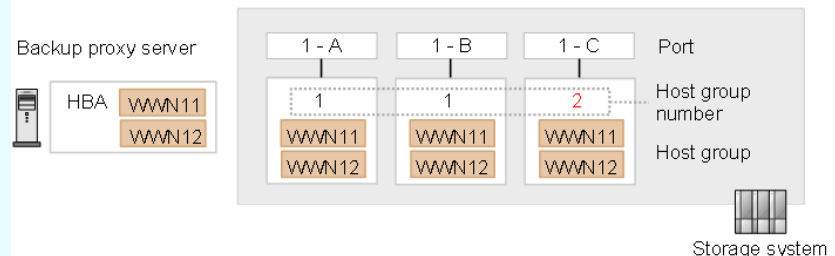
- The host group numbers of all host groups in which the target WWNs are registered must match.
- If multiple WWNs are used on the relevant backup proxy server, the host group numbers of the host groups in which they are registered must match for all WWNs.

The following shows examples of both a configuration that meets and a configuration that does not meet the conditions for reducing the execution time of backup jobs in Backup from storage snapshots.

An example of a configuration that meets the conditions for reducing the execution time of backup jobs in Backup from storage snapshots



An example of a configuration that does not meet the conditions
(The host group number for port 1-C in which WWN11 and WWN12 are registered does not match those for 1-A and 1-B.)



For an iSCSI connection

Create iSCSI targets without registering an iSCSI initiator. The total of all of the following iSCSI targets is required:

- The number of backup proxy servers
- The number of iSCSI initiators of the backup proxy servers or of the VMware ESXi hosts for restoration

When multiple backup proxy servers or multiple VMware ESXi hosts for restoration are to be used, or when there are multiple iSCSI initiators on the machine to be used, the number of iSCSI targets to be created is the total number of all iSCSI initiators.

For example, to use all iSCSI initiators in the following system configuration, you need to create six iSCSI targets:

- Backup proxy server A (number of iSCSI initiators: 2)
- Backup proxy server B (number of iSCSI initiators: 1)
- VMware ESXi host used for restoration (number of iSCSI initiators: 1)

If these settings are set, the iSCSI target is determined randomly and the iSCSI initiator of the host is automatically registered. If you want to specify the iSCSI target to which the iSCSI initiator of the host is registered, manually register the target iSCSI initiator to the iSCSI target. In such cases, register one iSCSI initiator for each iSCSI target.

4. Prepare a backup resource group and allocate storage resources as follows:

a. Create a new resource group or use an existing one.

- Specify the resource group name as follows:

- When you are not using a configuration file

You need to specify a resource group name using the storage system management software in the following format: *VBR_single-byte-character-string*

- When you are using a configuration file

Specify a name in the storage system management software, and then specify the same name in the configuration file.

For details about configuration files, see [Configuration file: For a Microsoft Windows-based backup server \(on page 32\)](#) and [Configuration file: For Veeam Software Appliance \(Linux\) \(on page 35\)](#).

- You can use only one backup resource group, so do not create more than one such group.

b. Allocate storage resources to the resource group created or prepared in step 4-a.

Allocate the following storage resources to the resource group:

- All LDEVs allocated as pool volumes to the Dynamic Provisioning pool for backup that was prepared in step 2
- The host groups or iSCSI targets created in step 3

- The port to which the host groups or iSCSI targets created in step 3 belong
The port to which the host groups or iSCSI targets created in step 3 belong must be allocated to either the resource group (meta_resource or business resource group) to which the LDEVs to be backed up are allocated, or to a resource group for backup.
- Unused LDEV ID
If you use Veeam Backup & Replication to orchestrate the creation of snapshots or snapshot clones, secondary volumes of Thin Image pairs or Thin Image Advanced pairs, or volumes cloned by using Thin Image will be created on the storage system. You must allocate a number of LDEV IDs equal to the number of these secondary volumes and cloned volumes. For this reason, prepare a sufficient number of unused LDEV IDs. Also, for the unused LDEV IDs, make sure that the virtual LDEV IDs are set equivalent to the actual LDEV IDs.



Caution: Do not allocate the serial number of a virtual ID to the backup resource group. If allocated, multiple different volumes created by using Storage Plug-in are connected to the same host as devices having the same SCSI ID, which might cause serious problems on the host.

5. Create a backup operation user group, and then create a user account for this group.
Assign the role Storage Administrator (View Only), Storage Administrator (Provisioning), and Storage Administrator (Local Copy) to the backup operation user group.
The user account is used to access the resource group where the LDEVs to be backed up are allocated (meta_resource or a business resource group) and the backup resource group you created in step 4.
6. Assign the resource group (the meta_resource or business resource group) where the LDEVs that are to be backed up are allocated and the backup resource group you created in step 4 to the user group.
Do not assign any resource group other than the above to the user group you created.
Do not assign the backup resource group to any other user group.



Tip: Built-in users also have access to the backup resource group.

7. Check the time zone and time of the Veeam backup server on which Storage Plug-in is installed and the time zone and time of the storage system. If the time zones and times do not match, change the settings so that they match.

Example of a system configuration

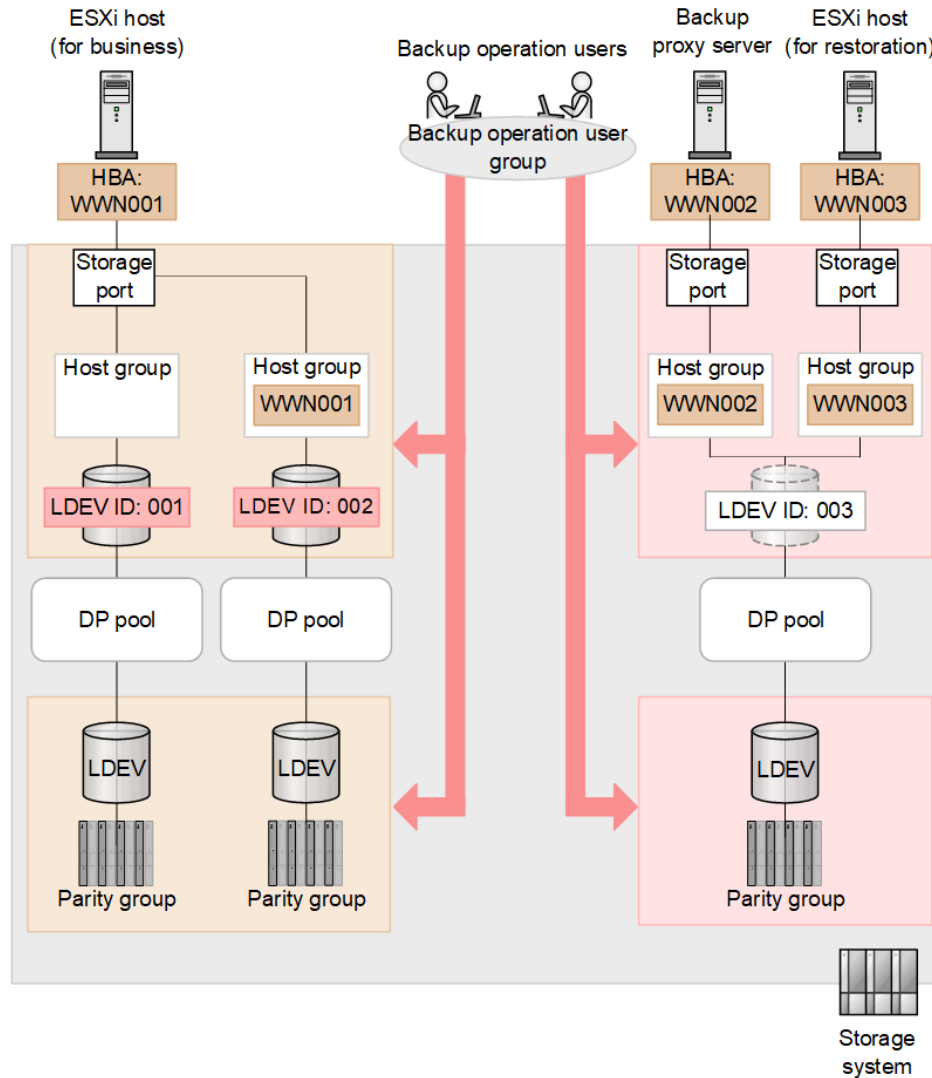
The following shows examples of system configurations for backing up volumes in meta_resource and for backing up volumes in a business resource group. In the provided examples, the following storage resources are created as backup storage resources:

- Parity groups
- LDEVs for pool volumes
- Dynamic Provisioning pool

- Host group for the backup proxy server
- Host group for the VMware ESXi host to be used for restoration
- Unused LDEV ID (LDEV ID: 003)

When backing up volumes in meta_resource

The following shows an example of backing up the LDEV allocated to meta_resource when there is no business resource group.

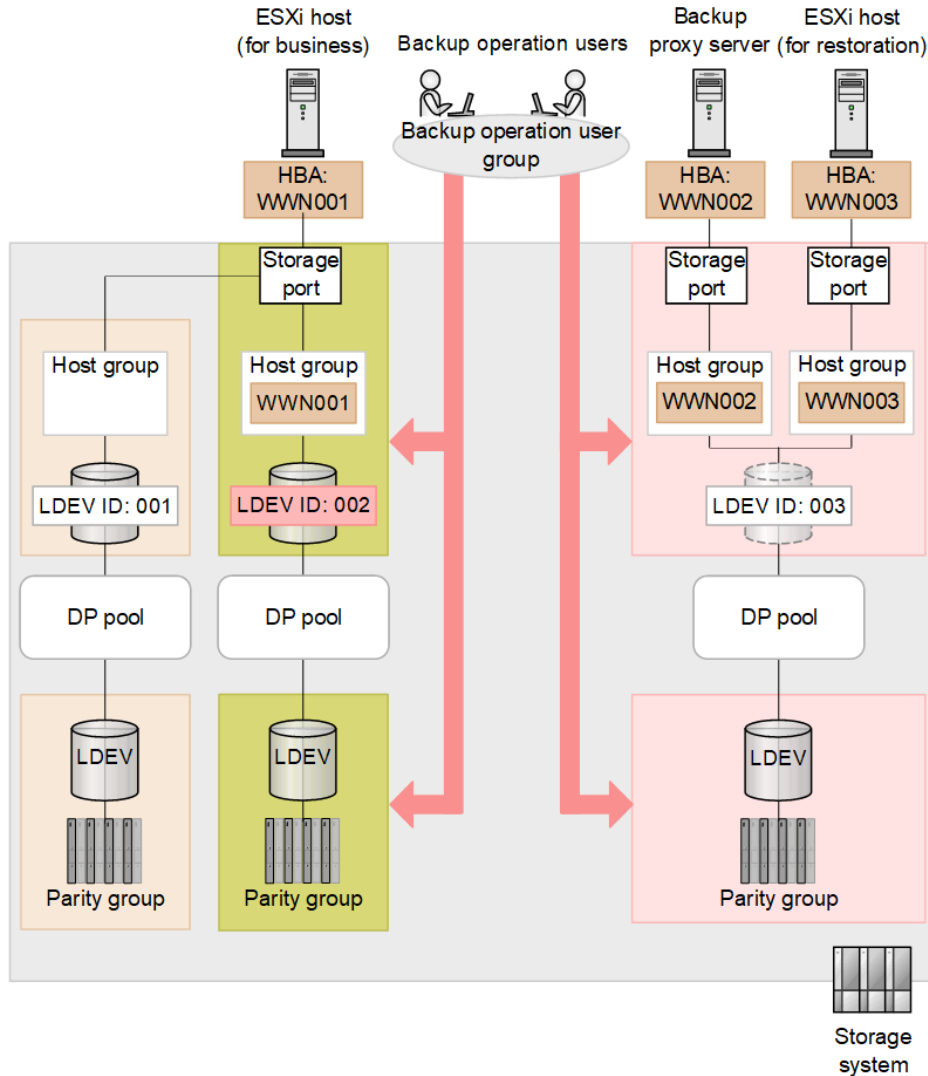


Legend

- Orange box : meta_resource
- Pink box : Backup resource group
- Red box : Volumes to be backed up
- Red arrow : User access to resource groups

When backing up volumes in a business resource group

The following shows an example where a business resource group has been created, and you back up the LDEVs allocated to the business resource group.



Legend

- : meta_resource
- : Business resource group
- : Backup resource group
- : Volumes to be backed up
- : User access to resource groups

Installing Storage Plug-in

Install Storage Plug-in. For details, see the description of Installing Storage System Plug-Ins in the Veeam Backup & Replication documentation.

Registering a storage system in Veeam Backup & Replication

Register the Hitachi storage system in Veeam Backup & Replication.

You can register multiple storage systems for one of the Veeam backup servers configured in the backup environment.

You can register one storage system for multiple Veeam backup servers, but the following operations might fail or unnecessary resources might remain without being deleted:

- Backup job
- Rescan (Storage Discovery) Process
- Creating and Deleting Snapshots Manually
- Data Recovery from Storage Snapshots
- On-Demand Sandbox for Storage Snapshots
- Removing Storage Systems

In such cases, identify the relevant storage resources based on the information displayed in Veeam Backup & Replication, such as the LDEV ID of the volume to be backed up, and use storage system management software such as Device Manager - Storage Navigator to perform operations such as deleting the relevant storage resources.

For details, see the description of Adding Universal Storage API Integrated Systems in the Veeam Backup & Replication documentation.

When you use the Add Storage wizard, note the following:

- In the vendor list, select HITACHI.
- For DNS name or IP address, specify the following IP address.

If an IPv4 address and an IPv6 address are set, specify the IPv4 address.

- VSP E series, VSP F350, F370, F700, F900, VSP G350, G370, G700, G900: CTL1 or CTL2

You can register only one of these controllers for each storage system.

- VSP 5000 series: SVP
- VSP One B20 series and VSP One B85: service IP address



Tip: You can specify an IPv6 address if the version of Veeam Backup & Replication is V12 or later.

- Specify Block or file storage for VMware vSphere for Role.
- For Credential, specify the user account created in [Preparing the backup environment for the storage system \(on page 17\)](#).

Unregistering a storage system from Veeam Backup & Replication

If a storage system no longer needed to be backed up, unregister the storage system from Veeam Backup & Replication, and then delete the host groups, iSCSI targets and any other related components that are no longer required.



Note:

- If you unregister a storage system from Veeam Backup & Replication, all of the following storage resources created in the resource group for backup that you created by performing the procedure in [Preparing the backup environment for the storage system \(on page 17\)](#) will also be deleted.
 - Volumes cloned from snapshots by using Thin Image or Thin Image Advanced (snapshot clones of Veeam Backup & Replication)
 - LU paths set for these volumes (LU paths set for the snapshots and for the snapshot clones of Veeam Backup & Replication)
- When you unregister a storage system, volumes for which Thin Image cloning is in progress will not be deleted. Instead, `_DEL` will be added to the end of the volume name and the volume will remain in the storage system. In such cases, make sure that the pair between the secondary volume of Thin Image and the volume cloned by Thin Image have been deleted by the storage system's management software, and then delete the corresponding volumes by using the storage system's management software.



Note:

This problem occurs for the following combinations of storage models and microcode versions. The problem has been fixed in microcode versions later than those listed below. Similarly, the problem does not affect storage models other than those listed below.

Storage model	Microcode version
<ul style="list-style-type: none"> ▪ VSP F350, F370, F700, F900 ▪ VSP G350, G370, G700, G900 	<ul style="list-style-type: none"> ▪ Earlier than 88-08-05-x0/00
VSP E590, E790, E990, E590H, E790H	<ul style="list-style-type: none"> ▪ Earlier than 93-05-05-x0/00 ▪ Earlier than 93-06-21-x0/00
VSP E1090, E1090H	<ul style="list-style-type: none"> ▪ Earlier than 93-06-02-x0/00 ▪ Earlier than 93-06-21-x0/00
VSP 5100, 5500, 5100H, 5500H	<ul style="list-style-type: none"> ▪ Earlier than 90-08-21-00/00 ▪ Earlier than 90-08-03-00/00

Storage model	Microcode version
	▪ Earlier than 90-07-04-00/00
VSP 5200, 5600, 5200H, 5600H	▪ Earlier than 90-08-21-00/00 ▪ Earlier than 90-08-03-00/00

Procedure

1. Unregister the Hitachi storage system from Veeam Backup & Replication.
For details, see the description of Removing Storage Systems in the Veeam Backup & Replication documentation.
2. Delete all of the host groups or iSCSI targets you created by performing the procedure in [Preparing the backup environment for the storage system \(on page 17\)](#) that remain on the unregistered storage system. However, you can skip this step if you want to continue using them.

Configuration file: For a Microsoft Windows-based backup server

By using a configuration file, you can specify backup storage resources (the storage resources used for backup).



Note:

Use this functionality optionally as needed.

Procedure

1. Create a configuration file in accordance with the following conditions:

- Configuration file to be created

Create one configuration file for one storage system.

- Configuration file specifications

- File name

serial-number-of-the-storage-system_config.txt

Example: For VSP One B20 series

123456_config.txt



Note:

- For the storage system's serial number, the number of digits varies depending on the storage model, as follows:

- VSP E series: Six digits
- VSP F350, F370, F700, F900: Six digits
- VSP G350, G370, G700, G900: Six digits
- VSP 5000 series and VSP One B85: One to five digits



Note: For the VSP 5000 series and VSP One B85, when the storage system's serial number is four digits or less, depending on the storage system management software, the serial number might appear in a 5-digit format with leading zeros. (Example: If the serial number is 1, it might appear as "00001" in the storage system management software). If you create a configuration file with these leading zero numbers, Storage Plug-in will no longer be loaded. Therefore, make sure that the *storage-system-serial-number* is created in a format where the leading zeros are not padded.

- VSP One B20 series: Six digits

- The suffix *_config.txt* at the file name must be lowercase.



- File format

Text

- Character encoding

UTF-8

- Storage resource specification format
Specify the backup storage resources in the following format: *KEY=VALUE*.
- Type of storage resources that can be specified

Resource type	KEY	VALUE
Dynamic Provisioning pool used for backup	PoolName	<p><i>pool-name</i></p> <p> Note:</p> <ul style="list-style-type: none"> For the <i>pool-name</i>, it is not necessary to follow the <i>VBR_single-byte-character-string</i> format. If the volumes to be backed up are data reduction shared volumes, volumes of snapshots or snapshot clones will be created in the same pool as the volumes to be backed up. For this reason, the specification of a Dynamic Provisioning pool used for backup is not used.
Resource group used for backup	RSGName	<p><i>resource-group-name</i></p> <p> Note:</p> <p>For the <i>resource-group-name</i>, it is not necessary to follow the <i>VBR_single-byte-character-string</i> format.</p>

The following shows an example of the content of a configuration file.

```
PoolName=Backup_Pool_001
RSGName=Backup_RSG_001
```

- Place the configuration file in the following location:

Veeam-Backup&Replication-path\Plugins\Storage\Hitachi\conf



Note: If you place the configuration file or modify the contents of the configuration file, the changes become effective immediately. Therefore, rescanning (Storage Discovery) is unnecessary.

Configuration file: For Veeam Software Appliance (Linux)

By using a configuration file, you can specify backup storage resources (the storage resources used for backup). For detailed procedures, see the explanation on Managing Configuration Files in the Veeam Backup & Replication documentation.



Note:

- Use this functionality optionally as needed.
- If you place the configuration file or modify the contents of the configuration file, the changes become effective immediately. Therefore, rescanning (Storage Discovery) is unnecessary.

Procedure

1. Download the configuration file from the configuration window for setting the Veeam Software Appliance configuration file. When you download the configuration file for the first time, it is an empty file.

The file path for the configuration file is as follows:

```
/etc/veeam/plugins/storages/hitachi-vsp/storage_plugin_advanced_settings.json
```

2. Edit a configuration file in accordance with the following conditions:
 - Configuration file specifications
 - File name
`storage_plugin_advanced_settings.json`
 - File format
JSON
 - Character encoding
UTF-8

- Contents of the configuration file

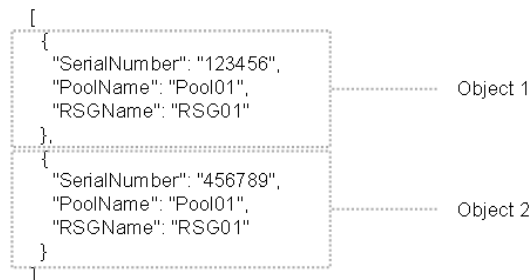
Describe the objects corresponding to the registered storage systems in JSON format . The following shows an example of the content of a configuration file.

```
[
  {
    "SerialNumber": "123456",
    "PoolName": "Pool01",
    "RSGName": "RSG01"
  },
  {
    "SerialNumber": "456789",
    "PoolName": "Pool01",
    "RSGName": "RSG01"
  }
]
```

About JSON objects

In JSON, data is represented as KEY and VALUE pairs (properties). One or more properties separated by commas and enclosed in curly brackets ({}) are called objects.

As an example, the object parts of a configuration file are shown as follows.




Note: KEY and VALUE need to be enclosed in double quotation marks (").



Object properties to be specified in the configuration file

For object properties to be specified in the configuration file, specify the following items:


- Serial number of the storage system which is specified as target for backup storage resource
Specification of this item is required.
- Backup storage resource
As this item needs to be specified depends on the user's environment, specification of this item is optional.

The following table shows the properties of each object to be specified in the configuration file.

Item	KEY	VALUE
Storage system to be specified as a backup storage resource	SerialNumber	<p><i>serial number</i></p> <div data-bbox="889 310 1393 1669" style="background-color: #e0f2f1; padding: 10px;"> <p> Note:</p> <p>For the storage system's serial number, the number of digits varies depending on the storage model, as follows:</p> <ul style="list-style-type: none"> ▪ VSP E series: Six digits ▪ VSP F350, F370, F700, F900: Six digits ▪ VSP G350, G370, G700, G900: Six digits ▪ VSP 5000 series and VSP One B85: One to five digits <p>For the VSP 5000 series and VSP One B85, when the storage system's serial number is four digits or less, depending on the storage system management software, the serial number might appear in a 5-digit format with leading zeros. (Example: If the serial number is 1, it might appear as "00001" in the storage system management software). If you create a configuration file with these leading zero numbers, Storage Plug-in will no longer be loaded. Therefore, make sure that the <i>storage-system-serial-number</i> is created in a format where the leading zeros are not padded.</p> <ul style="list-style-type: none"> ▪ VSP One B20 series: Six digits </div>
Dynamic Provisioning pool used for backup*	PoolName	<i>pool-name</i>

Item	KEY	VALUE
		<p> Note:</p> <ul style="list-style-type: none"> For the <i>pool-name</i>, it is not necessary to follow the <code>VBR_single-byte-character-string</code> format. If the volumes to be backed up are data reduction shared volumes, volumes of snapshots or snapshot clones will be created in the same pool as the volumes to be backed up. For this reason, the specification of a Dynamic Provisioning pool used for backup is not used.
Resource group used for backup*	RSGName	<p><i>resource-group-name</i></p> <p> Note:</p> <p>For the <i>resource-group-name</i>, it is not necessary to follow the <code>VBR_single-byte-character-string</code> format.</p>
<p>Notes:</p> <p>It is acceptable to specify only each of them.</p>		

- Upload the configuration file at the configuration window for setting the Veeam Software Appliance configuration file.

 **Note:** If the configuration file includes errors, you might not be able to successfully perform operations not only for the storage system targeted by the configuration file but also for all storage systems. To avoid any impact on operations, after you edit the configuration file, we recommend that you perform a backup or restore operation in advance for the backup storage resources targeted by the configuration file, and make sure that processing ends successfully without any errors.

Chapter 3: Backing up and restoring virtual machines using Storage Plug-in

You can use Storage Plug-in to back up virtual machines from primary or secondary storage system and restore them using storage snapshots.

The terms P-VOL and S-VOLs shown in this chapter correspond to Production Volume and Snapshot Volume, indicating their roles in the storage snapshot workflow.

For details on the operational procedures and terminology regarding the Veeam Backup & Replication functions related to backup and restore described in this chapter, refer to the Storage System Snapshot Integration Guide in the Veeam Backup & Replication documentation.

Restrictions on backup and restore using Storage Plug-in

This section describes the restrictions on backup and restore using Storage Plug-in.

- If you want to back up LDEVs in a Microsoft VSS environment, when you create backup jobs, do not set the Application-Aware Processing options. If you set these options, the backup jobs might not run successfully.
- You can manually create snapshots from Veeam Backup & Replication by specifying the volume to be backed up. In this case, note the following when setting snapshot names; otherwise, if the created snapshots are no longer needed, you might not be able to correctly delete them from Storage Plug-in.
 - Avoid using same character strings for snapshot names. Instead, set unique character strings. It is recommended to use character strings that contain unique information such as the purpose of use or date that can easily identify the snapshots.
 - Do not include symbols in snapshot names, such as the following:
Forward slash (/) or backslash (\)
- If a volume with the name *any-string-of-single-byte-characters_DEL (LDEV-ID)* appears in the Storage Infrastructure view, use storage system management software such as Device Manager - Storage Navigator, find the corresponding volume based on the LDEV ID in the volume name, and then delete that volume.

Restrictions on backup of data reduction shared volumes

When backing up a data reduction shared volume, the larger the capacity of the volume to be backed up, the longer the backup will take. Also, the backup might fail or take longer than expected if the following conditions are met.

Conditions that might cause a backup to fail or take longer than expected:

When the types of backup operations are divided as follows, two or more "Backup from storage snapshots with snapshot retention" jobs run on the same data reduction shared volume, or two or more types of backup operations are performed simultaneously on the same data reduction shared volume.

- Backup job (Snapshot-only job)
- Backup job (Backup from storage snapshots)
- Backup job (Backup from storage snapshots with snapshot retention)
- Select the volume from the Storage Infrastructure view, and then run Create Snapshot.



Note:

If a backup fails, one of the following messages will appear:

- The error is occurred in REST API. Please contact storage system administrator to check the details in the log file.*
- *When this error occurs, a message containing KART40009-E is output to the log file.
- The pre-check process before creating a snapshot/clone has timed out. Please check the status of the pairs created on the target production volume and try again after a while.

To prevent the above conditions, we recommend that you use only one backup job targeting virtual machines on a datastore composed of a single data reduction shared volume. This will ensure that the backup does not fail or take longer than expected.

When running multiple backup jobs targeting virtual machines on a datastore composed of a single data reduction shared volume, set a job execution schedule that avoids simultaneous execution of multiple jobs, and ensure sufficient intervals between the start time of each backup job.

After planning your backup operation taking the above into consideration, first run the backup job according to the schedule as a verification to make sure that the backup will not fail. In addition, when a backup job targeting virtual machines on a datastore composed of a data reduction shared volume is running, do not run Create Snapshot on the same volume.

Running and checking backup jobs with the Snapshot Immutability function enabled

You can use the Snapshot Immutability function to set a protection period for snapshots.

Before you begin

When using the Snapshot Immutability function, the storage system must meet the following prerequisites.

- Storage system and microcode version

To set a protection period for snapshot, you must use a storage system and microcode version that support the Snapshot Immutability function. For details on the applicable storage systems and microcode versions, see [Environment requirements \(on page 10\)](#).

- Volume to be backed up

To specify a protection period for snapshot, the volume to be backed up must be a data reduction shared volume. In this case, when the snapshot is created, a pair using Thin Image Advanced is created, and the specified retention period is applied. When the volume to be backed up is a supported volume other than a data reduction shared volume, even if a backup job with Snapshot Immutability enabled is run, the protection period specified by the user is invalidated.

- Snapshot protection period

The protection period for snapshot is implemented through the snapshot protection period function of Thin Image Advanced. As a result, the protection period that can specify with Snapshot Immutability depends on the snapshot protection period function of Thin Image Advanced. For details on the specifiable length of the protection period, see the storage system documentation.



Note: Veeam Backup & Replication might adjust the user-specified protection period to fit within the specifiable length of the protection period for the actual storage system. To confirm the protection period adjusted by Veeam Backup & Replication, display the snapshot details of the volume targeted by the backup job, and then check the time information of the protection period in the **Immutable Until** field.

When you run a backup job with the Snapshot Immutability function enabled, perform the following steps to confirm that snapshots with a protection period have been created on the target volumes. If the backup job that you run targets multiple data stores, verify all snapshots created within the job.

Procedure

1. Open the **Storage Infrastructure** view in Veeam Backup & Replication, and then select the volume targeted by the backup job that was run to display the list of snapshots under the target volume.
2. From the detailed information on the displayed snapshots, check whether the protection period is set as specified in the **Immutable Until** field.

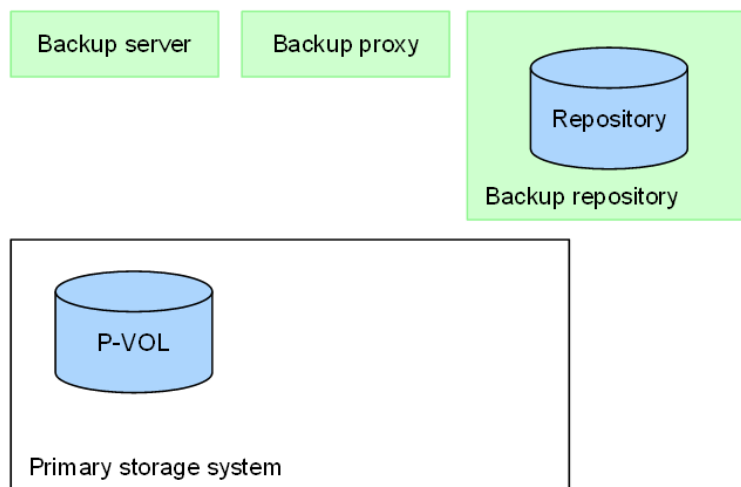
Backing up on a primary storage system

You can create a backup job by using such as Backup from storage snapshots, Snapshot orchestration, and Backup from storage snapshots with snapshot retention on a primary storage system.

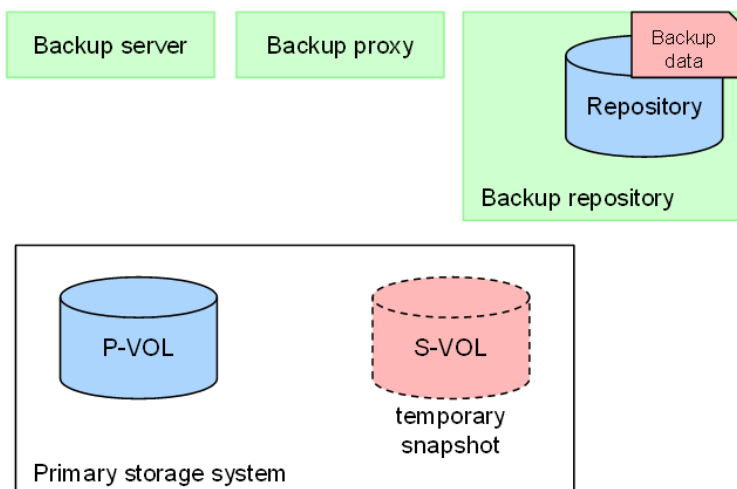
Backup from storage snapshots (primary storage system)

The following figure shows the storage system state before and after the backup job runs. The S-VOL (temporary snapshot) created on the primary storage system is deleted by Veeam Backup & Replication.

Before



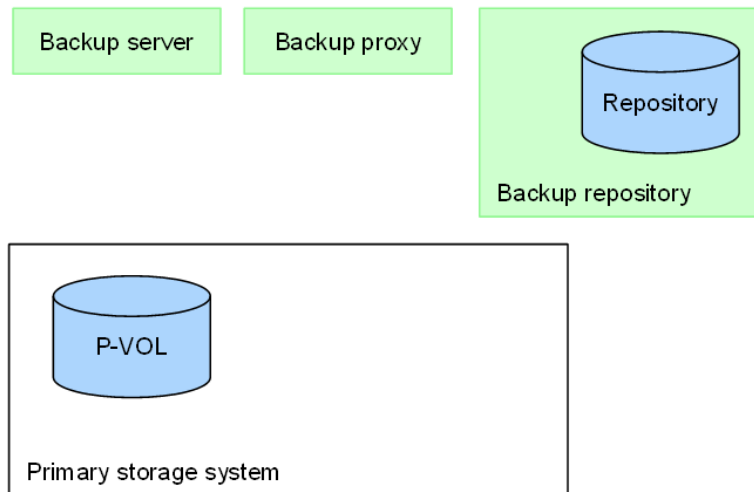
After



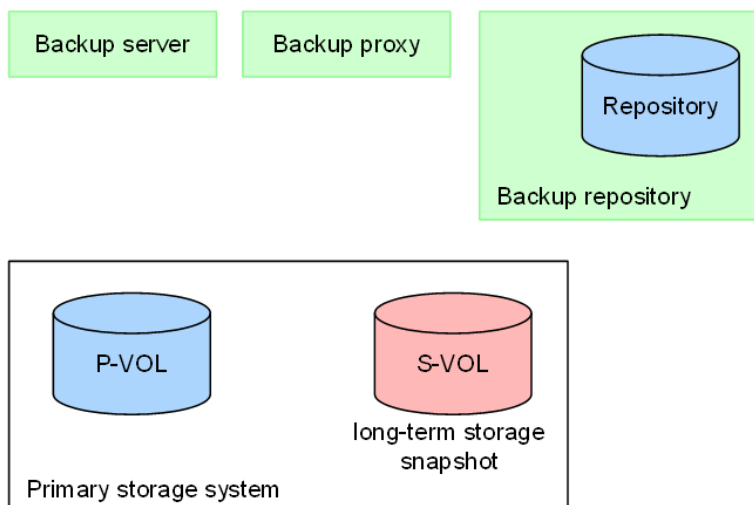
Snapshot orchestration (primary storage system)

The following figure shows the storage system state before and after the backup job runs. The S-VOL (long-term storage snapshot) created on the primary storage system is retained according to the retention policy specified when the job was created. Old storage snapshots (S-VOLs) that are no longer subject to be retained will be deleted by Veeam Backup & Replication.

Before



After





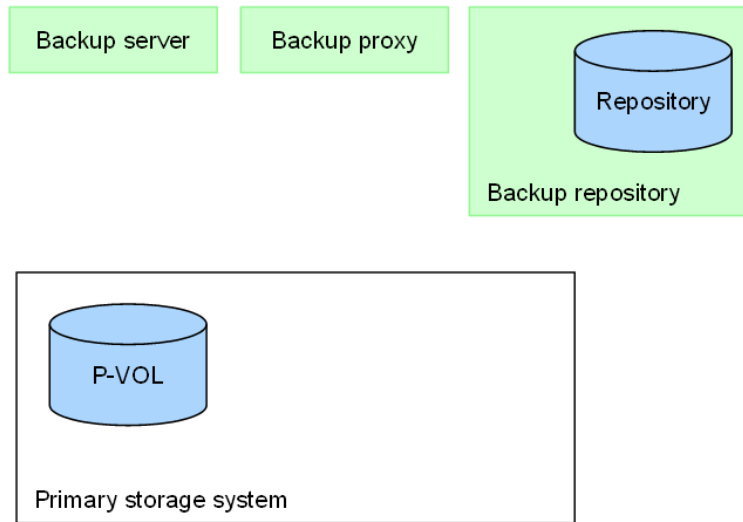
Note:

- When operating Veeam Backup & Replication, note the following:
When creating a Backup Job, for the backup repository in the storage settings, select HITACHI Snapshot (Primary storage snapshot only).
- When backing up data reduction shared volumes, you can use the Snapshot Immutability function to set a protection period for long-term storage snapshots.

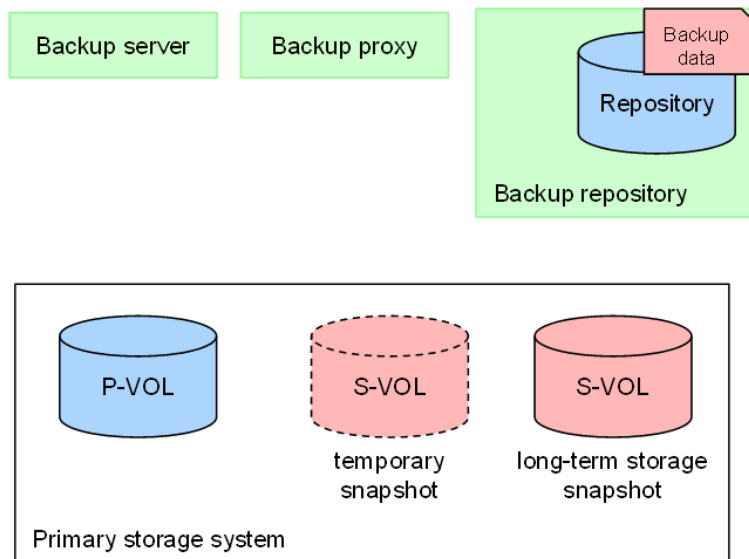
Backup from storage snapshots with snapshot retention (primary storage system)

The following figure shows the storage system state before and after the backup job runs. When the job is run, two S-VOLs, a temporary snapshot and a long-term storage snapshot, are created. The S-VOL (temporary snapshot) created on the primary storage system is deleted by Veeam Backup & Replication. The other S-VOL, which is the long-term storage snapshot, is retained according to the settings specified for saving snapshots when the job was created. Old storage snapshots (S-VOLs) that are no longer subject to be retained will be deleted by Veeam Backup & Replication.

Before



After



Note:

- When operating Veeam Backup & Replication, note the following:
When creating a Backup Job, for the secondary target settings, select HITACHI Snapshot.
- When backing up data reduction shared volumes, you can use the Snapshot Immutability function to set a protection period for long-term storage snapshots.

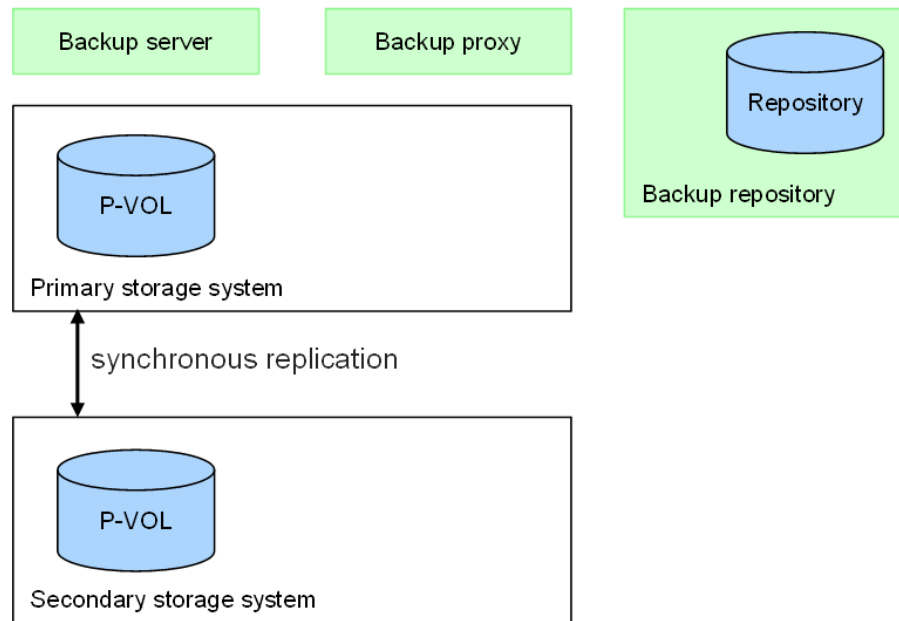
Backing up on a secondary storage system

You can create a backup job by using such as Backup from storage snapshots, Snapshot orchestration, and Backup from storage snapshots with snapshot retention on a secondary storage system.

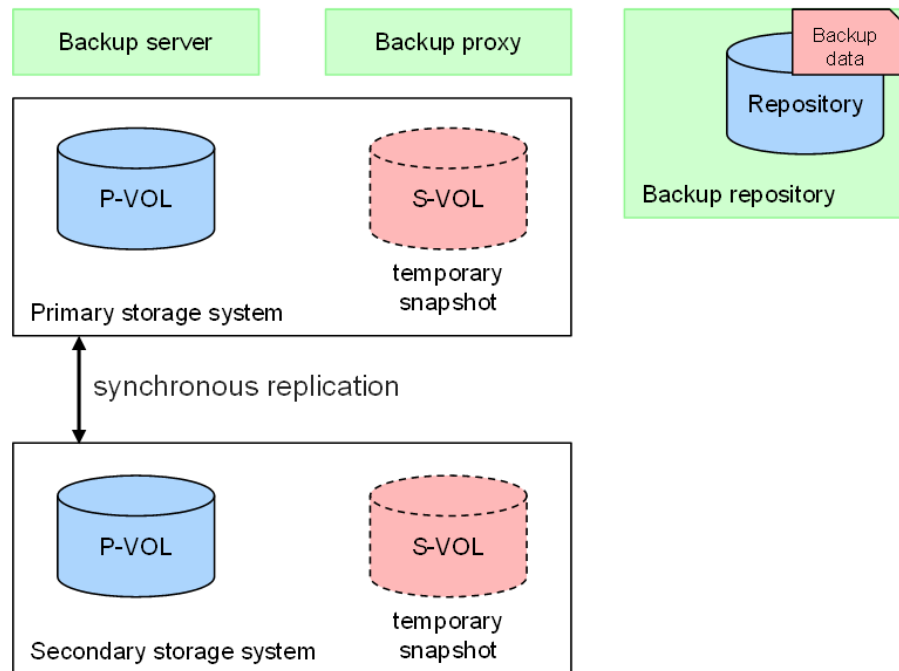
Backup from storage snapshots (secondary storage system)

The following figure shows the storage system state before and after the backup job using synchronous replication runs. When the job is run, S-VOLs (temporary snapshots) are created on both the primary storage system and the secondary storage system. The created S-VOLs are deleted by Veeam Backup & Replication from both the primary storage system and the secondary storage system.

Before



After



Note:

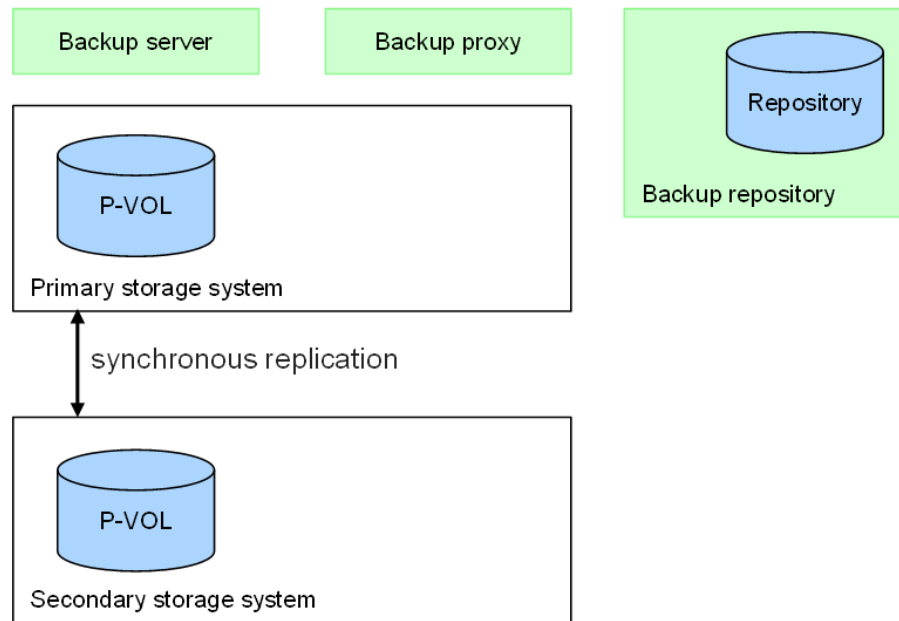
When operating Veeam Backup & Replication, note the following:

When creating a Backup Job, for the secondary target settings, select HITACHI Synchronous Replication and verify that HITACHI Synchronous Replication (data source) has been added.

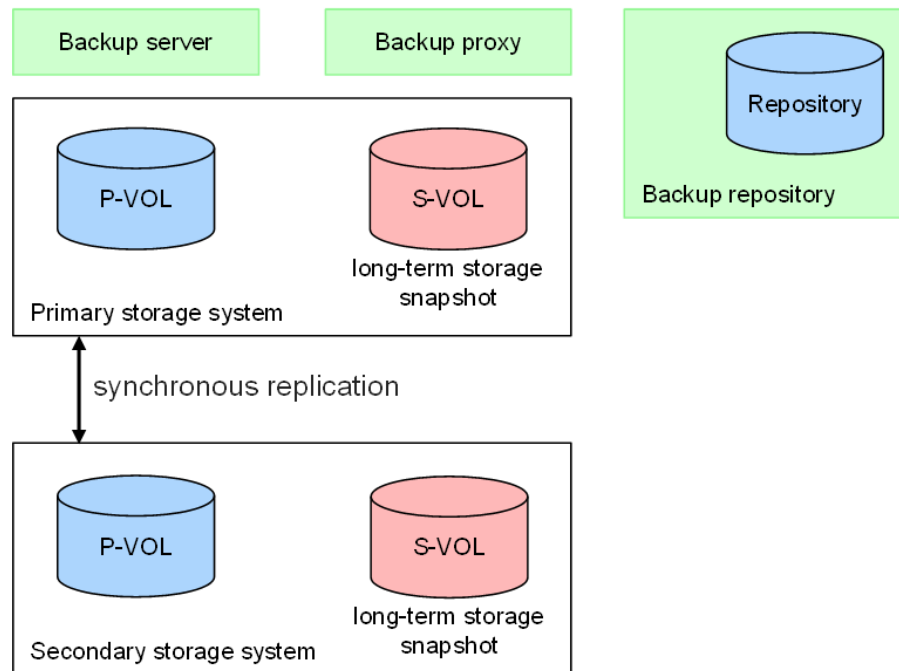
Snapshot orchestration (secondary storage system)

The following figure shows the storage system state before and after the backup job using synchronous replication runs. When the job is run, S-VOLs (long-term storage snapshots) are created on both the primary storage system and the secondary storage system. The created S-VOLs are retained according to the retention policy specified when the job was created. Old storage snapshots (S-VOLs) that are no longer subject to be retained will be deleted by Veeam Backup & Replication from both the primary storage system and the secondary storage system.

Before



After



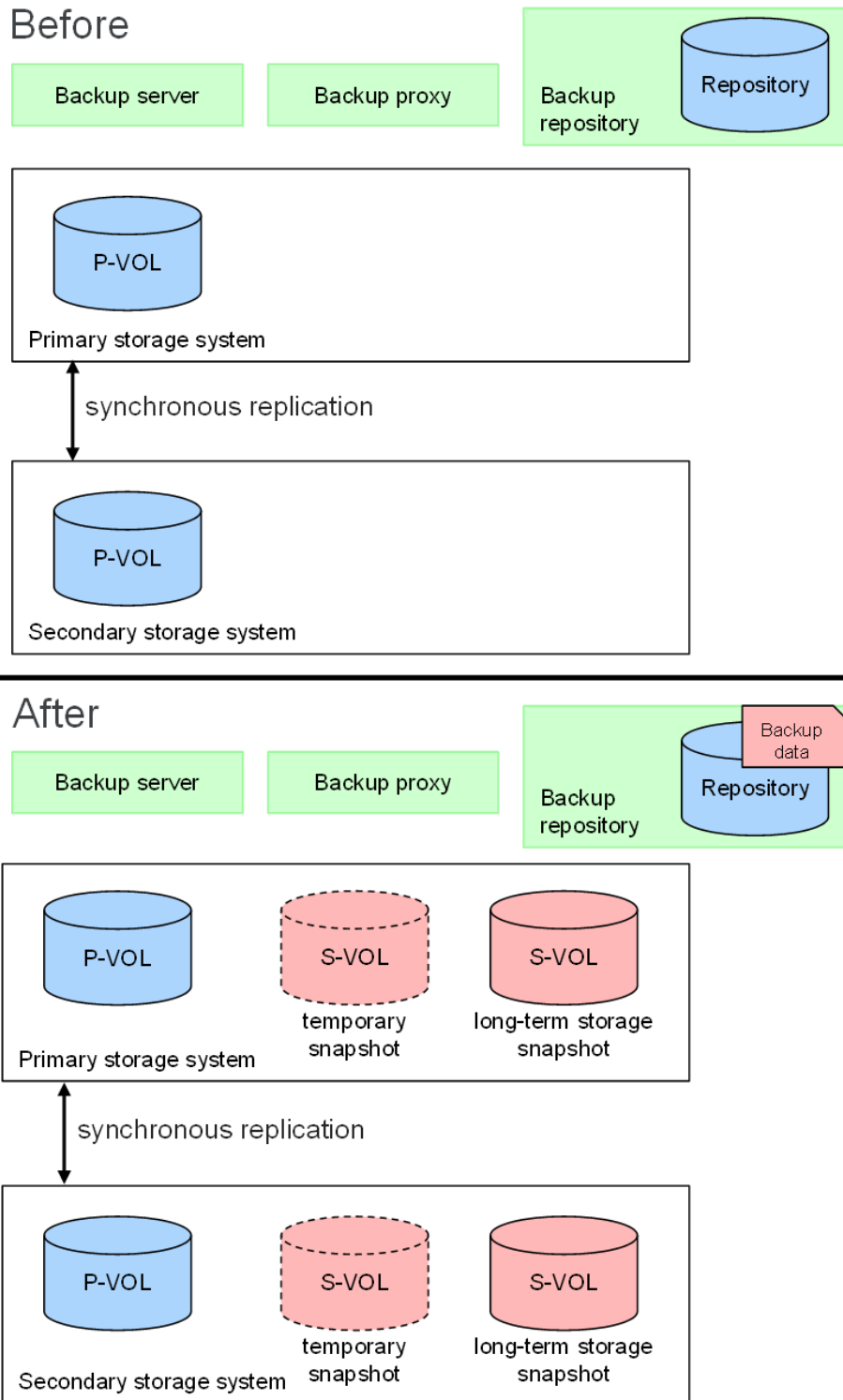


Note:

- When operating Veeam Backup & Replication, note the following:
When creating a Backup Job, for the backup repository in the storage settings, select HITACHI Snapshot (Primary storage snapshot only).
- When backing up data reduction shared volumes, you can use the Snapshot Immutability function to set a protection period for long-term storage snapshots.

Backup from storage snapshots with snapshot retention (secondary storage system)

The following figure shows the storage system state before and after the backup job using synchronous replication runs. When the job is run, two S-VOLs, a temporary snapshot and a long-term storage snapshot, are created on both the primary storage system and the secondary storage system. The created S-VOLs (temporary snapshots) are deleted by Veeam Backup & Replication from both the primary storage system and the secondary storage system. The other S-VOLs, which are the long-term storage snapshots, are retained according to the settings specified for saving snapshots when the job was created. Old storage snapshots (S-VOLs) that are no longer subject to be retained will be deleted by Veeam Backup & Replication from both the primary storage system and the secondary storage system.



**Note:**

- When operating Veeam Backup & Replication, note the following:
When creating a Backup Job, for the secondary target settings, select HITACHI Snapshot and HITACHI Synchronous Replication, and verify that HITACHI Snapshot and HITACHI Synchronous Replication (data source) have been added.
- When backing up data reduction shared volumes, you can use the Snapshot Immutability function to set a protection period for long-term storage snapshots.

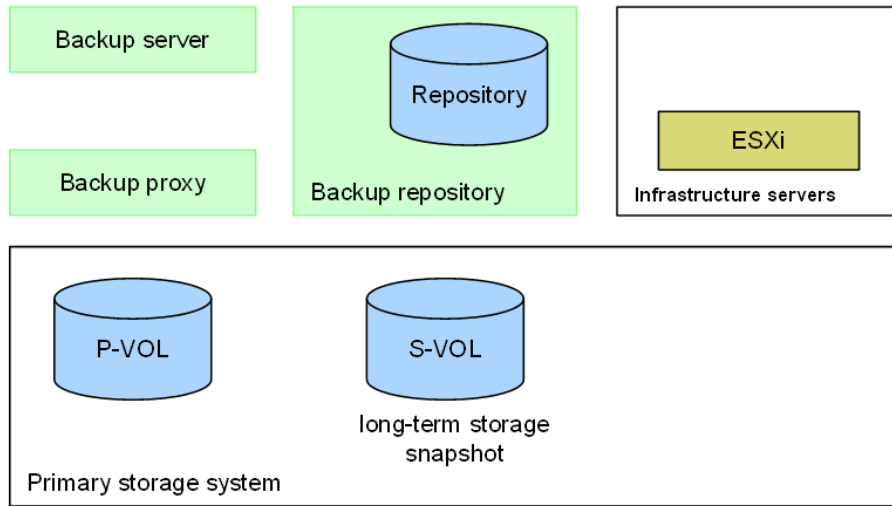
Restoring from storage snapshot

You can perform an Instant recovery from storage snapshots using a long-term storage snapshot on a storage system.

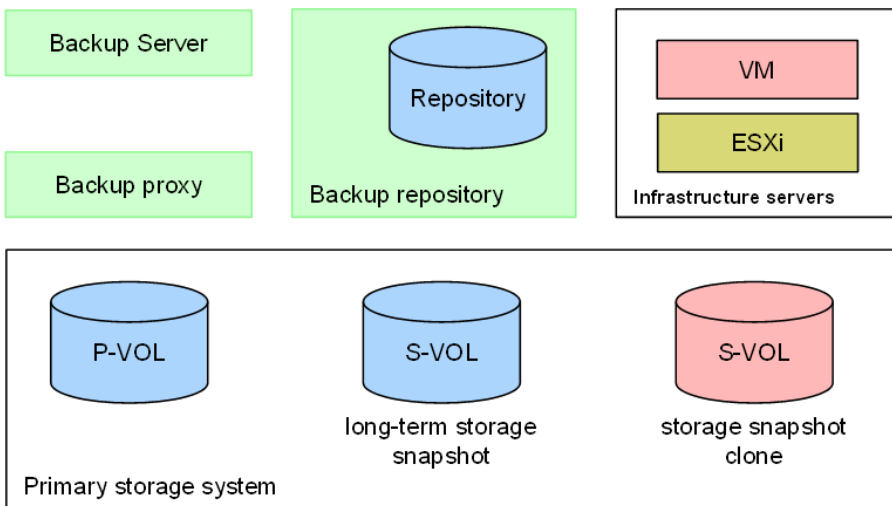
Instant recovery from storage snapshot

The following figure shows the storage system state before and after Instant Recovery. When performing Instant Recovery, a snapshot clone is created using S-VOL (long-term storage snapshot) on the primary storage system. The created snapshot clone is deleted by Veeam Backup & Replication after the Instant Recovery is complete.

Before



After




Chapter 4: Troubleshooting

The following describes how to handle failures that occur during operation and how to collect maintenance information.

What to check first

If an error occurs, first check the environment. The procedure for the check is as follows.

 **Note:** If the storage system and Veeam Backup & Replication are performing other processing in parallel, an operation might fail because of a temporarily high load or processing conflict. In such cases, try that operation again.

1. Refer to [Setting up the environment \(on page 17\)](#) and make sure that the storage system environment is configured correctly.

Also, perform the following checks to ensure that the status is normal.

- Make sure that the status of the network environment is normal.
- Make sure that the datastore and virtual machine to be operated are working correctly.

2. For the volumes to be used, perform the following checks using the storage system management software to ensure that the settings and status are correct.

For the snapshots and snapshot clones created using Veeam Backup & Replication, verify that the corresponding secondary volumes of the Thin Image pairs or Thin Image Advanced pairs and the corresponding volumes that were cloned by using Thin Image are correct.

- Make sure that the volume to be used and the Thin Image pair or Thin Image Advanced pair created for the volume are correct.
- Make sure that unused LDEV IDs have been allocated to the backup resource group created in [Preparing the backup environment for the storage system \(on page 17\)](#).

Make sure that a sufficient number of LDEV IDs have been allocated.

3. For the connection between the storage system and the backup proxy server or VMware ESXi host used for restoration, make sure that the environment is configured correctly as follows.

- Make sure that the Fibre Channel port or iSCSI port for the backup proxy server is not disabled and that its status is normal.
- Make sure that the Fibre Channel port or iSCSI port of the VMware ESXi host used for restoration is not disabled and does not have an abnormal status.
- Make sure the Fibre Channel or iSCSI communication channel is functioning properly.

For example, verify the following:

- The path is physically connected.
- Devices such as the relay switch are running.
- Logical settings such as zoning are specified correctly.

4. Refer to [Preparing the backup environment for the storage system \(on page 17\)](#) and make sure that the host group and iSCSI target are configured correctly.

Make sure that the following items are configured correctly:

- Host group name or iSCSI target name
- Host mode
- Host mode options

Handling failures

The following describes how to handle failures that occur during operation.

Message: The hostGroup used in the plugin does not exist

If you are using a Fibre Channel connection and the host group is not configured correctly, this message might appear.

Make sure to perform the following procedures listed in [Preparing the backup environment for the storage system \(on page 17\)](#).

- Creating a host group for the backup proxy server and VMware ESXi host
- Allocating the host group to a resource group for backup

After performing the above checks, rerun the processing.

Message: There is no iSCSI target to register iSCSI name

- If you are using an iSCSI connection and the iSCSI target is not configured correctly, this message might appear.

Make sure to perform the following procedures listed in [Preparing the backup environment for the storage system \(on page 17\)](#).

Message: Unable to access file snapshot

- Creating an iSCSI target for the backup proxy server and VMware ESXi host
 - Allocating the iSCSI target to a resource group for backup
- After performing the above checks, rerun the processing.
- If you see this message during **Rescan storage** or **Create Snapshot**, make sure to perform the following steps:
 - Create an iSCSI target prefixed with "VBR_", without registering any initiator IQNs.
 - Restart the Veeam services.

During the storage rescan or snapshot creation process, the plug-in automatically registers the Veeam initiator IQN with the iSCSI target.

Message: Unable to access file snapshot

If this message is output while the backup processing is running, make sure that there is sufficient space in the pool for business, and then rerun the processing.

Message: Cannot choose between the volume LUNs with the same ID / No synchronous replication relationship was detected for these volumes

If you perform a backup job for a global-active device pair, this message might be the output.

- If backup that uses synchronous replication fails due to the error in this message, see Environment requirements (on page 10) and correct the incorrect settings related to synchronous replication.
- If backup that does not use synchronous replication fails due to the error in this message, register only one of the two storage systems that make up the pair in Veeam Backup & Replication.
- In a global-active device configuration, if the secondary volume (SVOL) assigned to a Virtual Storage Machine (VSM) has the same serial number as the primary storage system, ensure that the VSM name does not include the "VBR_" prefix. In addition, create a separate resource group prefixed with "VBR_" on the secondary storage system.

Message: Unexpected character encountered while parsing value

A communication problem between Storage Plug-in and the storage system or a problem in the processing tasks on the storage system might prevent to obtain the correct information. To ensure that the status is normal, make sure:

- The status of the network environment is normal.
- The storage system is running.
- The REST API of the storage system is running.
- The load on the storage system is not high. For example, make sure that a large number of processing tasks are not performed on the storage system.

After performing the above checks, rerun the processing.

Message: The timeout (xx:xx:xx) occurred in the REST-API response. Try the operation again when the storage load is light

If there are multiple resource groups allocated to a backup operation user group and the values of those resource group IDs are not close to each other, depending on the load situation of the storage system, an attempt to rescan (Storage Discovery) or unregister the storage system might fail, resulting in the output of this message.

In the preceding situation, if this message is output, specify settings so that the values of those resource group IDs are as close to each other as possible.

Message: Synchronous replication relationships not found

If you are backing up a synchronized TrueCopy or global-active device pair and the settings are incorrect, the backup that uses synchronous replication might not work.

If this message is output, see [Environment requirements \(on page 10\)](#) and fix the incorrect settings.

Message: The pre-check process before creating a snapshot/clone has timed out. Please check the status of the pairs created on the target production volume and try again after a while

When you perform a backup, if data copy processing is already in progress for the business volumes to be backed up, this message might be output and the backup might fail. In addition, when you run Instant Recovery or SureBackup for storage snapshots, if data copy processing is already in progress for the volume of the target storage snapshots, this message might be output and the operation might fail.

While data copy processing is in progress, the Thin Image Advanced pair for which the primary volume is set as the volume to be backed up exists in the PSUP/PSUS(SP) state. Wait until the relevant Thin Image Advanced pair changes to the PSUS state, and then retry the operation that failed.



Note: This problem occurs when the volumes to be backed up are data reduction shared volumes. For details on how to avoid this problem in backup operation, see [Restrictions on backup of data reduction shared volumes \(on page 41\)](#).

Message: The error is occurred in REST API. Please contact storage system administrator to check the details in the log file. A message including KART40009-E is output to the log file

When an attempt is made to perform a backup or to run Instant Recovery or SureBackup for storage snapshots, the error message `The error is occurred in REST API.` Please contact storage system administrator to check the details in the log file appears, and the job fails, after that, if you check the log file, a message including `KART40009-E` might be output as follows:

```
"messageId" : "KART40009-E",
```

For backup, the reason why the attempt fails is that data copy processing is already in progress for the business volumes to be backed up. In addition, for Instant Recovery or SureBackup, the reason why the attempt fails is that data copy processing is already in progress for the volume of the target storage snapshots.

Message: The number of files in the gc folder exceeded the limit

While data copy processing is in progress, the Thin Image Advanced pair for which the primary volume is set as the volume to be backed up exists in the PSUP/PSUS(SP) state. Wait until the relevant Thin Image Advanced pair changes to the PSUS state, and then retry the operation that failed.



Note: This problem occurs when the volumes to be backed up are data reduction shared volumes. For details on how to avoid this problem in backup operation, see [Restrictions on backup of data reduction shared volumes \(on page 41\)](#).

Message: The number of files in the gc folder exceeded the limit

If problems such as intermittent failures in Storage Plug-in processing occur on the storage system or the Veeam backup server, this message might appear.

If this message appears, perform the following steps to resolve the problem, and then retry the failed operation.

Procedure

1. Make sure that there is a folder named `gc` in the following folder:

For a Microsoft Windows-based backup server:

`Veeam-Backup&Replication-path\Plugins\Storage\Hitachi\gc`

For Veeam Software Appliance (Linux):

`/etc/veeam/plugins/storages/hitachi-vsp/gc`

2. Move some files to any folder on the Veeam backup server, so that the number of files in the `gc` folder is less than 1,000. Do not delete the moved files.
3. Make sure that the number of files in the `gc` folder is less than 1,000, and then retry the failed operation.
4. After the operation succeeds, return the moved files to the `gc` folder.

Files remain in the gc folder after a storage system is unregistered

In the following folder where Veeam Backup & Replication is installed, there is a folder named `gc`:

For a Microsoft Windows-based backup server:

`Veeam-Backup&Replication-path\Plugins\Storage\Hitachi\gc`

For Veeam Software Appliance (Linux):

`/etc/veeam/plugins/storages/hitachi-vsp/gc`

In this folder, there might be files that contain the storage system names and storage system serial numbers registered in Veeam Backup & Replication.

File name example (when the storage system is VSP E1090, and the serial number is 123456):

```
VSP E1090-123456-111-VeeamCL_0112_20240925085242-113,3-20241010083743
```

Although this file is deleted from the `gc` folder when you unregister the target storage system, this file might remain without being deleted. If the file remains, perform the following procedure:

Procedure

1. Re-register the target storage system in Veeam Backup & Replication.
2. Unregister the target storage system again from Veeam Backup & Replication.
3. Check the `gc` folder, and make sure that there is no file containing the name and serial number of the target storage system.

Storage Plug-in processing and storage system processing are slow

When multiple users perform processing tasks at the same time, or when multiple jobs run at the same time, it might take a long time for Storage Plug-in processing and storage system processing to finish.

Avoid running multiple processing tasks simultaneously by reducing the number of users who perform operations, or by staggering the start times of multiple jobs.

An error or warning event is logged in the event log of the backup proxy server

The Windows Server that is operating as the backup proxy server might log any of the events listed in the following table. These events are issued when verification processing of the backup data completes in Veeam Backup & Replication and the volume is successfully disconnected. No action is necessary because this is normal behavior. If a path error occurs due to a cause other than the processing in Veeam Backup & Replication, check the cause of the error and take remedial action.

Event ID	Level	Message	Remarks
157	Warning	Disk <i>number</i> has been surprise removed.	None.
15	Error	The device, <i>a-path-of-device</i> , is not ready for access yet.	None.
20781	Error	KAPL05301-E A path has been removed. (The following part is omitted.)	This is issued when Hitachi Dynamic Link Manager is used.
32787	Error	KAPL08019-E The path (<i>path-id</i>) detected an error (<i>error-code</i>). (The following part is omitted.)	This is issued when Hitachi Dynamic Link Manager is used.
32790	Error	KAPL08022-E A path error occurred. (The following part is omitted.)	This is issued when Hitachi Dynamic Link Manager is used.

Event ID	Level	Message	Remarks
32794	Error	KAPL08026-E An error occurred on all the paths of the LU. (The following part is omitted.)	This is issued when Hitachi Dynamic Link Manager is used.

Information to be collected when a failure occurs

If a failure occurs in Storage Plug-in, collect the information and then contact customer support.

Collecting Storage Plug-in information

Storage Plug-in information is included in the log files of the Veeam backup server on which Storage Plug-in is installed. For details on how to collect those log files, see the description of Exporting Logs in the Veeam Backup & Replication documentation. When you select the target component for which to collect log files, select the Veeam backup server on which Storage Plug-in is installed.

Collecting storage system information

If you are using an SVP, collect the normal dump files. If you are not using an SVP, collect system dumps by using the maintenance utility. For details about how to collect the dump files of these storage systems, see the *System Administrator Guide*.

Hitachi Vantara



Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact