

Hitachi Storage (VASA) Provider for VMware vCenter vVols Replication Guide

v3.7.4

This document provides information on how to set up and operate the vVols Replication function on supported storage systems.

© 2021, 2024 Hitachi, 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., 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, OS/390, PowerHA, PowerPC, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, 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.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found in the product documentation, at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

Preface.....	6
Intended audience.....	6
Product version.....	6
Release notes.....	6
Changes in this revision.....	7
Referenced documents.....	7
Document conventions.....	7
Conventions for storage capacity values.....	9
Accessing product documentation.....	10
Getting help.....	10
Comments.....	10
Chapter 1: Overview.....	11
Purpose.....	11
System configuration.....	11
Chapter 2: Requirement.....	14
System requirement.....	14
Notes.....	15
Restrictions.....	17
Chapter 3: Upgrading the vVols Replication environment.....	22
Preparing to use Thin Image pairs for which the cascade attribute is enabled.....	22
Chapter 4: Settings to be configured in advance.....	24
Configuring a vVols environment at the local site.....	24
Configuring a vVols environment at the remote site.....	24
Storage system settings to be configured in advance.....	25
Configuring a remote path.....	25
Adding a remote connection at the local site.....	25
Adding a remote connection at the remote site.....	26
Creating a dummy LDEV.....	26
Creating a data flow host group.....	27
Protector settings to be configured in advance.....	27
Introducing a Master node.....	28

Introducing a Client node at the local site.....	28
Introducing a Client node at the remote site.....	28
Creating a Hitachi Block Device node at the local site.....	28
Creating a Hitachi Block Device node at the remote site.....	30
Creating a Hitachi Block Host node.....	31
Creating a policy.....	32
Creating a data flow.....	34
VASA Provider settings to be configured in advance.....	38
Specifying the information of VASA Provider at the remote site by using VASA Provider at the local site.....	38
Specifying the information of VASA Provider at the local site by using VASA Provider at the remote site.....	39
Configuring a port for placeholder host groups at the local site.....	39
Configuring a port for placeholder host groups at the remote site.....	40
Creating a replication group.....	40
vSphere settings to be configured in advance.....	41
Updating replication group information.....	41
Creating a VM storage policy.....	41

Chapter 5: Configuring vVols Replication settings for virtual machines.. 43

Enabling vVols Replication when you create a virtual machine.....	43
Enabling vVols Replication for an existing virtual machine.....	44
Enabling vVols Replication when you clone a virtual machine.....	45
Enabling vVols Replication when you migrate a virtual machine.....	46
Disabling vVols Replication for a virtual machine.....	47
Adding a disk to a virtual machine.....	47
Reverting a virtual machine.....	48
Expanding the capacity of a virtual disk.....	49

Chapter 6: Failover-related operations..... 51

Planned Failover and Failback.....	51
Performing a Planned Failover.....	51
Performing a Reprotect and Failback.....	55
Forced Failover.....	58
Performing a Forced Failover.....	58
Performing a Failback after restoring the local site.....	60
Continuing operations at the remote site.....	61
Test Failover (Planned).....	64
Starting a Test Failover (Planned).....	65
Stopping a Test Failover (Planned).....	67
Test Failover (UnPlanned).....	67
Starting a Test Failover (UnPlanned).....	68

Stopping a Test Failover (UnPlanned).....	70
Chapter 7: Deleting a vVols Replication environment.....	71
Deleting the settings of a virtual machine.....	71
Deleting a replication group.....	71
Deleting the general settings.....	73
Deleting a data flow and Protector settings.....	73
Deleting the settings of a storage system.....	74
Deleting a vVols environment.....	75

Preface

This document provides information on how to set up and operate the vVols Replication function on supported storage systems.

Intended audience

This document is intended for:

- vSphere™ system administrators
- Systems engineers

Readers of this document should be familiar with the basic operation of the following:

- Hitachi Virtual Storage Platform 5000 series
- Hitachi Virtual Storage Platform E series
- Hitachi Virtual Storage Platform F350, F370, F700, F900
- Hitachi Virtual Storage Platform G350, G370, G700, G900
- VMware vSphere
- Hitachi Storage Provider for VMware vCenter (VASA Provider)
- Hitachi Ops Center Protector
- Skills required to create programs that use PowerShell

Product version

This document describes Hitachi Storage Provider for VMware vCenter (VASA Provider) v3.7.4.

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>.

Changes in this revision

The following are the major changes:

- Supported VASA Provider configurations were added.
- Because of a change in the processing for a Reprotect after a Forced Failover, the procedure for performing a Forced Failover was changed.

Referenced documents

Hitachi documents:

- VASA Provider
 - Hitachi Storage (VASA) Provider for VMware vCenter Deployment Guide*
- Storage system
 - *Hitachi Universal Replicator User Guide*
 - *Hitachi TrueCopy® User Guide*
 - *System Administrator Guide*
- Hitachi Ops Center Protector
 - *Hitachi Ops Center Protector Quick Start Guide*
 - *Hitachi Ops Center Protector User Guide*
 - *Hitachi Ops Center Protector VMware Application Guide*

Hitachi Vantara Support Connect, <https://knowledge.hitachivantara.com/Documents>

VMware documents:


- vSphere
 - vSphere: <https://docs.vmware.com/en/VMware-vSphere/index.html>
 - PowerCLI: <https://developer.vmware.com/docs/powercli/latest/products/>






Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	<ul style="list-style-type: none"> Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. Indicates emphasized words in list items.
<i>Italic</i>	<ul style="list-style-type: none"> Indicates a document title or emphasized words in text. Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: <pre>pairdisplay -g group</pre> <p>(For exceptions to this convention for variables, see the entry for angle brackets.)</p>
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairdisplay -g oradb</code>
< > angle brackets	Indicates variables in the following scenarios: <ul style="list-style-type: none"> Variables are not clearly separated from the surrounding text or from other variables. Example: <pre>Status-<report-name><file-version>.csv</pre> Variables in headings.
[] square brackets	Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a b } indicates that you must choose either a or b.
vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a b] indicates that you can choose a, b, or nothing. { a b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
	Note	Calls attention to additional information.

Icon	Label	Description
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Important	Highlights information that is essential to the completion of a task.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	CAUTION	Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury.
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10 ³) bytes
1 megabyte (MB)	1,000 KB or 1,000 ² bytes
1 gigabyte (GB)	1,000 MB or 1,000 ³ bytes
1 terabyte (TB)	1,000 GB or 1,000 ⁴ bytes
1 petabyte (PB)	1,000 TB or 1,000 ⁵ bytes
1 exabyte (EB)	1,000 PB or 1,000 ⁶ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB

Logical capacity unit	Value
	Open-systems: <ul style="list-style-type: none"> ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2 ¹⁰) bytes
1 MB	1,024 KB or 1,024 ² bytes
1 GB	1,024 MB or 1,024 ³ bytes
1 TB	1,024 GB or 1,024 ⁴ bytes
1 PB	1,024 TB or 1,024 ⁵ bytes
1 EB	1,024 PB or 1,024 ⁶ bytes

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.

Getting help

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

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

Comments

Please send comments to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 1: Overview

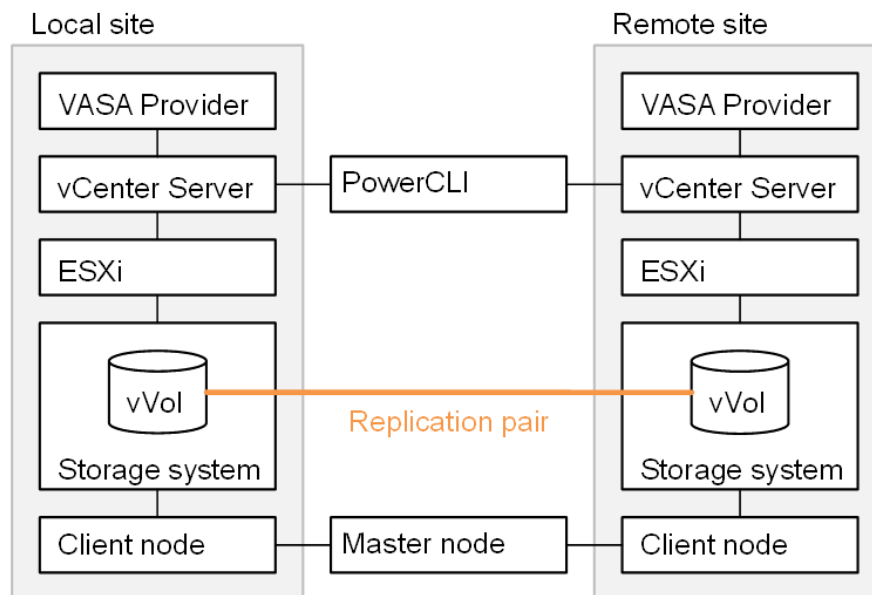
Purpose

vVols Replication feature provides functions for replicating storage systems in an environment that uses VMware vSphere Virtual Volumes (vVols).

System configuration

vVols Replication consists of an active site (the local site) and a standby site (the remote site). Each site consists of vSphere software (vCenter Server, ESXi, and PowerCLI), VASA Provider, Hitachi Ops Center Protector (Protector) software (Protector Master node and Protector Client node), and storage systems. (Hereinafter, the "Protector Master node" is referred to as the "Master node", and the "Protector Client node" is referred to as the "Client node".) Protector is software for managing the replication functions of storage systems. VASA Provider performs replication by using Protector. The vVols of the storage systems at the local site are copied to the storage systems at the remote site by using the remote copy feature, a function for replicating storage systems.

The system configuration diagram is as follows.



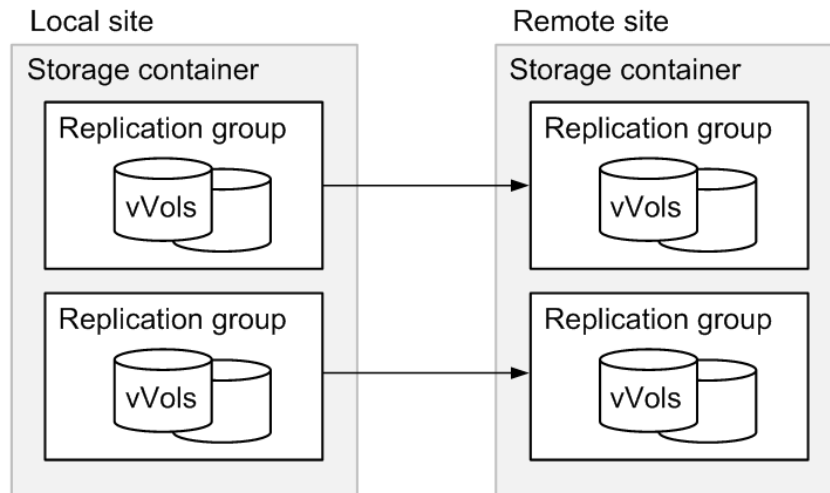


Note: This manual explains the operation of vSphere Client by using the operation of vCenter Server 7.0 Update 3 as an example.

Replication groups

Replication groups are a new type of vVols Replication object. To enable vVols Replication, you must register vVols in replication groups. For vVols for which vVols Replication is enabled, replicas are created and consistency is maintained in units of replication groups. In addition, Failovers and other operations related to vVols Replication are performed in units of replication groups.

The following figure shows the configuration of the replication groups.

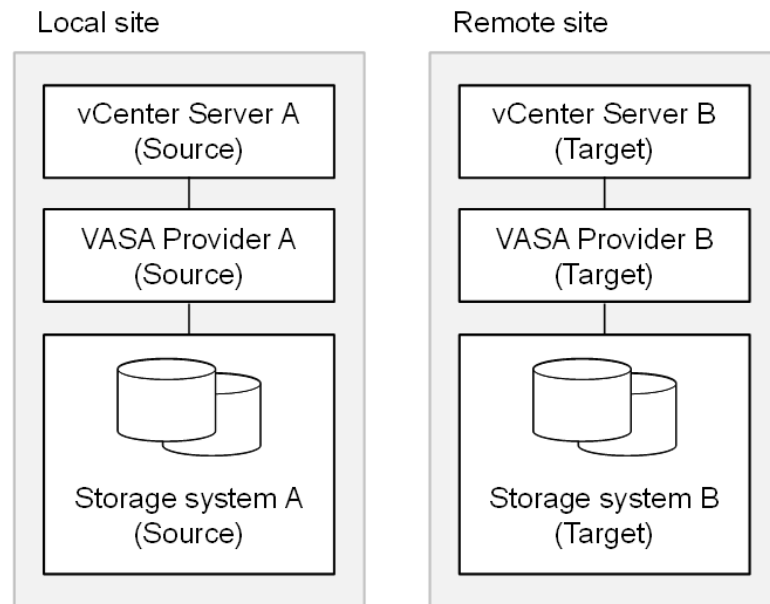


Supported vVols Replication configurations

The supported vVols Replication configuration is as follows.

Configuration in which two different vCenter Servers are used at the local and remote sites

The following figure shows an example of a configuration where two different vCenter Servers are used at the local and remote sites.

**Note:**

- You can register multiple storage systems at the local and remote sites with VASA Provider.

Chapter 2: Requirement

System requirement

The following table lists the vVols Replication system requirements. For the system requirements for configuring a vVols environment, see the *Hitachi Storage (VASA) Provider for VMware vCenter Deployment Guide*.

Component	Requirement
Storage system	<p>If you want to use Universal Replicator: The storage system must be of one of the following models.</p> <ul style="list-style-type: none">▪ VSP 5000 series*▪ VSP E series*▪ VSP F350, F370, F700, F900, and VSP G350, G370, G700, G900 <p>If you want to use TrueCopy: The storage system must be of one of the following models.</p> <ul style="list-style-type: none">▪ VSP 5000 series*▪ VSP E series*
Program product	<p>The following program products must be installed.</p> <ul style="list-style-type: none">▪ ShadowImage <p>If you want to use Thin Image pairs with the cascade attribute enabled, you do not need to install this program product.</p> <ul style="list-style-type: none">▪ Thin Image <p>Either of the following program products must be installed:</p> <ul style="list-style-type: none">▪ Universal Replicator▪ TrueCopy

Component	Requirement
Storage interface	Fibre Channel, iSCSI
Protector	Version 7.7.1
Command Control Interface	Depends on the Protector prerequisite version.
VASA Provider	Version 3.7.4
vSphere software	<ul style="list-style-type: none"> ▪ VMware vCenter Server 7.0 (Update 3) ▪ VMware vCenter Server 8.0/8.0 (Update 1/Update 2) ▪ VMware ESXi 7.0 (Update 3) ▪ VMware ESXi 8.0/8.0 (Update 1/Update 2) ▪ VMware PowerCLI 12.1.0 or later
* You can expand the capacity of virtual disks.	

Notes

General notes

- Even if you used vSphere Client to delete virtual machines for which vVols Replication is enabled, the vVols and PiT replicas remain on the storage system. These vVols and PiT replicas will be deleted according to the retention time for data flow snapshots.
- In Protector, when Universal Replicator pairs are created, path group IDs are used in ascending order. For this reason, if a failure occurs in a path group ID with a lower number, you must recover the path group from the failure.
- For virtual machines that have been restored, no VM storage policy is set. To set a VM storage policy for these virtual machines, use the PowerCLI command, because you might not be able to use vSphere Client to set a policy. For details on how to set a VM storage policy, see the steps pertaining to registering a virtual machine to an ESXi host in the following procedures:
 - [Performing a Planned Failover \(on page 51\)](#)
 - [Performing a Reprotect and Failback \(on page 55\)](#)
 - [Performing a Failback after restoring the local site \(on page 60\)](#)
 - [Continuing operations at the remote site \(on page 61\)](#)
- Before operating vVols Replication, verify that no failure (such as remote path failure) has occurred in the storage system.

- If a data flow exists in Protector in an unsupported configuration, the processing might fail after Set Protector Master information is executed.
- If you want to refresh VASA Provider management information, run Refresh Storage Systems on the Manage Storage Systems screen of the VASA Provider Web UI, and run Refresh Protector Information on the Replication Groups screen.

Information on each component will be synchronized.

Web UI

- After you perform a Planned Failover, Forced Failover, or Reverse Replication, some screen items will not be refreshed immediately. The value of Attribute, which is displayed by selecting the storage container on the Manage Storage Containers screen of the Web UI and then selecting the vVols tab, is not refreshed immediately. Wait for a while, or run Refresh Protector Information on the Replication Groups screen of the Web UI.
- Before refreshing a storage system, make sure that none of the following processes are in progress: processing to create a virtual machine, processing to enable vVols Replication, or processing to run Test Failover Start.

Creation of a virtual machine and enabling of vVols Replication

If vVols Replication cannot be enabled, first set a VM storage policy for vVols for which vVols Replication is disabled, and then re-set the VM storage policy for which vVols Replication is enabled.

To check whether vVols Replication has been enabled, select the storage container on the Manage Storage Containers screen of the Web UI, select the vVols tab, and then check Replication.

Deletion of a virtual machine and disabling of vVols Replication

If the EB301971 message is output to the log, volumes and replication pairs might not have been deleted. Use the Web UI of VASA Provider to access Resolve and Troubleshoot, and then perform the appropriate action for the message.

Failovers and snapshots

If you perform a Failover for a virtual machine that has a snapshot, you will no longer be able to use the snapshot after a Failback is performed on the vCenter Server. However, the snapshot data will remain on the storage system, so delete it as needed. If you create snapshots after a Failback is performed on the target virtual machine, before performing the Failback, delete all created snapshots visible on the vCenter Server and then delete the snapshot data in the storage system as necessary. For details on how to delete a snapshot, see the VMware documentation.

To delete unused snapshot data, perform the following procedure.

1. Check the LDEV IDs of the Data vVols and Memory vVols for the target virtual machine.
 - a. Click Manage Storage Containers on the Web UI of VASA Provider at the local site.
 - b. Click the vVols tab of the storage container used for the target replication group.
 - c. Find the target virtual machine name in the VM Name column and check the LDEV IDs in the Volume column.

- i. Check the LDEV IDs of volumes for which Data appears in the vVol Type column.
 - ii. Check the LDEV IDs of volumes for which Memory appears in the vVol Type column.
2. Delete the snapshots.
 - a. Click Local Replication for Replication in Storage Navigator of the storage system at the local site.
 - b. Click the TI Root Volumes tab and, in the list of LDEVs, find the LDEV ID that you checked in step 1-c-i.
 - c. Click the LDEV ID. TI Pairs appears. Select all pairs that have values for Snapshot SLU ID.
 - d. From More Actions, click Delete Pairs to delete the target snapshot data.
3. (Optional) Delete the Memory vVols.
 - a. Click Logical Devices in Storage Navigator of the storage system at the local site.
 - b. Select all LDEVs corresponding to the LDEV IDs in step 1-c-ii, and then click More Actions.
 - c. Click Delete LDEVs to delete the target LDEVs.
4. Refresh the configuration information of the storage system.
 - a. Click Manage Storage Containers on the Web UI of VASA Provider at the local site.
 - b. Select the target storage system and then click Refresh Storage Systems.

Planned Failover and Failback

- For virtual machines that have been restored, no VM storage policy is set. To set a VM storage policy again, use the `Set-SpbmEntityConfiguration` command of PowerCLI.

For details on the command, go to the following URL.

<https://code.vmware.com/docs/6978/cmdlet-reference/doc/Set-SpbmEntityConfiguration.html?h=Set-SpbmEntityConfiguration>

- After you perform a Planned Failover, if the VM File path does not appear and is not recognized on the datastore, restart the ESXi host. Then, perform a Planned Failover again to obtain the VM File path.

Forced Failover

After you perform a Forced Failover, if the VM File path does not appear and is not recognized on the datastore, restart the ESXi host. Then, perform a Forced Failover again to obtain the VM File path.

Restrictions

Note that the following functions and operations are restricted. Do not use these functions or perform the operations, because the results are currently not guaranteed.

General restrictions

- A single replication group cannot include more than 1024 vVols.
- You cannot use the `-RunAsync` option of the PowerCLI command for operations related to vVols Replication.
- You cannot change the data flow settings if there is a virtual machine for which vVols Replication is enabled.

To change the data flow settings, disable vVols Replication for all virtual machines. If you configured or changed settings in Protector, click Refresh Protector Information. After changing the data flow settings, reconfigure the replication groups on all virtual machines.

- You cannot perform operations related to vVols Replication for multiple replication groups at the same time.

To perform operations related to vVols Replication for multiple replication groups, perform the operation individually for each replication group.

- You cannot perform operations related to vVols Replication for one or multiple replication groups at the same time.

To perform multiple operations related to vVols Replication, perform them one by one.

- You cannot perform Failover-related operations for a virtual machine that is Noncompliant.
- You cannot use PowerCLI commands to specify variables through pipelines.
- 3DC configurations are not supported.
- Global-active device is not supported.

- If you performed the following procedure after using Storage Navigator or Hitachi Ops Center Protector to manually delete unnecessary vVols, attempts to create a memory snapshot might fail. In such cases, clone a virtual machine for which vVols Replication is enabled. This will allow you to create snapshots of the cloned virtual machine.

The aforementioned procedure is as follows.

1. Create a virtual machine for which vVols Replication is enabled.
2. Perform a Forced Failover of the Replication Group that includes the virtual machine created in step 1.
3. Enable vVols Replication for the relevant virtual machine.
4. Power on the relevant virtual machine.
5. Create a memory snapshot of the relevant virtual machine.



Note: The operations related to vVols Replication include Prepare Replication Group, Planned Failover, Reverse Replication, Forced Failover, Test Failover Start, Test Failover Stop, and Sync Replication Group.

Creation of a virtual machine and enabling of vVols Replication

- You cannot set up a virtual machine hard disk in different replication groups.
- You cannot create a virtual machine and perform operations related to vVols Replication at the same time. Also, you cannot enable vVols Replication and perform operations related to vVols Replication at the same time. Perform these operations individually, one at a time.



Note: The operations related to vVols Replication include Prepare Replication Group, Planned Failover, Reverse Replication, Forced Failover, Test Failover Start, Test Failover Stop, and Sync Replication Group.

- You cannot apply enabling vVols Replication and tier changes to the VM storage policy of an existing virtual machine at the same time. Perform these operations individually, one at a time.
- For either of the following virtual machines, you cannot directly set another VM storage policy in which vVols Replication is enabled.
 - A virtual machine for which a VM storage policy in which vVols Replication is enabled in vCenter Server is set
 - A virtual machine for which a VM storage policy in which vVols Replication is enabled in vCenter Server is not set, but a VM storage policy in which vVols Replication is enabled in VASA Provider is set

To check the setting on VASA Provider, select the storage container in the Web UI, and then use the vVols tab to check the setting of VM Policy Name for the target vVols.

In this situation, temporarily set a VM storage policy in which vVols Replication is disabled, and then set a VM storage policy in which vVols Replication is enabled.

- After a VM storage policy in which vVols Replication is enabled is set for a virtual machine, it might take several hours for the value of VM Storage Policy Compliance to change from Noncompliant to Compliant.
- You cannot enable vVols Replication for a virtual machine created with Linked Clone.
- The following restrictions apply for using both adaptive data reduction and vVols Replication:
 - When creating or cloning a virtual machine, the adaptive data reduction and vVols Replication VM storage policies cannot both be enabled.
 - If a virtual machine has the adaptive data reduction VM storage policy enabled, do not attempt to change its VM storage policy to vVols Replication.

To perform this operation, you must first disable the virtual machine's adaptive data reduction VM storage policy then apply the vVols Replication VM storage policy.
 - If a virtual machine has the vVols Replication VM storage policy enabled, do not attempt to change its VM storage policy to adaptive data reduction.

To perform this operation, you must first disable the virtual machine's vVols Replication VM storage policy then apply the adaptive data reduction VM storage policy.

Deletion of a virtual machine and disabling of vVols Replication

You cannot delete a virtual machine and perform operations related to vVols Replication at the same time. Also, you cannot disable vVols Replication and perform operations related to vVols Replication at the same time. Perform these operations individually, one at a time.



Note: The operations related to vVols Replication include Prepare Replication Group, Planned Failover, Reverse Replication, Forced Failover, Test Failover Start, Test Failover Stop, and Sync Replication Group.

Snapshot or Fast-clone

- You cannot enable vVols Replication for virtual machine snapshots.
- You cannot enable vVols Replication for a Fast-clone vVol. A Fast-clone vVol is a vVol that is created with Linked Clone or when a redo log is created.
- Reverting from a snapshot from which a Fast-clone vVol is created cannot succeed. To revert from such a snapshot, delete the Fast-clone vVol associated with the snapshot and then revert.

Failover-related

- Planned Failover, Forced Failover, and Test Failover Start might fail due to a timeout error of the `Datastore.updateVVolVirtualMachineFiles.label` task on the vCenter Server. If this problem occurs for Test Failover Start, perform Test Failover Stop before you retry Test Failover Start. If problem occurs for Planned Failover or Forced Failover, wait a while and then retry the operation.
- After a Planned Failover, Forced Failover, or Test Failover, it might take some time before the VM files in the datastore appear. If no virtual machines appear, wait a while and then check the VM files again.
- When a Planned Failover or Test Failover is performed, some virtual machines might not appear in the datastore.
- If you perform a Planned Failover or Test Failover in an environment of vSphere 7.0 Update 3 or later, unnecessary Swap vVols might remain due to the vSphere specifications. If you want to delete such unnecessary Swap vVols, contact customer support. These Swap vVols do not affect vVol environments.

Test Failover

After a Test Failover is performed, you cannot perform the following operations for the virtual machine that was created at the remote site:

- Deleting the virtual machine
- Creating snapshots
- Storage vMotion
- Cloning the virtual machine
- Editing the virtual machine to add or delete hard disks
- For the virtual machine, set a VM storage policy for which vVols Replication or adaptive data reduction is enabled.

Planned Failover, Forced Failover, and Failback

- It is recommended that you do not perform a planned failover or a Forced Failover for a virtual machine with a snapshot.
- After a Planned Failover or a Forced Failover is performed, you cannot perform the following operations on a virtual machine that was restored at the remote site:
 - Deleting the virtual machine
 - Creating snapshots
 - Storage vMotion
 - Cloning the virtual machine
 - Editing the virtual machine to add or delete hard disks
 - For the virtual machine, set a VM storage policy for which vVols Replication or adaptive data reduction is enabled.
- After a Planned Failover or a Forced Failover is performed, you cannot perform a Forced Failover from a remote site to the local site.
- After a Planned Failover or a Forced Failover is performed and hard disks are added at a remote site, vVols Replication will not be enabled.

For this reason, you will not be able to access hard disks that were added after a Failback was performed, from the local site. Furthermore, you might not be able to access those hard disks from the remote site.

- After a Planned Failover or a Forced Failover is performed, if you add a virtual machine for which vVols Replication is enabled at the Remote Site, vVols Replication will not be enabled.

For this reason, you will not be able to access virtual machines that were added after a Failback was performed, from the local site.

Expansion of virtual disk capacity

- You cannot perform any of the following operations at the same time as expanding the capacity of a virtual disk:
 - Enabling or disabling vVols Replication
 - Operations related to vVols Replication

Perform these operations individually, one at a time.



Note: The operations related to vVols Replication include Prepare Replication Group, Planned Failover, Reverse Replication, Forced Failover, Test Failover Start, Test Failover Stop, and Sync Replication Group.

- When performing a Planned Failover, Forced Failover, or Test Failover Start, you must specify a PiT replica obtained after the capacity was expanded.

Chapter 3: Upgrading the vVols Replication environment

If a vVols Replication environment is configured in VASA Provider, upgrade the following environments.

1. When using a Thin Image pair with the cascade attribute enabled, perform the following checks and operations.
 - Verify that the storage system at the local site and the storage system at the remote site support Thin Image pairs with the cascade attribute enabled. For details on supported storage systems, see the *Hitachi Storage (VASA) Provider for VMware vCenter Deployment Guide*.
 - If Thin Image pairs with the cascade attribute disabled are created on the storage system at the local site and the storage system at the remote site, perform the following operations:
 - Delete all snapshots of the corresponding virtual machines. For details on how to check and delete snapshots, see the documentation provided by VMware.
 - Configure the Cascade mode settings and then delete all PiT replicas of the corresponding virtual machines. For details, see [Preparing to use Thin Image pairs for which the cascade attribute is enabled \(on page 22\)](#).
2. Upgrade Protector.

Upgrade the Master node, the Client node at the local site, and the Client node at the remote site. For details on how to upgrade these nodes, see the documentation for Protector.
3. Upgrade VASA Provider.

Upgrade the VASA Providers at the local site and at the remote site. For details, see the *Hitachi Storage (VASA) Provider for VMware vCenter Deployment Guide*.
4. After performing an upgrade, if you want to create a new vVols Replication environment, perform the procedure described in [Settings to be configured in advance \(on page 24\)](#).

Preparing to use Thin Image pairs for which the cascade attribute is enabled

If a Thin Image pair with the cascade attribute disabled is created on the storage system, delete all PiT replicas of the corresponding virtual machine.

To use Thin Image pairs for which the cascade attribute is enabled, configure the Cascade mode settings.

Procedure

1. Change the **Cascade mode** settings of the existing Hitachi Block Host node. Select the target data flow, and then click **Edit**. Next, refer to step 7 in [Creating a data flow \(on page 34\)](#), and select the **Cascade mode** check box in **Configure Provisioning Options**.
2. Activate the target data flow. For details, see steps 10 to 12 in [Creating a data flow \(on page 34\)](#).
3. Check step 7 in [Continuing operations at the remote site \(on page 61\)](#), and then delete all snapshots (PiT replicas) in the target data flow at the local site. Step 7 is described as optional, but if you want to create a Thin Image pair for which the cascade attribute is enabled, you must perform step 7 regardless of the conditions described. The snapshots at the remote site are already Thin Image pairs for which the cascade attribute is enabled, so you do not need to delete them.
4. On the Manage Storage System screen of the Web UI of VASA Provider, run **Refresh Storage System** for the target storage system. Run this on VASA Provider at both the local site and the remote site.

Chapter 4: Settings to be configured in advance

This procedure is required for both Universal Replicator and TrueCopy.

Configuring a vVols environment at the local site

Configure an environment in which vVols operate at the local site. For the configuration procedure, see the *Hitachi Storage (VASA) Provider for VMware vCenter Deployment Guide*.



Note: If the storage container includes multiple pools for a snapshot, you might not be able to create a PiT replica.

The storage container supports only the following pool configurations:

- One HDP pool
- One Dynamic Tiering pool and one Thin Image pool

If a virtual machine exists in multiple HDP pools, temporarily migrate the virtual machine to a different datastore. Then, put the pools in the storage container into one of the above configurations, and then migrate the virtual machine back to the original datastore.

If a snapshot exists in multiple pools, delete the existing snapshot, and then put the pools in the storage container into one of the above configurations. Then, re-create the snapshot.

Configuring a vVols environment at the remote site

Configure an environment in which vVols operate at the remote site. For the configuration procedure, see the *Hitachi Storage (VASA) Provider for VMware vCenter Deployment Guide*.



Note: If the storage container includes multiple pools for a snapshot, you might not be able to create a PiT replica.

The storage container supports only the following pool configurations:

- One HDP pool
- One Dynamic Tiering pool and one Thin Image pool

If a virtual machine exists in multiple HDP pools, temporarily migrate the virtual machine to a different datastore. Then, put the pools in the storage container into one of the above configurations, and then migrate the virtual machine back to the original datastore.

If a snapshot exists in multiple pools, delete the existing snapshot, and then put the pools in the storage container into one of the above configurations. Then, re-create the snapshot.

Storage system settings to be configured in advance

Configure the required storage system settings in advance. Change the settings based on your environment. For the detailed configuration procedure, see the documentation for the storage system you are using.

Configuring a remote path

Configure a remote path between the storage system at the local site and the storage system at the remote site.

Procedure

1. Make sure that the following conditions are met:
 - A bidirectional connection is established between the local site storage system and the remote site storage system.
 - Remote paths are established.
2. On the storage system at the local site, configure a Fibre Channel or an iSCSI port.
3. On the storage system at the remote site, configure a Fibre Channel or an iSCSI port.

Adding a remote connection at the local site

Add to the storage system at the local site, a remote connection to a storage system at the remote site.

Procedure

1. Log in to Storage Navigator for the storage system at the local site.
2. In the **Storage Systems** tree, select **Replication > Remote Connections**.
3. Select the **Connections(To)** tab.

4. Select **Add Remote Connection**, and then add the storage system at the remote site.
5. On the **Connections(To)** tab, verify that the storage system has been added to the **Remote Storage System** column.

Adding a remote connection at the remote site

Add to the storage system at the remote site, a remote connection to a storage system at the local site.

Procedure

1. Log in to Storage Navigator for the storage system at the remote site.
2. In the **Storage Systems** tree, select **Replication > Remote Connections**.
3. Select the **Connections(To)** tab.
4. Select **Add Remote Connection**, and then add the storage system at the local site.
5. On the **Connections(To)** tab, verify that the storage system has been added to the **Remote Storage System** column.

Creating a dummy LDEV

Create an LDEV (dummy LDEV) at the local site. An LDEV is needed to use vVols Replication.



Note:

If you have not created a dummy LDEV, a failure occurs when you attempt to delete all vVols from a replication group.

Procedure

1. Log in to Storage Navigator.
2. Select **Pools**.
3. Click **Create LDEVs**.
4. On the Create LDEVs screen, set the following items.
 - **Provisioning Type:** Select **Dynamic Provisioning**.
 - **Pool Selection:** Select a pool (of your choice) that is used by the storage container at the local site.
 - **LDEV Capacity:** Enter 50 MB.
 - **Number of LDEVs:** Enter 1.
 - **LDEV Name:** You do not need to set this item.

Click **Options**, and then set the following items.

- **Initial LDEV ID:** Select an unused LDEV ID of the resource group that is used by the storage container at the local site.
 - Other items: Use the default values.
5. Click **Add**.

6. Click **Finish**.

Creating a data flow host group

Create a host group (data flow host group) at the local site. Data flow host groups are needed to use vVols Replication.

Procedure

1. Log in to Storage Navigator.
2. Select **Ports/Host Groups/iSCSI Targets**.
3. Select the **Host Groups / iSCSI Targets** tab.
4. Click **Create Host Groups**.
5. On the Create Host Groups screen, perform the following steps, and then click **Next**.
 - a. Set the following items.
 - **Host Group Name:** Enter a value of your choice.
 - **Resource Group Name (ID):** Select **meta_resource (0)**.
 - **Host Mode:** Select **00 [Standard]**.
 - **Host Mode Options:** You do not need to set this item.
 - **Hosts:** You do not need to set this item.
 - **Ports:** Specify a port of your choice.
 - b. Click **Add**.
6. Click **Next**.
7. For **Select LDEVs**, perform the following steps, and then click **Next**.
 - a. For **LDEVs**, select a dummy LDEV.
 - b. Click **Add**.
8. For **Select Host Groups / iSCSI Targets**, click **Next**.
9. For **View/Change LUN Paths**, click **Finish**.
10. For **Confirm**, click **Apply**.



Note:

You do not need to specify a port that is able to communicate. The port in a data flow host group is not used to communicate with ESXi hosts, but rather to manage the LDEVs used by vVols Replication.

Protector settings to be configured in advance

For the configuration procedure, see the documentation for Protector.

Introducing a Master node

Introduce a Master node. The Master node is software that manages the Protector environment and provides the Web UI.



Caution: A Master node stores the data that is needed for vVols Replication. If the Master node is lost or deleted, you will no longer be able to restore the vVols Replication environment. For this reason, configure the Master node in a location that will not be affected by a failure at the local site or the remote site. For the configuration procedure, see the documentation for Protector.

Introducing a Client node at the local site

Introduce a Client node to manage the storage system at the local site.

Introducing a Client node at the remote site

Introduce a Client node to manage the storage system at the remote site.

Creating a Hitachi Block Device node at the local site

Create a Hitachi Block Device node to manage storage systems at the local site.

Procedure

1. Log in to the Master node, and navigate to the **Dashboard**.
2. Select **Nodes** and then click **+**.
The Create Node screen appears.
3. For **Select Node type**, select **Storage** and **Hitachi Block Device**, and then click **Next**.
4. For **Specify Node name**, set the following items, and then click **Next**.
 - **Node Name:** Enter a string of your choice.
 - **I confirm that I have read and understood this requirement:** Select this check box.
5. For **Allocate node to Access Control Resource Group**, click **Next**.
6. For **Select proxy node**, select the Client node at the local site for **Proxy Node**, and then click **Next**.
7. For **Select Metadata directory**, select your desired directory for **Common Metadata Directory**, and then click **Next**.
8. For **Specify Device**, set the following items, and then click **Next**.
 - a. For **Specify Device**, select **Select from detected storage devices** or **Specify by IP or Hostname with a port**.

- b. If you select **Select from detected storage devices**, select the serial number of the storage system at the local site. If you select **Specify by IP or Hostname with a port**, enter the IP address and port number of the storage system at the local site.

For VSP 5000 series, enter the IP address and port number of the SVP.

For VSP E590, E790, E990, E1090, E590H, E790H, E1090H, VSP F350, F370, F700, F900, and VSP G350, G370, G700, G900, enter the IP address and port number of the controller of the storage system.

9. For **Specify credentials for device**, set the following items, and then click **Next**.

- **Username:** Enter the username for the storage system at the local site.
- **Password:** Enter the password for the storage system at the local site.

10. For **Specify configuration for Global Replication Reports**, click **Next**.

11. For **Specify LDEV Provisioning Range**, specify either of the following settings, and then click **Next**.

If you might use a Hitachi Block Device Node at the local site as a Hitachi Block Device Node at a remote site, select **User defined**.

- Select **All**.
- Select **User defined**. For **Start** and **End**, enter a range of available LDEV IDs that belong to meta_resource (for example, 0x10FE).



Note: Protector obtains an LDEV ID from the range specified for **Specify LDEV Provisioning Range** when creating a replica (an S-VOL of a replication pair). If there are LDEV IDs that are managed by another user's resource group, the resource group of the relevant LDEV ID might be changed.

12. For **Configure Command Device specification and priority**, perform the following steps, and then click **Next**.

- a. For **Configure Command Device specification and priority**, select **+**.
- b. If necessary, for **Configure Command Device**, set In-band (command device) or Out-of-band (IP address), and then click **Apply**.



Note: By default, a usable In-band (command device) is set.

13. For **Specify LDEV Ranges for each VSM**, click **Next**.



Note: Do not set **Configure Virtual LDEV Range**.

14. For **Specify ports used for provisioning**, perform the following steps, and then click **Next**.

- a. For **Specify ports used for provisioning**, select **+**.
- b. For **Specify Port**, enter the port number of the storage system at the local site, and then click **Apply**.

**Note:**

- This port number is used when Protector automatically creates host groups.
- This port is used only to manage replication pairs. For this reason, you do not need to connect it to the ESXi host.

15. On the Summary screen, confirm the information, and then click **Finish**.

Creating a Hitachi Block Device node at the remote site

Create a Hitachi Block Device node to manage storage systems at the remote site.

Procedure

1. Log in to the Master node, and navigate to the **Dashboard**.
2. Select **Nodes** and then click **+**.
The Create Node screen appears.
3. For **Select Node type**, select **Storage** and **Hitachi Block Device**, and then click **Next**.
4. For **Specify Node name**, set the following items, and then click **Next**.
 - **Node Name:** Enter a string of your choice.
 - **I confirm that I have read and understood this requirement:** Select this check box.
5. For **Allocate node to Access Control Resource Group**, click **Next**.
6. For **Select proxy node**, select the Client node at the remote site for **Proxy Node**, and then click **Next**.
7. For **Select Metadata directory**, select your desired directory for **Common Metadata Directory**, and then click **Next**.
8. For **Specify Device**, set the following items, and then click **Next**.
 - a. For **Specify Device**, select **Select from detected storage devices** or **Specify by IP or Hostname with a port**.
 - b. If you select **Select from detected storage devices**, select the serial number of the storage system at the remote site. If you select **Specify by IP or Hostname with a port**, enter the IP address and port number of the storage system at the remote site.

For VSP 5000 series, enter the IP address and port number of the SVP.

For VSP E590, E790, E990, E1090, E590H, E790H, E1090H, VSP F350, F370, F700, F900, and VSP G350, G370, G700, G900, enter the IP address and port number of the controller of the storage system.
9. For **Specify credentials for device**, set the following items, and then click **Next**.
 - **Username:** Enter the username for the storage system at the remote site.
 - **Password:** Enter the password for the storage system at the remote site.
10. For **Specify configuration for Global Replication Reports**, click **Next**.

11. For **Specify LDEV Provisioning Range**, specify the following items, and then click **Next**.
 - a. Select **User defined**.
 - b. For **Start** and **End**, enter a range of available LDEV IDs that belong to meta_resource (for example, 0x10FE).



Note: Protector obtains an LDEV ID from the range specified for **Specify LDEV Provisioning Range** when creating a replica (an S-VOL of a replication pair). If there are LDEV IDs that are managed by another user's resource group, the resource group of the relevant LDEV ID might be changed.

12. For **Configure Command Device specification and priority**, perform the following steps, and then click **Next**.
 - a. For **Configure Command Device specification and priority**, select **+**.
 - b. If necessary, for **Configure Command Device**, set In-band (command device) or Out-of-band (IP address), and then click **Apply**.



Note: By default, a usable In-band (command device) is set.

13. For **Specify LDEV Ranges for each VSM**, click **Next**.



Note: Do not set **Configure Virtual LDEV Range**.

14. For **Specify ports used for provisioning**, perform the following steps, and then click **Next**.
 - a. For **Specify ports used for provisioning**, select **+**.
 - b. For **Specify Port**, enter the port number of the storage system at the remote site, and then click **Apply**.



Note:

- This port number is used when Protector automatically creates host groups.
- This port is used only to manage replication pairs. For this reason, you do not need to connect it to the ESXi host.

15. On the Summary screen, confirm the information, and then click **Finish**.

Creating a Hitachi Block Host node

Create a Hitachi Block Host node to manage storage systems at the local site. A Hitachi Block Host node is required for each replication group.

Procedure

1. Log in to the Master node, and navigate to the **Dashboard**.
2. Select **Nodes** and then click **+**.
The Create Node screen appears.
3. For **Select Node type**, select **Host** and **Hitachi Block Host**, and then click **Next**.

4. For **Specify Node name**, set the following item, and then click **Next**.
 - **Node Name:** Enter a name in the format `VASA_hbh_<number>` (for example, `VASA_hbh_400106`). For `<number>`, specify a number in the range of 1 to 9999999999. Do not enter spaces before or after the input value.
5. For **Allocate node to Access Control Resource Group**, click **Next**.
6. For **Select Hitachi Block Device**, select **Hitachi Block Device** at the local site, and then click **Next**.
7. For **Specify Logical Devices**, enter the host group ID (for example, `CL1-A-10`) of a data flow host group for **Included Logical Devices**. After you enter the ID, click **Next**.
8. On the Summary screen, confirm the information, and then click **Finish**.

Creating a policy

Create a policy for managing replication.

Procedure

1. Log in to the Master node, and navigate to the **Dashboard**.
2. Select **Policies** and then click **+**.
The Create Policy screen appears.
3. For **Specify name and description**, set the following item, and then click **Next**.
 - **Name:** Enter a name in the format `VASA_policy_<number>` (for example, `VASA_policy_400106`). For `<number>`, specify a number in the range from 1 to 9999999999. Do not enter spaces before or after the input value.
4. For **Allocate Policy to Access Control Resource Group**, click **Next**.
5. For **Add one or more Classifications**, perform the following steps.
 - a. Click **+**.
 - b. For **Select Classification**, select **Physical** and **Hitachi Block**, and then click **Next**.
 - c. For **Specify Hitachi Block Storage classification attributes**, select **Use Hitachi Block Host selections**, and then click **Apply**.
 - d. Click **Next**.
6. For **Add one or more Operations**, perform the following steps, and then click **Finish**.
 - a. Click **+**.
 - b. For **Select Operation**, select **Replicate**, and then click **Next**.

- c. For **Specify Replication operation attributes**, set the following items, and then click **Apply**.

- **Name:** Enter `VASA_replicate`.



Note: If a data flow uses a policy set by `VASA_hur` or `VASA_tc` in a version of VASA Provider earlier than v3.7.0, you can continue to use the data flow even in VASA Provider v3.7.0 or later.

- **Refresh Options:** Select **Refresh when manually triggered**.
- **Source Options (Batch Only):**
 - **Quiesce configured application before backup:** Clear this check box.
 - **Pre Script:** Clear this check box.
 - **Post Script:** Clear this check box.

- d. Click **+**.

- e. For **Select Operation**, select **Snapshot**, and then click **Next**.

- f. For **Specify Snapshot operation attributes**, set the following items, and then click **Apply**.

- **Name:** Enter `VASA_snap`.

- **Mode Options:**

- **Mode:** Select **Hardware**.
- **Hardware Type:** Select **Hitachi Block**.

- **Run Options:** Select **Run on RPO**.

- **Schedule Options:**

- **Recovery Point Objective:** Enter a value of your choice. An entry for this item is required.
- **Retention:** Enter a value of your choice. An entry for this item is required.



Note:

- In Protector, snapshots are periodically created based on the recovery point objective (RPO) settings, and periodically deleted based on the value set for **Retention**. These snapshots are used as point-in-time (PIT) replicas for vVols Replication.
- We recommend setting a minimum of 60 minutes (1 hour) for **Recovery Point Objective**. If the specified time is too short, attempts to create snapshots might fail.

- **Source Options:**

- **Quiesce configured application before backup:** Clear this check box.
- **Pre Script:** Clear this check box.
- **Post Script:** Clear this check box.

Creating a data flow

Create a data flow to manage replication. A data flow is required for each replication group.

Procedure

1. Log in to the Master node, and navigate to the **Dashboard**.
2. Select **Data Flows** and then click **+**.
The Create Data Flow screen appears.
3. For **Specify name and description**, set the following item, and then click **Next**.
 - **Name:** For Universal Replicator, enter a name in the format VASA_df_hur_<number>. For TrueCopy, enter a name in the format VASA_df_tc_<number>. For <number>, specify a number in the range from 1 to 9999999999. For example, specify VASA_df_hur_400106. Do not enter spaces before or after the input value.
4. For **Allocate Data Flow to Access Control Resource Group**, click **Next**.
5. Perform the following steps on the screen that appears.
 - a. Drag the Hitachi Block Host node at the local site to the workspace.
 - b. Drag the Hitachi Block Device node at the remote site to the workspace.
 - c. Select the Hitachi Block Host node, and then move the cursor to the Hitachi Block Device node.
This action draws a mover (an arrow) from the Hitachi Block Host node to the Hitachi Block Device node.
6. Select the mover (arrow), and then set the following items for **Mover Settings**.
 - **Transfer Type:** Select **Continuous**.
 - **Label:** Enter a string of your choice. You can leave this item blank.
7. Select the Hitachi Block Host node, and then perform the following steps.
 - a. For **Policies**, select a policy and a snapshot operation.
 - b. Perform the following steps on the screen for configuring the snapshot operation.
 - i. For **Configure Snapshot Settings**, set the following items.
 - **Storage Node:** Select the Hitachi Block Device node at the local site.
 - **Snapshot Pool:** Select **User Selected**, and then select the pool that is used by the storage container at the local site.
 - ii. Select **Advanced Configuration**.
 - iii. For **Configure Resource Group**, select **User Selected**, and then select the resource group that is used by the storage container at the local site. After you select this item, click **Next**.

- iv. For **Configure Provisioning Options**, set the following items, and then click **Next**.
 - **Consistency group**: Select this check box.
 - **Fully provisioned**: Clear this check box.
 - **Cascade mode**: For VSP 5000 series, select this check box to use Thin Image pairs for which the cascade attribute is enabled. If you performed a new installation of VASA Provider, the cascade attribute is enabled by default, so you must select this check box. Clear this check box when using Thin Image pairs with the cascade attribute disabled.

For VSP E series, VSP F350, F370, F700, F900, and VSP G350, G370, G700, G900, clear this check box.
 - v. For **Specify Naming Options**, set the following items, and then click **Next**.
 - **Secondary Logical Device Name**: Select **Match Origin**.
 - **Snapshot Group Name**: Select **Automatically Generated**.
 - vi. For **Configure Data Retention Utility Options**, click **Next**.
 - vii. On the Summary screen, confirm the information, and then click **Finish**.
8. Select the Hitachi Block Device node, and then perform the following steps.
- a. For **Policies**, select a snapshot operation.
 - b. Perform the following steps on the screen for configuring the snapshot operation.
 - i. Select a pool for **Snapshot Pool** in **Configure Snapshot Settings**. Select the pool that is used by the storage container at the remote site.
 - ii. Select **Advanced Configuration**.
 - iii. For **Configure Resource Group**, select **User Selected**, and then select the resource group that is used by the storage container at the remote site. After you select this item, click **Next**.
 - iv. For **Configure Provisioning Options**, set the following items, and then click **Next**.
 - **Consistency group**: Select this check box.
 - **Fully provisioned**: Clear this check box.
 - **Cascade mode**: Select this check box.
 - v. For **Specify Naming Options**, set the following items, and then click **Next**.
 - **Secondary Logical Device Name**: Select **Match Origin**.
 - **Snapshot Group Name**: Select **Automatically Generated**.
 - vi. For **Configure Data Retention Utility Options**, click **Next**.
 - vii. On the Summary screen, confirm the information, and then click **Finish**.
 - c. For **Policies**, select **Replicate Operation**.
 - d. Perform the following steps on the screen for configuring **Replicate Operation**.
The steps vary depending on whether you use Universal Replicator or TrueCopy.

For Universal Replicator:

- i. For **Select Creation Mode**, select **Configure new replication**, and then click **Next**.
- ii. For **Select Replication Type**, select **Asynchronous Remote Clone (Universal Replicator)**, and then click **Next**.
- iii. For **Configure Secondary Settings**, select **None** for **Capacity Saving Mode**, and then click **Next**.
- iv. For **Configure Replication Settings**, set the following items, and then click **Next**.
 - **Pool**: Select the pool that is used by the storage container at the remote site.
 - **Mirror Unit**: Select **Allocate Automatically**.
- v. For **Select Journal Mode**, select **Create New Journals**.
- vi. For **Create Journals**, set the following items, and then click **Next**.
 - **Source Journal Pool**: Select a pool at the local site.



Note: We recommend selecting a pool other than pools in the storage container used by the local site.

- **Destination Journal Pool**: Select a pool at the remote site.



Note: We recommend selecting a pool other than pools in the storage container used by the remote site.

- **Journal Sizes**: Enter a value of your choice.



Note: The value of **Journal Size** varies depending on the environment you are using. For details on how to set **Journal Size**, see the documentation for the storage system you are using.

- vii. For **Select Remote Path Group**, select either of the following items, and then click **Next**.
 - Select **Automatically Selected**
Perform this operation if you do not need to specify the Remote Path Group for vVols Replication.
 - Select **User Selected**
Perform this operation if you want to specify the Remote Path Group for vVols Replication, and then select Hitachi Block Device node and Remote Path Group at the local site.
- viii. For **Configure Resource Group**, select **User Selected**, and then select the resource group that is used by the storage container at the remote site. After you select this item, click **Next**.

- ix. For **Secondary Volume Host Groups**, set the following items, and then click **Next**.
 - **Use Automatically Provisioned Host Group**: Select this check box.
 - **Enforce LUN ID Matching (fail if primary LUN IDs are not available in the destination host groups)**: Clear this check box.
 - **Optionally specify one or more host groups on the destination storage system.**: You do not need to set this item.
- x. For **Specify Naming Options**, select **Match Origin**, and then click **Next**.
- xi. On the Summary screen, confirm the information, and then click **Finish**.

For TrueCopy:

- i. For **Select Creation Mode**, select **Configure new replication**, and then click **Next**.
- ii. For **Select Replication Type**, select **Synchronous Remote Clone (TrueCopy)**, and then click **Next**.
- iii. For **Configure Secondary Settings**, select **None** for **Capacity Saving Mode**, and then click **Next**.
- iv. For **Configure Replication Settings**, set the following items, and then click **Next**.
 - **Pool**: Select the pool that is used by the storage container at the remote site.
 - **On Destination Write Failure**: Select **Ignore**.
 - **Copy Pace**: Enter a value of your choice.
 - **Use Consistency Group**: Select this check box.
- v. For **Select Remote Path Group**, select either of the following items, and then click **Next**.
 - Select **Automatically Selected**
Perform this operation if you do not need to specify the Remote Path Group for vVols Replication.
 - Select **User Selected**
Perform this operation if you want to specify the Remote Path Group for vVols Replication, and then select Hitachi Block Device node and Remote Path Group at the local site.
- vi. For **Configure Resource Group**, select **User Selected**, and then select the resource group that is used by the storage container at the remote site. After you select this item, click **Next**.

- vii. For **Secondary Volume Host Groups**, set the following items, and then click **Next**.
 - **Use Automatically Provisioned Host Group** check box: Select this check box.
 - **Enforce LUN ID Matching (fail if primary LUN IDs are not available in the destination host groups)** check box: Clear this check box.
 - **Optionally specify one or more host groups on the destination storage system.:** You do not need to set this item.
 - viii. For **Specify Naming Options**, select **Match Origin**, and then click **Next**.
 - ix. On the Summary screen, confirm the information, and then click **Finish**.
9. Click **Finish**.
 10. Select the created data flow, and then run **Activate**.
 11. On the Activate Data Flow(s) screen, click **Activate**.
 12. From **Dashboard**, go to **Jobs** and then **Logs**, and then wait for a while. Make sure that the data flow is successfully created.

VASA Provider settings to be configured in advance

Specifying the information of VASA Provider at the remote site by using VASA Provider at the local site

Procedure

1. Log in to the Web UI of VASA Provider.
2. Select **General Settings**.
3. For **Set Protector Master information** in **Replication Connection Setting**, perform the following steps.
 - a. Set the following items.
 - **Protector IP Address or FQDN:** Enter the IP address or DNS name of the Master node.
 - **Port Number:** Enter the port number of the Master node (default: 443).
 - **User:** Enter <username>@master.
For <username>, enter the user ID of the Master node.
 - **Password:** Enter the password for the Master node.
 - b. Click **Set**.
4. For **Set Remote VASA Provider information**, perform the following steps.

- a. For **Remote VASA Provider IP Address or FQDN**, enter the IP address or DNS name of VASA Provider at the remote site.
- b. For **Port Number**, enter the port number of VASA Provider at the remote site (default: 50001).
- c. Click **Set**.

Specifying the information of VASA Provider at the local site by using VASA Provider at the remote site

Procedure

1. Log in to the Web UI of VASA Provider.
2. Select **General Settings**.
3. For **Set Protector Master information** in **Replication Connection Setting**, perform the following steps.
 - a. Set the following items.
 - **Protector IP Address or FQDN**: Enter the IP address or DNS name of the Master node.
 - **Port Number**: Enter the port number of the Master node (default: 443).
 - **User**: Enter <username>@master.
For <username>, enter the user ID of the Master node.
 - **Password**: Enter the password for the Master node.
 - b. Click **Set**.
4. For **Set Remote VASA Provider information**, perform the following steps.
 - a. For **Remote VASA Provider IP Address or FQDN**, enter the IP address or DNS name of VASA Provider at the local site.
 - b. For **Port Number**, enter the port number of VASA Provider at the local site (default: 50001).
 - c. Click **Set**.



Note: When you configure a remote connection, you must configure settings so that VASA Provider at the local site and VASA Provider at the remote site are always in a 1-to-1 configuration.

Configuring a port for placeholder host groups at the local site

Configure a port for placeholder host groups by using VASA Provider at the local site.

Procedure

1. Log in to the Web UI of VASA Provider.
2. Select **Manage Storage Containers**.
3. Select a storage container at the local site, and then click **Edit Storage Container**.

4. For **Step 2**, select **Used in Replication**, and then select the port number of the storage system at the local site.



Note: VASA Provider automatically creates placeholder host groups, which it uses to manage replication. For this reason, for vVols Replication, you need to set the port number where the host groups are to be created for the storage container. You do not need to connect placeholder host groups to an ESXi host because they are only used to manage replication.

5. Click **Submit**.

Configuring a port for placeholder host groups at the remote site

Configure a port for placeholder host groups by using VASA Provider at the remote site.



Note: Placeholder host groups are used only by storage containers at the local site. For this reason, you usually do not need to configure placeholder host groups at the remote site.

However, if you want to use a storage container at the remote site as the storage container for the local site in the settings of another replication group, you will need to perform the following procedure.

Procedure

1. Log in to the Web UI of VASA Provider.
2. Select **Manage Storage Containers**.
3. Select a storage container at the remote site, and then click **Edit Storage Container**.
4. For **Step 2**, select **Used in Replication**, and then select the port number of the storage system at the remote site.



Note: VASA Provider automatically creates placeholder host groups, which it uses to manage replication. For this reason, for vVols Replication, you need to set the port number where the host groups are to be created for the storage container. You do not need to connect placeholder host groups to an ESXi host because they are only used to manage replication.

5. Click **Submit**.

Creating a replication group



Note: If you create a source replication group by using VASA Provider at the local site, a target replication group is automatically created by VASA Provider at the remote site. For this reason, be sure to create replication groups by using VASA Provider at the local site.

Procedure

1. Log in to the Web UI of VASA Provider.
2. Select **Replication Groups**.



Note: If you created or changed settings by using Protector, click **Refresh Protector Information**.

3. Select **Create Replication Group**.
4. For **Step 1**, if you are using Universal Replicator, select **Asynchronous(HUR)**. If you are using TrueCopy, select **Synchronous(TC)**.
5. For **Step 2**, set the following items.
 - **Storage Container:** Select the storage container of VASA Provider at the local site.
 - **Pool:** Select the pool used by the storage container of VASA Provider at the local site.
6. For **Step 3**, select the data flow.
7. Click **Submit**.

vSphere settings to be configured in advance

Updating replication group information

You need to apply the replication group information created by using VASA Provider to vCenter Server. For the detailed configuration procedure, see the documentation for vSphere.

Procedure

1. Log in to vSphere Client at the local site, and then go to **Hosts and Clusters**.
2. Select the target vCenter Server.
3. Select **Configure** and **Storage Providers**.
4. Select the target VASA Provider, and then click **Rescan**.
5. Log in to vSphere Client at the remote site, and then go to **Hosts and Clusters**.
6. Select the target vCenter Server.
7. Select **Configure** and **Storage Providers**.
8. Select the target VASA Provider, and then click **Rescan**.

Creating a VM storage policy

To enable vVols Replication, create a VM storage policy. For the detailed configuration procedure, see the documentation for vSphere.

Procedure

1. Log in to vSphere Client at the local site, and then go to **Policies and Profiles**.
2. Select **VM Storage Policies**.
3. Select **CREATE**.

The Create VM Storage Policy screen appears.

4. For **Name and description**, enter a name for the VM storage policy for **Name**, and then click **NEXT**.
5. For **Datastore Specific rules in Policy structure**, enable **Enable rules for "com.hitachi.storageprovider.vvol" storage**, and then click **NEXT**.
6. For **com.hitachi.storageprovider.vvol rules**, perform the following steps, and then click **NEXT**.
 - a. Select the **Placement** tab, click **ADD RULE**, and then add a rule of your choice. For details on the rules that can be set, see the *Hitachi Storage (VASA) Provider for VMware vCenter Deployment Guide*.
 - b. Select the **Replication** tab, perform the following steps, and then click **NEXT**.
 - i. Select **Custom**.
 - ii. For **Provider**, select **com.hitachi.storageprovider.vvol.replication**.
 - iii. Click **ADD RULE**, and then add a rule of your choice. Be sure to specify and add **Replication Mode**.

You can set the following rules.

Remote Storage Container

Select the storage container of VASA Provider at the remote site for which you want to create a replica.

Replication Mode

Select **Asynchronous(HUR)** or **Synchronous(TC)**.

Active-Active(GAD) is not currently supported.

Local Snapshot Frequency

Enter the frequency (time) with which a snapshot is to be taken at the local site.

Local Snapshot Retention

Enter the retention period (time) for snapshots taken at the local site.

Remote Snapshot Frequency

Enter the frequency (time) with which a snapshot is to be taken at the remote site.

Remote Snapshot Retention

Enter the retention period (time) for snapshots taken at the remote site.



Note: A VM storage policy is only used as a condition when selecting a datastore. Datastores that match the condition are listed as compatible datastores. The storage characteristics that apply to virtual machines depend on the datastore. The replication functions that apply to virtual machines depend on the replication group.

7. For **Storage compatibility**, verify that a compatible datastore appears, and then click **NEXT**.
8. For **Review and finish**, confirm the settings, and then click **FINISH**.

Chapter 5: Configuring vVols Replication settings for virtual machines

For the detailed configuration procedure, see the documentation for vSphere.

Enabling vVols Replication when you create a virtual machine

Enable vVols Replication when you create a virtual machine.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. Right-click the target data center, and then select **New Virtual Machine**.
3. On the New Virtual Machine screen, select **Create a new virtual machine**, and then click **NEXT**.
4. For **Select a name and folder**, set the following items, and then click **NEXT**.
 - **Virtual machine name:** Enter a name.
 - **Select a location for the virtual machine:** Select a location.
5. For **Select a compute resource**, select a compute resource, and then click **NEXT**.
6. For **Select storage**, perform the following steps, and then click **NEXT**:
 - a. For **VM Storage Policy**, select the VM storage policy that was created in [Creating a VM storage policy \(on page 41\)](#).
 - b. Select a datastore.
 - c. For **Replication Group**, select a replication group.
7. For **Select compatibility**, select the information about your desired ESXi, and then click **NEXT**.
8. For **Select a guest OS**, select the information about your desired guest OS, and then click **NEXT**.
9. For **Customize hardware**, select the hardware information of your desired virtual machine, and then click **NEXT**.
10. For **Ready to complete**, check the settings, and then click **FINISH**.
11. Make sure that the **Create virtual machine** task ends successfully.



Note: After you create a virtual machine, a replica will be asynchronously created. To verify that a replica has been created, perform the following operations:

- a. Select the virtual machine, and then make sure that **Compliant** is displayed for **VM Storage Policies** of **Summary**.

If **Not Compliant** is displayed, verify the contents of procedure b.

- b. On the Manage Storage Containers screen of the Web UI, select the storage container, and then make sure that **Completed** is displayed for **Replication** on the **vVols** tab.

If **Failed** is displayed, check the troubleshooting information.

Enabling vVols Replication for an existing virtual machine

Set a VM storage policy for an existing virtual machine to enable vVols Replication.

The virtual machine must be stored in a datastore containing replication groups.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. Right-click the virtual machine, and then select **VM Policies > Edit VM Storage Policies**.

The Edit VM Storage Policies screen appears.

3. For **Edit VM Storage Policies**, select the VM storage policy that was created in [Creating a VM storage policy \(on page 41\)](#).



Note: Disable the **Configure per disk** option because it is not supported.

If you enable the **Configure per disk** option, you will be able to enable vVols Replication for each disk, but you might not be able to start the virtual machine normally after a Failover.

4. For **Replication groups**, click **CONFIGURE**.
5. On the Configure VM Replication Groups screen, select **Replication group**, and then click **OK**.



Note: Disable the **Configure per disk** option because it is not supported.

If you enable the **Configure per disk** option, you will be able to enable vVols Replication for each disk, but you might not be able to start the virtual machine normally after a Failover.

6. Click **OK**.
7. Make sure that the **Reconfigure Virtual Machine** task ends successfully.



Note: After you enable vVols Replication, a replica will be asynchronously created. To verify that a replica has been created, perform the following operations:

- a. Select the virtual machine, and then make sure that **Compliant** is displayed for **VM Storage Policies** of **Summary**.

If **Not Compliant** is displayed, verify the contents of procedure b.

- b. On the Manage Storage Containers screen of the Web UI, select the storage container, and then make sure that **Completed** is displayed for **Replication** on the **vVols** tab.

If **Failed** is displayed, check the troubleshooting information.

Enabling vVols Replication when you clone a virtual machine

Enable vVols Replication when you clone a virtual machine.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. Right-click the virtual machine, and then select **Clone > Clone to Virtual Machine**. The Clone Existing Virtual Machine screen appears.
3. For **Select a name and folder**, set the following items, and then click **NEXT**.
 - **Virtual machine name:** Enter a name.
 - **Select a location for the virtual machine:** Select a location.
4. For **Select a compute resource**, select a compute resource, and then click **NEXT**.
5. For **Select storage**, perform the following steps, and then click **NEXT**.



Note: Disable the **Configure per disk** option because it is not supported.

If you enable the **Configure per disk** option, you will be able to enable vVols Replication for each disk, but you might not be able to start the virtual machine normally after a Failover.

- a. For **Select virtual disk format**, select **Thin Provision**.
 - b. For **VM storage policy**, select the VM storage policy that was created in [Creating a VM storage policy \(on page 41\)](#).
 - c. Select a datastore.
 - d. For **Replication Group**, select a replication group.
6. For **Select clone options**, set your desired clone option, and then click **NEXT**.
 7. For **Ready to complete**, check the settings, and then click **FINISH**.
 8. Make sure that the **Clone virtual machine** task ends successfully.



Note: After you clone a virtual machine, a replica will be asynchronously created. To verify that a replica has been created, perform the following operations:

- a. Select the virtual machine, and then make sure that **Compliant** is displayed for **VM Storage Policies** of **Summary**.
If **Not Compliant** is displayed, verify the contents of procedure b.
- b. On the Manage Storage Containers screen of the Web UI, select the storage container, and then make sure that **Completed** is displayed for **Replication** on the **vVols** tab.
If **Failed** is displayed, check the troubleshooting information.

Enabling vVols Replication when you migrate a virtual machine

Enable vVols Replication when you migrate a virtual machine.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. Right-click the virtual machine, and then select **Migrate**.
The Migrate screen appears.
3. For **Select a migration type**, select **Change Storage only** or **Change both compute resource and storage**, and then click **NEXT**.
4. If you select **Change both compute resource and storage**, select a compute resource for **Select a compute resource**, and then click **NEXT**.
5. For **Select storage**, perform the following steps, and then click **NEXT**.



Note: Disable the **Configure per disk** option because it is not supported.

If you enable the **Configure per disk** option, you will be able to enable vVols Replication for each disk, but you might not be able to start the virtual machine normally after a Failover.

- a. For **Select virtual disk format**, select **Thin Provision**.
 - b. For **VM storage policy**, select the VM storage policy that was created in [Creating a VM storage policy \(on page 41\)](#).
 - c. Select a datastore.
 - d. For **Replication Group**, select a replication group.
6. If you select **Change both compute resource and storage**, select a network for **Select networks**, and then click **NEXT**.
 7. For **Ready to complete**, check the settings, and then click **FINISH**.
 8. Make sure that the **Relocate virtual machine** task ends successfully.
 9. Perform a compliance check for the virtual machine.
 - a. Log in to vSphere Client, and then go to **VMs and Templates**.

- b. Right-click the virtual machine, and then select **VM Policies > Check VM Storage Policy Compliance**.
- c. Click the virtual machine, and then make sure that the value of **VM Storage Policy Compliance** in **VM Storage Policies** is **Compliant**.



Note: After you migrate a virtual machine, a replica will be asynchronously created. To verify that a replica has been created, perform the following operations:

- a. Select the virtual machine, and then make sure that **Compliant** is displayed for **VM Storage Policies** of **Summary**.

If **Not Compliant** is displayed, verify the contents of procedure b.

- b. On the Manage Storage Containers screen of the Web UI, select the storage container, and then make sure that **Completed** is displayed for **Replication** on the **vVols** tab.

If **Failed** is displayed, check the troubleshooting information.

Disabling vVols Replication for a virtual machine

Set a VM storage policy for a virtual machine to disable vVols Replication.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. Right-click the virtual machine, and then select **VM Policies > Edit VM Storage Policies**.

The Edit VM Storage Policies screen appears.

3. For **VM storage policy**, select a VM storage policy.
In this step, select a VM storage policy for which vVols Replication is disabled.
4. Click **OK**.
5. Make sure that the **Reconfigure Virtual Machine** task ends successfully.

Adding a disk to a virtual machine

Add a disk to a virtual machine for which vVols Replication is enabled.



Note: If vVols Replication is configured for each disk, this operation is not supported because you might not be able to start the virtual machine normally after a Failover.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. Right-click the virtual machine, and then select **Edit Settings**.

The Edit Settings screen appears.

3. Click **ADD NEW DEVICE**, and then select a hard disk.
4. For **New Hard disk ***, set the following items.
 - **Location:** Select **Store with the virtual machine**.
 - **VM storage policy:** Select the same value as that of other disks in the virtual machine.
 - **Replication Group:** Select the same value as that of other disks in the virtual machine.
 - Other items: Set a value of your choice.
5. Click **OK**.
6. Verify that the **Reconfigure Virtual Machine** task ends successfully.



Note: After you add a disk to a virtual machine, a replica will be asynchronously created. To verify that a replica has been created, perform the following operations:

- a. Select the virtual machine, and then make sure that **Compliant** is displayed for **VM Storage Policies** of **Summary**.

If **Not Compliant** is displayed, verify the contents of procedure b.

- b. On the Manage Storage Containers screen of the Web UI, select the storage container, and then make sure that **Completed** is displayed for **Replication** on the **vVols** tab.

If **Failed** is displayed, check the troubleshooting information.

Reverting a virtual machine

To revert a virtual machine for which vVols Replication is enabled, you need to temporarily suspend replication.



Note: If you suspend replication (running of Pause) to revert a virtual machine, the replication of vVols in the same replication group is suspended until the Resume task finishes successfully.

Procedure

1. Log in to the Master node, and then select **Storage** in the top pane.
2. Select Hitachi Block Device for the remote site.
3. Select **Replications and Clones**.
4. Select the results for the replications and clones for which the Hitachi Block Host node associated with the target data flow is displayed.
5. Run **Pause**.
6. Follow the on-screen instructions to confirm.

**Note:**

The following check box appears. Clear the check box.

Make secondary writable when the primary is not available. Only supported for remote replications and should only be used when the primary side is down or has failed.

7. On the Protector Jobs screen, confirm that the operation of the target node ended normally.
8. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
9. Right-click the virtual machine, and then select **Snapshots > Manage Snapshots**.
10. On the displayed screen, select the target snapshot, and then click **REVERT**.
11. On the Revert to selected Snapshot screen, click **REVERT**.
12. Make sure that the **Revert snapshot** task ends successfully.
13. Return to the Protector screen, and then run Resume for the Replications and Clones for which you ran Pause.
14. On the Confirm Resume Replication screen, click **Confirm**.
15. On the Protector Jobs screen, confirm that the operation of the target node ended normally.

Expanding the capacity of a virtual disk

Expand the virtual disk capacity of a virtual machine for which vVols Replication is enabled.



Note: If you expand the capacity of a virtual disk, the replication of vVols in the same replication group is suspended until the Reconfigure Virtual Machine task finishes successfully.

Before you begin

- The storage system model must support the expansion of the capacity of virtual disks. For details, see [System requirement \(on page 14\)](#).
- The method for managing the differential data of the storage system must be the hierarchical difference method.

To use the hierarchical difference method, set system option mode 1198 to ON and 1199 to OFF. For details on how to set the system option mode, see the Hitachi Universal Replicator User Guide and the Hitachi TrueCopy® User Guide. Specify this setting for the storage systems at both the local site and the remote site.



Note: The system option mode setting affects all remote copy pairs in the storage system. For details on the impact of changing this setting, see the documentation for the storage system you are using.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. Right-click the virtual machine, and then select **Edit Settings**.
The Edit Settings screen appears.
3. Resize the hard disk, and then click **OK**.
4. Make sure that the **Reconfigure Virtual Machine** task ends successfully.
5. Right-click the virtual machine, and then select **VM Policies > Check VM Storage Policy Compliance**.
6. Click the virtual machine, and then make sure that the value of **VM Storage Policy Compliance** in **VM Storage Policies** is **Compliant**.
7. Run Sync Replication Group. For the detailed procedure, see [Failover-related operations \(on page 51\)](#).



Caution: When performing a Planned Failover, Forced Failover, or Test Failover Start, you must specify a PiT replica obtained after the capacity was expanded.

Chapter 6: Failover-related operations



Note: The following describes the basic procedures for Failover-related operations. If you perform a procedure that is not described here, the procedure might not end successfully. For this reason, procedures other than those described here are not supported.

Planned Failover and Failback



Note:

- Virtual machines at the remote site are intended to be used for the temporary backup of data, and the operations that can be performed for these virtual machines are restricted. If you want to be able to perform all operations on a virtual machine at the remote site, you must perform a Failback to return the operation of the virtual machine to the local site. Thus, always perform a Failback after you perform a Planned Failover.

If you cannot perform a Failback for reasons such as a failure at the local site, clone the virtual machine and then use the cloned virtual machine.

- If you want to completely migrate the operation of a virtual machine to the remote site, perform a Forced Failover.

Performing a Planned Failover

Use PowerCLI to perform a Planned Failover. For the detailed configuration procedure, see the documentation for vSphere.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. (Optional) If snapshots exist for virtual machines for which a Planned Failover is to be performed, select each of the virtual machines, and then select **Snapshot > Delete All Snapshots**.



Caution: If you performed a Planned Failover without deleting the snapshots, do not revert or delete these snapshots at the remote site. If you revert or delete these snapshots, you might not be able to start the virtual machines that have these snapshots. Furthermore, unnecessary data might remain in the VASA Provider Web UI or on storage systems. For the detailed procedure, see *Failovers and snapshots* in [Notes \(on page 15\)](#).

3. Select the virtual machine, and then select **Power > Power Off**.
4. Select the virtual machine, and then select **Remove from Inventory**.



Note: Always perform the **Remove from Inventory** operation before performing a Planned Failover. If you do not perform this operation, the virtual machine might not be restored successfully.

5. Start PowerCLI.
6. Connect to vCenter Server at the local site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

7. Configure the settings needed to perform operations on multiple instances of vCenter Server.

```
Set-PowerCLIConfiguration -DefaultVIServerMode 'Multiple' -Scope
([VMware.VimAutomation.ViCore.Types.V1.ConfigurationScope]::Session) -Confirm:0
```

8. Connect to vCenter Server at the remote site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

9. From the **Replication Groups** screen of the VASA Provider Web UI, obtain the name of the target replication group that is in the SOURCE status.

```
$sourceRg = Get-SpbmReplicationGroup -Name <name-of-replication-group-in-SOURCE-
status>
```

10. Obtain information about the replication group pairs.

```
$pairRg = Get-SpbmReplicationPair -source $sourceRg
```

11. Obtain information about the replication group that is in the TARGET status at the remote site.

```
$targetRg = $pairRg.target
```

12. (Optional) Run Sync Replication Group.



Note: Run the following command if you want to perform restoration with the latest status. If you specify an existing PiT replica, you do not need to run the command.

```
Sync-SpbmReplicationGroup -ReplicationGroup $targetRg -PointInTimeReplicaName
<replica_name>
```

For <replica_name>, enter the name of your desired PiT replica.

13. (Optional) Obtain information about the PiT replica.



Note: Run the following command if you want to perform restoration by specifying a PiT replica. If you do not want to specify a PiT replica, you do not need to run the command.

```
$pitList = Get-SpbmPointInTimeReplica -ReplicationGroup $targetRg
$pit = $pitList[0]
```

For the `Get-SpbmPointInTimeReplica`, specify one or more of the following:

```
[[[-Name] <String[]>], [-FromDate <DateTime>], [-ToDate
<DateTime>]]
```

For `$pitList[0]`, specify the PiT replica. For 0, specify a value according to the environment.

14. Perform a Prepare Failover for the replication group that is in the SOURCE status at the local site.

```
Start-SpbmReplicationPrepareFailover -ReplicationGroup $sourceRg
```

15. Perform a Planned Failover for the replication group that is in the TARGET status at the remote site.

```
$remoteVMs = Start-SpbmReplicationFailover -ReplicationGroup $targetRg
```

If you specified a PiT replica, add `-PointInTimeReplica $pit`. If you do not specify a PiT replica, the newest PiT replica will be used.



Caution: If the capacity of the virtual disk was expanded, you must specify a PiT replica obtained after the capacity was expanded.

16. Check the list of virtual machines.

```
$remoteVMs
```



Note: If the VM File path does not appear and is not recognized on the datastore, restart the ESXi host. Then, perform step 15 again to obtain the VM File path.

17. Register the virtual machine on an ESXi host at the remote site.

```
New-VM -VMFilePath $remoteVMs -VMHost <ip_address>
```

For `<ip_address>`, enter the IP address of your desired ESXi host.

If the replication group includes more than one virtual machine, `$remoteVMs` will be in an array. To register more than one virtual machine, use a for-each loop to run the command for each applicable VM File path.



Note: If you want to obtain the `$remoteVMs` value again, perform step 15 again.



Caution: If snapshots created at the local site appear in the remote site after a Planned Failover is performed, do not revert or delete these snapshots at the remote site. If you revert or delete these snapshots, you might not be able to start the virtual machines that have these snapshots, whether at the remote site where the Planned Failover was performed or at the local site where the Failback was performed. Furthermore, unnecessary data might remain in the VASA Provider Web UI or on storage systems. For the detailed procedure, see *Failovers and snapshots* in [Notes \(on page 15\)](#).

18. Set a VM Storage Policy for the virtual machine.

Specify a VM Storage Policy with the same settings as those assigned to the virtual machine on the local site side and with vVols Replication enabled.

a. Obtain information about the VM Storage Policy.

```
$policy = Get-SpbmStoragePolicy -Name <polycyname> -Server <vcenter_ip>
```

For <polycyname>, enter the name of the VM Storage Policy.

For <vcenter_ip>, enter the IP address of vCenter Server at the remote site.

b. Obtain information about the virtual machine and its disk.

```
$vm = Get-VM -Name <vmname>
$hd = Get-HardDisk -VM <vmname>
```

For <vmname>, enter the name of the virtual machine.

c. Obtain an object for changing the policy of the virtual machine.

```
$configuration = Get-SpbmEntityConfiguration -VM $vm -HardDisk $hd -Server
<vcenter_ip>
```

For <vcenter_ip>, enter the IP address of vCenter Server.

d. Set a VM Storage Policy for the virtual machine.

```
Set-SpbmEntityConfiguration -Configuration $configuration -StoragePolicy
$policy -ReplicationGroup $targetRg -Server <vcenter_ip>
```

For <vcenter_ip>, enter the IP address of vCenter Server.

19. (Optional) Refresh the Protector information for VASA Provider at the remote site.

If you do not perform this step, the result of the compliance check might indicate non-compliance.

- a. Log in to the Web UI of VASA Provider.
- b. Select **Replication Groups**.
- c. Run **Refresh Protector Information**.

20. Perform a compliance check for the virtual machine at the remote site.

- a. Log in to vSphere Client, and then go to **VMs and Templates**.

- b. Right-click the virtual machine, and then select **VM Storage Policies > Check VM Storage Policy Compliance**.
- c. Click the virtual machine, and then make sure that the value of **VM Storage Policy Compliance** in **VM Storage Policies** is **Compliant**.



Note: You can use the virtual machine at the remote site after you power it on.

Performing a Reprotect and Failback

Use PowerCLI to perform a Failback. For the detailed configuration procedure, see the documentation for vSphere.

Procedure

1. Log in to vSphere Client at the remote site, and then go to **VMs and Templates**.
2. Select the virtual machine, and then select **Power > Power Off**.
3. Select the virtual machine, and then select **Remove from Inventory**.



Note:

- Always perform the **Remove from Inventory** operation before performing a Planned Failover. If you do not perform this operation, the virtual machine might not be restored successfully.
- Before performing a Forced Failover, if you have not already removed the virtual machines of the local site from the inventory, remove them from the inventory. Also, before performing a Failback from a remote site to a local site, you must remove the virtual machines of the local site from the inventory.

4. Start PowerCLI.
5. Connect to vCenter Server at the local site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

6. Configure the settings needed to perform operations on multiple instances of vCenter Server.

```
Set-PowerCLIConfiguration -DefaultVIServerMode 'Multiple' -Scope
([VMware.VimAutomation.ViCore.Types.V1.ConfigurationScope]::Session) -Confirm:0
```

7. Connect to vCenter Server at the remote site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

8. From the **Replication Groups** screen of the VASA Provider Web UI, obtain the name of the target replication group that is in the SOURCE status.

```
$sourceRg = Get-SpbmReplicationGroup -Name <name-of-replication-group-in-SOURCE-status>
```

9. Obtain information about the replication group pairs.

```
$pairRg = Get-SpbmReplicationPair -source $sourceRg
```

10. Obtain information about the replication group that is in the FAILEDOVER status at the remote site.

```
$targetRg = $pairRg.target
```

11. Perform a Reverse Replication for the replication group that is in the FAILEDOVER status at the remote site.

```
Start-SpbmReplicationReverse -ReplicationGroup $targetRg
```

12. From the **Replication Groups** screen of the VASA Provider Web UI, again obtain the name of the target replication group that is in the SOURCE status.

```
$sourceRg = Get-SpbmReplicationGroup -Name <name-of-replication-group-in-SOURCE-status>
```

13. Obtain information about the replication group pairs again.

```
$pairRg = Get-SpbmReplicationPair -source $sourceRg
```

14. Obtain information about the replication group in the TARGET status at the local site again.

```
$targetRg = $pairRg.target
```

15. (Optional) Run Sync Replication Group.



Note: Run the following command if you want to perform restoration with the latest status. If you specify a PiT replica, you do not need to run the command.

```
Sync-SpbmReplicationGroup -ReplicationGroup $targetRg -PointInTimeReplicaName <replica_name>
```

For <replica_name>, enter the name of your desired PiT replica.

16. (Optional) Obtain information about the PiT replica.



Note: Run the following command if you want to perform restoration by specifying a PiT replica. If you do not want to specify a PiT replica, you do not need to run the command.

```
$pitList = Get-SpbmPointInTimeReplica -ReplicationGroup $targetRg
$pit = $pitList[0]
```

For the `Get-SpbmPointInTimeReplica` option, specify one or more of the following:

```
[[[-Name] <String[]>], [-FromDate <DateTime>], [-ToDate <DateTime>]]
```

For `$pitList[0]`, specify the PiT replica. For 0, specify a value according to the environment.

17. Perform a Prepare Failover for the replication group that is in the SOURCE status at the remote site.

```
Start-SpbmReplicationPrepareFailover -ReplicationGroup $sourceRg
```

18. Perform a Planned Failover for the replication group that is in the TARGET status at the local site.

```
$remoteVMs = Start-SpbmReplicationFailover -ReplicationGroup $targetRg
```

If you specified a PiT replica, add `-PointInTimeReplica $pit`. If you do not specify a PiT replica, the newest PiT replica will be used.



Caution: If the capacity of the virtual disk was expanded, you must specify a PiT replica obtained after the capacity was expanded.

19. Check the list of virtual machines.

```
$remoteVMs
```



Note: If the VM File path does not appear and is not recognized on the datastore, restart the ESXi host. Then, perform step 18 again to obtain the VM File path.

20. Register the virtual machine on an ESXi host at the local site.

```
New-VM -VMFilePath $remoteVMs -VMHost <ip_address>
```

For `<ip_address>`, enter the IP address of your desired ESXi host.

If the replication group includes more than one virtual machine, `$remoteVMs` will be in an array. To register more than one virtual machine, use a `for-each` loop to run the command for each applicable VM File path.



Note: If you want to obtain the `$remoteVMs` value again, perform step 18 again.



Caution: If previously created snapshots appear in the local site after a Failback is performed, delete the snapshots.

In addition, do not revert these snapshots. If you revert them, you might not be able to start the virtual machines that have these snapshots.

Furthermore, unnecessary data might remain in the VASA Provider Web UI or on storage systems. For the detailed procedure, see *Failovers and snapshots* in [Notes \(on page 15\)](#).

21. Perform a Reverse Replication for the replication group that is in the FAILEDOVER status at the local site.

```
Start-SpbmReplicationReverse -ReplicationGroup $targetRg
```

22. Set a VM Storage Policy for the virtual machine. For details on this step, see the procedure for setting a VM storage policy in [Performing a Planned Failover \(on page 51\)](#).



Note: For the `Set-SpbmEntityConfiguration` command in step 18-d of [Performing a Planned Failover \(on page 51\)](#), for `-ReplicationGroup`, specify the replication group at the local site before the Planned Failover is run.

23. (Optional) Refresh the Protector information for VASA Provider at the local site.

If you do not perform this step, the result of the compliance check might indicate non-compliance. For details on this step, see the procedure for refreshing the Protector information in [Performing a Planned Failover \(on page 51\)](#).

24. Perform a compliance check for the virtual machine at the local site. For details on this step, see the procedure for performing a compliance check in [Performing a Planned Failover \(on page 51\)](#).



Note: You can use the virtual machine at the local site after you power it on.

Forced Failover




Note: It is assumed that a Forced Failover will be performed when the local site cannot be accessed because of a failure or some other reason.

If you want to temporarily migrate the operation of a virtual machine to the remote site, refer to [Planned Failover and Failback \(on page 51\)](#) and perform the described procedure.

Performing a Forced Failover

Use PowerCLI to perform a Forced Failover. For the detailed configuration procedure, see the documentation for vSphere.

 **Note:** If the virtual machine cannot be operated from vSphere Client, skip the following steps 1 to 4.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. (Optional) If snapshots exist for virtual machines for which a Forced Failover is to be performed, select each of the virtual machines, and then select **Snapshot > Delete All Snapshots**.



Caution: If you performed a Forced Failover without deleting the snapshots, do not revert or delete these snapshots at the remote site. If you revert or delete these snapshots, you might not be able to start the virtual machines that have these snapshots. Furthermore, unnecessary data might remain in the VASA Provider Web UI or on storage systems. For the detailed procedure, see *Failovers and snapshots* in [Notes \(on page 15\)](#).

3. Select the virtual machine, and then select **Power > Power Off**.
4. Select the virtual machine, and then select **Remove from Inventory**.



Note: Always perform the **Remove from Inventory** operation before performing a Forced Failover. If you do not perform this operation, the virtual machine might not be restored successfully.

5. Start PowerCLI.
6. Connect to vCenter Server at the remote site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

7. From the **Replication Groups** screen of the VASA Provider Web UI, obtain the ID of the target replication group that is in the TARGET status.

```
$targetRg = Get-SpbmReplicationGroup -Name <ID-of-replication-group-in-TARGET-
status>
```

8. Perform a Forced Failover for the replication group that is in the TARGET status at the remote site. When you run this command, if a confirmation message appears, enter *y*.

```
$remoteVMs = Start-SpbmReplicationFailover -ReplicationGroup $targetRg -Unplanned
```



Note:

- If the Forced Failover fails, retry the operation. Virtual machines cannot be restored unless the Forced Failover succeeds.
- If you specified a Pit replica, the Forced Failover is performed without the specification being applied.

9. Check the list of virtual machines.

```
$remoteVMs
```



Note: If the VM File path does not appear and is not recognized on the datastore, restart the ESXi host. Then, perform step 8 again to obtain the VM File path.

10. Register the virtual machine on an ESXi host at the remote site.

```
New-VM -VMFilePath $remoteVMs -VMHost <ip_address>
```

For <ip_address>, enter the IP address of your desired ESXi host.

If the replication group includes more than one virtual machine, `$remoteVMs` will be in an array. To register more than one virtual machine, use a `for-each` loop to run the command for each applicable VM File path.



Note: If you want to obtain the `$remoteVMs` value again, perform step 8 again.



Caution: If snapshots created at the local site appear in the remote site after a Forced Failover is performed, do not revert or delete these snapshots at the remote site. If you revert or delete these snapshots, you might not be able to start the virtual machines that have these snapshots, whether at the remote site where the Forced Failover was performed or at the local site where the Failback was performed. Furthermore, unnecessary data might remain in the VASA Provider Web UI or on storage systems. For the detailed procedure, see *Failovers and snapshots* in [Notes \(on page 15\)](#).

11. If the local site is restored, perform the procedure in [Performing a Failback after restoring the local site \(on page 60\)](#). If the local site cannot be restored and you want to continue operations at the remote site, perform the procedure in [Continuing operations at the remote site \(on page 61\)](#).

Performing a Failback after restoring the local site

If the local site can be restored and you want to perform a Failback, perform the following procedure.

Procedure

1. Set a VM Storage Policy for the virtual machine.

Specify a VM Storage Policy with the same settings as those assigned to the virtual machine on the local site side and with vVols Replication enabled.

- a. Obtain information about the VM Storage Policy.

```
$policy = Get-SpbmStoragePolicy -Name <policyname> -Server <vcenter_ip>
```

For <policyname>, enter the name of the VM Storage Policy.

For <vcenter_ip>, enter the IP address of vCenter Server at the remote site.

- b. Obtain information about the virtual machine and its disk.

```
$vm = Get-VM -Name <vmname>
$hd = Get-HardDisk -VM <vmname>
```

For <vmname>, enter the name of the virtual machine.

- c. Obtain an object for changing the policy of the virtual machine.

```
$configuration = Get-SpbmEntityConfiguration -VM $vm -HardDisk $hd -Server
<vcenter_ip>
```

For <vcenter_ip>, enter the IP address of vCenter Server.

- d. Set a VM Storage Policy for the virtual machine.

```
Set-SpbmEntityConfiguration -Configuration $configuration -StoragePolicy
$policy -ReplicationGroup $targetRg -Server <vcenter_ip>
```

For <vcenter_ip>, enter the IP address of vCenter Server.

2. (Optional) Refresh the Protector information for VASA Provider at the remote site.

If you do not perform this step, the result of the compliance check might indicate non-compliance.

- a. Log in to the Web UI of VASA Provider.
- b. Select **Replication Groups**.
- c. Run **Refresh Protector Information**.

3. Perform a compliance check for the virtual machine at the remote site.

- a. Log in to vSphere Client, and then go to **VMs and Templates**.
- b. Right-click the virtual machine, and then select **VM Storage Policies > Check VM Storage Policy Compliance**.
- c. Click the virtual machine, and then make sure that the value of **VM Storage Policy Compliance** in **VM Storage Policies** is **Compliant**.



Note: You can use the virtual machine at the remote site after you power it on.

4. Refer to [Performing a Reprotect and Failback \(on page 55\)](#) and perform the described operation.

Continuing operations at the remote site

If the local site cannot be restored and you want to continue operations at the remote site, perform the following procedure.

Procedure

1. Forcibly delete the replication group at the remote site.



Note: If you perform a Forced Failover, you cannot reuse the replication group. You must delete the replication group.

- a. Log in to the Web UI of VASA Provider at the remote site.
 - b. Select **Replication Groups**.
 - c. Select the target replication group.
 - d. Select **Forced Delete Replication Group**.
 - e. On the Delete Replication Group screen, click **Submit**.
2. (Optional) Forcibly delete the replication group at the local site.

If a replication group remains at the local site, delete the replication group.



Note: If you perform a Forced Failover, you cannot reuse the replication group. You must delete the replication group.

- a. Log in to the Web UI of VASA Provider at the local site.
 - b. Select **Replication Groups**.
 - c. Select the target replication group.
 - d. Select **Forced Delete Replication Group**.
 - e. On the Delete Replication Group screen, click **Submit**.
3. Set a VM storage policy in which vVols Replication is disabled for the virtual machine. For details on this step, see the procedure for setting a VM storage policy in [Performing a Planned Failover \(on page 51\)](#).

However, as the command for setting a VM storage policy for the virtual machine, run the following command.

```
Set-SpbmEntityConfiguration -Configuration $configuration -StoragePolicy $policy
-Server <vcenter_ip>
```

For <vcenter_ip>, enter the IP address of vCenter Server at the remote site.

- a. Log in to the Master node, and navigate to the **Dashboard**.
 - b. Select **Data Flows**.
 - c. Select the target data flow, and then run **Deactivate**.
 - d. On the Deactivate Data Flow(s) screen, click **Deactivate**.
5. Run **Dissociate** for the replication generated by the data flow.



Note: If you perform a Forced Failover, you will not be able to reuse the data flow and replication. You must delete the data flow and replication settings from Protector.

- a. Log in to the Master node, and select **Storage** in the upper pane.
- b. Select the Hitachi Block Device at the remote site.
- c. Select **Replications and Clones**.

- d. Select the results for the replications and clones for which the Hitachi Block Host node associated with the target data flow is displayed.
 - e. Run **Dissociate**.
 - f. On the Dissociate Hitachi Block Replication screen, enter the confirmation word, and then click **Dissociate**.
6. Delete the data flow.
 - a. Log in to the Master node, and navigate to the **Dashboard**.
 - b. Select **Data Flows**.
 - c. Select the target data flow, and then run **Delete**.
 - d. On the Confirm Data Flow Deletion screen, click **Confirm**.
 7. (Optional) Delete the snapshot associated with the data flow.

This step is required to delete host groups. Note that you cannot perform this step if you cannot access the Hitachi Block Device node to which the target snapshot belongs.

- a. Log in to the Master node, and then select **Storage** in the top pane.
 - b. Select the Hitachi Block Device node at the local site.
 - c. Select **Snapshots**.
 - d. Select all snapshots of the Hitachi Block Host node for which the source is used for the target data flow, and then run **Delete**.
 - e. On the Confirm Record Deletion screen, enter the confirmation word, and then click **Delete**.
 - f. Select **Storage** in the top pane.
 - g. Select the Hitachi Block Device node at the remote site.
 - h. Select **Snapshots**.
 - i. Select all snapshots of the Hitachi Block Host node for which the source is used for the target data flow, and then run **Delete**.
 - j. On the Confirm Record Deletion screen, click **Delete**.
8. (Optional) Among the nodes and policies created in [Protector settings to be configured in advance \(on page 27\)](#), if you do not need nodes and policies other than replication and data flow, delete the vVols Replication environment.
For details on how to delete a vVols Replication environment, see [Deleting a data flow and Protector settings \(on page 73\)](#).

If the storage system at the local site can be used, perform the procedure up to and including the step in which you delete the Hitachi Block Host node.

If the storage system at the local site cannot be used, perform the procedure up to and including the step in which you delete the Hitachi Block Device node.
 9. (Optional) If the vVols environment at the local site remains but is no longer needed, delete the vVols Replication environment.
For details on how to delete a vVols Replication environment, see [Deleting a vVols Replication environment \(on page 71\)](#).

The following steps in [Deleting the settings of a storage system \(on page 74\)](#) must be performed at the remote site as well.

- Deleting journals.
- Deleting snapshots.
- Deleting host groups.

The target host groups are as follows:

- The host groups must be included in the port specified by the Hitachi Block Device Node at the remote site.
- The name of the host group must be in the format **HDIDProvisioningHostGroup_RG<RGID>**.

<RGID> is the remote-site resource group ID that was specified when the data flow was created.

- Deleting dummy LDEVs.

10. (Optional) If the configuration of a storage system registered in VASA Provider has been changed, refresh the storage system information.
 - a. Log in to the Web UI of VASA Provider.
 - b. Select **Manage Storage Systems**.
 - c. Select the target storage system, and then run **Refresh Storage Systems**.
 - d. Click **OK** twice.
11. (Optional) If the configuration of Protector registered in VASA Provider has been changed, refresh the configuration of Protector information.
 - a. Log in to the Web UI of VASA Provider.
 - b. Select **Replication Groups**.
 - c. Run **Refresh Protector Information**.



Note:

- You can use the virtual machine after you power it on.
- To protect a virtual machine by using vVols Replication after a Forced Failover is performed, set the site containing the virtual machine to be protected as the SOURCE, and then reconfigure the vVols Replication environment.

For details on how to reconfigure the vVols Replication environment, see the following procedures.

- [Settings to be configured in advance \(on page 24\)](#)
- [Enabling vVols Replication for an existing virtual machine \(on page 44\)](#)

Test Failover (Planned)

**Note:**

- The description of this procedure indicates Test Failover (Planned) when the `UnPlanned` option is not specified.
- A virtual machine created by starting a Test Failover is intended for temporary use. Thus, as a general rule, be sure to stop any Test Failovers that you start.
- You cannot enable vVols Replication while a Test Failover is being performed (when the replication group is in the `INTEST` status). Stop the Test Failover, and then perform the operation.

Starting a Test Failover (Planned)

Use PowerCLI to start a Test Failover (Planned). For the detailed configuration procedure, see the documentation for vSphere.

Procedure

1. Start PowerCLI.
2. Connect to vCenter Server at the local site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

3. Configure the settings needed to perform operations on multiple instances of vCenter Server.

```
Set-PowerCLIConfiguration -DefaultVIServerMode 'Multiple' -Scope
([VMware.VimAutomation.ViCore.Types.V1.ConfigurationScope]::Session) -Confirm:0
```

4. Connect to vCenter Server at the remote site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

5. From the **Replication Groups** screen of the VASA Provider Web UI, obtain the ID of the target replication group that is in the `TARGET` status.

```
$targetRg = Get-SpbmReplicationGroup -Name <ID-of-replication-group-in-TARGET-
status>
```

6. (Optional) Run Sync Replication Group.



Note: Run the following command if you want to perform restoration with the latest status. If you specify a PiT replica, you do not need to run the command.

```
Sync-SpbmReplicationGroup -ReplicationGroup $targetRg -PointInTimeReplicaName
<replica_name>
```

For `<replica_name>`, enter the name of your desired PiT replica.

7. (Optional) Obtain information about the PiT replica.



Note: Run the following command if you want to perform restoration by specifying a PiT replica. If you do not want to specify a PiT replica, you do not need to run the command.

```
$pitList = Get-SpbmPointInTimeReplica -ReplicationGroup $targetRg
$pit = $pitList[0]
```

For the `Get-SpbmPointInTimeReplica` option, specify one or more of the following:

```
[[-Name] <String[]>], [-FromDate <DateTime>], [-ToDate <DateTime>]
```

For `$pitList[0]`, specify the PiT replica. For 0, specify a value according to the environment.

8. Start a Test Failover for the replication group that is in the TARGET status at the remote site. When you run this command, if a confirmation message appears, enter `y`.

```
$remoteVMs = Start-SpbmReplicationTestFailover -ReplicationGroup $targetRg
```

If you specified a PiT replica, add `-PointInTimeReplica $pit`. If you do not specify a PiT replica, the newest PiT replica will be used.



Caution: If the capacity of the virtual disk was expanded, you must specify a PiT replica obtained after the capacity was expanded.

9. Check the list of virtual machines.

```
$remoteVMs
```



Note: If the VM File path does not appear and is not recognized on the datastore, restart the ESXi host. Then, perform step 8 again to obtain the VM File path.

10. Register the virtual machine on an ESXi host at the remote site.

```
New-VM -VMFilePath $remoteVMs -VMHost <ip_address>
```

For `<ip_address>`, enter the IP address of your desired ESXi host.

If the replication group includes more than one virtual machine, `$remoteVMs` will be in an array. To register more than one virtual machine, use a `for-each` loop to run the command for each applicable VM File path.



Note:

- You can use the virtual machine at the remote site after you power it on.
- If you want to obtain the `$remoteVMs` value again, perform step 8 again.

Stopping a Test Failover (Planned)



Note: Before performing a Test Failover Stop, delete snapshots that were created on virtual machine at the remote site. In addition, specify a VM storage policy in which vVols Replication is disabled.

Use PowerCLI to stop a Test Failover (Planned). For the detailed configuration procedure, see the documentation for vSphere.

Procedure

1. Log in to vSphere Client at the remote site, and then go to **VMs and Templates**.
2. Select the virtual machine, and then select **Power > Power Off**.
3. Select the virtual machine, and then select **Remove from Inventory**.
4. Start PowerCLI.
5. Connect to vCenter Server at the local site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

6. Configure the settings needed to perform operations on multiple instances of vCenter Server.

```
Set-PowerCLIConfiguration -DefaultVIServerMode 'Multiple' -Scope
([VMware.VimAutomation.ViCore.Types.V1.ConfigurationScope]::Session) -Confirm:0
```

7. Connect to vCenter Server at the remote site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

8. From the **Replication Groups** screen of the VASA Provider Web UI, obtain the ID of the target replication group that is in the INTEST status.

```
$targetRg = Get-SpbmReplicationGroup -Name <ID-of-replication-group-in-INTEST-
status>
```

9. Stop the Test Failover for the replication group that is in the INTEST status at the remote site.

```
Stop-SpbmReplicationTestFailover -ReplicationGroup $targetRg
```



Note: If you start a Test Failover and then immediately attempt to stop it, the attempt might fail. If the Test Failover fails to stop, wait for a while, and then retry the operation.

Test Failover (UnPlanned)

**Note:**

- For a Test Failover, the `UnPlanned` option to enable execution is available even in the state in which VASA Provider at the local site has stopped. The description of this procedure indicates Test Failover (UnPlanned) when the `UnPlanned` option is specified.
- A virtual machine created by starting a Test Failover is intended for temporary use. Thus, as a general rule, be sure to stop any Test Failovers that you start.
- You cannot enable vVols Replication while a Test Failover is being performed (when the replication group is in the `INTEST` status). Stop the Test Failover, and then perform the operation.
- When you run a Test Failover (UnPlanned), there is no change in the Replication Group status displayed in the Web UI of VASA Provider at the local site.

Starting a Test Failover (UnPlanned)

Use PowerCLI to start a Test Failover (UnPlanned). For the detailed configuration procedure, see the documentation for vSphere.

Procedure

1. Start PowerCLI.
2. Connect to vCenter Server at the remote site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

3. From the **Replication Groups** screen of the VASA Provider Web UI, obtain the ID of the target replication group that is in the `TARGET` status.

```
$targetRg = Get-SpbmReplicationGroup -Name <ID-of-replication-group-in-TARGET-
status>
```

4. (Optional) Run Sync Replication Group.



Note: Run the following command if you want to perform restoration with the latest status. If you specify a PiT replica, you do not need to run the command.

```
Sync-SpbmReplicationGroup -ReplicationGroup $targetRg -PointInTimeReplicaName
<replica_name>
```

For `<replica_name>`, enter the name of your desired PiT replica.

5. (Optional) Obtain information about the PiT replica.



Note: Run the following command if you want to perform restoration by specifying a PiT replica. If you do not want to specify a PiT replica, you do not need to run the command.

```
$pitList = Get-SpbmPointInTimeReplica -ReplicationGroup $targetRg
$pit = $pitList[0]
```

For the `Get-SpbmPointInTimeReplica` option, specify one or more of the following:

```
[[[-Name] <String[]>], [-FromDate <DateTime>], [-ToDate <DateTime>]]
```

For `$pitList[0]`, specify the PiT replica. For 0, specify a value according to the environment.

6. Start a Test Failover for the replication group that is in the TARGET status at the remote site. When you run this command, if a confirmation message appears, enter `y`.

```
$remoteVMs = Start-SpbmReplicationTestFailover -ReplicationGroup $targetRg -
UnPlanned
```

If you specified a PiT replica, add `-PointInTimeReplica $pit`. If you do not specify a PiT replica, the newest PiT replica will be used.



Caution: If the capacity of the virtual disk was expanded, you must specify a PiT replica obtained after the capacity was expanded.

7. Check the list of virtual machines.

```
$remoteVMs
```



Note: If the VM File path does not appear and is not recognized on the datastore, restart the ESXi host. Then, perform step 6 again to obtain the VM File path.

8. Register the virtual machine on an ESXi host at the remote site.

```
New-VM -VMFilePath $remoteVMs -VMHost <ip_address>
```

For `<ip_address>`, enter the IP address of your desired ESXi host.

If the replication group includes more than one virtual machine, `$remoteVMs` will be in an array. To register more than one virtual machine, use a `for-each` loop to run the command for each applicable VM File path.



Note:

- You can use the virtual machine at the remote site after you power it on.
- If you want to obtain the `$remoteVMs` value again, perform step 6 again.

Stopping a Test Failover (UnPlanned)



Note: Before performing a Test Failover Stop, delete snapshots that were created on virtual machine at the remote site. In addition, specify a VM storage policy in which vVols Replication is disabled.

Use PowerCLI to stop a Test Failover (UnPlanned). For the detailed configuration procedure, see the documentation for vSphere.

Procedure

1. Log in to vSphere Client at the remote site, and then go to **VMs and Templates**.
2. Select the virtual machine, and then select **Power > Power Off**.
3. Select the virtual machine, and then select **Remove from Inventory**.
4. Start PowerCLI.
5. Connect to vCenter Server at the remote site.

```
Connect-VIServer -Server <ip_address> -Protocol https -User <user_name> -
Password <password>
```

6. From the **Replication Groups** screen of the VASA Provider Web UI, obtain the ID of the target replication group that is in the INTEST status.

```
$targetRg = Get-SpbmReplicationGroup -Name <ID-of-replication-group-in-INTEST-
status>
```

7. Stop the Test Failover for the replication group that is in the INTEST status at the remote site.

```
Stop-SpbmReplicationTestFailover -ReplicationGroup $targetRg -Force
```



Note: If you start a Test Failover and then immediately attempt to stop it, the attempt might fail. If the Test Failover fails to stop, wait for a while, and then retry the operation.

Chapter 7: Deleting a vVols Replication environment

Deleting the settings of a virtual machine

If you want to delete the vVols Replication settings of a virtual machine, disable vVols Replication by performing the procedure in [Disabling vVols Replication for a virtual machine \(on page 47\)](#). Alternatively, delete the virtual machine.

If you want to delete the settings of a virtual machine after a Forced Failover, perform the following procedure.

Procedure

1. Log in to vSphere Client at the local site, and then go to **VMs and Templates**.
2. If the virtual machine is not already powered off, power it off.
 - a. Select the virtual machine, and then select **Power > Power Off**.
 - b. Verify that the **Power Off virtual machine** task ends successfully.

If VASA Provider at the local site cannot be used because of a failure, the virtual machine becomes inaccessible, but this does not indicate a problem. Proceed with the procedure.
3. Right-click the virtual machine, and then select **Remove from Inventory**.
4. Verify that the **Unregister virtual machine** task ends successfully.

Deleting a replication group

Delete a replication group.

Procedure

1. Log in to the Web UI of VASA Provider.
2. Select **Manage Storage Containers**.
3. Select the storage container used by the target replication group.
4. Select the **vVols** tab, and make sure there are no vVols whose group name in **Replication** matches the name of the target replication group.
5. If there is a vVol whose group name matches the name of the target replication group, perform the procedure in [Deleting the settings of a virtual machine \(on page 71\)](#) or [Disabling vVols Replication for a virtual machine \(on page 47\)](#).

6. If the vVol remains even after you perform the procedure in [Deleting the settings of a virtual machine \(on page 71\)](#) or [Disabling vVols Replication for a virtual machine \(on page 47\)](#), check the task status.
If the task status is **Removing (In Progress)**, processing to delete the replication pair is in progress. Wait for the task to finish.
7. If the applicable vVols have been deleted from the **vVols** tab or their group names in **Replication** are not -, perform the following steps to delete the replication group. In all other cases, proceed to step 8.
 - a. Log in to the Web UI of VASA Provider at the local site.
 - b. Select **Replication Groups**.
 - c. Select the target replication group, and then select **Forced Delete Replication Group**.
 - d. Click **Submit**.
 - e. Log in to the Web UI of VASA Provider at the remote site.
 - f. Select **Replication Groups**.
 - g. Select the replication group in the replication group pair that was deleted at the local site, and then select **Forced Delete Replication Group**.
 - h. Click **Submit**.
 - i. Refer to the procedure in [Deleting a data flow and Protector settings \(on page 73\)](#), and delete each of the Protector settings.
Be sure to perform the following steps.
 - Delete the data flow.
 - Perform Dissociate for replications and clones.
 - Delete snapshots.
 - Delete the Hitachi Block Host node.
 - j. Perform the procedure in [Deleting the settings of a storage system \(on page 74\)](#).
With the exception of optional steps, be sure to perform all steps at the local site and at the remote site.
 - k. (Optional) Refresh the Protector information at the local site.
 - i. Log in to the Web UI of VASA Provider.
 - ii. Select **Replication Groups**.
 - iii. Run **Refresh Protector Information**.
 - l. (Optional) Refresh the storage systems at the local site and at the remote site.
 - i. Log in to the Web UI of VASA Provider.
 - ii. Select **Manage Storage Systems**.
 - iii. Select the target storage systems, and then run **Refresh Storage Systems**.
 - iv. Click **OK** twice.
8. Select **Replication Groups**.



Note: If you are using Universal Replicator and want to delete one or more journals, note down the journal IDs before you delete the replication group.

9. Select **Delete Replication Group**.
To delete a replication group after a Forced Failover, select **Forced Delete Replication Group**.
10. Click **Submit**.



Note: For **Delete Replication Group**, running this command at either the local site or the remote site deletes the replication group at both sites. However, for **Forced Delete Replication Group**, you must run the command at both the local site and the remote site.

Deleting the general settings

Delete the general settings.

Procedure

1. Log in to the Web UI of VASA Provider.
2. Select **General Settings**.
3. Delete **Set Remote VASA Provider information** in **Replication Connection Setting**.
 - a. For **Set Remote VASA Provider information**, click **Delete**.
 - b. Click **OK**.
4. Delete **Set Protector Master information** in **Replication Connection Setting**.
 - a. For **Set Protector Master information**, click **Delete**.
 - b. Click **OK**.

Deleting a data flow and Protector settings

Delete the replication settings, and then delete the data flow.



Note: You might not be able to delete the Protector settings if they are being used by other settings. If you cannot delete the Protector settings, make sure that they are not being used by any other settings.

For details on the procedure, see the documentation for Protector.

Procedure

1. Log in to the Master node.
2. Select a data flow that was created in [Creating a data flow \(on page 34\)](#), and then run **Deactivate**.
3. Run **Dissociate** for the replication generated by the data flow.
4. Delete the data flow.
5. Delete the snapshot.
6. (Optional) Delete the policy that was created in [Creating a policy \(on page 32\)](#).

7. (Optional) Delete the applicable Hitachi Block Host node that was created in [Creating a Hitachi Block Host node \(on page 31\)](#).
8. (Optional) Delete the Hitachi Block Device nodes that were created in [Creating a Hitachi Block Device node at the local site \(on page 28\)](#) and [Creating a Hitachi Block Device node at the remote site \(on page 30\)](#).
If the storage system is powered off, you will not be able to delete the Hitachi Block Device nodes, but this will not affect the re-creation of a vVols Replication environment after a Forced Failover.
9. (Optional) Delete the applicable Client nodes that were created in [Introducing a Client node at the local site \(on page 28\)](#) and [Introducing a Client node at the remote site \(on page 28\)](#).
10. (Optional) Delete the Master node.
 - a. Log out of the Master node.
 - b. Delete the server on which the Master node is installed.

Deleting the settings of a storage system

Delete the settings of a storage system.

For details on the procedure, see the documentation for the storage system you are using.

Procedure

1. Log in to Storage Navigator.
2. For **Storage System**, select **Replication**.
3. If replication pairs exist, delete them.
4. If you are using Universal Replicator and one or more journals remain, delete them.
Perform the following steps to check the target journals.
 - a. Log in to the Web UI of VASA Provider.
 - b. Select **Replication Groups**.
 - c. Convert the local journal ID into a hexadecimal number.
This number is the ID of the target journal.
5. If snapshots exist, delete them.
Perform the following steps to check the primary volumes of the target snapshots.
 - a. For **Storage System**, select **Replication**.
 - b. Select **Local Replication**.
 - c. Select **TI Root Volumes**.
 - d. Confirm that the LDEV of the data flow host group created in [Creating a data flow host group \(on page 27\)](#) appears in **Host Group Name / iSCSI Target Alias**.
This LDEV is the primary volume of the target snapshot.
6. Delete the data flow host group that was created in [Creating a data flow host group \(on page 27\)](#).
7. If the vVols are bound, unbind them.
Use the Web UI of VASA Provider to check whether the vVols are bound.

- a. Select **Managed Storage Containers**.
 - b. Select the name of the storage container that is used as the datastore of the virtual machine.
 - c. Select the **vVols** tab.
 - d. Check the value displayed for **Binding ALUs** for each vVol.
This value is the LDEV ID of the target ALU.
8. Delete the dummy LDEVs and vVols.
 - a. For **Storage System**, select **Pools**.
 - b. Select the target pool.
 - c. Select the **Virtual Volumes** tab.
 - d. Select the target LDEV IDs, and then select **Delete LDEVs** from the **More Actions** list.
 - e. On the Delete LDEVs screen, click **Apply**.
 - f. Click **OK**.
 9. In the Manage Storage Systems screen in the Web UI of VASA Provider, select the target storage system, and then run **Refresh Storage Systems**.
 10. (Optional) Delete the remote connections.
 11. (Optional) Delete the remote paths.

Deleting a vVols environment

If you no longer need a vVols environment, delete it. For details on how to delete a vVols environment, see the *Hitachi Storage (VASA) Provider for VMware vCenter Deployment Guide* and the documentation for the storage system you are using.

Hitachi Vantara



Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact