Hitachi Ops Center Administrator

10.8.2

High Availability User Guide

This document provides instructions for configuring Hitachi storage for high availability.

MK-99ADM003-10
May 2022

Contents

Chapter 1: Overview of global-active device..... 11
About global-active device..... 11
Global-active device components..... 12
Global-active device solutions..... 15
Fault-tolerant storage infrastructure..... 15
Failover clustering without storage impact..... 15
Server load balancing without storage impact..... 16
System configurations for global-active device solutions..... 17
Global-active device and global storage virtualization..... 20
About the virtual ID..... 20
Global-active device status monitoring..... 21
Global-active device status..... 21
High Availability status transitions..... 23
Pair status..... 23
High Availability suspend types..... 24
I/O modes..... 25
Relationship between High Availability status, pair status, and I/O mode.... 26
Global-active device and server I/O..... 27
Server I/O (GAD status: Mirrored)..... 28
Server I/O (GAD status: Mirroring or Quorum disk blocked or no quorum disk volume)..... 28
Server I/O when the GAD status is Suspended..... 29
Server I/O when the global-active device status is Blocked..... 30
Quorum disk and server I/O..... 30
High availability pairs without a volume set for the quorum disk..... 31
I/O stoppage detected in the counterpart system..... 35
I/O stoppage not detected in the counterpart system..... 35
Server I/Os and data mirroring with blocked quorum disk or without quorum disk volumes..... 35
Quorum disk status..... 37
Global-active device consistency groups..... 38
Global-active device pairs by consistency group..... 39
Suspension of GAD pairs by consistency group..... 39
Use cases for consistency groups..... 41

High Availability consistency group statuses....41
Initial copy and differential copy....42
User interfaces for global-active device operations....42
Storage Advisor Embedded....43
Storage Navigator....43
Ops Center Administrator....43
Ops Center Protector....43

Chapter 2: System requirements....44

Requirements and restrictions....44
Interoperability requirements....55
Volume types supported for global-active device....55
Dynamic Provisioning / Dynamic Tiering / Active flash....57
ShadowImage....58
Limitations when sharing global-active device and ShadowImage volumes....59
ShadowImage operations and global-active device pair status....59
GAD operations and SI pair status....62
Thin Image....64
Limitations for using both global-active device and Thin Image....65
Thin Image operations and global-active device status....66
Global-active device operations and Thin Image pair status....68
Use cases for pairing global-active device volumes with ShadowImage or Thin Image....70
Universal Replicator....70
global-active device pair and Universal Replicator pair interoperability..72
Data Retention Utility....75
Global-active device status and I/O allowance by access attribute....76
Volume Migration....77
Restrictions for using global-active device with Volume Migration....78
Global-active device status and Volume Migration pair operations....78
Volume Migration pair statuses and global-active device pair operations....80
LUN Manager....82
Virtual Partition Manager....82
Nondisruptive migration (VSP G1x00, F1500)....83
Restrictions for using global-active device with nondisruptive migration....83
Global-active device status and nondisruptive migration pair operations....84
Volume Shredder....88
Performance Monitor....88
Server I/Os added to Performance Monitor....89

Port I/Os added to Performance Monitor..... 91
Connection types..... 91
Direct connection.....91
Connection using switches.....92
Connection using channel extenders..... 93

Chapter 3: Setting up high availability.....95
Overview of the workflow for global-active device..... 95
Register the global-active device license.....96
Registering the global-active device license for VSP E series and VSP G200, G/F400, G/F600, G/F800 storage systems 96
Registering the global-active device license for VSP E series and VSP G/F350, G/F370, G/F700, G/F900 storage systems..... 96
Registering the global-active device license for VSP G1x00, F1500 and VSP 5000 series storage systems..... 97
Add an external storage system for the quorum disk..... 97
Configure remote paths..... 98
Configuring remote paths for VSP 5000 series and VSP E series, VSP F series, VSP G series..... 98
Configuring remote paths for VSP E series and VSP G/F350, G/F370, G/F700, G/F900 storage systems..... 100
Configure the quorum disk.....100
Configuring the quorum disk for VSP E series, VSP G200, G/F400, G/F600, G/F800, VSP G1x00, F1500 , and VSP 5000 series..... 101
Discover and add external volumes.....101
Adding the quorum disk 101
Configuring the quorum disk for VSP E series and VSP G/F350, G/F370, G/F700, G/F900 models.....102
Configuring a quorum disk by creating an external volume 102
Configuring a quorum disk by selecting an external volume 104
Configuring a quorum disk without using an external volume 104
Onboard primary and secondary storage systems in Ops Center Protector... 105
Onboard primary and secondary storage systems in Ops Center Administrator.....107
Adding a storage system in Ops Center Administrator..... 107
Adding servers.....109
Register Ops Center Protector with Ops Center Administrator.....110
Managing virtual storage machines for high availability..... 111
Creating virtual storage machines 111
Manage virtual storage machines.....112
Virtual storage machine inventory 113
Creating virtual storage machines 114
Removing undefined resources from a virtual storage machine 115

Moving defined volumes to a virtual storage machine..... 116
Adding resources to a virtual storage machine..... 117
Virtual storage machine details 118
Adding storage systems to a virtual storage machine.....118
Adding undefined volumes to a virtual storage machine.....119
Adding undefined host groups to a virtual storage machine..... 120
Removing storage systems from a virtual storage machine..... 121
Removing undefined volumes from a virtual storage machine..... 121
Removing host groups from a virtual storage machine.....122

Chapter 4: Provisioning for high availability..... 124
Prerequisites to provisioning for high availability..... 124
Creating, attaching, and protecting volumes with high availability 125
Attaching volumes and selecting secondary servers.....127
Selecting volume protection options..... 129
Configuring connections to the primary and secondary sites 130

Chapter 5: Monitoring high availability operations in Ops Center Protector.....133
Mounting a block snapshot or replication..... 135
How to swap (takeover/takeback) a replication..... 136

Chapter 6: Disabling high availability functions.....139
Disable by deleting the replication group and primary volumes..... 140
Disable by deleting the replication group and retaining the primary volume... 140
Disable by deleting some global-active device pairs but retaining the replication group..... 141
Disable by deleting some global-active device pairs but retaining the replication group and primary volumes.....142

Preface

This document provides instructions for configuring your Hitachi storage for high availability.

Intended Audience

This document is intended for system administrators, Hitachi Vantara representatives, and authorized service providers who configure and operate Virtual Storage Platform storage systems with Hitachi Ops Center Administrator.

Readers of this document should be familiar with the following:

- RAID storage systems and their basic functions.
- High Availability (HA), also known as global-active device (GAD)
- Volume creation and management.
- Pool creation and management.
- Parity group creation and management.

Product version

This document revision applies to Hitachi Ops Center Administrator version 10.8.2 or later.

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 located on Support Connect at https://knowledge.hitachivantara.com/Documents.

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. ▪ Indicates emphasized words in list items.
Italic	▪ Indicates a document title or emphasized words in text. ▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: ▪ Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` ▪ 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 for Storage Navigator

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: ▪ 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 the Hitachi Vantara Support Website: https://knowledge.hitachivantara.com/Documents. 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 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 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 us your comments on this document 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 of global-active device

High availability is enabled by Hitachi global-active device technology.

You can configure high availability for the following storage systems by using Storage Navigator, Ops Center Protector, and Ops Center Administrator:

- VSP 5000 series
- VSP E series
- VSP G1x00, F1500
- VSP G200, VSP G350, G370, G700, G900, VSP G400, G600, G800, VSP F350, F370, F700, F900, VSP F400, F600, F800

About global-active device

Global-active device (GAD) enables you to create and maintain synchronous, remote copies of data volumes.

A virtual storage machine is configured in the primary and secondary storage systems using the information of the primary storage system, and the global-active device (GAD) primary and secondary volumes are assigned the same virtual LDEV number in the virtual storage machine. This enables the host to see the pair volumes as a single volume on a single storage system, and both volumes receive the same data from the host.

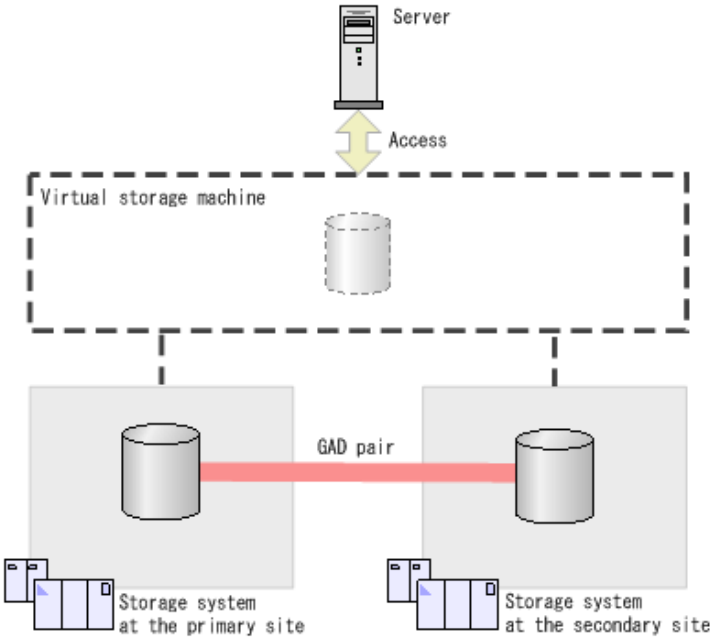
A quorum disk, which can be located in a third and external storage system, is used to monitor the GAD pair volumes. The quorum disk acts as a heartbeat for the GAD pair, with both storage systems accessing the quorum disk to check on each other. A communication failure between systems results in a series of checks with the quorum disk to identify the problem for the system able to receive host updates.

Alternate path software on the host runs in the Active/Active configuration. While this configuration works well at campus distances, at metro distances you must use multi-pathing software with ALUA (asymmetric logical unit access) or Hitachi Dynamic Link Manager to support preferred/nonpreferred paths and ensure that the shortest path is used.

If the host cannot access the primary volume (P-VOL) or secondary volume (S-VOL), host I/O is redirected by the alternate path software to the appropriate volume without any impact to the host applications.

Global-active device provides the following benefits:

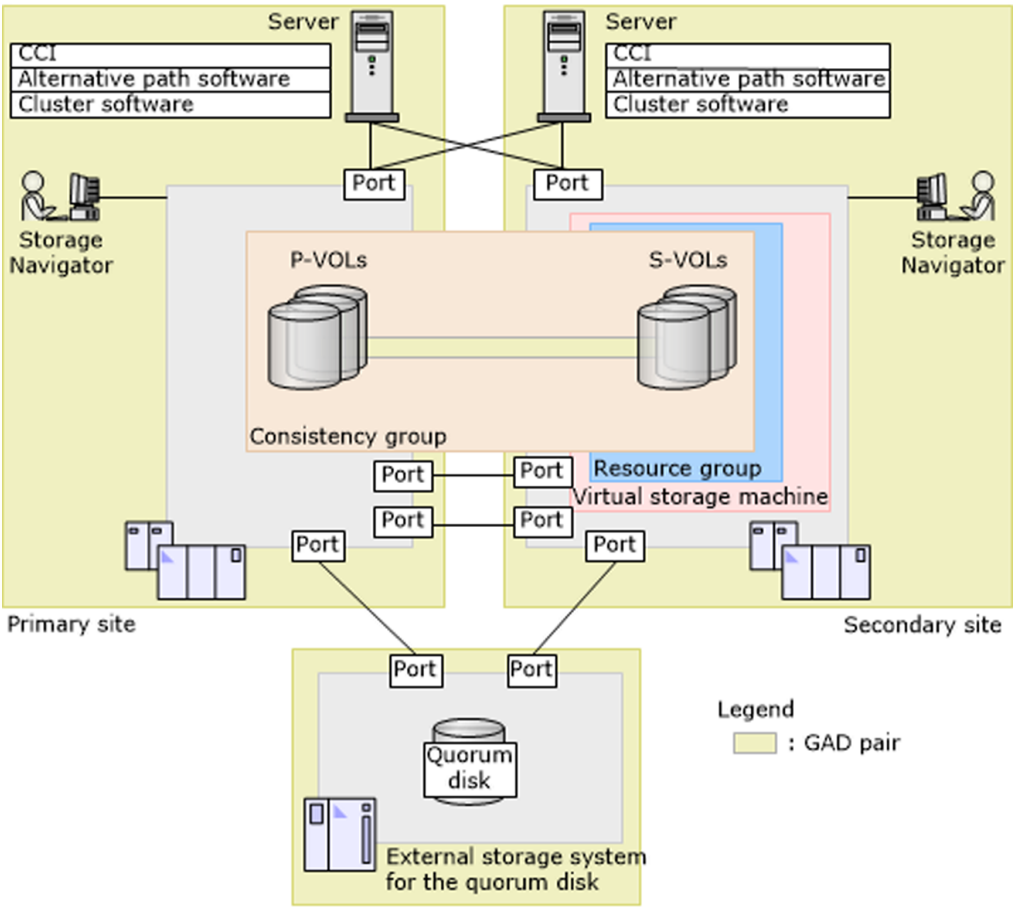
- Continuous server I/O when a failure prevents access to a data volume
- Server failover and failback without storage impact
- Migrating virtual machines without storage impact



Global-active device components

A typical global-active device system consists of storage systems, paired volumes, a consistency group, a quorum disk, a virtual storage machine, paths and ports, alternate path software, and cluster software.

The following illustration shows the components of a typical global-active device system.



Storage systems

Both of the primary and secondary storage systems should be the same model type, but they do not have to be the same model. For example:

- If the primary storage system is a VSP 5000 series, the secondary storage system must also be a VSP 5000 series ,VSP E series or VSP G/F350, G/F370, G/F700, G/F900.
- If the primary storage system is a VSP G1x00, F1500, the secondary storage system can be a VSP E series or VSP G/F350, G/F370, G/F700, G/F900.
- If the primary storage system is a VSP G350, G370, G700, G900, the secondary storage system can be a VSP G350, G370, G700, G900.
- If the primary storage system is a VSP F350, F370, F700, F900 storage system, the secondary storage system can be VSP F350, F370, F700, F900.
- If the primary storage system is a VSP G1000, the secondary storage system must also be a VSP G1000.

An external storage system or iSCSI-attached server that is connected to the primary and secondary storage systems using Universal Volume Manager is required for the quorum disk.

Paired volumes

A global-active device pair consists of a P-VOL in the primary storage system and an S-VOL in the secondary storage system. For model connectivity support requirements, refer to System requirements.

Consistency group

A consistency group consists of multiple global-active device pairs. By registering GAD pairs to a consistency group, you can resynchronize or suspend the GAD pairs by consistency group.

For details about storage system support (microcode) for consistency groups, refer to Requirements and restrictions (on page 44).

Quorum disk

The quorum disk, required for global-active device, determines the storage system on which server I/O should continue when a storage system or path failure occurs. The quorum disk is virtualized from an external storage system that is connected to both the primary and secondary storage systems. Alternatively, a disk in an iSCSI-attached server can be used as a quorum disk if the server is supported by external storage. If you do not set a volume for the quorum disk, you do not need to prepare a volume in an external storage system for the quorum disk.

Virtual storage machine

A virtual storage machine (VSM) is configured in the secondary storage system with the same model and serial number as the (actual) primary storage system. The servers treat the virtual storage machine and the storage system at the primary site as one virtual storage machine.

You can create GAD pairs using volumes in virtual storage machines. When you want to create a GAD pair using volumes in VSMs, the VSM for the volume in the secondary site must have the same model and serial number as the VSM for the volume in the primary site.

Paths and ports

GAD operations are carried out between hosts and primary and secondary storage systems that are connected by data paths composed of one of more physical links.

The data path, also referred to as the remote connection, connects ports on the primary storage system to ports on the secondary storage system. Both Fibre Channel and iSCSI remote copy connections are supported. The ports have attributes that enable them to send and receive data. One data path connection is required, but you should use two or more independent connections for hardware redundancy.

Note: You do not need to set the port attributes (Initiator, RCU Target, Target External) for VSP E series and VSP G/F350, G/F370, G/F700, G/F900 storage systems.

Alternate path software

Alternate path software is used to set redundant paths from servers to volumes and to distribute host workload evenly across the data paths. Alternate path software is required for the single-server and cross-path GAD system configurations.

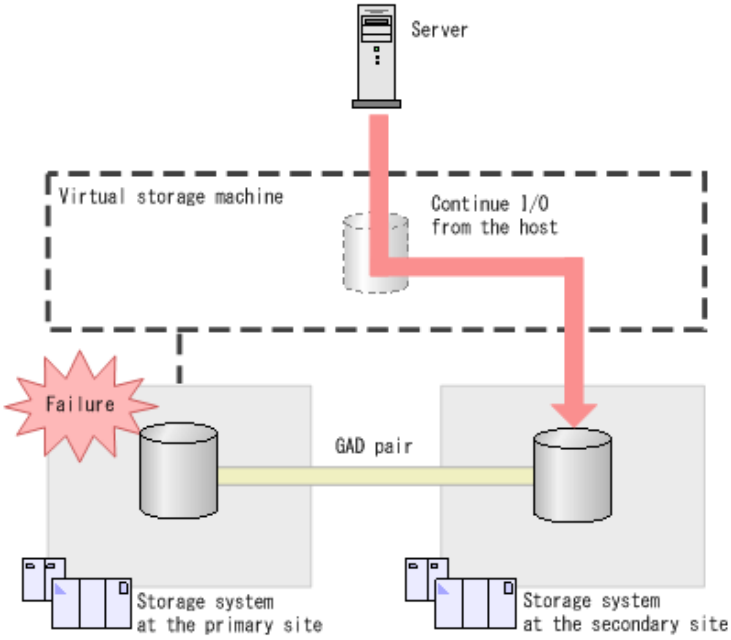
Cluster software

Cluster software is used to configure a system with multiple servers and to switch operations to another server when a server failure occurs. Cluster software is required when two servers are in a global-active device server-cluster system configuration.

Global-active device solutions

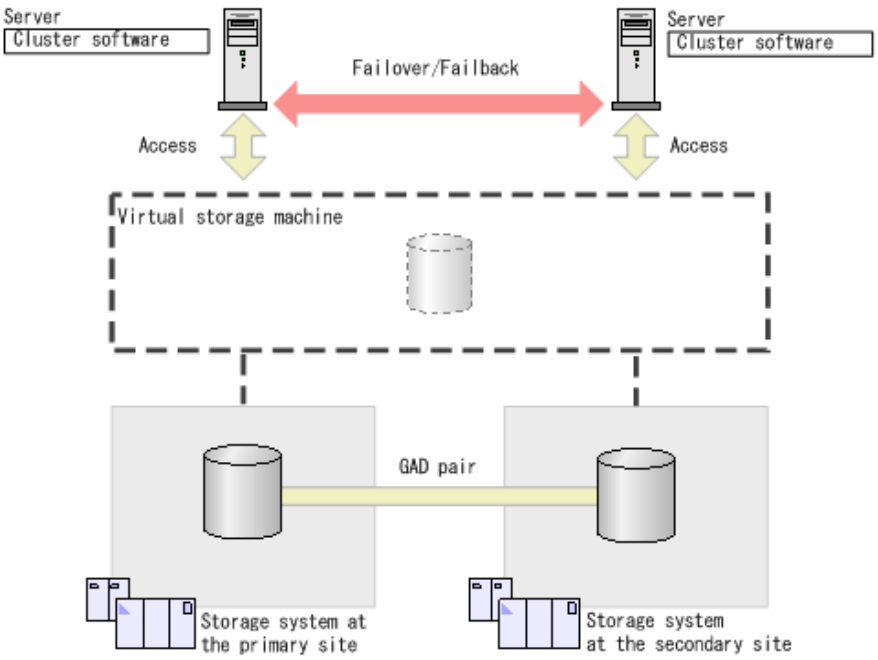
Fault-tolerant storage infrastructure

If a failure prevents host access to a volume in a GAD pair, read and write I/O can continue to the pair volume in the other storage system to provide continuous server I/O to the data volume.



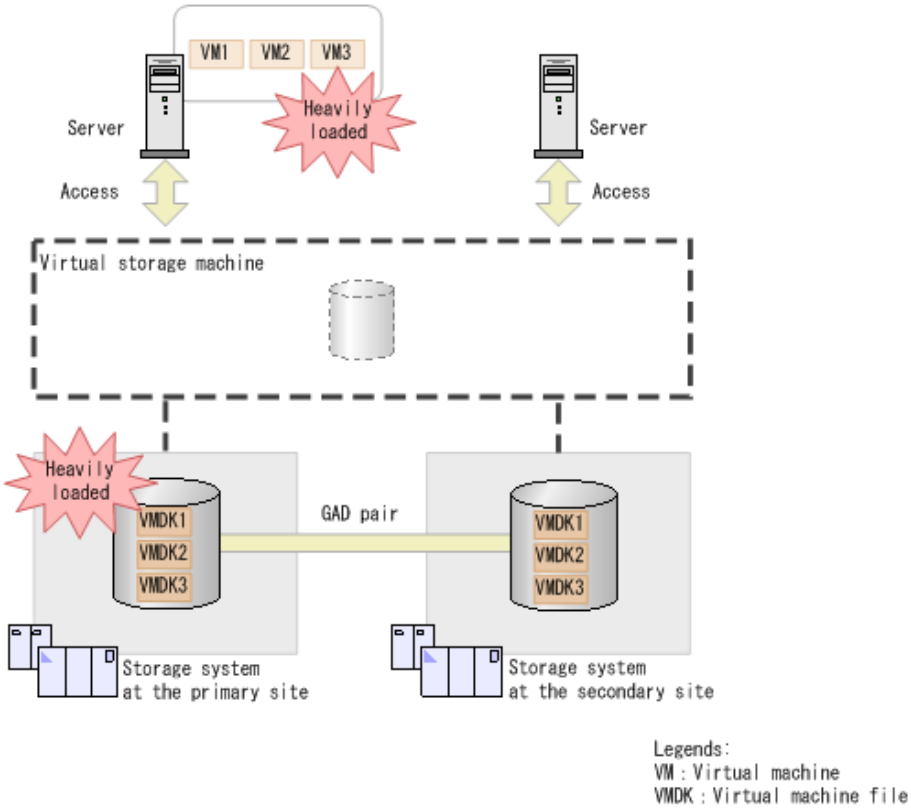
Failover clustering without storage impact

In a server-cluster configuration with global-active device, the cluster software is used to perform server failover and failback operations, and the global-active device pairs do not need to be suspended or resynchronized.

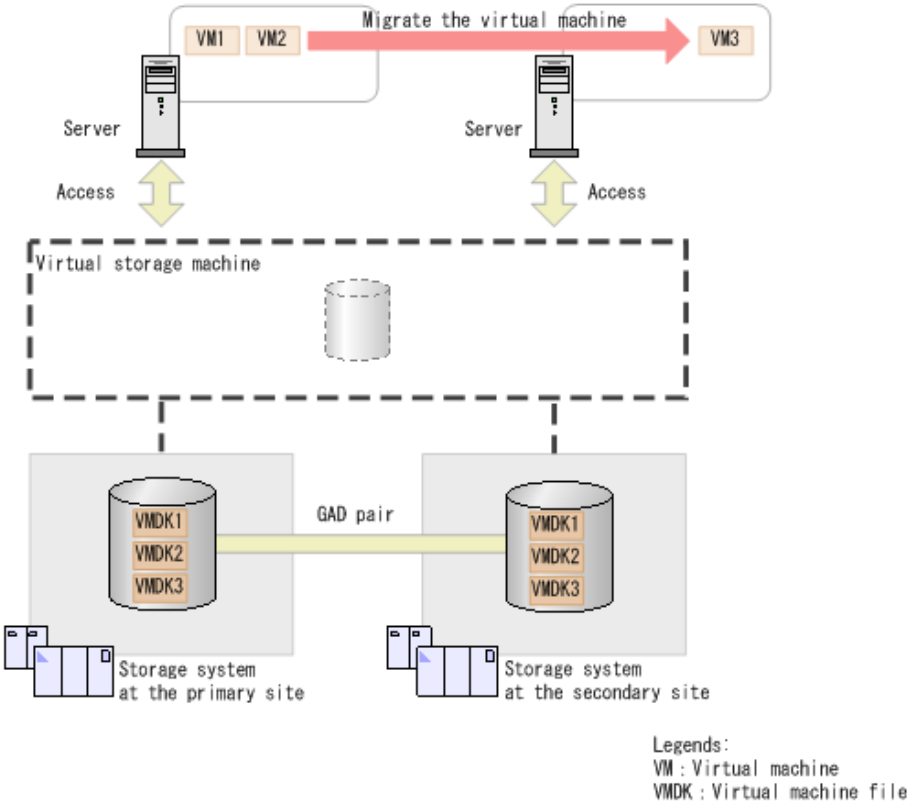


Server load balancing without storage impact

When the I/O load on a virtual storage machine at the primary site increases global-active device enables you to migrate the virtual machine to the paired server without performing any operations on the storage systems.



As shown in this example, the server virtualization function is used to migrate virtual machine VM3 from the primary-site server to the secondary-site server. Because the GAD primary and secondary volumes contain the same data, you do not need to migrate any data between the storage systems.



System configurations for global-active device solutions

You have the option of implementing three different system configurations: a single-server configuration, a server-cluster configuration, and a cross-path configuration. The system configuration depends on the GAD solution that you are implementing.

The following table lists the GAD solutions and specifies the system configuration for each solution.

Note: When you register GAD pairs to a consistency group, you should use the cross-path configuration. If GAD pairs in the Mirrored status are suspended due to a path failure between the primary site and the secondary site in the following condition, some GAD pairs might be able to be accessed only from the server at the primary site, and other GAD pairs might be able to be accessed only from the server at the secondary site.

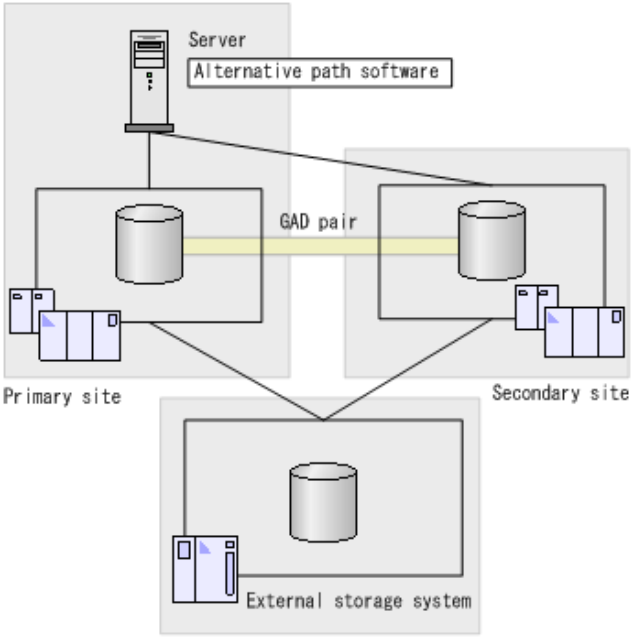
- GAD pairs both in the Mirrored status and in the Mirroring status are in the consistency group.
- GAD pairs both in the Mirrored status and in the Suspended status are in the consistency group.

When you use the cross-path configuration that enables both servers at the primary and secondary sites to access both volumes at the primary and secondary sites, the servers can continue to access the GAD volumes even in this situation. If you use a configuration other than the cross-path configuration, the servers cannot access the GAD volumes.

GAD solution	Software		System configuration
	Alternate path software	Cluster software	
Continuous server I/O (if a failure occurs in a storage system)	Required	Not required	Single-server configuration
Failover and failback on the servers without using the storage systems	Not required	Required	Server-cluster configuration
Migration of a virtual machine of a server without using the storage systems	Not required	Required	Server-cluster configuration
Both of the following: ▪ Continuous server I/O (if a failure occurs in a storage system) ▪ Migration of a virtual storage machine of a server without using the storage systems	Required	Required	Cross-path configuration

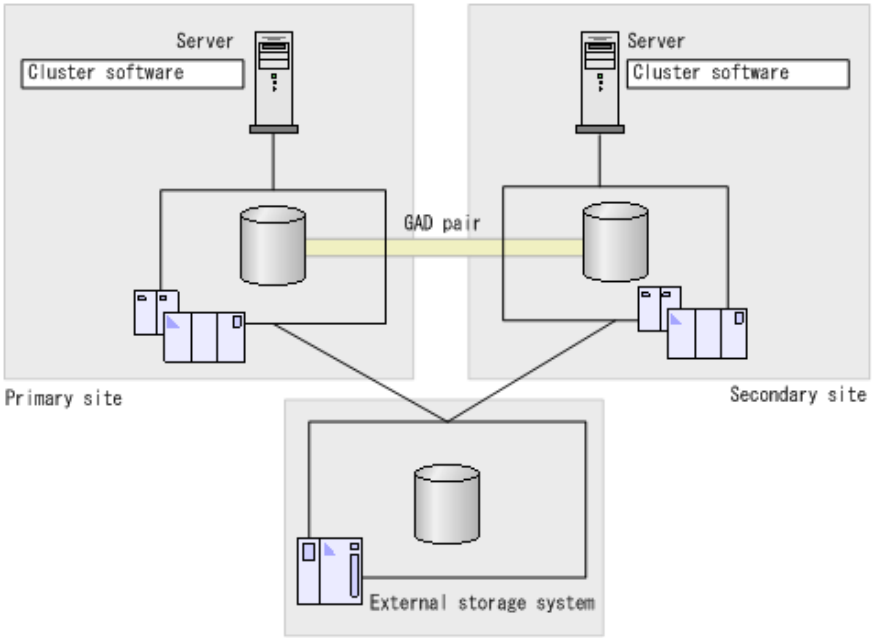
Single-server configuration

In a single-server configuration, the primary and secondary storage systems connect to the host server at the primary site. If a failure occurs in one storage system, you can use alternate path software to switch server I/O to the other site.



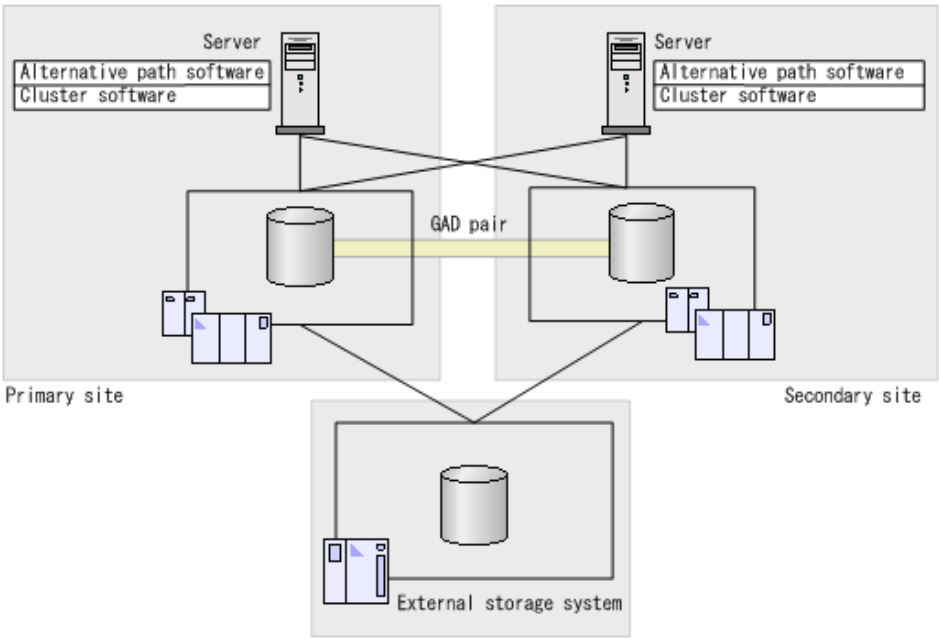
Server-cluster configuration

In a server-cluster configuration, servers are located at both the primary and secondary sites. The primary storage system connects to the primary-site server, and the secondary storage system connects to the secondary-site server. The cluster software is used for failover and failback. When I/O on the virtual machine of one server increases, you can migrate the virtual machine to the paired server to balance the load.



Cross-path configuration

In a cross-path configuration, primary-site and secondary-site servers are connected to both the primary and secondary storage systems. If a failure occurs in one storage system, alternate path software is used to switch server I/O to the paired site. The cluster software is used for failover and failback.



Global-active device and global storage virtualization

GAD operations are based on the global storage virtualization function. When virtual information is sent to the server in response to the SCSI Inquiry command, the server views multiple storage systems as multiple paths to a single storage system.

The global storage virtualization function is enabled when you install the license for Resource Partition Manager, which is provided with the Storage Virtualization Operating System (SVOS). For more information about Resource Partition Manager, see the *Provisioning Guide* for the storage system.

About the virtual ID

The server is able to identify multiple storage systems as a single virtual storage machine when the resources listed below are virtualized and the virtual identification (virtual ID) information is set. You can set virtual IDs on resource groups and on individual volumes, as described in the following table.

Virtual information required by the server	Resource on which virtual IDs are set
Serial number	Resource group

Virtual information required by the server	Resource on which virtual IDs are set
Product	Resource group
LDEV ID*	Volume
Emulation type	Volume
Number of concatenated LUs of LUN Expansion (LUSE)	Volume
SSID	Volume
* A volume whose virtual LDEV ID has been deleted cannot accept I/O from a server. The virtual LDEV ID is temporarily deleted on a volume to be used as a GAD S-VOL because, when the pair is created, the P-VOL's physical LDEV ID is set as the S-VOL's virtual LDEV ID.	

When using global storage virtualization you can set the following:

- The same serial number or product as the virtual ID for more than one resource group
- Up to 15 virtual IDs for resource groups in a single storage system (VSP 5000 series, VSP E series, VSP F1500, and VSP G1x00)
- Up to seven types of virtual IDs for resource groups in a single storage system (VSP G/F350, G/F370, G/F700, G/F900)
- Virtual IDs for a maximum of 1,023 resource groups (excluding resource group #0)
- Virtual IDs for a maximum of 65,279 volumes

For instructions on setting virtual IDs, see the *Command Control Interface Command Reference*.

Global-active device status monitoring

GAD operations are managed based on the following information: Pair status, I/O mode of the P-VOL and S-VOL, and GAD status, which is a combination of pair status and I/O mode.

Global-active device status

It is important to be able to understand what the meaning of a GAD status is and what that status tells you about the GAD pair.

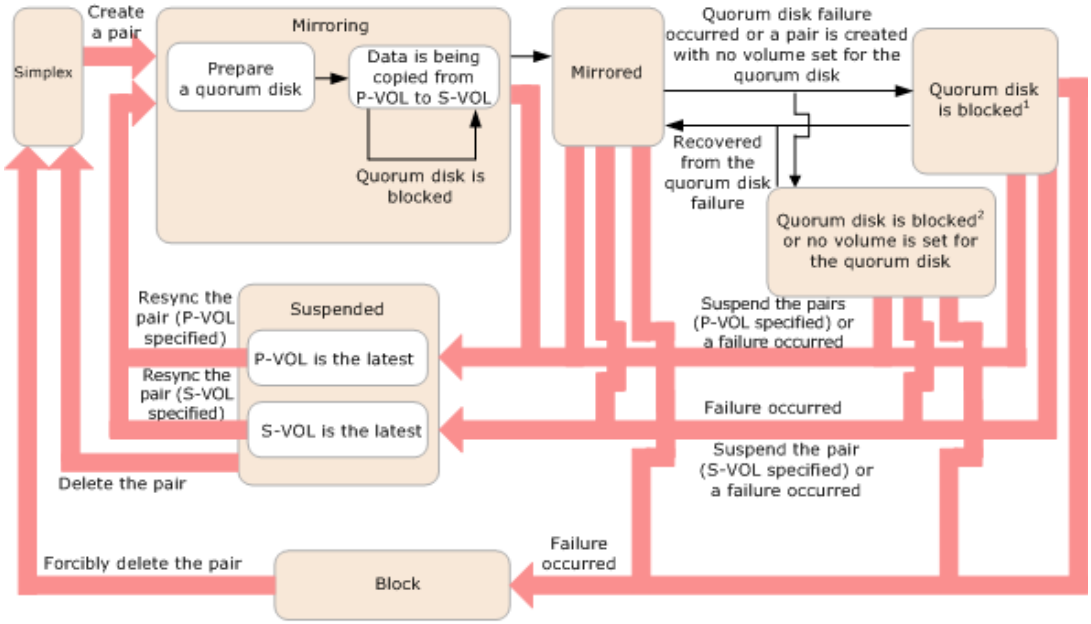
The following table lists and describes the GAD statuses.

GAD status	Description	Data redundancy	Updated volume	Volume with latest data
Simplex	The volume is not a pair volume.	No	Not applicable	Not applicable
Mirroring	The pair is changing to Mirrored status. This status is issued when you do the following: ▪ Prepare a quorum disk. ▪ Copy data from the P-VOL to the S-VOL.	No	P-VOL and S-VOL	P-VOL
Mirrored	The pair is operating normally.	Yes	P-VOL and S-VOL	P-VOL and S-VOL
Quorum disk blocked or no quorum disk volume	The Quorum disk is blocked, but the data is mirrored. The data is mirrored when no volume is set for the quorum disk.	Yes	P-VOL and S-VOL	P-VOL and S-VOL
Suspended	The pair is suspended. I/O from the server is sent to the volume with the latest data. When a failure occurs or the pair is suspended, the status changes to Suspended. The status changes to Suspended after the time specified for Read Response Guaranteed Time When Quorum Monitoring Stopped elapses.	No	P-VOL or S-VOL	P-VOL or S-VOL
Blocked	I/O is not accepted by either pair volume. This status occurs when: ▪ Both the P-VOL and S-VOL have the latest data. If the pair is forcibly deleted, I/O can be restarted in either of the volumes. ▪ A failure occurs in the primary or secondary storage system, and I/O to the volume in the paired system is also stopped. If more than one failure occurs at the same time, the GAD status changes to Blocked.	No	None	P-VOL and S-VOL

High Availability status transitions

The GAD status changes depending on the pair operation and failure.

The following illustration shows the GAD pair status transitions.



Legend:
P-VOL: Primary volume
S-VOL: Secondary volume
Resync: Resynchronize
: Status which is changed automatically
: Operation or failure workflow
: GAD status

Notes:
1. For VSP F1500, G1x00, the Microcode version is 80-04-2x or earlier.
For VSP Fx00 models and VSP Gx00 models, the firmware version is 83-03-3x or earlier.
2. For VSP F1500, G1x00, the Microcode version is 80-05-0x or later.
For VSP Fx00 models and VSP Gx00 models, the firmware version is 83-04-0x or later.

If you resynchronize a pair specifying the P-VOL, I/O continues on the P-VOL. If you resynchronize a pair specifying the S-VOL, data flow switches from the S-VOL to the P-VOL, and then I/O continues on the new P-VOL.

If you suspend a pair specifying the P-VOL, I/O continues to the P-VOL. If you suspend a pair specifying the S-VOL, I/O continues to the S-VOL.

Pair status

The pair status provides information about the current state of a global-active device pair.

The following table lists and describes the pair statuses, which indicate the current state of a global-active device pair. As shown in the following table, the pair status terms displayed by the user interfaces are slightly different.

Pair status		Description
CCI	**HDvM - SN**	
SMPL	SMPL	The volume is not paired.
COPY	INIT/COPY	The initial copy or pair resynchronization is in progress (including creation of a GAD pair that does not perform data copy). A quorum disk is being prepared.
	COPY	The initial copy is in progress; data is being copied from the P-VOL to the S-VOL (including creation of a GAD pair that does not perform data copy).
PAIR	PAIR	The pair is synchronized.
PSUS	PSUS*	The pair was suspended by the user. This status appears on the P-VOL.
PSUE	PSUE*	The pair was suspended due to a failure.
SSUS	SSUS*	The pair was suspended by the user, and update of the S-VOL is interrupted. This status appears on the S-VOL.
SSWS	SSWS*	The pair was suspended either by the user or due to a failure, and update of the P-VOL is interrupted. This status appears on the S-VOL.
* When a GAD pair is suspended, you can view the suspend type on the View Pair Properties window.		

High Availability suspend types

When a GAD pair is suspended, the suspend type is displayed in Status field of the **View Pair Properties** window. The suspend type is not displayed by CCI.

The following table lists and describes the GAD suspend types.

Suspend type	Volume	Description
Primary Volume by Operator	P-VOL	The user suspended the pair from the primary storage system. The S-VOL suspend type is "by MCU".
Secondary Volume by Operator	P-VOL S-VOL	The user suspended the pair from the secondary storage system.

Suspend type	Volume	Description
by MCU	S-VOL	The secondary storage system received a request from the primary storage system to suspend the pair. The P-VOL suspend type is Primary Volume by Operator or Secondary Volume by Operator.
by RCU	P-VOL	The primary storage system detected an error condition at the secondary storage system, which caused the primary storage system to suspend the pair. The S-VOL suspend type is Secondary Volume Failure.
Secondary Volume Failure	P-VOL S-VOL	The primary storage system detected an error during communication with the secondary storage system, or an I/O error during update copy. In this case, the S-VOL suspend type is usually Secondary Volume Failure. This suspend type is also used when the number of paths falls below the minimum number of paths setting on the Add Remote Connection window.
MCU IMPL	P-VOL S-VOL	The primary storage system could not find valid control information in its nonvolatile memory during IMPL. This condition occurs only if the primary storage system is without power for more than 48 hours (that is, power failure and fully discharged backup batteries).
Initial Copy Failed	P-VOL S-VOL	The pair was suspended before the initial copy operation was complete. The data on the S-VOL is not identical to the data on the P-VOL.

I/O modes

You should understand the I/O actions on the P-VOL and the S-VOL of a GAD pair.

The following table lists and describes the GAD I/O modes. As shown in the following table, the I/O mode terms displayed by the user interfaces are slightly different.

I/O mode			Read processing	Write processing
I/O mode	CCI [1]	HDvM - SN		
Mirror (RL)	L/M	Mirror (Read Local)	Sends data from the storage system that received a read request to the server.	Writes data to the P-VOL and then the S-VOL.

I/O mode			Read processing	Write processing
I/O mode	**CCI [1]**	**HDvM - SN**		
Local	L/L	Local	Sends data from the storage system that received a read request to the server.	Writes data to the volume on the storage system that received a write request.
Block[2]	B/B	Block	Rejected (Replies to illegal requests).	Rejected (Replies to illegal requests).

Notes:

1. In CCI, the I/O mode is displayed as <read processing>/<write processing> in which L indicates Local, M indicates Mirror, and B indicates Block (for example, L/L indicates Local read processing and Local write processing).
2. For volumes whose I/O mode is Block, a response indicating that the LU is undefined is returned to the Report LUN and Inquiry commands. Therefore, servers cannot identify a volume whose I/O mode is Block, or the path of this volume is blocked.

Relationship between High Availability status, pair status, and I/O mode

You should understand the relationship between the GAD status, pair status, and I/O mode to be informed about your GAD pairs.

The following table lists the GAD statuses and describes the relationship between the GAD status, pair status, and I/O mode. "N" indicates that pair status or I/O mode cannot be identified due to a failure in the storage system.

GAD status	When to suspend	P-VOL		S-VOL		Volume that has the latest data
		Pair status	I/O mode	Pair status	I/O mode	
Simplex	Not applicable	SMPL	Not applicable	SMPL	Not applicable	Not applicable
Mirroring	Not applicable	INIT	Mirror(RL)	INIT	Block	P-VOL
	Not applicable	COPY	Mirror(RL)	COPY	Block	P-VOL
Mirrored	Not applicable	PAIR	Mirror(RL)	PAIR	Mirror(RL)	P-VOL and S-VOL

GAD status	When to suspend	P-VOL		S-VOL		Volume that has the latest data
		Pair status	I/O mode	Pair status	I/O mode	
Quorum disk blocked or no quorum disk volume	Not applicable	PAIR	Mirror(RL)	PAIR	Mirror(RL)	P-VOL and S-VOL
Suspended	Pair operation	PSUS	Local	SSUS	Block	P-VOL
	Failure	PSUE*	Local	PSUE	Block	P-VOL
		PSUE*	Local	SMPL	Not applicable	P-VOL
		PSUE*	Local	N	N	P-VOL
	Pair operation	PSUS	Block	SSWS	Local	S-VOL
	Failure	PSUE	Block	SSWS*	Local	S-VOL
		SMPL	Not applicable	SSWS*	Local	S-VOL
		N	N	SSWS*	Local	S-VOL
Blocked	Not applicable	PSUE	Block	PSUE	Block	P-VOL and S-VOL
	Not applicable	PSUE	Block	N	N	P-VOL and S-VOL
	Not applicable	N	N	PSUE	Block	P-VOL and S-VOL
*: If the server does not issue the write I/O, the pair status might be PAIR, depending on the failure location.						

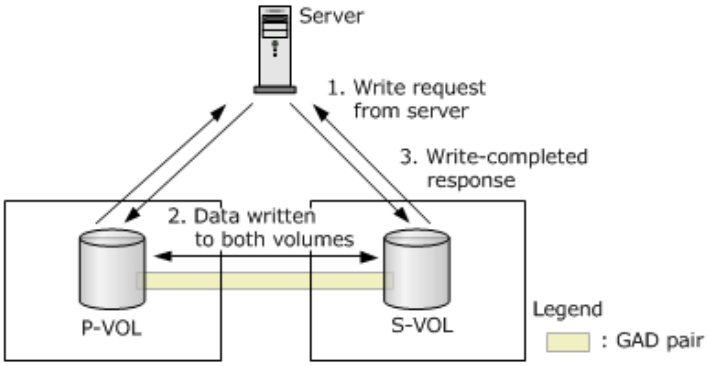
Global-active device and server I/O

I/O requests from the server to a GAD pair volume are managed according to the volume's I/O mode. The GAD status determines the I/O mode of the P-VOL and S-VOL of a pair.

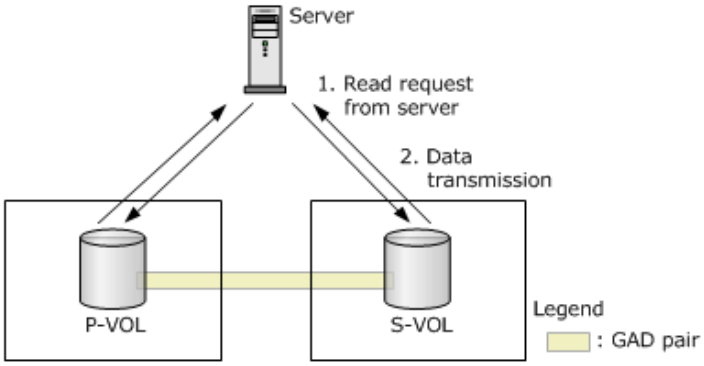
Server I/O (GAD status: Mirrored)

When the GAD status is Mirrored, the I/O mode of the P-VOL and S-VOL is Mirror (RL).

As shown in the following figure, a write request sent to a GAD volume is written to both pair volumes, and then a write-completed response is returned to the host.



Read requests are read from the volume connected to the server and then sent to the server. There is no communication between the primary and secondary storage systems.

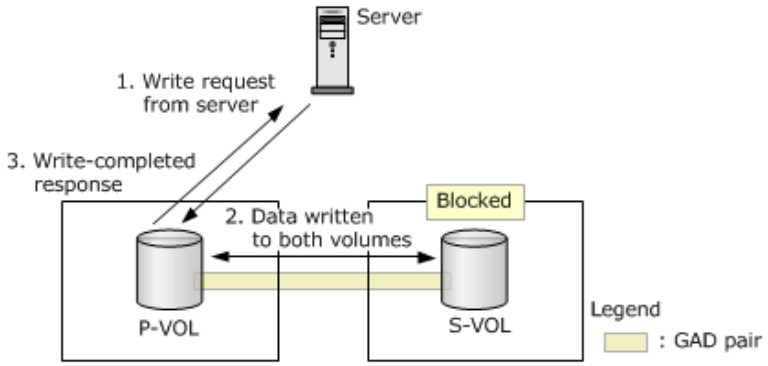


Server I/O (GAD status: Mirroring or Quorum disk blocked or no quorum disk volume)

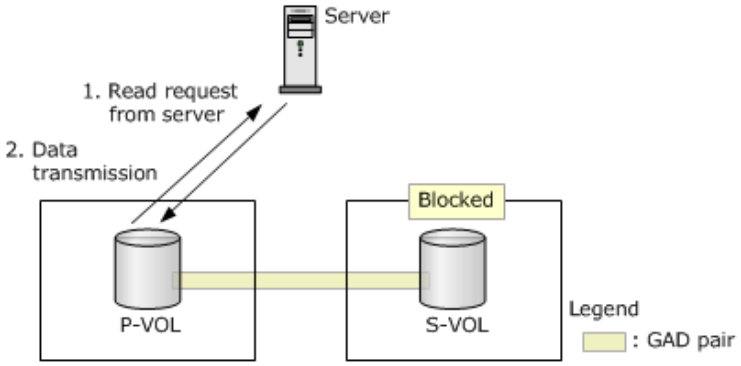
When the GAD status is Mirroring or Quorum disk blocked or no volume is set for the quorum disk, the I/O mode for the P-VOL is Mirror(RL), and the I/O mode for the S-VOL is Block. The I/O mode and the I/O flow vary depending on the microcode or firmware version.

When the GAD status is Mirroring or Quorum disk blocked or no volume is set for the quorum disk, the I/O mode for the P-VOL is Mirror(RL), and the I/O mode for the S-VOL is Mirror(RL).

Write requests are written to both pair volumes and then the write-completed response is returned to the server.



Read requests are read by the P-VOL or S-VOL and then sent to the server.



Server I/O when the GAD status is Suspended

When the GAD status is Suspended, the I/O mode differs depending on where the latest data is.

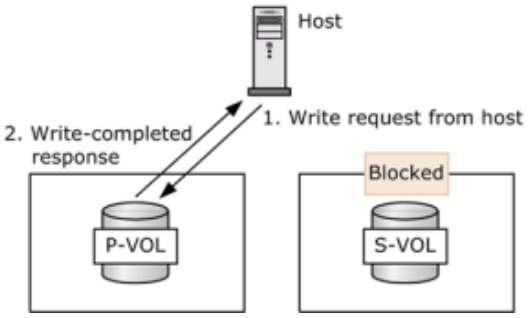
When the GAD status is Suspended and the latest data is on the P-VOL, the I/O mode is as follows:

- P-VOL: Local
- S-VOL: Block

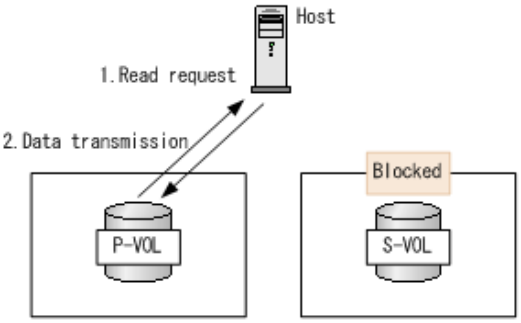
When the latest data is on the S-VOL, the I/O mode is as follows:

- P-VOL: Block
- S-VOL: Local

When the latest data is on the P-VOL, write requests are written to the P-VOL, and then the write-completed response is returned to the host, as shown in the following figure. The S-VOL's I/O mode is Block, so it does not accept I/O from the server, and the P-VOL's I/O mode is Local, so the data written to the P-VOL is not written to the S-VOL.



Read requests are read by the P-VOL and then sent to the host. There is no communication between the primary and secondary storage systems.



Server I/O when the global-active device status is Blocked

When the GAD status is Blocked, the I/O mode of the P-VOL and S-VOL is Block. Neither volume accepts read/write processing.

Quorum disk and server I/O

The quorum disk is used to determine the storage system on which server I/O should continue when a path or storage system failure occurs.

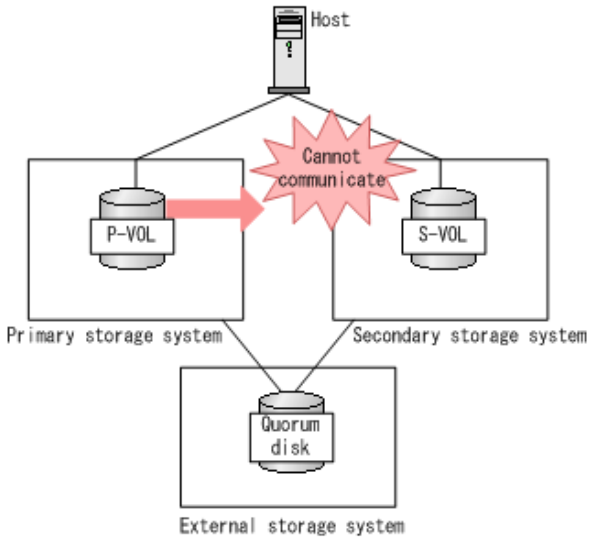
The quorum disk is a volume virtualized from an external storage system. The primary and secondary storage systems check the quorum disk for the physical path statuses. Alternatively, a disk in an iSCSI-attached server can be used as a quorum disk if the server is supported by Universal Volume Manager.

Note: The server and storage systems are connected using iSCSI.

When the primary and secondary storage systems cannot communicate, the storage systems take the following actions:

1. The primary storage system cannot communicate over the data path and writes this status to the quorum disk.
2. When the secondary storage system detects from the quorum disk that storage systems cannot communicate over the data path, it stops accepting read/write.

3. The secondary storage system communicates to the quorum disk that it cannot accept read/write.
4. When the primary storage system detects that the secondary storage system cannot accept read/write, the primary storage system suspends the pair. Read/write continues to the primary storage system.



If the primary storage system cannot detect from the quorum disk that the secondary storage system cannot accept I/O within five seconds of a communication stoppage, the primary storage system suspends the pair and I/O continues.

If both systems simultaneously write to the quorum disk that communication has stopped, this communication stoppage is considered to be written by the system with the smaller serial number.

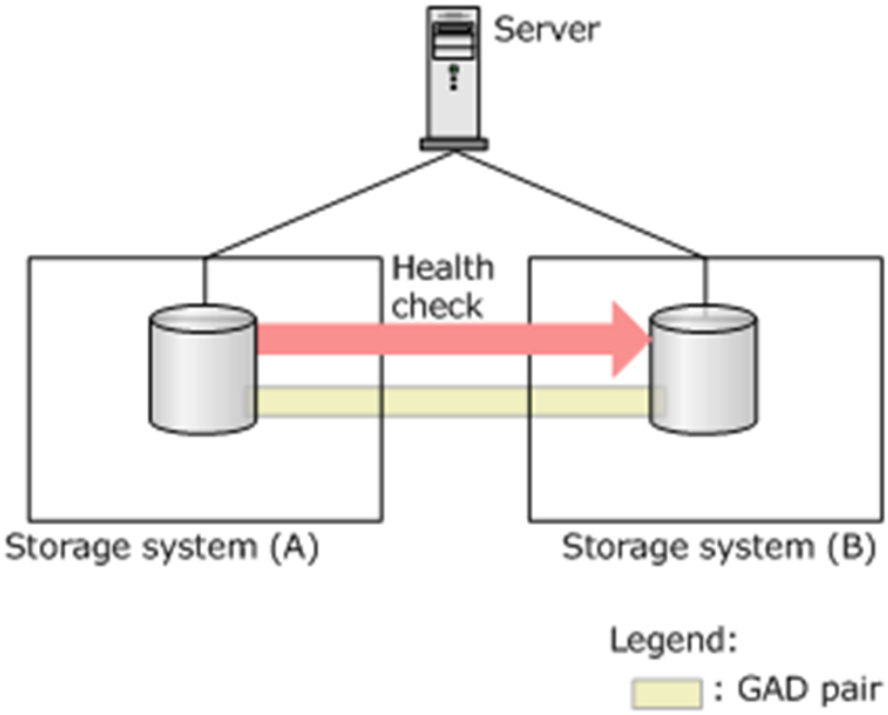
In addition, you can create a GAD pair without setting a volume in an external storage system as the quorum disk volume.

High availability pairs without a volume set for the quorum disk

For VSP E series and VSP G/F350, G/F370, G/F700, G/F900 storage systems, an external storage system is required to use a quorum disk. Because of this, if you need a temporary GAD pair to migrate data, you must set up an external storage system. A quorum disk on an external storage system is no longer required for data migration.

If you do not set a volume for the quorum disk, you can create GAD pairs without using an external storage system.

In this configuration, I/Os from the server might stop if a failure occurs in a path or a storage system. Therefore, determine whether to set a volume using an external volume for the quorum disk or not according to the requirements of your planned usage. The following figure illustrates the configuration without a volume set for the quorum disk.



The GAD configuration without a volume set for the quorum disk supports migrating data for the following:

- From a VSP G1x00 storage system to another VSP G1x00.
- From a VSP G200, G/F400, G/F600, G/F800 storage system to a VSP 5000 series.
- From a VSP G1x00, F1500 storage system to a VSP G/F350, G/F370, G/F700, G/F900.
- From a VSP G200, G/F400, G/F600, G/F800 storage system to a VSP G/F350, G/F370, G/F700, G/F900.
- From a VSP G/F350, G/F370, G/F700, G/F900 storage system to another VSP G/F350, G/F370, G/F700, G/F900.
- From a VSP E series storage system to another VSP E series

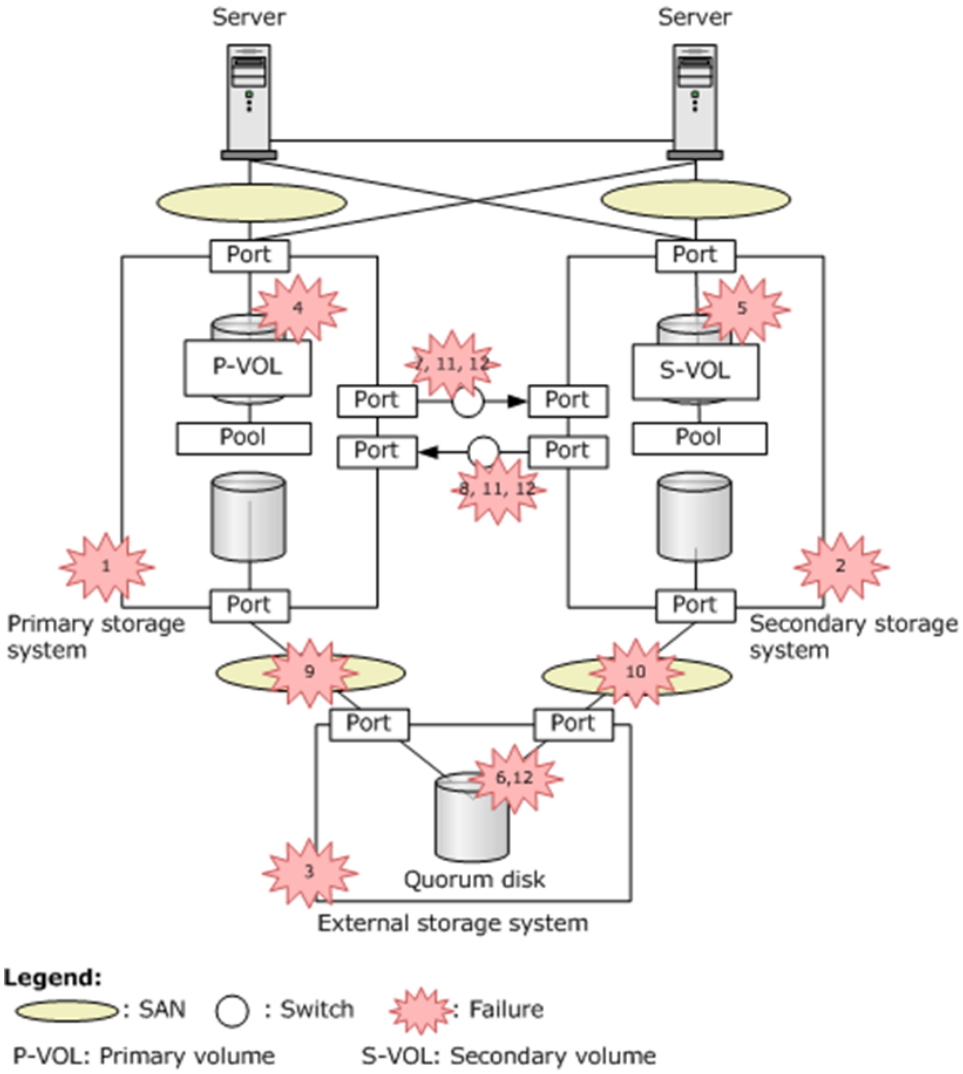
When you do not set a volume for a quorum disk, you do not need the following components and steps:

- External storage system
- External port between storage systems (A) and (B)
- Path and a switch between storage system (A) and the external storage system
- Path and a switch between storage system (B) and the external storage system

The following describes the differences between the configuration with a volume set for the quorum disk and the configuration without a volume set for the quorum disk.

As shown in the following figure and table, if a failure occurs in the primary storage system when an external storage system is not used for the quorum disk, the process stops. Because this failure can occur, you should use the configuration that does not set volumes for the quorum disk temporarily for migrating data (VSP E series and VSP G/F350, G/F370, G/F700, G/F900). If the process is not allowed to stop due to a failure in the primary storage system, create a configuration with a volume set for the quorum disk (VSP 5000 series and VSP G1x00, F1500).

The figure shows failure points and the table describes whether the process stops or not according to the location in which the failure occurred.



Number in the figure	Failure location	Operation	
		With volumes set for quorum disks	**Without volumes set for quorum disks**
1	Primary storage system	Continues	Stops
2	Secondary storage system	Continues	Continues
3	External storage system	Continues	Not applicable
4	Primary volume	Continues	Continues
5	Secondary volume	Continues	Continues
6	Quorum disk	Continues	Not applicable
7	Remote path from the primary storage system to the secondary storage system	Continues	Continues
8	Remote path from the secondary storage system to the primary storage system	Continues	Continues
9	Path between the primary storage system and the quorum disk	Continues	Not applicable
10	Path between the secondary storage system and the quorum disk	Continues	Not applicable
11	When the failures occur at the same time in the following locations: ▪ Remote path from the primary storage system to the secondary storage system ▪ Remote path from the secondary storage system to the primary storage system	Continues	Continues
12	When the failures occur at the same time in the following locations: ▪ Remote path from the primary storage system to the secondary storage system ▪ Remote path from the secondary storage system to the primary storage system ▪ Quorum disk	Stops	Not applicable

Cost

A second difference between the configuration with a volume set for the quorum disk and the configuration without a volume set for the quorum disk is cost. If you do not set a volume for the quorum disk, you can save the preparation cost because you do not need an external storage system and the path. Also, some steps for configuring the GAD environment are not necessary.

I/O stoppage detected in the counterpart system

When a stoppage is detected within 5 seconds in the counterpart system, the pair volume that will continue to receive read/write after the stoppage is determined based on the pair status.

- When the pair status is PAIR, read/write continues to the volume that wrote the communication stoppage to the quorum disk.
- When the pair status is INIT/COPY, read/write continues to the P-VOL. Read/write to the S-VOL remains stopped.
- When the pair status is PSUS, PSUE, SSWS, or SSUS, read/write continues to the volume whose I/O mode is Local. Read/write is stopped to the volume whose I/O mode is Block.

I/O stoppage not detected in the counterpart system

When a stoppage is not detected within 5 seconds in the counterpart system, the pair volume whose system wrote the communication stoppage to the quorum disk will continue to receive read/write after the stoppage.

Read/write processing depends on the pair status and I/O mode of the volume that did not detect the write as follows:

- When the pair status is PAIR, read/write continues.
- When the pair status is INIT/COPY, read/write continues to the P-VOL.

  Read/write to the S-VOL remains stopped.
- When the pair status is PSUS, PSUE, SSWS, or SSUS, read/write continues to the volume whose I/O mode is Local.

  Read/write is stopped to the volume whose I/O mode is Block. In addition, server I/O does not continue to the volume that should have notified the quorum disk that it cannot accept I/O, because either a storage system failure occurred or the quorum disk is no longer accessible.

Server I/Os and data mirroring with blocked quorum disk or without quorum disk volumes

You should understand the server I/Os and data mirroring that occur when a failure occurs on the quorum disk or when no volume is set for the quorum disk.

GAD pairs that meet the following requirements can continue operation using the S-VOL if the P-VOL is blocked:

- The option for setting no LDEVs for the quorum disk is enabled when the quorum disk is created.
- The pair is created using the quorum ID assigned when the quorum disk is created.

If the quorum disk is blocked, GAD pairs can keep the same data in the P-VOL and S-VOL, but the operation stops if the P-VOL is blocked. To continue the operation, you must delete the GAD pair.

Server I/Os for GAD pairs and GAD pair data mirrorings

Server I/Os for GAD pair and GAD pair data mirroring are as follows:

- **When the quorum disk is blocked and the pair status is PAIR or when no volume is set for the quorum disk and the pair status is PAIR** The primary and secondary storage systems communicate through remote paths. Because the P-VOL and S-VOL pair status and the I/O mode remain PAIR (Mirror(RL)), server I/Os continue in the PVOL and the S-VOL. Data mirroring can be maintained through remote paths between the primary and secondary storage systems.
- **When the quorum disk is blocked and the pair status is INIT/COPY Server** I/Os continue in the P-VOL; however, that the pair might be suspended if the quorum disk is blocked immediately after the pair status changes to COPY.
- When no volume is set for the quorum disk and the pair status is INIT/COPY Server I/Os continue in the P-VOL.
- **When the pair is suspended (pair status is PSUS, PSUE, SSWS, or SSUS) and the quorum disk is blocked or when the pair is suspended and no volume is set for the quorum disk** Server I/Os continue in the volume with Local I/O mode. I/Os to the volume with Block I/O mode remain stopped, and data mirroring remains suspended.
- **When the remote paths are disconnected after the quorum disk is blocked or when the remote paths are disconnected and no volume is set for the quorum disk** after the quorum disk is blocked, the pair is suspended when the remote paths are disconnected or if no volume is set for the quorum disk. The P-VOL status and the I/O mode change to PSUE (Local), and the S-VOL status and the I/O mode change to PAIR (Block). Server I/Os continue in the P-VOL. The pair might be suspended and the status and the I/O mode of the P-VOL and the S-VOL might change to PSUE (Block) depending on the timing of the remote path disconnection after the quorum disk is blocked or if no volume is set for the quorum disk.

Before the pair status of the S-VOL and the I/O mode change to PAIR (Block), reading data might be delayed. If you want to minimize the delay, set a smaller value for Read Response Guaranteed Time When Quorum Monitoring Stopped. The time between the remote path disconnection and the pair suspension is also shortened.

When you want to restore the remote path quickly and do not want to suspend pairs immediately after the remote path is disconnected, set a larger value for Read Response Guaranteed Time When Quorum Monitoring Stopped. If you set a value larger than the server timeout time, a timeout might occur on the server.

The following table lists the recommended values for Read Response Guaranteed Time When Quorum Monitoring Stopped.

Setting value for Blocked Path Monitoring (sec)	Recommended setting value for Read Response Guaranteed Time When Quorum Monitoring Stopped
40 (Default)	40 (Default)
2 to 5	5*
6 to 25	6 to 25*
26 to 44	26 to 44
45	45
* A GAD pair might be suspended if remote path communication is blocked temporarily due to an MP or path failure. To avoid this, a value which is greater than the RIO MIH time or at least 25 seconds must be set for Read Response Guaranteed Time When Quorum Monitoring Stopped. Note, however, that reading data might delay up to the time set for Read Response Guaranteed Time When Quorum Monitoring Stopped.	

Setting the same value as the blocked path monitoring for Read Response Guaranteed Time When Quorum Monitoring Stopped is recommended. Until the pair status and I/O mode of the S-VOL change to PSUE (Block), delay of reading data can be maintained within the seconds set for Read Response Guaranteed Time When Quorum Monitoring Stopped. Note that if a value equal to or less than 5 seconds is set for the blocked path monitoring, you must set 5 for Read Response Guaranteed Time When Quorum Monitoring Stopped.

If a value equal to or greater than 46 seconds is set for Read Response Guaranteed Time When Quorum Monitoring Stopped, GAD pair suspension caused by a remote path failure might be avoided. When you set a value of 46 or a greater, make sure that the application timeout setting for server I/Os is greater than this value. Also, make sure that multiple remote paths are set (at least four paths are recommended). Reading data might be delayed until the time set for Read Response Guaranteed Time When Quorum Monitoring Stopped elapses.

Quorum disk status

You need to check the status of the quorum disk before you replace the external storage system currently used by the quorum disk while you keep GAD pairs.

You can check the quorum disk status using the **`raidcom get quorum`** command. For details, see the *Command Control Interface Command Reference*.

You can replace the external storage system currently used by the quorum disk with a new external storage system while keeping GAD pairs.

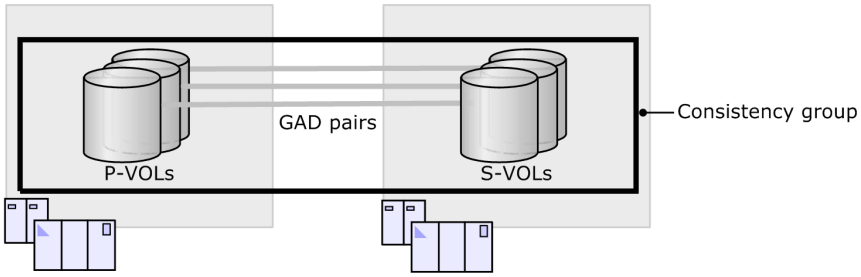
There are five statuses for the quorum disk.

Quorum disk status	Display by CCI	Description
Normal	NORMAL	The quorum disk is operating normally.
Transitioning	TRANSITIONING	The status of the quorum disk is being changed.
Blocked	BLOCKED	The quorum disk is blocked.
Replacing	REPLACING	The quorum disk is being replaced.
Failed	FAILED	The primary and secondary storage systems are connected to different quorum disks. Specify the external volume again, so that they can be connected to the same quorum disk, and reconfigure the quorum disk.
- (Hyphen)	- (Hyphen)	No volume is set for the quorum disk.

Global-active device consistency groups

You can manage multiple GAD pairs as a group by using consistency groups.

The GAD pairs in a GAD 3DC delta resync (GAD+UR) configuration must be registered to a consistency group.



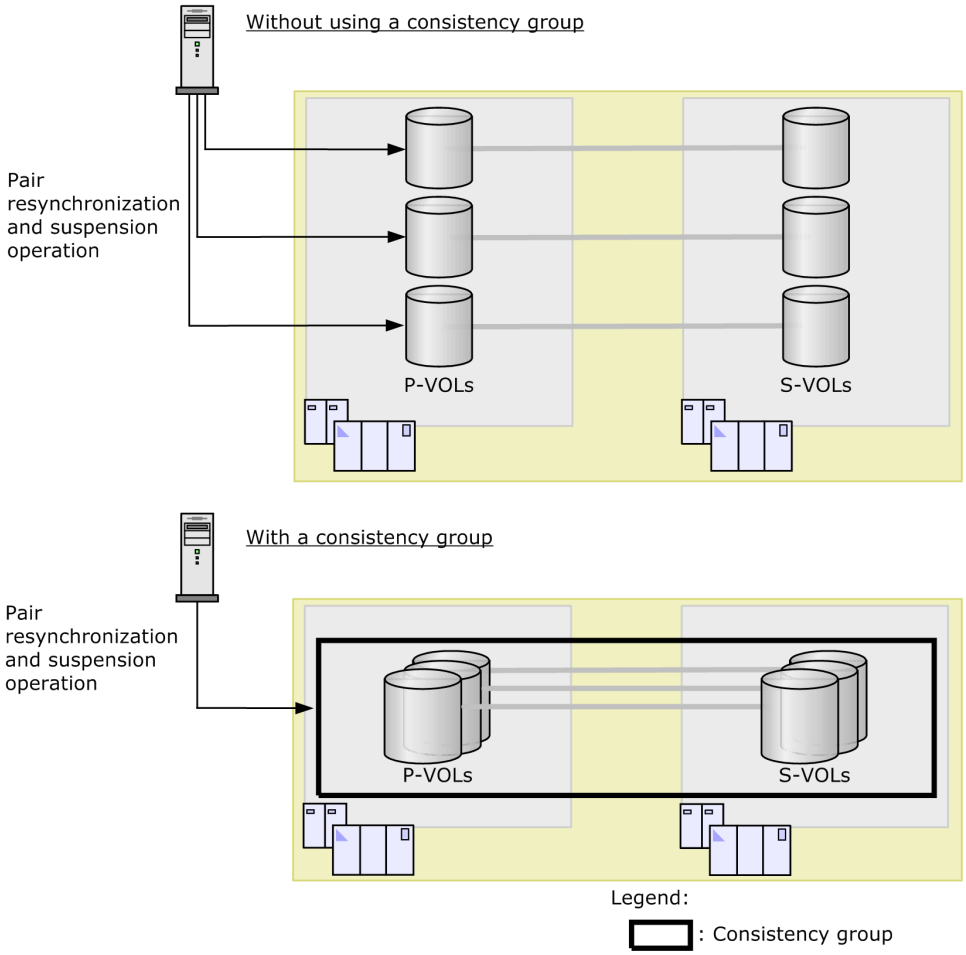
Registering GAD pairs to consistency groups enables you to perform operations on all GAD pairs in a consistency group at the same time. In addition, when a failure occurs, the GAD pairs are suspended by consistency group (concurrent suspension).

For details about storage system support (microcode) for consistency groups, see Requirements and restrictions (on page 44).

> **Note:** When you register GAD pairs to a consistency group, use the cross-path configuration. For details, see System configuration for global-active device solutions (on page 17).

Global-active device pairs by consistency group

By registering multiple GAD pairs to a consistency group, you can resynchronize or suspend the GAD pairs by consistency group. You can resynchronize all GAD pairs registered to a consistency group by running a single pair resynchronization. In addition, you can suspend all GAD pairs registered to a consistency group by running a single pair suspension.



For details about storage system support (microcode) for consistency groups, see Requirements and restrictions (on page 44).

Suspension of GAD pairs by consistency group

When a failure occurs, suspension of GAD pairs by consistency group guarantees data consistency among primary volumes if the I/O mode of a primary volume changes to Block, or among secondary volumes if the I/O mode of a secondary volume changes to Block.

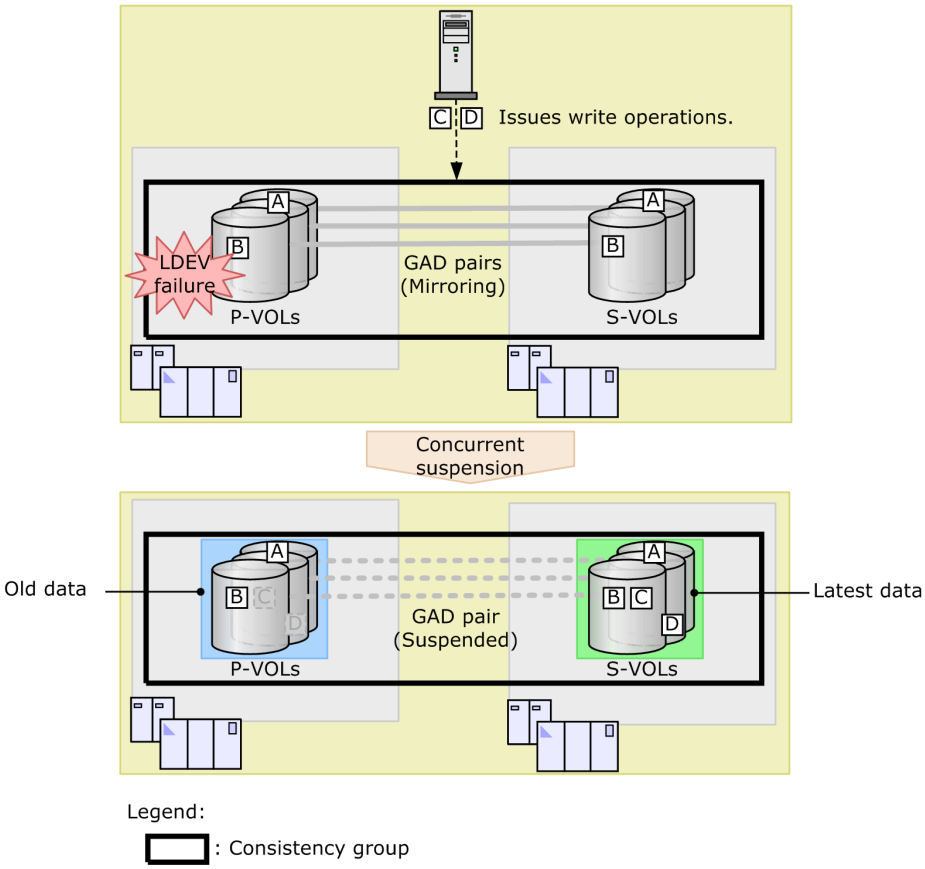
If some GAD pairs in a consistency group are suspended due to a failure, all GAD pairs in the consistency group to which the suspended GAD pairs are registered change to the suspended state. This is called concurrent suspension.

- The volumes that have the most recent data are aggregated to a single storage system.

  If a failure occurs in some pairs, and all GAD pairs registered to a consistency group are in the Suspended state, the volumes that have the most recent data are aggregated to the storage system at either the primary site or the secondary site.

- Data consistency is guaranteed before and after the suspension of the GAD pairs.

  If all GAD pairs registered to a consistency group are in the Suspended state, only the volumes (of either the primary or the secondary site) that have the most recent data will receive I/O from the server. The volumes of the other site will stop receiving I/O from the server (including I/O for volumes where no failure occurred). In addition, processing to write data will also stop. This ensures data consistency before and after the GAD pair suspension in the volumes that stopped receiving I/O from the server.



For example, a server issues write operations A to D. After the storage system receives write operation B, all GAD pairs registered to the consistency group change to the Suspended state because of an LDEV failure in the primary volume. In such a case, write operations A and B received before the GAD pairs changed to the Suspended state were completed for both the primary and secondary volume. Write operations C and D received after the GAD pairs changed to the Suspended state were completed only for the secondary volume.

Therefore, the volumes that have the most recent data are aggregated to the storage system at the secondary site.

For details about storage system support (microcode) for consistency groups, see Requirements and restrictions (on page 44).

Use cases for consistency groups

You can use GAD consistency groups for many use cases, for example, batch failover or resuming operations by using consistent backup data.

High Availability consistency group statuses

You can view the status of a consistency group by using Device Manager - Storage Navigator.

The following table describes the statuses of GAD consistency groups.

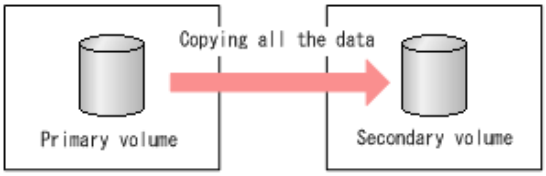
Status	Description
SMPL	All volumes in the consistency group are not used as GAD pair volumes.
INIT/COPY	The initial copy or pair resynchronization of all GAD pairs in the consistency group is in progress (including creation of a GAD pair that does not perform data copy). A quorum disk is being prepared.
COPY	The initial copy of all GAD pairs in the consistency group is in progress; data is being copied from the P-VOL to the S-VOL (including creation of a GAD pair that does not perform data copy).
PAIR	All GAD pairs in the consistency group are synchronized, including pairs whose quorum disk is blocked. The data is duplicated.
PSUS	All GAD pairs in the consistency group were suspended by the user. This status appears when the volumes in the consistency group on the local storage system are P-VOLs.
PSUE	All GAD pairs in the consistency group were suspended due to a failure.
SSUS	All GAD pairs in the consistency group were suspended by the user, and update of the S-VOL is interrupted. This status appears when the volumes in the consistency group on the local storage system are S-VOLs.
SSWS	All GAD pairs in the consistency group were suspended either by the user or due to a failure, and update of the P-VOL is interrupted. This status appears when the volumes in the consistency group on the local storage system are S-VOLs.
Suspending	GAD pair suspension processing is being performed by consistency group.
Resynchronizing	GAD pair resynchronization processing is being performed by consistency group.

Status	Description
Mixed	More than one pair status exists in the consistency group.
Unknown	The consistency group status cannot be obtained.
Blank	The consistency group is not used.

Initial copy and differential copy

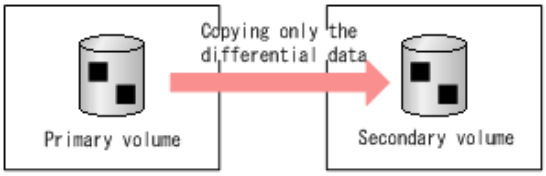
There are two types of GAD copy operations that synchronize the data on the P-VOL and S-VOL of a pair, initial copy and differential copy.

For an initial copy operation, all data in the P-VOL is copied to the S-VOL, which ensures that the data in the two volumes is consistent. The initial copy is run when the GAD status changes from Simplex to Mirrored.



For a differential copy operation, only the differential data between the P-VOL and the S-VOL is copied. Differential copy is used when the GAD status changes from Suspended to Mirrored.

When a GAD pair is suspended, the storage systems record the update locations and manage the differential data. The following figure shows the differential copy operation for a pair in which the P-VOL received server I/O while the pair was suspended. If the S-VOL receives server I/O while a pair is suspended, the differential data is copied from the S-VOL to the P-VOL.



User interfaces for global-active device operations

Global-active device operations are performed using the management software and optionally, the command-line interface (CLI) software for the storage system.

Storage Advisor Embedded

You use Storage Advisor Embedded to configure the remote paths and the quorum disk required when using global-active device for VSP E series and VSP F350, F370, F700, F900 storage systems with firmware 88-03-0x or later. You must configure these settings on the primary and secondary storage systems in the global-active device environment.

Storage Navigator

You can perform many, but not all, global-active device operations using the Storage Navigator (SN) software. Disaster recovery procedures are performed using the Command Line Interface (CCI) and cannot be performed using Storage Navigator.

Ops Center Administrator

Use Ops Center Administrator to configure and manage virtual storage machine (VSM), GAD pairs, and monitor and manage your global-active device environment.

Ops Center Protector

Use Ops Center Protector to perform pair operations in a global-active device environment.

Chapter 2: System requirements

You should understand all requirements and restrictions for global-active device.

Requirements and restrictions

The following table lists the requirements and restrictions for global-active device.

Item	Requirements and restrictions
Primary and secondary storage systems	▪ Model: The following information is current as of the publish date. See the TC, UR, GAD ▪ Global-active device license: The global-active device feature must be installed and enabled on the primary and secondary storage systems. ▪ Controller emulation type: The controller emulation type of the primary and secondary storage systems must be same. ▪ Shared memory: VSP E series and VSP G/F350, G/F370, G/F700, G/F900: You can use GAD only with shared memory in the basic part. Adding shared memory expands the capacity of the pairs being created.
GAD 3DC delta resync (GAD+UR)	▪ All storage systems in a GAD+UR configuration must be VSP 5000 series. Microcode: DKCMAIN version 90-01-00 or later ▪ 3DC delta resync in a GAD+UR configuration is supported only for VSP 5000 series, VSP E series, and VSP G/F350, G/F370, G/F700, G/F900.
External storage systems or servers (for quorum disk)	▪ The storage system or server must be supported for attachment using Universal Volume Manager. The server must be attached using iSCSI. For details, see the *Hitachi Universal Volume Manager User Guide* for the storage system. ▪ The maximum distance between the external storage system and the primary site and secondary site is 1,500 km.

Item	Requirements and restrictions
Licensed capacity	▪ The page size assigned to the virtual volume is counted as a licensed capacity for GAD; however, for a volume with capacity saving enabled, the GAD licensed capacity is the capacity before savings. ▪ If the actual licensed capacity exceeds the available licensed capacity, GAD can be used as usual for 30 days. After 30 days, only pair split and pair delete operations are allowed.
Host server platforms	▪ AIX ▪ HP-UX ▪ OpenVMS ▪ Red Hat Enterprise Linux ▪ Solaris ▪ SuSE Linux ▪ VMware ESX ▪ Windows Server
Maximum number of storage systems that can be connected	One storage system can create pairs with a maximum of 15 storage systems.
SCSI commands	▪ The Dynamic Provisioning function of Windows Server 2012 is supported. ▪ The SCSI-2 Reserve command, the SCSI-3 Persistent Reserve command, and the VAAI command are supported. ▪ The reservation information is duplicated when the Reserve command or the Persistent Reserve command is received, or when the initial copy or resync copy starts.
Physical paths connecting the primary and secondary storage systems	▪ Maximum number of physical paths: 8 ▪ Maximum distance between the primary and secondary storage systems: 500 km

Item	Requirements and restrictions
	▪ The maximum value of the round-trip delay, including the delay due to the failure of an interface device, is 20 ms. However, you must meet the following conditions to connect storage systems over the distance of 100 km or more. • The primary and secondary storage systems are connected by Fibre Channel interfaces. • The DKCMAIN microcode version of the primary and secondary storage systems is 80-04-21-00/00 or later for VSP 5000 series and VSP G1x00, F1500. • The line speed between the primary and secondary storage systems is 1 Gbps or more. • The host mode option 51 is set to ON. ▪ Port type: Fibre Channel, iSCSI (VSP 5000 series 80-03-3*x* and later) with direct, switch, or channel extenders. For details, see Connection types (on page 91).
Remote paths and path groups	▪ Maximum number of remote paths per path group: 8 ▪ Maximum number of path groups per storage system: 64 (sum of the path groups used by TC, UR, and URz) ▪ Path group ID: 0-255. ▪ Protocol: All remote paths in a path group must be the same protocol, either Fibre Channel or iSCSI. Remote paths for Fibre Channel and iSCSI cannot coexist within the same path group. ▪ If iSCSI is used in a remote path, the blocked path monitoring remote replica option must be set to at least 40 seconds (default). If blocked path monitoring is less than 40 seconds, the path might be blocked due to a delay in the network such as many switches in a spanning tree protocol (STP) network or a long distance connection. ▪ The path group is specified during the create pair operation and cannot be changed by resynchronization.

Item	Requirements and restrictions
	▪ The remote path must be set by each path group of the storage systems at the primary site and the secondary site. You can also use multiple path groups with the same combination of the storage systems at the primary and the secondary sites. ▪ When using the System connection type and not the CU connection type (specified on the Add Remote Connection window), specify different paths and path groups for TrueCopy, Universal Replicator, and Universal Replicator for Mainframe secondary storage systems.
Virtual storage machines (VSMs)	▪ Maximum number of VSMs per storage system: 15 • VSP 5000 series, VSP E series, and VSP G1x00, F1500: 15 • VSP G/F350, G/F370, G/F700, G/F900: 7 ▪ Maximum number of GAD volumes per VSM: 65,280 • VSP 5000 series, VSP G1x00, VSP F1500, VSP G/F900, VSP E990: 65,280 • VSP G/F350: 16,384 • VSP G/F370: 32,768 • VSP G/F700: 49,152 • VSP E590, VSP E590H: 32,768 • VSP E790, VSP E790H: 49,152 ▪ You can create GAD pairs using volumes in virtual storage machines. When you want to create a GAD pair using volumes in VSMs, the VSM for the volume in the secondary site must have the same model and serial number as the VSM for the volume in the primary site. ▪ For VSP G200, G/F400, G/F600, G/F800, VSP G/F350, G/F370, G/F700, G/F900 when a resource group (virtual storage machine) in a storage system at the secondary site has the same virtual LDEV ID as the P-VOL, you cannot create a GAD pair. In addition, when a volume is not created and only LDEV IDs exist, virtual LDEV IDs must be deleted.

Item	Requirements and restrictions
Resource groups (VSP G1000, VSP G1500, VSP F1500)	▪ DKCMAIN 80-02-*xx* or later: You can use a volume in a resource group that was migrated from a VSP or USP V/VM storage system to a VSP G1x00, F1500 as a GAD volume. ▪ DKCMAIN 80-01-*xx* or earlier: You cannot use a volume in a resource group that was migrated from a VSP or USP V/VM storage system to a VSP G1x00, F1500 as a GAD volume.
Maximum number of GAD pairs	▪ When all pairs are created with DP-VOLs and external volumes (calculated by subtracting the number of quorum disks (at least one) from the maximum number of virtual volumes that can be defined in a storage system): • VSP 5000 series, VSP E series, VSP G1x00, F1500 and VSP G/F900 : 63,231 • VSP G/F350: 16,382 • VSP G/F370: 32,766 • VSP G/F700: 49,150 ▪ When CCI is used in the in-band method and all pairs are created with DP-VOLs or external volumes, and one virtual volume or external volume is used as a command device, and a volume is set for the quorum disk: • VSP 5000 series, VSP E series, VSP G1x00, F1500 and VSP G/F900 : 63,231 • VSP G/F350: 16,382 • VSP G/F370: 32,766 • VSP G/F700: 49,150 ▪ When CCI is used in the in-band method and all pairs are created with DP-VOLs or external volumes, one normal volume (VSP F400, F600, F800, VSP G200, VSP G400, G600, G800, VSP G/F350, G/F370, G/F700, G/F900) or internal volume (VSP 5000 series) is used as a command device, and a volume is set for the quorum disk: 63,231 • VSP 5000 series, VSP E series, VSP G1x00, F1500 and VSP G/F900 : 63,231 • VSP G/F350: 16,382 • VSP G/F370: 32,766 • VSP G/F700: 49,150

Item	Requirements and restrictions
	▪ When CCI is used in the in-band method and all pairs are created with DP-VOLs or external volumes, one virtual volume (DP-VOL) or external volume is used as a command device, and no volume is set for the quorum disk: VSP G1x00, 1500 : 63,231 ▪ When CCI is used in the in-band method and all pairs are created with DP-VOLs or external volumes, one internal volume is used as a command device, and no volume is set for the quorum disk: VSP G1x00, F1500: 63,232 ▪ When all pairs are created with internal volumes (calculated by subtracting the number of quorum disks (at least one) from the maximum number of internal volumes that can be defined in a storage system): • VSP 5000 series, VSP E series, VSP G1x00, F1500 and VSP G/F900 : 65,279 • VSP G/F350: 16,383 • VSP G/F370: 32,767 • VSP G/F700: 49,151 ▪ When all pairs are created with internal volumes, and no volume is set for the quorum disk, the maximum number of GAD pairs: VSP G1x00, F1500: 65,280 ▪ When CCI is used in the in-band method and all pairs are created with internal volumes, and one virtual volume or external volume for VSP 5000 series, VSP G1x00, F1500 is used as a command device, and a volume is set for the quorum disk: • VSP 5000 series, VSP E series, VSP G1x00, F1500 and VSP G/F900 : 65,277 • VSP G/F350: 16,381 • VSP G/F370: 32,767 • VSP G/F700: 49,149

Item	Requirements and restrictions
	▪ When CCI is used in the in-band method and all pairs are created with internal volumes, and one normal volume (VSP G200, G/F400, G/F600, G/F800, VSP G/F350, G/F370, G/F700, G/F900) or internal volume (VSP 5000 series) is used as a command device, and a volume is set for the quorum disk: • VSP 5000 series, VSP E series, VSP G1x00, F1500 and VSP G/F900: 65,278 • VSP G/F350: 16,382 • VSP G/F370: 32,766 • VSP G/F700: 49,150 ▪ When CCI is used in the in-band method and all pairs are created with internal volumes, and one virtual volume or external volume for VSP 5000 series or VSP G1x00, F1500 is used as a command device, and no volume is set for the quorum disk: VSP G1x00, F1500 : 65,278 ▪ When CCI is used in the in-band method and all pairs are created with internal volumes, and one normal volume (VSP G200, G/F400, G/F600, G/F800, VSP G/F350, G/F370, G/F700, G/F900) or internal volume VSP 5000 series is used as a command device, and no volume is set for the quorum disk: VSP G1x00, F1500 : 65,279 ▪ Virtual storage machine: same as the maximum number of pairs for the storage system model.
Pair volumes	▪ Provisioning type: The following provisioning types are supported for the GAD pair volumes. The provisioning type of the P-VOL and S-VOL must be same. For example, if the P-VOL is a DP-VOL, the S-VOL must also be a DP-VOL. • Dynamic Provisioning virtual volumes (DP-VOLs) For DP-VOLs, you can only create a GAD pair when both DP-VOLs do not have the Data Direct Mapping attribute or when both DP-VOLs have the Data Direct Mapping attribute. You cannot create a GAD pair when the Data Direct Mapping attribute is enabled for one DP-VOL but not for the other. • Internal volumes • External volumes ▪ Emulation type: OPEN-V. ▪ Volume size: The P-VOL and S-VOL must be equal in size.

Item	Requirements and restrictions
	▪ Maximum volume size: VSP 5000 series, VSP G1x00, F1500 DP-VOL: same as the maximum size of a DP-VOL. For details, see the *Provisioning Guide* for the storage system. • Internal volume: 3,145,663 MB (6,442,317,824 blocks) • External volume: 4,194,304 MB (8,589,934,592 blocks) (VSP E series, VSP G/F350, G/F370, G/F700, G/F900) • Internal volume: 256 TB • External volume: 256 TB ▪ SAN boot: You can use GAD pair volumes for SAN boot. ▪ Virtual LDEV ID: The same virtual LDEV ID as the P-VOL must not exist in the resource group of the secondary storage system (virtual storage machine). You cannot create a GAD pair when the same virtual LDEV ID as the P-VOL exists in the resource group of the secondary storage system (virtual storage machine). To use the P-VOL, you must delete the virtual LDEV ID in the resource group of the secondary storage system. You must delete the virtual LDEV ID even if the volume is not created and only the LDEV ID exists. ▪ T10 PI: The same value must be set for the T10 PI attribute of the P-VOL and the S-VOL. ▪ A volume (LDEV) from a parity group with accelerated compression enabled cannot be used directly as a GAD pair volume. Such volumes must be used as pool volumes for an HDP or HDT pool.
Quorum disks	▪ Maximum number of quorum disks: 32 per storage system in the primary storage system and secondary storage system. ▪ Quorum disk ID: Specify a value from 0 to 31.

Item	Requirements and restrictions
	▪ Maximum number of pairs per quorum disk: • VSP 5000 series, VSP G1x00, F1500 : 63,231 when you create all pairs with DP-VOLs or external volumes, and 65,279 when you create all pairs with internal volumes. • VSP G150, VSP G/F350: 16,382 when you create all pairs with DP-VOLs or external volumes, and 16,383 when you create all pairs with internal volumes. • VSP G/F370: 32,766 when you create all pairs with DP-VOLs or external volumes, and 32,767 when you create all pairs with internal volumes. • VSP G/F700: 49,150 when you create all pairs with DP-VOLs or external volumes, and 49,151 when you create all pairs with internal volumes. • VSP G/F900: 63,232 when you create all pairs with DP-VOLs or external volumes, and 65,279 when you create all pairs with internal volumes. • VSP E series 63,232 when you create all pairs with DP-VOLs or external volumes, and 65,279 when you create all pairs with internal volumes. ▪ Emulation type: VSP 5000 series, VSP E series, VSP G1x00, F1500: OPEN-V ▪ Minimum size: 12,292 MB (25,174,016 blocks) ▪ Maximum size: same as the maximum limit for an external volume supported by Universal Volume Manager: 4 TB. ▪ In addition to a volume in an external storage system, a disk in an iSCSI-attached server can be used as a quorum disk if the server is supported by Universal Volume Manager. **Note:** The server and storage systems are connected using iSCSI. See the *Hitachi Universal Volume Manager User Guide* for details. ▪ One external volume group must be mapped to one external volume. ▪ Interoperability: A GAD quorum disk cannot also be used as a quorum disk with High Availability Manager for VSP, HUS VM, and USP V/VM.

Item	Requirements and restrictions
	▪ Requirements for the external storage system volume: • The T10 PI attribute must not be enabled. • The Data Direct Mapping attribute must not be set. ▪ The maximum number of GAD groups that are allowed for a quorum disk is 1,024 (VSP 5000 series, VSP G1x00, F1500).
Consistency groups	▪ Maximum number of consistency groups per storage system: • VSP 5000 series: 1,024 (CTG ID 0-1023) • VSP E series, VSP G/F900: 256 (CTG ID 0-255) • VSP G/F350, G/F370, G/F700, G/F900: 128 (CTG ID 0-127) • VSP G1x00, F1500 ▪ Maximum number of GAD pairs per consistency group: • VSP 5000 series , VSP E series, VSP G1x00, F1500 : 8,192 • VSP G/F350, G/F370, G/F700, G/F900: 8,192 When different storage system models are connected, the smaller maximum number is applied (for example, the maximum is 128 when VSP G350 and VSP G900 are connected). ▪ Quorum disk ID: The same quorum disk ID must be set for all GAD pairs in a single consistency group. ▪ VSM: GAD pairs in the same consistency group must be created on the same virtual storage machine. ▪ CTG ID: If consistency groups have the same ID but their physical storage systems are different, they are treated as different consistency groups. You can use the same consistency group ID for groups on different storage systems.
Alternate path software	Alternate path software is required for the single-server GAD configuration and the cross-path GAD configuration (two servers). When ALUA is used in the cross-path configuration, use the same models at both the primary and secondary sites. Refer to the Hitachi Vantara interoperability matrix: https://support.hitachivantara.com/en_us/interoperability.html
Cluster software	Cluster software is required for the server-cluster and cross-path GAD configurations.

Item	Requirements and restrictions
	Refer to the Hitachi Vantara interoperability matrix: https://support.hitachivantara.com/en_us/interoperability.html
User interfaces	▪ Storage Advisor Embedded: For VSP E series, VSP G/F350, G/F370, G/F700, G/F900: firmware 88-03-0x or later, use Storage Advisor Embedded to configure the remote paths and the quorum disk required for using global-active device. These settings must be configured on the primary and secondary storage systems in the global-active device environment. ▪ Device Manager - Storage Navigator: Device Manager - Storage Navigator must be connected to the primary and secondary storage systems. ▪ Command Control Interface: version 01.32.00 or later. • VSP 5000 series, VSP G1x00, F1500: 01-32-03/00 or later • VSP E series: 01-53-03/xx or later • VSP G/F350, G/F370, G/F700, G/F900: 01-45-03/02 or later CCI must be installed on the host connected to the primary and secondary storage systems. The CCI command device is required on the primary and secondary storage systems. ▪ Ops Center Administrator Use Ops Center Administrator to configure and manage virtual storage machine (VSM), GAD pairs, and monitor and manage your global-active device environment. ▪ Ops Center Protector Use Ops Center Protector to perform pair operations in a global-active device environment.
LU number	LU number: 0 to 4095. ▪ The number of LU paths that can be created can be up to 4096 for VSP 5000 series, VSP G1x00, F1500 with a DKCMAIN program version of 90-02-0x-xx/xx or later. ▪ The number of LU paths that can be created when connecting a VSP 5000 series, VSP G1x00, F1500 with an earlier DKCMAIN program version is limited to 2048. ▪ The number of LU paths that can be created when connecting a different source storage system is limited to 2048.

Interoperability requirements

Before implementing global-active device (GAD) in your environment, it is important to understand how GAD functions with other features of your storage systems. It is possible that volume types that are used for features other than GAD can be used as GAD P-VOL or S-VOL.

Volume types supported for global-active device

In some cases, volumes that are used for functions other than global-active device can be used with global-active device P-VOLs and S-VOLs.

The following table shows which volume types used for other features can also be used with global-active device P-VOLs or S-VOLs.

Volume type	Used as a GAD P-VOL?	Used as a GAD S-VOL?	Used as a quorum disk?
Dynamic Provisioning / Dynamic Tiering / Active flash			
Virtual volume	Yes[1]	Yes[1]	No
Pool volume	No	No	No
V-VOL with capacity saving enabled	Yes	Yes	No
Deduplication system data volume	No	No	No
ShadowImage / Thin Image[2]			
P-VOL	Yes	Yes	No
S-VOL	No	No	No
TrueCopy			
P-VOL	No	No	No
S-VOL	No	No	No
Universal Replicator			
P-VOL	Yes	Yes[3]	No
S-VOL	No	No	No
Journal volume	No	No	No
Universal Volume Manager			

Volume type	Used as a GAD P-VOL?	Used as a GAD S-VOL?	Used as a quorum disk?
External volume	Yes[1]	Yes[1]	Yes
Data Retention Utility			
Volume with access attribute	Yes	Yes[4]	No
Volume Migration			
Source volume	No: ▪ VSP G series ▪ VSP F series Yes: ▪ VSP G1000 ▪ VSP G1500, F1500 ▪ VSP 5000 series	No: ▪ VSP G series ▪ VSP F series Yes: ▪ VSP G1000 ▪ VSP G1500, F1500 ▪ VSP 5000 series	No
Target volume	No	No	No
Hitachi Virtual LUN			
Virtual LUN volume	Yes	Yes	Yes[5]
LUN Manager			
The volume on which paths are defined	Yes	Yes	No
Volume on which paths are not defined	No	No	Yes
CCI command device			
Command device	No	No	No
Remote command device	No	No	No
Encryption License Key			

Volume type	Used as a GAD P-VOL?	Used as a GAD S-VOL?	Used as a quorum disk?
Volume whose parity groups have been encrypted	Yes	Yes	You can use an encrypted volume in the external storage system as a quorum disk.[6]
Nondisruptive migration			
Volume which is being migrated	Yes	No	No

Notes:

1. A DP-VOL that uses an external volume as a pool volume can be used as a GAD P-VOL or S-VOL.
2. For the Thin Image node or leaf volume, see the description of the S-VOL, not the P-VOL.
3. GAD S-VOL is used as a UR delta resync pair P-VOL.
4. If you set the S-VOL Disable attribute of the Data Retention Utility to the GAD S-VOL, GAD pair operations using CCI are restricted. Release the S-VOL Disable attribute on the GAD S-VOL, and then perform the GAD pair operations.
5. Quorum disks can only be set on external volumes that are configured so that one external volume group is mapped to one external volume.
6. You cannot encrypt a nonencrypted quorum disk in the external storage system from the primary or secondary storage system.

Dynamic Provisioning / Dynamic Tiering / Active flash

Dynamic Provisioning, Dynamic Tiering, and active flash virtual volumes (DP-VOLs) can be used as GAD pair volumes.

A V-VOL with capacity saving enabled can be used as a P-VOL or S-VOL of a GAD pair. A deduplication system data volume cannot be used as a P-VOL or S-VOL of a GAD pair.

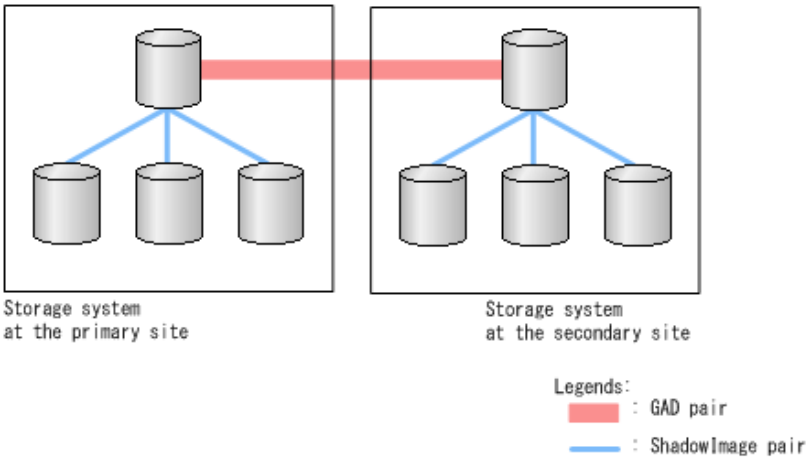
Note:

- Data compressed or deduplicated by the capacity saving function is copied to a volume after compression and deduplication are released, that is, the capacity saving function is not performed immediately for copied data. Therefore, before creating or resynchronizing a GAD pair, make sure that the available capacity in the copy destination volume is greater than the used capacity in the copy origination volume before capacity saving. For details, see the *Provisioning Guide for Open Systems*.
- If you create a GAD pair using a volume for which the capacity saving function is used, compressed or deduplicated data is copied. Because of this, copy or I/O performance might be degraded.
- When the capacity saving function is used, management information is stored in a pool. As a result, there might be a difference in the number of used pages or licensed capacity between a P-VOL and an S-VOL.

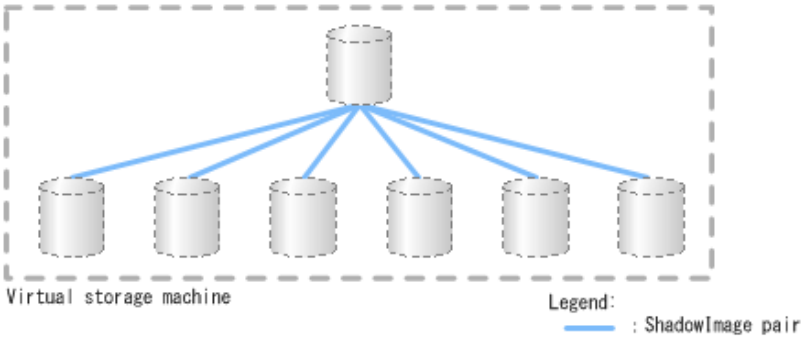
ShadowImage

You can use the GAD P-VOL and S-VOL as a ShadowImage P-VOL.

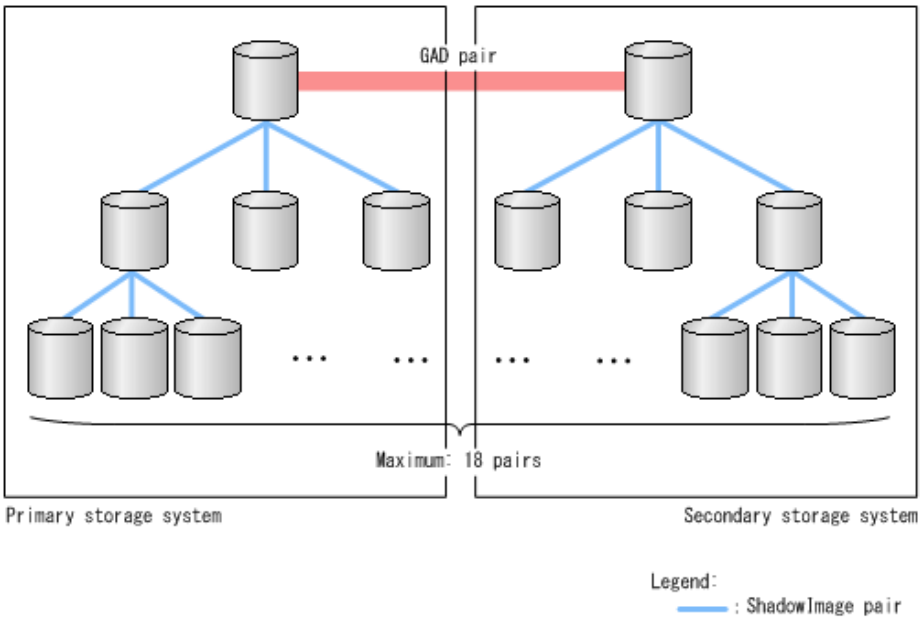
You can create up to three ShadowImage pairs respectively on the GAD primary and secondary storage systems.



Because the server recognizes a GAD pair as one volume, it sees the volume as paired with six ShadowImage volumes.



You can create three additional, cascaded SI pairs using the SI S-VOLs. This means that up to nine SI pairs can be created with the GAD P-VOL, and nine SI pairs can be created with the GAD S-VOL.



Note:

- Pairs in an SI consistency group must reside in the same storage system. Because of this, the SI pairs that are associated with both the GAD P-VOL and the S-VOL cannot be registered to the same consistency group.
- When you use GAD pair volumes to create an SI pair, you must specify the physical LDEV ID, not the virtual LDEV ID.

Limitations when sharing global-active device and ShadowImage volumes

Any operation that deletes the virtual LDEV ID of a volume used as a ShadowImage volume cannot be performed.

When a GAD pair is deleted with the P-VOL specified, the virtual LDEV ID of the S-VOL is deleted. If you delete the pair with the S-VOL specified, the virtual LDEV ID of the P-VOL is deleted. When the virtual LDEV ID is deleted, the server does not recognize the volume.

ShadowImage operations and global-active device pair status

The ability to perform a SI pair operation depends on the SI pair status and GAD pair status.

The following tables show SI pair operations and whether they can be performed (Yes, No) with the listed GAD status. The information assumes the required SI status for the operation.

The Virtual LDEV ID column shows whether the volume has a virtual LDEV ID or not (Yes, No).

Table 1 ShadowImage operations when global-active device status is Simplex

GAD pair status	Virtual LDEV ID	I/O		ShadowImage pair operation				
		Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs/ Suspend copy
SMPL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	No	No	No	Yes	Yes	Yes	Yes	Yes
	No, but the GAD reserve attribute is set	No	No	No	No	No	No	Yes

Table 2 ShadowImage operations when global-active device status is Mirroring

GAD pair status	I/O mode	Pair location	I/O		ShadowImage pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs/ Suspend copy
INIT/ COPY	Mirror (RL)	Primary	Yes	Yes	Yes	Yes	Yes	No[1]	Yes
	Block	Secondary	No	No	Yes	No[2]	No[2]	No[1, 3]	Yes
COPY	Mirror (RL)	Primary	Yes	Yes	Yes	Yes	Yes	No[1]	Yes
	Block	Secondary	No	No	Yes	No[2]	No[2]	No[1, 3]	Yes

Notes:

1. Cannot be used because GAD pairs are not suspended.
2. Cannot be used because S-VOL data is not fixed.
3. Cannot be used because the volume at the GAD copy destination is the same as the volume at the ShadowImage copy destination.

Table 3 ShadowImage operations when global-active device status is Mirrored

GAD pair status	I/O mode	Pair location	I/O		ShadowImage pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs/ Suspend copy
PAIR	Mirror (RL)	Primary	Yes	Yes	Yes	Yes	Yes	No*	Yes
		Secondary	Yes	Yes	Yes	Yes	Yes	No*	Yes
* Cannot be used because GAD pairs are not suspended, and also because the volume at the GAD copy destination is the same as the volume at the ShadowImage copy destination.									

Table 4 ShadowImage operations when no volume is set for the quorum disk or global-active device status of global-active device pairs

GAD pair status	I/O mode	Pair location	I/O		ShadowImage pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs/ Suspend copy
PAIR	Mirror(RL)	Primary	Yes	Yes	Yes	Yes	Yes	No*	Yes
	Mirror(RL)	Secondary	Yes	Yes	Yes	Yes	Yes	No*	Yes
* Cannot be used because GAD pairs are not suspended, and also because the volume at the GAD copy destination is the same as the volume at the ShadowImage copy destination.									

Table 5 ShadowImage operations when global-active device status is Suspended

GAD pair status	I/O mode	Pair location	I/O		ShadowImage pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs/ Suspend copy
PSUS	Local	Primary	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Block	Primary	No	No	Yes	Yes	Yes	No	Yes
PSUE	Local	Primary	Yes	Yes	Yes	Yes	Yes	Yes	Yes

GAD pair status	I/O mode	Pair location	I/O		ShadowImage pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs/ Suspend copy
	Block	Primary	No	No	Yes	Yes	Yes	No	Yes
		Secondary	No	No	Yes	Yes	Yes	No	Yes
SSUS	Block	Secondary	No	No	Yes	Yes	Yes	No	Yes
SSWS	Local	Secondary	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 6 ShadowImage operations when global-active device status is Blocked

GAD pair status	I/O mode	Pair location	I/O		SI pair operations				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs/ Suspend copy
PSUE	Block	Primary	No	No	Yes	Yes	Yes	No	Yes
		Secondary	No	No	Yes	Yes	Yes	No	Yes

GAD operations and SI pair status

The ability to perform a GAD pair operation depends on GAD pair status and SI pair status.

The following tables show GAD operations and whether they can be performed (Yes, No) with the listed SI status. The information assumes the required GAD status for the operation.

Table 7 GAD operations and SI pair statuses, when GAD P-VOL is shared

SI pair status	GAD pair operations							
	Create pairs	Suspend pairs		Delete pairs			Resync pairs	
		P-VOL selected	S-VOL selected	P-VOL selected [1]	S-VOL selected [2]	Forced deletion	P-VOL selected	S-VOL selected
SMPL(PD)	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes

SI pair status	GAD pair operations							
	Create pairs	Suspend pairs		Delete pairs			Resync pairs	
		P-VOL selected	S-VOL selected	P-VOL selected [1]	S-VOL selected [2]	Forced deletion	P-VOL selected	S-VOL selected
COPY	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes
PAIR	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes
COPY(SP)	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes
PSUS(SP)	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes
PSUS	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes
COPY(RS)	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes
COPY(RS-R)	No[4]	impossible	impossible	Yes	No[3]	Yes	No[4]	No[4]
PSUE	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes

Notes:

1. You can delete a GAD pair by specifying the P-VOL, only when the I/O mode is Local and the GAD pair status of the P-VOL is PSUS or PSUE.
2. You can delete a GAD pair by specifying the S-VOL, only when the I/O mode is Local and the GAD pair status of the S-VOL is SSWS.
3. Cannot be used because, when you delete a GAD pair specifying the S-VOL, the P-VOL's virtual LDEV ID is also deleted, which makes it unusable as the SI P-VOL.
4. To continue SI restore copy, the GAD pairs must be suspended.

Table 8 GAD operations and SI pair statuses, when GAD S-VOL is shared

SI pair status	GAD pair operations							
	Create pairs	Suspend pairs		Delete pairs			Resync pairs	
		P-VOL selected	S-VOL selected	P-VOL selected [1]	S-VOL selected [2]	Forced deletion	P-VOL selected	S-VOL selected
SMPL(PD)	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
COPY	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
PAIR	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
COPY(SP)	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes

SI pair status	GAD pair operations							
	Create pairs	Suspend pairs		Delete pairs			Resync pairs	
		P-VOL selected	S-VOL selected	P-VOL selected [1]	S-VOL selected [2]	Forced deletion	P-VOL selected	S-VOL selected
PSUS(SP)	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
PSUS	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
COPY(RS)	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
COPY(RS-R)	No[3, 5]	impossible	impossible	No[4]	Yes	Yes	No[5, 6]	No[6]
PSUE	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes

Notes:

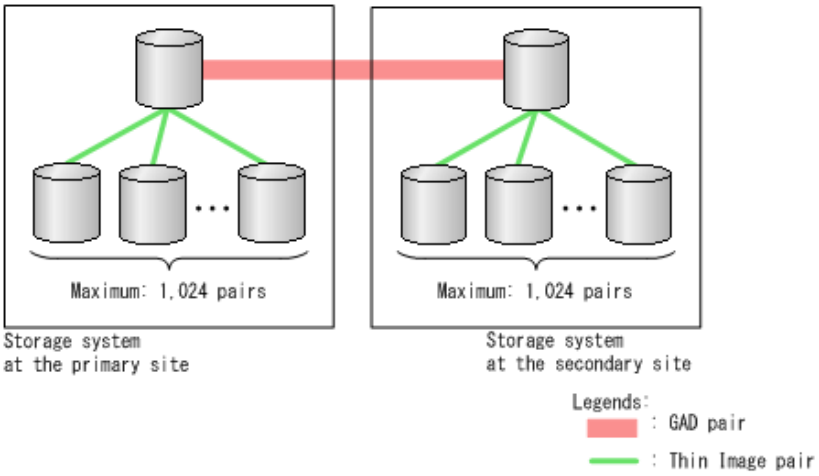
1. You can delete a GAD pair by specifying the P-VOL, only when the I/O mode is Local and the GAD pair status of the P-VOL is PSUS or PSUE.
2. You can delete a GAD pair by specifying the S-VOL, only when the I/O mode is Local and the GAD pair status of the S-VOL is SSWS.
3. When a GAD pair is created, the GAD reserve attribute is assigned to the volume that will become the S-VOL, which removes the virtual LDEV ID of this volume, making it unusable as an SI pair volume.

   The GAD reserve attribute is set, and the virtual LDEV ID is deleted for the volume that will become the GAD S-VOL, making it unusable as an SI volume.
4. Cannot be used because, when you delete a GAD pair specifying the S-VOL, the P-VOL's virtual LDEV ID is also deleted, which makes it unusable as the SI P-VOL.
5. Cannot be used because the volume at the GAD copy destination is the same as the volume at the ShadowImage copy destination.
6. To continue ShadowImage restore copy, GAD pairs must be suspended.

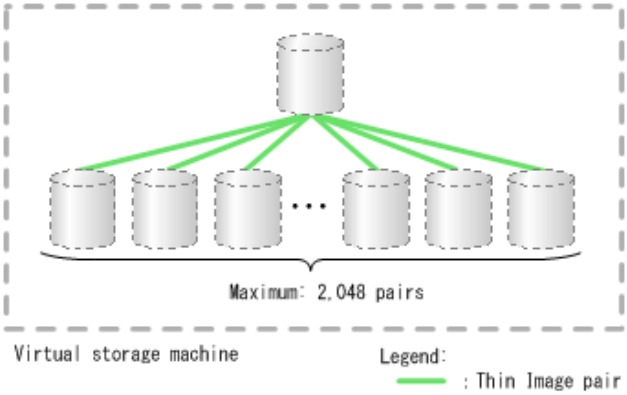
Thin Image

You can use a GAD P-VOL or S-VOL as a Thin Image (HTI) P-VOL.

You can create up to 1,024 Thin Image pairs using a GAD P-VOL, and up to 1,024 Thin Image pairs using a GAD S-VOL.



Because the server recognizes the GAD pair as one volume, it sees the volume as paired with 2,048 HTI volumes.



Note:

- Pairs in an HTI consistency group and snapshot group must reside in the same storage system. Because of this, the HTI pairs that are associated with both the GAD P-VOL and S-VOL cannot be registered to the same consistency group or snapshot group.
- When you use GAD pair volumes to create a Thin Image pair, specify the physical LDEV ID, not the virtual LDEV ID.

Limitations for using both global-active device and Thin Image

Any operation that deletes the virtual LDEV ID of a volume used as a Thin Image volume cannot be performed.

When a GAD pair is deleted with the P-VOL specified, the virtual S-VOL's LDEV ID is deleted. If you delete the pair with the S-VOL specified, the P-VOL's virtual LDEV ID is deleted. When the virtual LDEV ID is deleted, the server does not recognize the volume, making it unusable as a Thin Image volume.

Thin Image operations and global-active device status

The ability to perform a Thin Image pair operation depends on the HTI pair status and the GAD pair status.

The following tables show HTI operations and whether they can be performed (Yes, No) with the listed GAD status. The information assumes the required HTI status for the operation.

The Virtual LDEV ID column shows whether the volume has a virtual LDEV ID or not (Yes, No).

Table 9 Thin Image operations when GAD status is Simplex

GAD pair status	Virtual LDEV ID	I/O		Thin Image pair operation				
		Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs
SMPL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	No	No	No	Yes	Yes	Yes	Yes	Yes
	No, but the GAD reserve attribute is set	No	No	No	No	No	No	Yes

Table 10 Thin Image operations when GAD status is Mirroring

GAD pair status	I/O mode	Pair location	I/O		Thin Image pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs
INIT/ COPY	Mirror (RL)	Primary	Yes	Yes	Yes	Yes	Yes	No[1]	Yes
	Block	Secondary	No	No	No	No[2]	No[2]	No[1, 3]	Yes
COPY	Mirror (RL)	Primary	Yes	Yes	Yes	Yes	Yes	No[1]	Yes
	Block	Secondary	No	No	No	No[2]	No[2]	No[1, 3]	Yes

Notes:

1. Cannot be used because GAD pairs are not suspended.
2. Cannot be used because the data is being copied and the volume data is not fixed yet.
3. Cannot be used because the volume at the GAD copy destination is the same as the volume at the Thin Image copy destination.

Table 11 Thin Image operations when GAD status is Mirrored

GAD pair status	I/O mode	Pair location	I/O		Thin Image pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs
PAIR	Mirror (RL)	Primary	Yes	Yes	Yes	Yes	Yes	No*	Yes
		Secondary	Yes	Yes	Yes	Yes	Yes	No*	Yes
* Cannot be used because GAD pairs are not suspended, and also because the volume at the GAD copy destination is the same as the volume at the Thin Image copy destination.									

Table 12 Thin Image operations when no volume is set for the quorum disk or GAD status of GAD pairs

GAD pair status	I/O mode	Pair location	I/O		Thin Image pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs/ Suspend copy
PAIR	Mirror(RL)	Primary	Yes	Yes	Yes	Yes	Yes	No*	Yes
	Mirror(RL)	Secondary	Yes	Yes	Yes	Yes	Yes	No*	Yes
* Cannot be used because GAD pairs are not suspended, and also because the volume at the GAD copy destination is the same as the volume at the Thin Image copy destination.									

Table 13 Thin Image operations when GAD status is Suspended

GAD pair status	I/O mode	Pair location	I/O		Thin Image pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs
PSUS	Local	Primary	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Block	Primary	No	No	Yes	Yes	Yes	No	Yes
PSUE	Local	Primary	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Block	Primary	No	No	Yes	Yes	Yes	No	Yes
		Secondary	No	No	Yes	Yes	Yes	No	Yes

GAD pair status	I/O mode	Pair location	I/O		Thin Image pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs
SSUS	Block	Secondary	No	No	Yes	Yes	Yes	No	Yes
SSWS	Local	Secondary	Yes	Yes	Yes	Yes	Yes	No	Yes

Table 14 Thin Image operations when GAD status is Blocked

GAD pair status	I/O mode	Pair location	I/O		Thin Image pair operation				
			Read	Write	Create pairs	Split pairs	Resync pairs	Restore pairs	Delete pairs
PSUE	Block	Primary	No	No	Yes	Yes	Yes	No	Yes
		Secondary	No	No	Yes	Yes	Yes	No	Yes

Global-active device operations and Thin Image pair status

The ability to perform a GAD pair operation depends on the GAD pair status and the HTI pair status.

The following tables show GAD operations and whether they can be performed (Yes, No) with the listed HTI status. The information assumes the required GAD status for the operation.

Table 15 GAD operations and HTI pair status, when the GAD P-VOL is shared

TI pair status	GAD pair operations							
	Create GAD Pairs	Suspend Pairs		Delete Pairs			Resync Pairs	
		P-VOL specified	S-VOL specified	P-VOL specified[1]	S-VOL specified[2]	Forced deletion	P-VOL specified	S-VOL specified
SMPL(PD)	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes
COPY	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes
PAIR	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes
PSUS	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes

TI pair status	GAD pair operations							
	Create GAD Pairs	Suspend Pairs		Delete Pairs			Resync Pairs	
		P-VOL specified	S-VOL specified	P-VOL specified[1]	S-VOL specified[2]	Forced deletion	P-VOL specified	S-VOL specified
COPY(RS-R)	No[4]	impossible	impossible	Yes	No[3]	Yes	No[4]	No[4]
PSUE	Yes	Yes	Yes	Yes	No[3]	Yes	Yes	Yes

Notes:

1. You can delete a GAD pair by specifying the P-VOL, only when the I/O mode is Local and the GAD pair status of the P-VOL is PSUS or PSUE.
2. You can delete a GAD pair by specifying the S-VOL, only when the I/O mode is Local and the GAD pair status of the S-VOL is SSWS.
3. Cannot be used because, when you delete a GAD pair specifying the S-VOL, the P-VOL's virtual LDEV ID is also deleted, which makes it unusable as the HTI P-VOL.
4. To continue resynchronizing the HTI pair, you must split the GAD pair.

Table 16 GAD operations and HTI pair status, when the GAD S-VOL is shared

TI pair status	GAD pair operations							
	Create GAD Pairs	Suspend Pairs		Delete Pairs			Resync Pairs	
		P-VOL specified	S-VOL specified	P-VOL specified[1]	S-VOL specified[2]	Forced deletion	P-VOL specified	S-VOL specified
SMPL(PD)	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
COPY	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
PAIR	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
PSUS	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes
COPY(RS-R)	No[3, 5]	No	No	No[4]	Yes	Yes	No[5, 6]	No[6]
PSUE	No[3]	Yes	Yes	No[4]	Yes	Yes	Yes	Yes

Notes:

1. You can delete a GAD pair by specifying the primary volume, only when the I/O mode is Local and the GAD pair status of the primary volume is PSUS or PSUE.
2. You can delete a GAD pair by specifying the secondary volume, only when the I/O mode is Local and the GAD pair status of the secondary volume is SSWS.

TI pair status	GAD pair operations							
	Create GAD Pairs	Suspend Pairs		Delete Pairs			Resync Pairs	
		P-VOL specified	S-VOL specified	P-VOL specified[1]	S-VOL specified[2]	Forced deletion	P-VOL specified	S-VOL specified

3. To create a GAD pair, you must assign the GAD reserve attribute to the volume used as an S-VOL. Because the virtual LDEV ID of the volume to which the GAD reserve attribute is assigned is deleted, you cannot create a GAD pair by specifying the volume shared with HTI as the S-VOL of the pair.
4. Cannot be used because, when you delete a GAD PAIR specifying the P-VOL, the S-VOL's virtual LDEV ID is also deleted, which makes it unusable as an HTI P-VOL.
5. Cannot be used because the GAD pair's target volume is the same as the HTI pair's target volume.
6. To continue resynchronizing the HTI pair, you must split the GAD pair.

Use cases for pairing global-active device volumes with ShadowImage or Thin Image

Backing up GAD pair volumes with ShadowImage (SI) or Thin Image (HTI) provides further protection for GAD data.

Further protection for GAD data is provided in the following ways:

- When the GAD pair is resynchronized, pair status changes to COPY. While in this status, S-VOL consistency is temporarily lost. You can protect data when in COPY status by pairing the S-VOL with SI or HTI before resynchronizing the GAD pair.
- Though data in a blocked GAD pair is inconsistent, host activity can continue with the P-VOL or S-VOL. Therefore, before correcting the failure by forcibly deleting the pair, you should pair the volumes with SI or HTI.
- The SI and HTI pairs can then be copied, and the copies used for other purposes.

Universal Replicator

You can combine GAD and Universal Replicator to create a configuration that can continue to operate in the event of a multi-site failure.

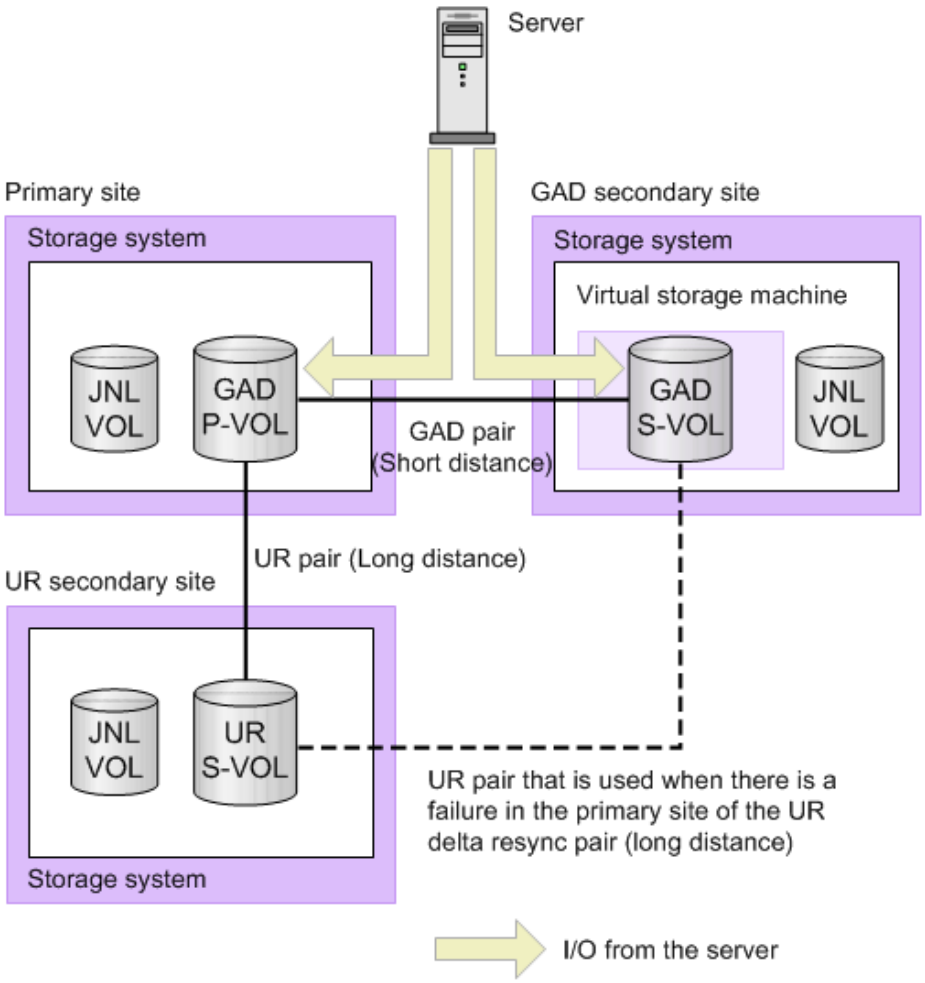
In a global-active device system, the server accesses the primary and secondary sites simultaneously and shares the same data between the two sites (at campus distance). If a failure occurs at one site, you can continue operations at the other site. However, if a failure occurs at both sites, for example due to a large-scale disaster, you will not be able to continue operations with the data redundancy provided only by GAD.

To manage this situation, you can implement a 3-data-center (3DC) configuration by combining GAD and Universal Replicator (UR). This configuration is called a GAD 3DC delta resync (GAD+UR) configuration. If there is a failure at both the primary site and the GAD secondary site, the GAD+UR configuration enables you to continue operations using the UR secondary site (at metro distance).

Note:

- The CCI remote command device is not required in GAD+UR configurations.
- Volumes in a 3DC GAD+UR configuration cannot be shared with the following volumes:
  - UR volumes in a system with multiple storage systems in the primary and secondary sites
  - UR volumes in a 3DC multi-target configuration with TC and UR
  - UR volumes in a 3DC multi-target configuration with 3 UR sites
  - UR volumes in a 3DC cascade configuration with 3 UR sites
- 3DC delta resync configuration with GAD and UR is not supported by VSP G130 or VSP G/F350.

The following figure shows the required configuration for GAD+UR operations. You must use this configuration when combining GAD with UR.



In a GAD+UR configuration:

- The P-VOL of the GAD pair functions as the P-VOL of the UR pair.
- The S-VOL of the GAD pair functions as the P-VOL of the UR delta resync pair.
- The UR S-VOL has two mirror IDs, one for the UR pair, and one for the UR delta resync pair.
- The UR delta resync pair consists of the GAD S-VOL at the GAD secondary site and the UR S-VOL at the UR secondary site. This UR delta resync pair allows you to synchronize the UR pair S-VOL by using the journal data at the GAD secondary site in the event of a failure at the primary site.
- When combining GAD with UR, create the GAD pair first, and then create the UR pair. The GAD pair cannot be used with a UR pair that was created first.

global-active device pair and Universal Replicator pair interoperability

You should know how GAD pairs and Universal Replicator pairs work together for different pair statuses for GAD pairs or UR pairs.

The following table shows GAD pair operations and whether they can be performed (Yes or No) with the listed UR pair status.

Table 17 GAD operations and UR pair statuses

UR pair status	Attribute of the target UR pair	GAD pair operation					
		Create pairs[1]	Split pairs	Suspend pairs	Resynchronize pairs		Delete pairs
			P-VOL specified	S-VOL specified	P-VOL specified	S-VOL specified	P-VOL or S-VOL specified
COPY	P-VOL	No	Yes	No	Yes	Yes	No[2]
	S-VOL	No	No[3]	No	No	No	No[2]
PAIR	P-VOL	No	Yes	No	Yes	Yes	No[2]
	S-VOL	No	No[3]	No	No	No	No[2]
PSUS	P-VOL	No	Yes	No	Yes	Yes	No[2]
PSUE	P-VOL	No	Yes	No	Yes	Yes	No[2]
	S-VOL	No	No[3]	No	No	No	No[2]
SSUS	S-VOL	No	No[3]	No	No	No	No[2]
SSWS	S-VOL	No	No[3]	No	No	No	No[2]
HOLD	P-VOL	No	No	Yes	No	No	No[2]
	S-VOL	No	No	No	No	No	No[2]
HLDE	P-VOL	No	No	Yes	No	No	No[2]
	S-VOL	No	No	No	No	No	No[2]

Note:

1. When creating a GAD and UR configuration, create a GAD pair first.
2. When deleting a GAD pair, delete the UR pair and the UR delta resync pair first.
3. The UR S-VOL is also used as the GAD P-VOL only when the UR S-VOL is duplicated using GAD. In this case, the GAD P-VOL status must be PSUS, therefore, the pair split terminates abnormally.

The following table shows UR pair operations and whether they can be performed (Yes or No) with the listed GAD pair status.

Table 18 UR pair operations and GAD pair statuses

GAD pair status	I/O mode	Attribute of the target GAD pair	UR pair operation				
			Create pairs	Split pairs	Suspend pairs	Resynchronize pairs	
				P-VOL specified	S-VOL specified	P-VOL specified	S-VOL specified
INIT/ COPY	Mirror (RL)	P-VOL	No	Yes	No	Yes[1]	No
	Block	S-VOL	No	No	No	No	No
COPY	Mirror (RL)	P-VOL	No	Yes	No	Yes[1]	No
	Block	S-VOL	No	No	No	No	No
PAIR	Mirror (RL)	P-VOL	Yes[2]	Yes	No	Yes[1]	No
		S-VOL	No	No	No	No	No
PSUS	Local	P-VOL	No	Yes	Yes[3]	Yes[1]	Yes[3]
	Block	P-VOL	No	Yes	Yes[3]	No	No
PSUE	Local	P-VOL	No	Yes	Yes[3]	Yes[1]	Yes[3]
	Block	P-VOL	No	Yes	Yes[3]	No	No
SSUS	Block	S-VOL	No	No	No	No	No
SSWS	Local	S-VOL	No	Yes	No	Yes	No

Note:

1. Can be performed only when the UR delta resync pair status is HLDE.
2. GAD pairs can be used with UR pairs only when the volume specified as the UR S-VOL is a UR delta resync S-VOL.
3. The UR S-VOL is also used as the GAD P-VOL only when the UR S-VOL is duplicated using GAD.

The following table shows UR delta resync pair operations and whether they can be performed (Yes or No) with the listed GAD pair status.

Table 19 UR delta resync pair operations and GAD pair statuses

GAD pair status	I/O mode	Attribute of the target GAD pair	UR delta resync pair operation					
			Create UR delta resync pair	Delta resync	Delete pairs			
					P-VOL specified	S-VOL specified	UR delta resync P-VOL	UR delta resync S-VOL
INIT/ COPY	Mirror (RL)	P-VOL	No	No[1]	Yes	No	No	No
	Block	S-VOL	No	No[1]	No	No	No	No
COPY	Mirror (RL)	P-VOL	No	No[1]	Yes	No	No	No
	Block	S-VOL	No	No[1]	No	No	No	No
PAIR	Mirror (RL)	P-VOL	No	No[1]	Yes	No	No	No
		S-VOL	Yes	No[1]	No	No	Yes[4]	No
PSUS	Local	P-VOL	No	No[1]	Yes	Yes[3]	Yes[4]	No
	Block	P-VOL	Yes[2]	No[1]	Yes	Yes[3]	Yes[4]	No
PSUE	Local	P-VOL	No	No[1]	Yes	Yes[3]	Yes[4]	No
	Block	P-VOL	Yes[2]	No[1]	Yes	Yes[3]	Yes[4]	No
SSUS	Block	S-VOL	No	No[1]	No	No	Yes[4]	No
SSWS	Local	S-VOL	No	No[1]	Yes	No	Yes[4]	No

Note:

1. Cannot be performed by users. The storage system performs the operation automatically.
2. If a failure occurs at the primary site, the operation can be performed only when the volume specified as the UR delta resync S-VOL is the UR S-VOL.
3. The UR S-VOL is also used as the GAD P-VOL only when the UR S-VOL is duplicated using GAD.
4. Deleting a UR delta resync pair deletes the UR pair.

Data Retention Utility

You can create a GAD pair using volumes that have been assigned the Data Retention Utility access attribute.

- When you create or resynchronize a GAD pair, the access attribute set for the P-VOL is copied to the S-VOL.
- If you change the access attribute when GAD status is Mirrored or Mirroring, make sure to set the access attribute to both the P-VOL and S-VOLs.
- Server I/O can be controlled, depending on GAD status and the access attribute.
- If you set the Data Retention Utility S-VOL Disable attribute on the GAD S-VOL, GAD pair operations using CCI are restricted. Release the S-VOL Disable attribute from the S-VOL, then perform CCI operations.

Global-active device status and I/O allowance by access attribute

Even when the access attribute is assigned to a GAD volume, the initial copy and pair resynchronization operations are not controlled. The following table shows whether server I/O is allowed for the listed GAD status and access attribute.

GAD statuses	Access attribute		I/O	
	P-VOL	S-VOL	P-VOL	S-VOL
Mirrored	Read/Write	Read/Write	Ends normally	Ends normally
	Read Only or Protect	Read/Write	Depends on the attribute*	Ends normally
	Read/Write	Read Only or Protect	Ends normally	Depends on the attribute*
	Read Only or Protect	Read Only or Protect	Depends on the attribute*	Depends on the attribute*
Quorum disk blocked or no quorum disk volume	Read/Write	Read/Write	Ends normally	Ends normally
	Read Only or Protect	Read/Write	Depends on the attribute*	Ends normally
	Read/Write	Read Only or Protect	Ends normally	Depends on the attribute*
	Read Only or Protect	Read Only or Protect	Depends on the attribute*	Depends on the attribute*
Mirroring	Read/Write	Read/Write	Ends normally	Rejected
	Read Only or Protect	Read/Write	Depends on the attribute*	Rejected
	Read/Write	Read Only or Protect	Ends normally	Rejected

GAD statuses	Access attribute		I/O	
	P-VOL	**S-VOL**	**P-VOL**	**S-VOL**
Suspended (when the I/O mode of the primary volume is Local and the I/O mode of the secondary volume is Block)	Read Only or Protect	Read Only or Protect	Depends on the attribute*	Rejected
Suspended (when the I/O mode of the primary volume is Block and the I/O mode of the secondary volume is Local)	Read/Write	Read/Write	Rejected	Ends normally
	Read Only or Protect	Read/Write	Rejected	Ends normally
	Read/Write	Read Only or Protect	Rejected	Depends on the attribute*
	Read Only or Protect	Read Only or Protect	Rejected	Depends on the attribute*
Block	Read/Write	Read/Write	Rejected	Rejected
	Read Only or Protect	Read/Write	Rejected	Rejected
	Read/Write	Read Only or Protect	Rejected	Rejected
	Read Only or Protect	Read Only or Protect	Rejected	Rejected
* If the attribute is Read Only, Read is allowed but not Write. If the attribute is Protect, Read and Write are not allowed.				

Volume Migration

You can use Volume Migration to move volumes in an overloaded drive to a non-overloaded drive online.

Volume Migration moves volumes by specifying the P-VOL and S-VOL of a GAD pair in an overloaded drive as the migration source volume which then moves the volumes to a non-overloaded drive.

Restrictions for using global-active device with Volume Migration

- The GAD pair must be split before you specify the volumes as the migration source volumes for Volume Migration.
- Provisioning types of the GAD P-VOL and S-VOL must be the same. Ensure that the provisioning types of the GAD P-VOL and S-VOL are still the same after the migration by Volume Migration.
- When a GAD pair volume is shared by an SI pair volume, you cannot specify it as the source volume during Quick Restore of the SI pair. When Quick Restore completes, start using Volume Migration.
- For Volume Migration operation when using GAD with nondisruptive migration, see Global-active device status and nondisruptive migration pair operations (on page 84).
- When combining GAD with Volume Migration, create the GAD pair first, and then operate Volume Migration. The GAD pair cannot be paired with the volumes for which Volume Migration is being operated.

Global-active device status and Volume Migration pair operations

The ability of Volume Migration to create or cancel migration plans depends on the status of the GAD pair.

The following table describes if you can create or cancel migration plans when GAD volumes are not mirrored.

GAD pair status	Virtual LDEV ID	I/O from the server		Volume Migration operation	
		Read	Write	Create migration plans	Cancel migration plans
SMPL	Available	Y	Y	Y	Y
	Not available	N	N	N	Y
	Not available (Virtual attribute: GAD reserve)	N	N	N	Y
Legend Y: Can be performed N: Cannot be performed					

The following table describes if you can create or cancel migration plans when GAD volumes are being mirrored.

GAD pair status	I/O mode	Pair location	I/O from the server		Volume Migration operation	
			Read	Write	Create migration plans	Cancel migration plans
INIT/COPY	Mirror(RL)	Primary	Y	Y	N	Y
	Block	Secondary	N	N	N	Y
Legend Y: Can be performed N: Cannot be performed						

The following table describes if you can create or cancel migration plans when GAD volumes are mirrored.

GAD pair status	I/O mode	Pair location	I/O from the server		Volume Migration operation	
			Read	Write	Create migration plans	Cancel migration plans
PAIR	Mirror(RL)	Primary	Y	Y	N	Y
		Secondary	Y	Y	N	Y
Legend Y: Can be performed N: Cannot be performed						

The following table describes if you can create or cancel migration plans when the GAD pair is suspended.

GAD pair status	I/O mode	Pair location	I/O from the server		Volume Migration operation	
			Read	Write	Create migration plans	Cancel migration plans
PSUS/ PSUE	Local	Primary	Y	Y	Y	Y
	Block	Any	N	N	Y	Y

GAD pair status	I/O mode	Pair location	I/O from the server		Volume Migration operation	
			Read	Write	Create migration plans	Cancel migration plans
SSUS	Block	Secondary	N	N	Y	Y
SSWS	Local	Secondary	Y	Y	Y	Y
Legend Y: Can be performed N: Cannot be performed						

The following table describes if you can create or cancel migration plans when the GAD pair is blocked.

GAD pair status	I/O mode	Pair location	I/O from the server		Volume Migration operation	
			Read	Write	Create migration plans	Cancel migration plans
PSUE	Block	Primary	N	N	Y	Y
		Secondary	N	N	Y	Y
Legend Y: Can be performed N: Cannot be performed						

Volume Migration pair statuses and global-active device pair operations

You should understand what GAD operations you can perform given the Volume Migration pair status and whether the GAD P-VOL or S-VOL is shared by Volume Migration.

The following table describes operations you can perform according to the Volume Migration pair status when the GAD P-VOL is shared by Volume Migration.

Volume Migration pair status	GAD pair operation							
	Create	Suspend		Delete			Resynchronize	
		P-VOL specified	S-VOL specified	P-VOL specified [1]	S-VOL specified [2]	Force delete	P-VOL specified	S-VOL specified
SMPL(PD)	No[4]	Yes[5]	Yes[5]	Yes	No[3]	Yes	No	No
COPY	No[4]	Yes[5]	Yes[5]	Yes	No[3]	Yes	No	No
PSUS	No[4]	Yes[5]	Yes[5]	Yes	No[3]	Yes	No	No
PSUE	No[4]	Yes[5]	Yes[5]	Yes	No[3]	Yes	No	No

Note:

1. You can delete a GAD pair by specifying the P-VOL, only when the I/O mode is Local and the GAD pair status of the P-VOL is PSUS or PSUE.
2. You can delete a GAD pair by specifying the S-VOL, only when the I/O mode is Local and the GAD pair status of the S-VOL is SSWS.
3. Cannot be performed because the virtual LDEV ID of the GAD P-VOL (volume for Volume Migration) is deleted if you specify the S-VOL to delete the GAD pair.
4. To perform Volume Migration, you must suspend the GAD pair.
5. To perform Volume Migration, you must suspend the GAD pair. Therefore, you can suspend the GAD pair, however the status of the GAD pair does not change because the GAD pair is already suspended.

The following table describes operations you can perform according to the Volume Migration pair status when the GAD S-VOL is shared by Volume Migration.

Volume Migration pair status	GAD pair operation							
	Create	Suspend		Delete			Resynchronize	
		P-VOL specified	S-VOL specified	P-VOL specified[1]	S-VOL specified[2]	Force delete	P-VOL specified	S-VOL specified
SMPL(PD)	No[3]	Yes[5]	Yes[5]	No[4]	Yes	Yes	No	No
COPY	No[3]	Yes[5]	Yes[5]	No[4]	Yes	Yes	No	No
PSUS	No[3]	Yes[5]	Yes[5]	No[4]	Yes	Yes	No	No
PSUE	No[3]	Yes[5]	Yes[5]	No[4]	Yes	Yes	No	No

Note:

Volume Migration pair status	GAD pair operation							
	Create	Suspend		Delete			Resynchronize	
		P-VOL specified	S-VOL specified	P-VOL specified[1]	S-VOL specified[2]	Force delete	P-VOL specified	S-VOL specified

1. You can delete a GAD pair by specifying the primary volume, only when the I/O mode is Local and the GAD pair status of the primary volume is PSUS or PSUE.
2. You can delete a GAD pair by specifying the secondary volume, only when the I/O mode is Local and the GAD pair status of the secondary volume is SSWS.
3. To create a GAD pair, you must assign the GAD reserve attribute to the volume used as an S-VOL. Because the virtual LDEV ID of the volume to which the GAD reserve attribute is assigned is deleted, you cannot create a GAD pair by specifying the volume used for Volume Migration as the S-VOL of the pair.
4. Cannot be performed because the virtual LDEV ID of the GAD S-VOL (volume for Volume Migration) is deleted if you specify the P-VOL to delete the GAD pair.
5. To perform Volume Migration, you must suspend the GAD pair. Therefore, you can suspend the GAD pair, however the status of the GAD pair does not change because the GAD pair is already suspended.

LUN Manager

Use the volumes for which LU paths have been set to create a GAD pair. You can add LU paths to or delete LU paths from GAD pair volumes. However, you cannot delete the last LU path because at least one LU path must be set for GAD pair volumes.

A volume for which no LU path has been set cannot be used as a GAD pair volume.

Note: When you remove the path that is defined on an LDEV with the GAD reserve attribute, the path removal might fail if the number of LDEVs whose path is to be removed is too large.

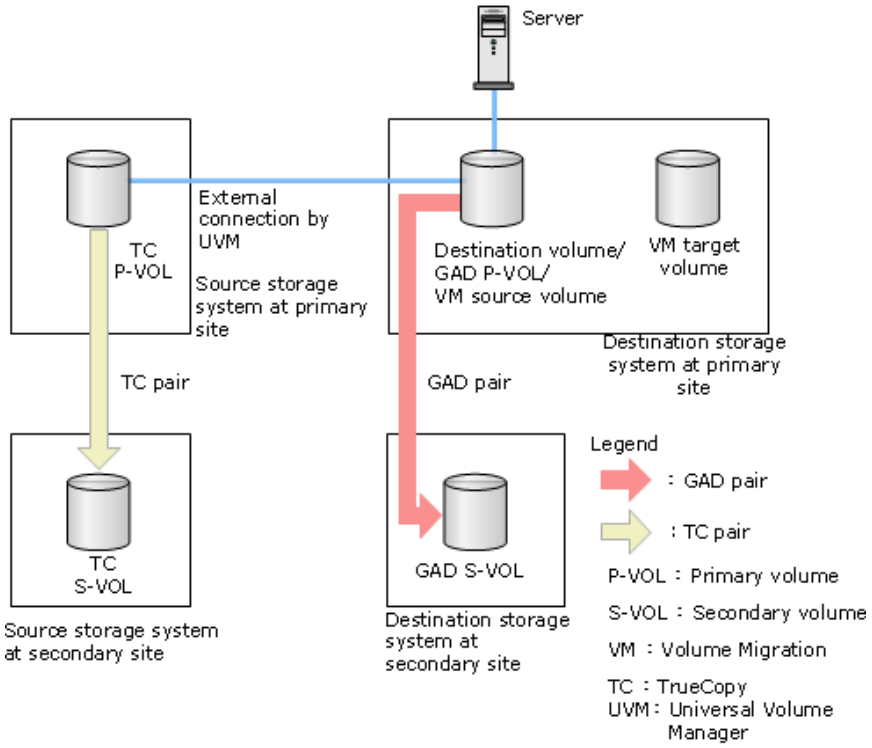
When a port has a path defined for an LDEV with the GAD reserve attribute and you need to configure the port (delete a host group, set a command device, or change the host mode, topology, AL-PL, or transfer speed), the operation might fail if you configure more than one port at a time. For ports that have a path defined on an LDEV with the GAD reserve attribute, perform these operations on one port at a time.

Virtual Partition Manager

GAD pair volumes and quorum disks can migrate across CLPRs.

Nondisruptive migration (VSP G1x00, F1500)

You can create a GAD pair using a volume being migrated by nondisruptive migration to migrate your data without changing system configuration, even if your system is designed for disaster recovery. The following figure shows an example of such data migration. For example, if you create a GAD pair using a volume being migrated while maintaining the configuration of the disaster recovery system using TrueCopy, you can maintain the disaster recovery system by GAD soon after migration.



Restrictions for using global-active device with nondisruptive migration

You should be aware of restrictions if you want to use GAD with nondisruptive migration.

- When creating a GAD pair, you cannot specify a volume being migrated by nondisruptive migration as its S-VOL.
- Before creating a GAD pair, you need to change the cache mode of the destination volume to Write Sync. Use CCI when changing the cache mode.
- I/O operations from the host to the GAD S-VOL cannot be performed until Volume Migration is completed. If you want to perform the operation which allows the host to recognize the GAD S-VOL, perform this operation after Volume Migration is completed.
- You cannot swap resynchronize GAD pairs. If you want to swap resynchronize them, delete Volume Migration pairs after Volume Migration ends.

- Before you start Volume Migration, set the same provisioning type for both the target volume of Volume Migration and the GAD S-VOL.
- 3-data-center (3DC) configurations using both GAD and Universal Replicator (UR) cannot be used for destination volumes. To use a 3DC configuration combining GAD and UR, configure the 3DC system after volumes are completely migrated by Volume Migration.

Global-active device status and nondisruptive migration pair operations

The following table shows the cache modes of nondisruptive migration and GAD pair operations.

Operation target	Virtual LDEV ID	GAD pair operation	
		P-VOL	S-VOL
Cache modes for external volume groups of the destination storage system	TM (Cache Through)	N	N
	SM (Write Sync)	Y	N
Legend Y: Can be performed N: Cannot be performed			

The following table shows the possibility of GAD pair operation and cache mode change in nondisruptive migration.

Operation target	Cache modes to which GAD P-VOL can be changed		
	TM (Cache Through)	SM	EM/DM
GAD P-VOL	N	Y	N
Legend Y: Can be performed N: Cannot be performed			

The following table shows the possibility of Volume Migration pair operations (when a GAD pair operating with nondisruptive migration is in the initial status).

GAD pair status	Virtual LDEV ID	I/O from the server		Volume Migration operation	
		Read	Write	Migrate volumes	Stop migrating volumes
SMPL	Specifed	Y	Y	Y	Y
	None	N	N	N	Y
	None (GAD reserve is specified as the virtual attribute)	N	N	N	Y
Legend Y: Can be performed N: Cannot be performed					

The following table shows the possibility of Volume Migration pair operations (when a GAD pair operating with nondisruptive migration is being mirrored).

GAD pair status	I/O mode	Pair location	I/O from the server		Volume Migration operation	
			Read	Write	Migrate volumes	Stop migrating volumes
INIT/COPY	Mirror (RL)	P-VOL	Y	Y	N	Y
	Block	S-VOL	N	N	N	Y
Legend Y: Can be performed N: Cannot be performed						

The following table shows the possibility of Volume Migration pair operations (when a GAD pair operating with nondisruptive migration is already mirrored).

GAD pair status	I/O mode	Pair location	I/O from the server		Volume Migration operation	
			Read	Write	Migrate volumes	Stop migrating volumes
PAIR	Mirror (RL)	P-VOL	Y	Y	Y	Y
	Block	S-VOL	N	N	N	Y
Legend Y: Can be performed N: Cannot be performed						

The following table shows the possibility of Volume Migration pair operations (when a GAD pair operating with nondisruptive migration is suspended).

GAD pair status	I/O mode	Pair location	I/O from the server		Volume Migration operation	
			Read	Write	Migrate volumes	Stop migrating volumes
PSUS/ PSUE	Local	P-VOL	Y	Y	Y	Y
	Block	Volume of your own choice (P-VOL or S-VOL)	N	N	Y	Y
SSUS	Block	S-VOL	N	N	Y	Y
SSWS	Local	S-VOL	Y	Y	Y	Y
Legend Y: Can be performed N: Cannot be performed						

The following table shows the possibility of Volume Migration pair operations (when a GAD pair operating with nondisruptive migration is blocked).

GAD pair status	I/O mode	Pair location	I/O from the server		Volume Migration operation	
			Read	Write	Migrate volumes	Stop migrating volumes
PSUE	Block	P-VOL	N	N	Y	Y
		S-VOL	N	N	Y	Y

Legend

Y: Can be performed

N: Cannot be performed

The following table shows the GAD pair status in Volume Migration when GAD and nondisruptive migration are used together, and the possibility of Volume Migration pair operations (when the GAD P-VOL is a target volume of Volume Migration).

Volume Migration pair status	Is VM P-VOL shared with NDM?	Is VM S-VOL shared with NDM?	GAD pair operation							
			Create	Suspend		Delete			Resynchronize	
				P-VOL specified	S-VOL specified	P-VOL specified [1]	S-VOL specified [2]	Force delete	P-VOL specified [3]	S-VOL specified
SMPL (PD)	Yes	No[4]	Y	Y	Y	Y	N	Y	N	N
COPY	Yes	No[4]	N	Y	Y	Y	N	Y	N	N
PSUE	Yes	No[4]	N	Y	Y	Y	N	Y	N	N
PSUS	No[4]	Yes	N	Y	Y	Y	N	Y	N	N

Legend

VM: Volume Migration

NDM: nondisruptive migration

Y: Can be performed

N: Cannot be performed

Volume Migration pair status	Is VM P-VOL shared with NDM?	Is VM S-VOL shared with NDM?	GAD pair operation							
			Create	Suspend		Delete			Resynchronize	
				P-VOL specified	S-VOL specified	P-VOL specified [1]	S-VOL specified [2]	Force delete	P-VOL specified [3]	S-VOL specified

Note:

1. You can delete a GAD pair by specifying its P-VOL, only when the I/O mode is Local and the pair status of the P-VOL is PSUS or PSUE.
2. You can delete a GAD pair by specifying its S-VOL, only when the I/O mode is Local and the pair status of the S-VOL is SSWS.
3. If a GAD pair is suspended due to a failure, you can resynchronize it by deleting the Volume Migration pair, and then specifying the GAD P-VOL.
4. You cannot use the S-VOL of Volume Migration as a volume of nondisruptive migration.

Volume Shredder

GAD pair volumes and quorum disks cannot use the Volume Shredder to delete data.

Performance Monitor

Performance Monitor can be used to collect performance information about GAD pair volumes and the quorum disk.

The amount of a port's I/O that can be added to Performance Monitor depends on the type of the volume to which I/O is issued, or on the volume's I/O mode.

For example, when the I/O mode of both GAD volumes is Mirror (RL), each time the server writes to the P-VOL, performance data is recorded for all of the following ports and volumes:

- Primary storage system port connected to the host (Target)
- Primary storage system port connected to the secondary storage system (Initiator)
- Secondary storage system port connected to the primary storage system (RCU Target)
- P-VOL
- S-VOL

When the I/O mode of both GAD volumes is Mirror (RL), each time the server reads the P-VOL data, performance data is recorded for only the primary storage system host (Target) port and the P-VOL.

Server I/Os added to Performance Monitor

The number of I/Os (reads and writes) to GAD volumes that is added to Performance Monitor depends on the GAD status, as shown the following tables.

Table 20 Writes to GAD volumes to be added to Performance Monitor

GAD status	P-VOL	S-VOL
Mirrored	The sum of the following values: ▪ Number of writes to the P-VOL ▪ Number of RIOs to the P-VOL from the S-VOL	The sum of the following values: ▪ Number of reads from the S-VOL ▪ Number of RIOs to the S-VOL from the P-VOL
Quorum disk blocked or no quorum disk volume	Number of writes to the P-VOL	The sum of the following values: ▪ Number of writes from the server to the S-VOL ▪ Number of RIOs from the P-VOL to the S-VOL
Mirroring	Number of writes to the P-VOL	Number of RIOs to the S-VOL from the P-VOL
Suspended (when the P-VOL has the latest information)	Number of writes to the P-VOL	Not counted*
Suspended (when the S-VOL has the latest information)	Not counted*	Number of writes to the S-VOL
Blocked	Not counted*	Not counted*
* Reads and writes by a server are illegal requests and cause an error. However, they could be counted as I/O.		

Table 21 Reads to GAD volumes to be added to Performance Monitor

GAD status	P-VOL	S-VOL
Mirrored	Number of reads from the P-VOL	Number of reads from the S-VOL
Quorum disk blocked or no quorum disk volume	Number of reads from the P-VOL	Number of reads from the S-VOL
Mirroring	Number of reads from the P-VOL	Not counted*

GAD status	P-VOL	S-VOL
Suspended (when the P-VOL has the latest information)	Number of reads from the P-VOL	Not counted*
Suspended (when the S-VOL has the latest information)	Not counted*	Number of reads from the S-VOL
Blocked	Not counted*	Not counted*
* Reads and writes from a server are illegal requests and cause an error. However, they could be counted as I/O.		

Table 22 Relation between the number of I/Os added to Performance Monitor and the number of server I/Os

GAD status	Number of writes	Number of reads
Mirrored	Approximately the same* as the number of writes to the P-VOL or S-VOL	The same as the total number of reads from the P-VOL and S-VOL
Quorum disk blocked	The same as the number of writes to the P-VOL	The same as the number of reads from the P-VOL
Quorum disk blocked or no quorum disk volume	The same as the number of writes to the P-VOL	The same as the total number of reads from the P-VOL and S-VOL
Mirroring	The same as the number of writes to the P-VOL	The same as the number of reads from the P-VOL
Suspended (P-VOL has latest data)	The same as the number of writes to the P-VOL	The same as the number of reads from the P-VOL
Suspended (S-VOL has latest data)	The same as the number of writes to the S-VOL	The same as the number of reads from the S-VOL
Blocked	Not counted	Not counted
* For writes by a server, RIOs might be divided before being issued. For this reason, this number might differ from the number of writes by a server.		

Port I/Os added to Performance Monitor

The number of I/Os (reads or writes) of the port added to Performance Monitor depends on the P-VOL or S-VOL (I/O destination), or on the I/O mode of the destination volume, as shown in the following table.

I/O destination volume I/O mode	I/O destination volume	Primary storage system			Secondary storage system		
		Target	Initiator	RCU Target	Target	Initiator	RCU Target
Mirror (RL)	P-VOL	Total writes and reads	Number of writes	Not added	Not added	Not added	Number of writes
	S-VOL	Not added	Not added	Number of writes	Total writes and reads	Number of writes	Not added
Local	P-VOL	Total writes and reads	Not added	Not added	Not added	Not added	Not added
	S-VOL	Not added	Not added	Not added	Total writes and reads	Not added	Not added
Block	P-VOL	Total writes and reads*	Not added	Not added	Not added	Not added	Not added
	S-VOL	Not added	Not added	Not added	Total writes and reads*	Not added	Not added
* Reads and writes by a server are illegal requests and cause an error. However, they might be counted as I/Os.							

Connection types

Three types of connections are supported for GAD physical paths: direct, switch, and channel extenders.

You can use Ops Center Administrator, or CCI to configure ports and topologies.

Establish bidirectional physical path connections from the primary to the secondary storage system and from the secondary to the primary storage system.

Direct connection

You can connect two storage systems directly to each other.

You can use the `HMO 51 (Round Trip Set Up Option)` host mode option (HMO) to improve response time of host I/O by improving response time between the storage systems for distance direct connections (up to 10 km Long Wave) when the open package is used.

Note: If you use iSCSI, the HMO settings become invalid.

For more information about HMOs, see the *Provisioning Guide* for your storage system.

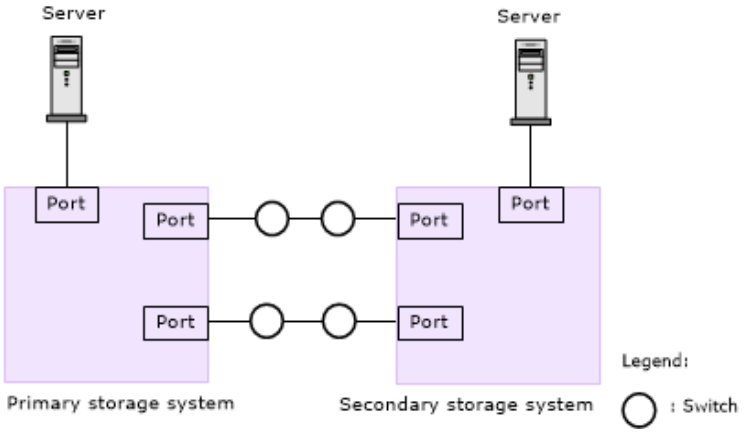
The fabric and topology settings depend on the settings of packages, the protocol used for the connection between the storage systems, and the setting of HMO 51. The link speed that can be specified differs for each condition.

Package name	Protocol	HMO 51 setting	Fabric setting	Topology: remote replication ports	Link speed that can be specified
CHB(FC32G)	32GbpsFC	OFF	OFF	FC-AL	▪ 4 Gbps ▪ 8 Gbps

Connection using switches

You can use host mode options to improve response times when switches are used for distance connections.

Note: You do not need to set the port attributes on VSP E series, VSP G/F350, VSP G/F370, VSP G/F700, or VSP G/F900 models.



Switches from some vendors (for example, McData ED5000) require F_port.

You can use the `HMO 51 (Round Trip Set Up Option)` host mode option (HMO) to improve response time of host I/O by improving response time between the storage systems when switches are used for distance connections (up to approximately 500 km with a round-trip response of 20 ms or less) and the open package is used.

For details about HMOs, see the *Provisioning Guide* for the storage system.

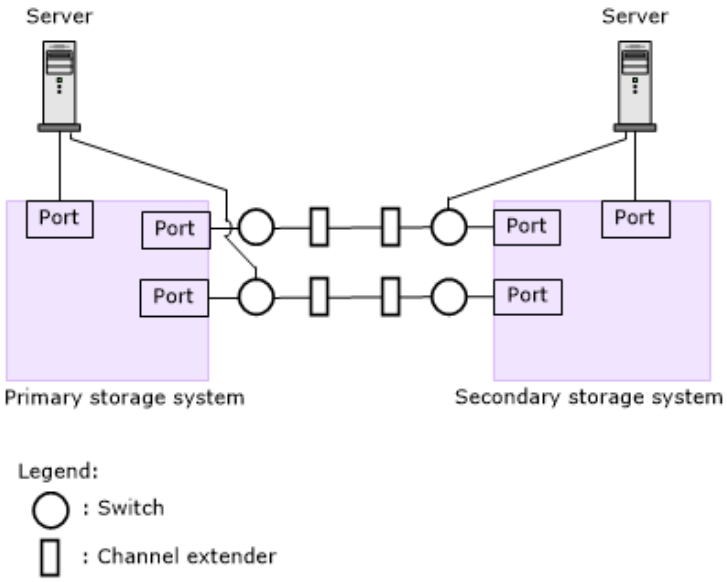
The fabric and topology settings depend on the settings of packages, and protocol used for the connection between storage systems, and the HMO 51 setting. The link speed that can be specified differs on each condition.

Package name	Protocol	HMO 51 setting	Fabric setting	Topology: Initiator and RCU Target	Link speed that can be specified
CHB(FC32G)	32GbpsFC	OFF	ON	Point-to-Point	▪ 4 Gbps ▪ 8 Gbps ▪ 16 Gbps ▪ 32 Gbps
CHB(FC32G) (VSP E series, VSP G/F350, G/F370, G/F700, G/F900)	32GbpsFC	ON	ON	Point-to-Point	▪ 4 Gbps ▪ 8 Gbps ▪ 16 Gbps ▪ 32 Gbps

Connection using channel extenders

You should use channel extenders and switches for long-distance connections (up to 500 km and the round trip time is 20 ms or less). Set Fabric to ON and topology to Point-to-Point for the remote replication ports.

Note: You do not need to set the port attributes on VSP G/F350, G/F370, G/F700, G/F900, or VSP E series.



Note:

- When the primary and secondary storage systems are connected using switches with a channel extender, and multiple data paths are configured, the capacity of data to be transmitted might concentrate on particular switches, depending on the configuration and the settings of switch routing. Contact customer support for more information.
- Make sure that your channel extenders can support remote I/O. For details, contact customer support.
- Create at least two independent physical paths (one per cluster) between the primary and secondary storage systems for hardware redundancy for this critical element.
- If you plan to use more than 4,000 pairs, when creating pairs you should restrict the number of pairs to 4,000 or less per physical path to distribute the load across multiple physical paths.

Chapter 3: Setting up high availability

You can use Ops Center Administrator to set up your environment for high availability.

Ops Center Administrator enables you to perform essential high availability setup tasks that include the following:

- Managing remote paths
- Managing external volumes and quorum disks
- Managing virtual storage machines

Procedure

1. On the **Storage Systems** window, click **Settings** and select **High Availability Setup**.
2. On the **High Availability Setup** window, select the primary and secondary storage systems.
3. For each setup procedure, open the menu, then click **Launch for Primary Storage** to complete the procedure for the primary storage system. Then click **Launch for Secondary Storage** and perform the procedure for that storage system.
   For managing remote paths, external volumes, and quorum disks, either Device Manager - Storage Navigator or Storage Advisor Embedded starts, depending on the storage system model. VSMs are managed by Ops Center Administrator. Storage Advisor Embedded is started only for VSP E series and VSP G/F350, G/F370, G/F700, G/F900 storage systems without an SVP.

Overview of the workflow for global-active device

The workflow for setting up the environment for global-active device is as follows.

Procedure

1. Register the global-active device license.
2. Add the external storage system for the quorum disk in your environment.
3. Configure remote paths between the primary and secondary storage systems.
   - Use Storage Navigator for VSP 5000 series, VSP G1x00, F1500 and VSP G200, G/F400, G/F600, G/F800.
   - Use Storage Advisor Embedded for VSP E series and VSP G/F350, G/F370, G/F700, G/F900.
4. Configure the quorum disk.
5. Onboard primary and secondary storage systems in Ops Center Protector using Hitachi Block Storage Node Wizard.

6. Onboard primary and secondary storage systems in Ops Center Administrator .
   - Use storage systems onboarding workflow in Ops Center Administrator
   - Add servers
7. Register Ops Center Protector with Ops Center Administrator.
8. Create and manage virtual storage machines for high availability.

Register the global-active device license

Follow the instructions in the next sections to register the global-active device license with your virtual storage platform.

Registering the global-active device license for VSP E series and VSP G200, G/F400, G/F600, G/F800 storage systems

Register the global-active device license to install the software on your virtual storage platform.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to complete this task.
- You must install a license key for each software application before you use it.

Procedure

To register the global-active device license, perform the following steps:

1. From the **Administration** tree, click **License Keys**.
2. In the **License Keys** window, click **Install Licenses**.
3. Select whether to enter a key code or specify a license key file:
   - **License Key Code**: Enter the license key code for the software.
   - **License Key File**: Specify a license key file to install the software. Click **Browse** and navigate to the license key file. You can use a file name of up to 200 alphanumeric characters, excluding several symbols (" \ ; : * ? < > | / ,). The file extension is "plk".
4. Click **Add**, and then click **Finish**.

   If a software installation fails, the **Error Message** window opens. To display the cause of error, from the **Error Message** window, select the software and click **Detail**.

Registering the global-active device license for VSP E series and VSP G/F350, G/F370, G/F700, G/F900 storage systems

Register the global-active device license to install the software on your virtual storage platform.

Before you begin

- Prepare the license key code or the license key file for the software you are installing.
- Start the maintenance utility from Hitachi Storage Advisor Embedded.
- Complete the following procedure on the primary and secondary storage system.

Procedure

1. In the navigation bar, click (**Settings**), and then select **Licenses**.
2. In the maintenance utility, click **Install**.
3. Specify the license key code or the license key file, and register the license key.

   Tip: For more information, refer to Help in the maintenance utility.

4. In the list of license keys, confirm that the status of the software product has changed to **Installed**.
5. In the maintenance utility, click **Log Out**.

Registering the global-active device license for VSP G1x00, F1500 and VSP 5000 series storage systems

Register the global-active device license to install the software on your virtual storage platform.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to complete this task.
- You must install a license key for each software application before you use it.

Procedure

1. From the **Settings** menu, click **Environmental Settings.**
2. In the **Environmental Settings** window, click **Install Licenses**.
3. Select whether to enter a key code or specify a license key file:
   - **License Key Code**: Enter the license key code for the software.
   - **License Key File**: Specify a license key file to install the software. Click **Browse** and naviage to the license key file. You can use a file name of up to 200 alphanumeric characters, excluding several symbols (" \ ; : * ? < > | / ,). The file extension is "plk".
4. Click **Add**, and then click **Finish**.
5. Click **Apply**.

Add an external storage system for the quorum disk

Install an external storage system for the quorum disk. The storage system must be supported by Universal Volume Manager for connection as external storage.

Configure remote paths

To configure remote paths between the primary and secondary storage systems that make up a high availability environment, follow these instructions. To send data to the connection-destination storage system, you must configure remote paths for both storage systems so they can send data to each other.

Configuring remote paths for VSP 5000 series and VSP E series, VSP F series, VSP G series

Use Storage Navigator to configure remote paths between the primary and secondary storage systems.

Before you begin

- Storage Administrator (Remote Copy) role is required.
- Physical paths are set between the primary and secondary storage systems.
- The port attributes of local and remote storage systems are defined for high availability.
- You know the remote storage system model, serial number, and path group ID.

Procedure

1. Navigate to the **Storage Systems** window click **Settings** and then click **High Availability Setup**.
2. On the **High Availability Setup** window, select the primary and secondary storage systems, then click **Proceed**.
3. Click **Remote Paths** to expand the window, then click **Launch for Primary Storage** or **Launch for Secondary Storage** to open the **Remote Connections** window in Device Manager - Storage Navigator.
4. Click **Add Remote Connection** to open the **Add Remote Connection** window.
   - **Model**: Select the remote storage system model.
     - For VSP G1x00, F1500 storage systems, select 7.
     - For VSP G200, G/F400, G/F600, G/F800 and VSP E series storage systems, select 18.
     - For VSP 5000 series storage systems, select 8.
   - **Serial Number**: Enter the five- or six-digit serial number for the remote storage system.

5. Set the items in **Remote Paths**.
   - **Path Group ID**: Select the ID for the path group.
   - **Minimum Number of Paths**: Specify the minimum number or paths that are required for each remote storage systems that are connected to the current local storage system. When the number of normal paths become fewer than the value specified in **Minimum Number of Paths**, the local storage system suspends all GAD pairs that will be affected and prevents the server performance from being harmed due to insufficient number of paths.
   - For **Select Type**, select the port type. Then select the port to be used for both the local storage system and the remote storage system. These are the ports by which the storage systems are already physically connected. To add more paths, click **Add Path**. You can also add and delete paths later as needed using the **Add Remote Paths** window.
6. (Optional) Enter the **RIO MIH Time**.

   You can enter a value between 10 and 100. The default setting is 15.

   The RIO MIH (Remote I/O Missing Interrupt Handler) is the waiting time from when copy starts until when it ends. This value applies to the slots which received the request of copying data between storage systems.
7. (Optional) Enter **Round Trip Time** in milliseconds, if necessary.

   The round-trip time is a time limit for data to travel from the P-VOL to the S-VOL. This value is the reference value to control the copy pace of the initial copy automatically when the initial copy is performed, and to lessen the impact to the response time of the remote I/O for the update I/O.
8. Click **Finish**.
9. In the **Confirm** window, verify the settings you made, and then enter the task name in **Task Name**.
10. Click **Apply**.

    The task is registered. The **Tasks** window appears if the **Go to tasks window for status** check box is selected.
11. On the **Tasks & Alerts** tab, you can click the task name to view progress and other details.

Configuring remote paths for VSP E series and VSP G/F350, G/F370, G/F700, G/F900 storage systems

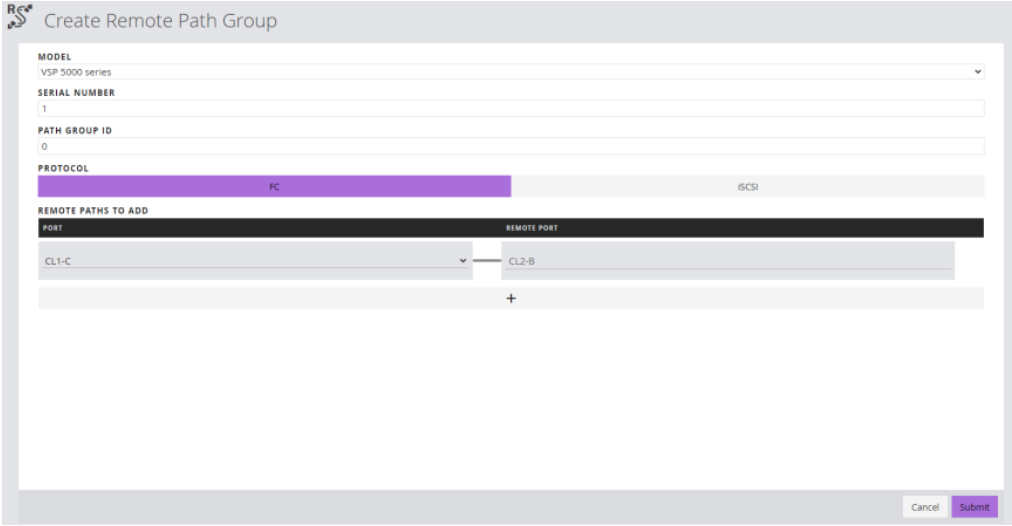
Before you begin

Use Storage Advisor Embedded to configure remote paths between the primary and secondary storage systems.

- Connect the physical paths between the two storage systems making up the global-active device environment.
- Identify the following items:
  - The model and serial number of the connection-destination storage system
  - The ID of the path group
  - The port to be used on the connection-source storage system and the port of the connection-destination storage system

Procedure

1. In the **High Availability Setup** page, open the **Remote Paths** menu, then click **Launch for Primary Storage** or **Launch for Secondary Storage** to open the **Create Remote Path Group** page in Storage Advisor Embedded.
2. In the navigation bar, click **Others** > **Remote Path Groups**.
3. Click the plus sign (**+**).



4. Specify the required items, and then configure the remote path.
5. Click the ID of the path group to open the details page. Make sure that the status of the remote path you configured is **Normal**.

Configure the quorum disk

Configure the quorum disk for your virtual storage platform.

Configuring the quorum disk for VSP E series, VSP G200, G/F400, G/F600, G/F800, VSP G1x00, F1500 , and VSP 5000 series

Configure the quorum disk for your virtual storage platform.

Discover and add external volumes

Discover and add external volumes for your virtual storage platform.

Procedure

1. In the **High Availability Setup** page, expand the **Manage Quorum Disks** menu, then click **Launch for Primary Storage** or **Launch for Secondary Storage** to open the **External Storage** page in Device Manager - Storage Navigator.
2. In the **External Storage Systems** window click **Add External Volumes**.
3. In the **Add External Volumes** window, click **Create External Path Group** and enter an **Initial External Path Group ID**. Click **Discover External Target Ports**.
4. Select an **External Storage System** and then click **Discover External Target Ports**.
5. Select the ports you want to scan, then click **Add** to move them to **Selected External Ports**.
6. Click **OK**, then click **Next**.

   If there are no external volumes discovered, you can add one to the host group.
7. In the **Add External Volumes** window click **Next**.
8. Enter an LDEV name and then select the volumes you want to use in **Discovered External Volumes**.
9. Click **Finish** and then **Apply**.

Adding the quorum disk

Add the quorum disk on the primary and secondary storage systems.

Before you begin

- Storage Administrator (Provisioning) role is required.
- The mapping of volumes of the external storage system for the quorum disk has been completed.

Procedure

1. Click **Add Quorum Disks** to open the **Add Quorum Disks** window.
2. Select a **Quorum Disk ID**.
3. In the **Available LDEVs** table, select the volume you want to set to the quorum disk.
4. Select a Remote Storage System.
5. Click **Add**. To remove the selected quorum disks from the **Selected Quorum Disks** table, select the quorum disk, and then click **Remove**.
6. Click **Finish**.
7. In the **Confirm** window, verify the settings you made, and then enter the task name in **Task Name**.

8. Click **Apply**. The task is registered. The Tasks window appears if the Go to tasks window for status check box is selected.

Configuring the quorum disk for VSP E series and VSP G/F350, G/F370, G/F700, G/F900 models

You can use Storage Advisor Embedded to create an external volume to configure a quorum disk, or to configure a quorum disk by using an external volume that has already been created.

Configuring a quorum disk by creating an external volume

Before you begin

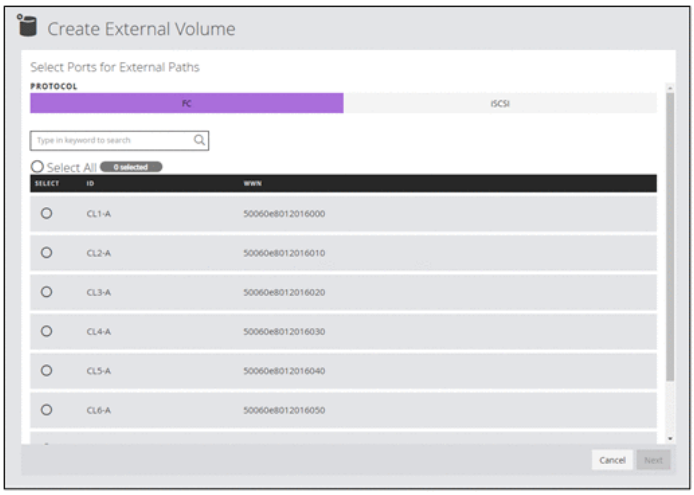
Create an external volume in the two storage systems making up the global-active device environment, and specify settings to use the external volume as a quorum disk.

- Ensure that the two storage systems making up the global-active device environment and the external storage system in which the volume used as the quorum disk is configured are connected by physical paths.
- Ensure that the volume that is used as the quorum disk is assigned a port on each of the two storage systems making up the global-active device environment.
- Identify the following items required to configure the external volume:
  - The port to be used for external connection
  - The model and serial number of the external storage system
  - The port information for the external storage system that is connected with a port for external connections:
    - When using Fibre Channel for the protocol you can specify WWN
  - The LUN of the volume used as the quorum disk

    If you use a volume whose size exceeds 4 TiB, the size of the external volume that is created will be 4 TiB.
  - The name of the external volume
  - The ID of the external parity group
  - The ID of the external path group
- Identify the following information required to configure the quorum disk:
  - The ID of the quorum disk
  - The models and serial numbers of the paired storage system that shares the quorum disk

Procedure

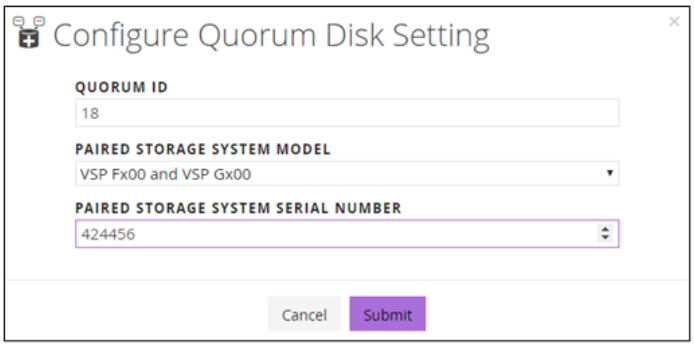
1. In the navigation bar, click **Others** > **External Volumes**.
2. Click the plus sign (**+**).



3. Select the port for external connection, and then click **Next**.
4. Select the external path to be used, and then click **Next**.
5. Select the LUN of the volume used as the quorum disk, and specify the name of the external volume, the ID of the external parity group, and the ID of the external path group. Click **Submit**.

   Information about the newly configured external volume is displayed in the list of external volumes.

6. Click (**Configure Quorum Disk Setting**) for the external volume for which the quorum disk is to be configured.



7. Specify the required items, and then click **Submit**.

Configuring a quorum disk by selecting an external volume

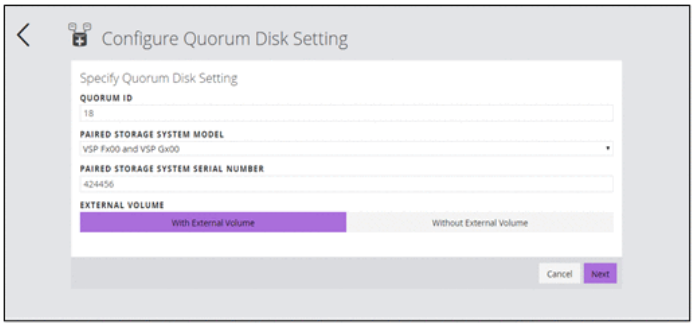
Before you begin

You can configure a quorum disk by using an existing external volume.

- Identify the following information required to configure the quorum disk:
  - The ID of the quorum disk
  - The models and serial numbers of the paired storage system that shares the quorum disk
  - The external volume name

Procedure

1. In the navigation bar, click **Others** > **Quorum Disks**.
2. Click the plus sign (**+**).



3. Specify the required items.

   To specify the external volume to be used, select **With External Volume**, and then click **Next**.
4. Select the external volume to be used, and then click **Submit**.

Configuring a quorum disk without using an external volume

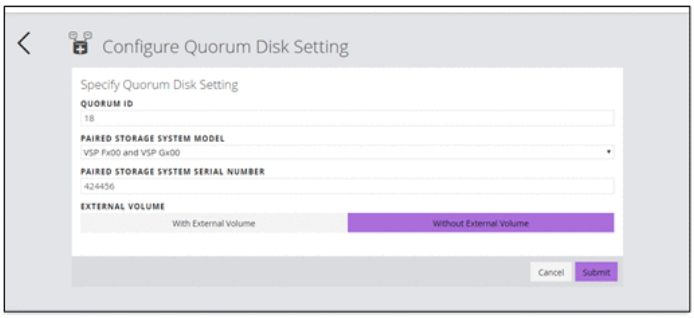
Before you begin

To temporarily configure a global-active device environment for such purposes as system migration, you can configure a quorum disk without using an external volume.

- Identify the following information required to configure the quorum disk:
  - The ID of the quorum disk
  - The models and serial numbers of the paired storage system that shares the quorum disk

Procedure

1. In the navigation bar, click **Others** > **Quorum Disks**.
2. Click the plus sign (**+**).



3. Specify the required items.

   To configure a quorum disk without using an external volume, select **Without External Volume**, and then click **Submit**.

Onboard primary and secondary storage systems in Ops Center Protector

Onboard the primary and secondary storage systems in Ops Center Protector.

Procedure

1. To add a block node to the nodes inventory, click **Nodes** in the navigation sidebar. Click the plus sign (**+**).
2. In the **Create Node** window, select **Storage**. Select **Hitachi Block Device** as the storage type to launch the Hitachi Block Storage Node wizard. Follow the wizard prompts to complete the workflow.
3. Specify the node name, select the check box to confirm the requirements, and then click **Next**.
4. Select the resource group to which this node is allocated for the purposes of RBAC and click **Next**. All nodes are automatically allocated to the 'default' resource group.
5. Select a Hitachi Ops Center Protector node to act as a proxy and click **Next**.

   Note: The proxy node is responsible for interfacing with the block storage system. It can be a Windows or Linux machine with the Hitachi Ops Center Protector Client software installed and must be connected using a command device to the Block storage system. The command device must only have user authentication enabled. The proxy node must have supported version of CCI installed. See the *Command Control Interface Installation and Configuration Guide* for more information.

6. Enter the directory location on the proxy node where Hitachi Ops Center Protector can place metadata files related to Block snapshots and replications. Click the **Browse** button to open the Path window if required.

   Note: The metadata directory is defined once for this proxy and all storage nodes on this proxy will use this setting. It cannot be changed after initial configuration.

7. Specify the storage system. You can either select from detected storage systems or specify the IP address of a storage system.

   Note: For HUS VM storage systems, use the IP address of the SVP. For VSP storage systems, use the IP address of CTL1 or CTL2. DO NOT use the IP address of the SVP.

8. Specify the credentials for the storage system.

   Enter the username and password for the Block storage.

   Note:

   - The username specified must be a member of the Storage Administrator (Provisioning, Local Copy, Remote Copy) and Security Administrator (View Only, View and Modify) on the Block device. If the Block storage cannot be accessed or its credentials are invalid then the node will fail authorization. The configuration wizard can be reopened to correct any errors.
   - The password for authorizing a Block storage system must contain only CCI command characters: A-Zaz0- 9'-./:@_

9. Specify the LDEV Provisioning Range. You can select one of the following options:

   - All: Select this option if you want Ops Center Protector to automatically detect the LDEV range from which snapshots and replications should be allocated.
   - User defined: Select this option if you want to manually specify the LDEV range from which snapshots and replications should be allocated.
   - Start: Enabled only if User defined is selected. Enter the lower limit of the LDEV range to use for allocation.
   - End: Enabled only if User defined is selected. Enter the upper limit of the LDEV range to use for allocation.

10. Specify the command device specification and priority.

    If no command devices are specified, Hitachi Ops Center Protector will attempt to control the hardware storage device using any fibre connected command device, available to the Proxy Node specified, in an order specified by HORCM. If one or more command devices are specified, Hitachi Ops Center Protector will attempt to control the hardware storage device using a command device in the order specified by the user. If the first command device fails, Hitachi Ops Center Protector will progress to the next. If all specified command devices fail then the operation fails. Hitachi Ops Center Protector will not attempt to use any command devices that are not specified, even if they are available.

    For example, it is possible to specify a specific fibre command device, followed by any fibre command device, followed by a specific IP command device.

11. Configure the command device.

    - Fibre: You can either use any available fibre command device or select from detected fibre command devices.
    - IP: Enter the IP address and port number of the command device.

> **Note:** When configuring IP command devices for VSP storage devices, we recommend adding one for CTL1 and one for CTL2, to maintain dual redundancy. For HUS VM storage devices, use the IP address of the SVP. For VSP storage devices, use the IP address of CTL1 or CTL2. DO NOT use the IP address of the SVP.

12. Specify the LDEV ranges for each VSM.

> **Note:** Note: global-active device replications require P-VOLs and S-VOLs to have matching virtual serial numbers and virtual LDEV IDs. To avoid virtual LDEV ID collisions between global-active device volumes and non-global-active device S-VOLs (created by Hitachi Ops Center Protector for other types of replications and snapshots), it is possible to define virtual LDEV ID ranges to be used by those non-global-active device operations. Virtual LDEV ranges can be specified for each VSM (Virtual Storage Machine) to be used.

13. Configure the virtual LDEV range.
    - Enter the VSM serial number.
    - Enter the lower limit of the LDEV range to use for allocation.
    - Enter the upper limit of the LDEV range to use for allocation.
14. Specify the ports used for provisioning.
    Enter the port identifier in the following format:

    CLc-s

    where:
    - c is the physical channel number in the range 1 …n
    - s is the physical slot number in the range A … Z

    > **Note:** If more than one provisioning port is selected, the port with the least amount of LUNs will be used.

15. Review the summary of the Block storage system and click **Finish**.

Onboard primary and secondary storage systems in Ops Center Administrator

Onboard the primary and secondary storage systems in Ops Center Administrator.

Adding a storage system in Ops Center Administrator

Onboarding a storage system is the process of associating it with Ops Center Administrator. After the storage system is onboarded, manage it from the Ops Center Administrator dashboard.

To add a storage system without an SVP, you can specify either of the GUM IP addresses.

Before you begin

Ops Center Administrator requires access to all resources groups on the storage system so that the workflows function correctly. Verify that the service processor (SVP) user name used to onboard a storage system in Ops Center Administrator has access to all custom resource groups and meta resource groups.

The user must be a member of the Administration Users Group.

Procedure

1. On the Ops Center Administrator dashboard, click **Storage Systems** on the left pane.
2. Click the plus sign (**+**) to add a storage system.
3. Enter values for the following parameters on the **Onboard Storage System** page.
   - **IP Address:** For a storage system with an SVP, enter the IP address of the external service processor for the storage system you want to discover.
   - **User name and password:** Log in as a user that has administrator privileges on this storage system. For example, you can log in as the user `maintenance`.
4. Click **Submit**.

Result

The Jobs tab is updated with the job called `Create Storage System`. If multiple storage systems are being added, there will be a job for each one.

Wait a while for the storage system to be added. Refresh the Jobs tab to verify that storage system is onboarded.

The dashboard shows the displayed number of storage systems has been incremented by one. Additionally, when you click Storage Systems, you are redirected to the storage system inventory where you can see the newly added storage system.

When a storage system is onboarded, Ops Center Administrator goes through an initialization process where it gathers the information about the current configuration of the storage system. During this time you will see that the ports, volumes, pools, and parity groups in the storage system are "Not accessible". Once the initialization is complete, you can see the port, pool, volume, and parity group information in the storage system details.

Note: If operations are performed outside of Ops Center Administrator, it takes time to update in Ops Center Administrator (approximately 20 minutes, depending on cache refresh).

Next steps

1. In the parity group inventory for the storage system, create parity groups to convert the raw disk capacity into usable capacity.
2. From the settings menu, access the tier definitions before creating pools.

Adding servers

Use Ops Center Administrator to add servers so you can attach volumes. You can add multiple server parameters from a file, or add one server at a time.

There are two methods of adding servers:

- Manually add information for one server at a time.
- Import a CSV (comma-separated values) file with information for one server in each row.

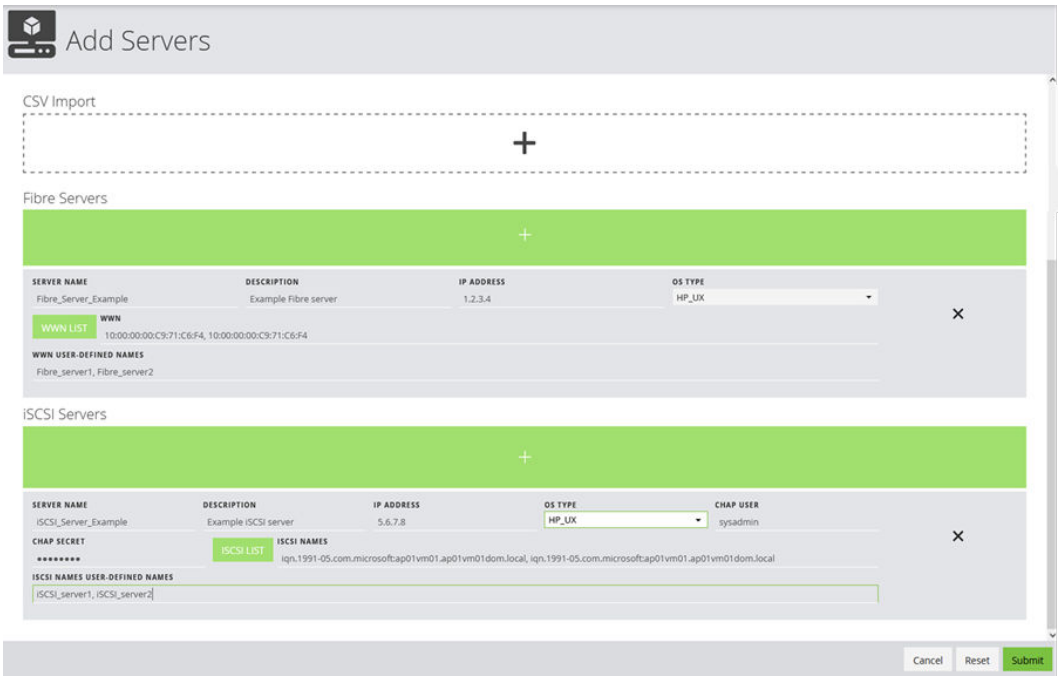
  The CSV file must have the following headings, in the order specified: Name, Description, IPAddress, OSType, WWNs (comma separated list of WWNs), WWNsUserDefinedNames (comma-separated list of user-defined names for WWNs). All fields are required except Description, IPAddress and WWNsUserDefinedNames.Valid OSType values are as follows:

  - AIX
  - HP_UX
  - LINUX
  - NETWARE
  - OVMS
  - SOLARIS
  - TRU64
  - VMWARE
  - VMWARE_EX
  - WIN
  - WIN_EX

Procedure

1. On the Ops Center Administrator dashboard, click **Servers**. Then click the plus sign (**+**) to open the **Add Server** page.

   Note: iSCSI is not currently supported for high availability.



2. In the **Add Server** window, do one of the following:
   - Click the upper plus sign (**+**) to browse for the CSV file or drag the file to the plus sign. The values from the file populate the window. Example:

     ```
     Name,Description,IPAddress,OSType,WWNS,WWNsUserDefinedNames
     Esxi,ESXI
     HOST,10.30.90.200,VMWARE_EX,10:00:00:05:33:26:f7:21,Esxi_HBA_1
     Win,WINDOWS
     HOST,10.30.91.80,WIN_EX,"10:00:00:05:33:26:f7:37,10:00:00:05:3
     3:26:f7:36","HOST_HBA_1,HOST_HBA_2"
     ESXi_Cisco_1,ESXi HOST connected to Cisco
     Fabric,,VMWARE_EX,"10:00:00:05:33:26:e0:fc,10:00:00:05:33:26:e
     0:fd","Fabric_HBA_1"
     ESXi_Cisco_2,ESXi HOST connected to Cisco
     Fabric,,VMWARE_EX,"100000053326df1a,100000053326df1b",",Fabric
     _HBA_2"
     ```
   - Click the plus sign (**+**) in the table to add a row and enter the required information for Fibre Channel. You can add more servers by clicking the plus sign again.
   - (Optionally) You can use the **WWN List** to add/edit a server.
   - (Optionally) You can add comma-separated user-defined names for WWNs names in the order they are specified.
3. Click **Submit** to add the servers.

Next steps

Create volumes and attach them to the server.

Register Ops Center Protector with Ops Center Administrator

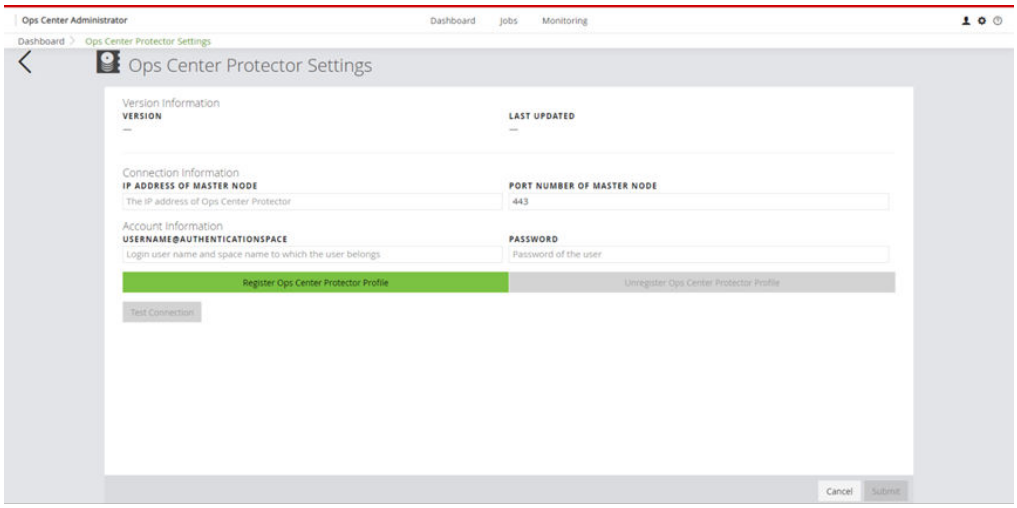
You can use Ops Center Administrator to register Ops Center Protector.

Before you begin

Ops Center Protector is installed. The user with permissions to perform pair management operations is identified.

Procedure

1. From the **Settings** menu, click **Ops Center Protector Settings**.
2. Under **Connection Information**, enter the IP address of the Master node. The port number of the Master node displays automatically.
3. Under **Account Information**, enter the user name and password of the Ops Center Protector user who can perform pair management operations for high availability.
4. Click **Test Connection** to verify that you connected to the Master node successfully.
5. Click **Submit**.



Managing virtual storage machines for high availability

You can manage virtual storage machines for high availability in Ops Center Administrator.

You can either create a new VSM, or use an existing one. The VSM must contain the primary and secondary storage systems.

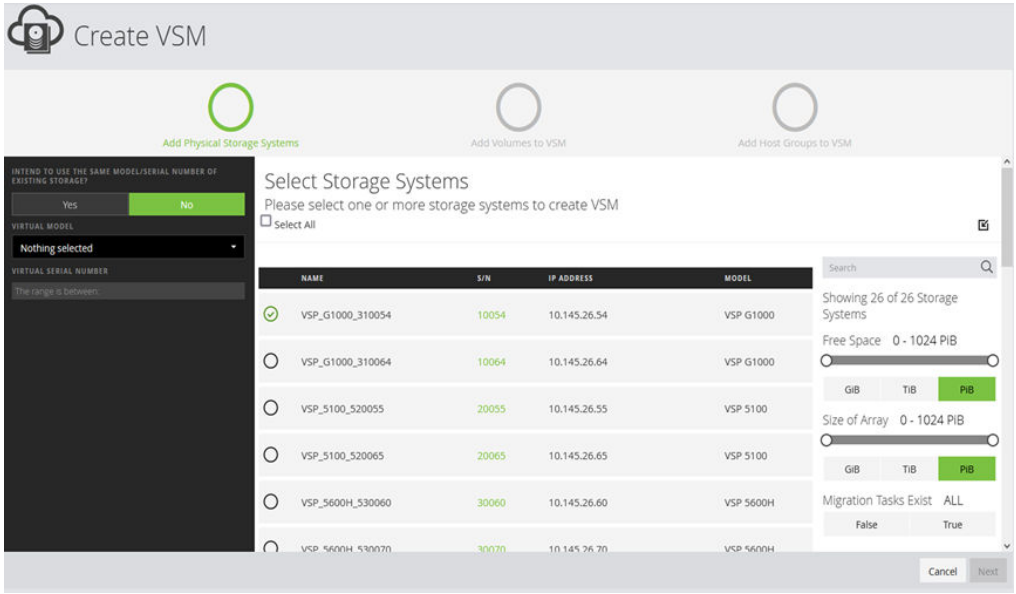
Creating virtual storage machines

You can use Ops Center Administrator to create virtual storage machines.

Each virtual storage machine must have a model number and a serial number. After assigning those, you can add volumes and host groups.

Procedure

1. On the dashboard, click **Virtual Storage Machines** and then click the plus sign (+) on the **Virtual storage machines** window.
2. On the **Create VSM** window, select the storage systems you want to use.



3. Choose whether to use the model and serial number of one of the selected storage systems for the new virtual storage machine.
   - If you choose **YES**, the entire meta_resource group of the storage system will be the virtual storage machine.
   - Click **NO** to select a virtual model and a virtual serial number.

   Note: If a resource group already exists, it will be used and a new one will not be created.

4. Click **Next** to add volumes to the virtual storage machine.

   You can add volumes from any or all selected storage systems, or skip this and the next step and add volumes later.
5. For each storage system you selected, specify undefined volumes you want to add by choosing one of the following from the **Specify Volumes By** drop down:
   - Select **Number of Volumes** and enter a number in the **Number of Volumes** field beneath it.
   - Select **Number of volumes and volume ID range** and enter the **Number of Volumes** and **Volume ID/Range** in the fields beneath it.
   - Select **Volume ID range (add all volumes within the range)** and enter the **Volume ID/Range** in the field beneath it.
6. Click **Next** to add host groups. Add host groups from one storage system at a time, then click the plus sign (**+**) to add them to the list.
7. Click **Submit** to create a job to add the virtual storage machine.

Manage virtual storage machines

Ops Center Administrator allows you to create virtual storage machines and add volumes and host groups to them.

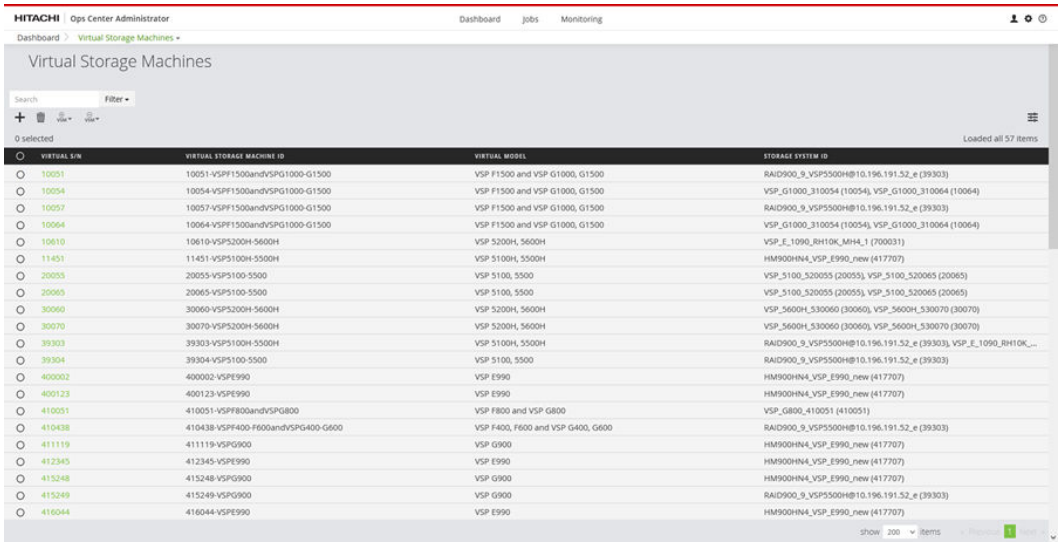
You can also add defined and undefined resources to an existing virtual storage machine and remove defined and undefined resources from an existing virtual storage machine.

> **Note:** To manage VSMs for high availability setup, click Go to VSM Inventory in the High Availability Setup window.

Virtual storage machine inventory

You can access the Virtual Storage Machines window to view all virtual storage machines and perform procedures on them.

Click Virtual Storage Machines on the dashboard to open the **Virtual Storage Machines** inventory.



The following actions are available on this window:

- Click a storage system ID to open the virtual storage machine details window.
- Select one or more virtual storage machines, then click Delete to permanently remove them.

  All resources will be removed from the virtual storage machine and the virtual storage machine will be deleted. Removed resources will be moved to the meta resource group. A virtual storage machine with attached volumes or HA pairs cannot be deleted.

- Select a virtual storage machine, then click Remove VSM to open the menu and do one of the following:
  - Click Remove Defined Volumes from VSM to open the **Remove Defined Volumes from VSM** window and remove volumes from the virtual storage machine.
  - Click Remove Undefined Resources from VSM to open the **Remove Undefined Resources from VSM** window and remove resources from the virtual storage machine.
- Select a virtual storage machine, then click Add VSM to open the menu and do one of the following:
  - Click Move Volumes to VSM to open the **Move Volumes to VSM** window and move volumes from a storage system to a virtual storage machine.
  - Click Add Resources to VSM to open the **Add Undefined Resources to VSM** window and add resources from one or more storage systems to a virtual storage machine.

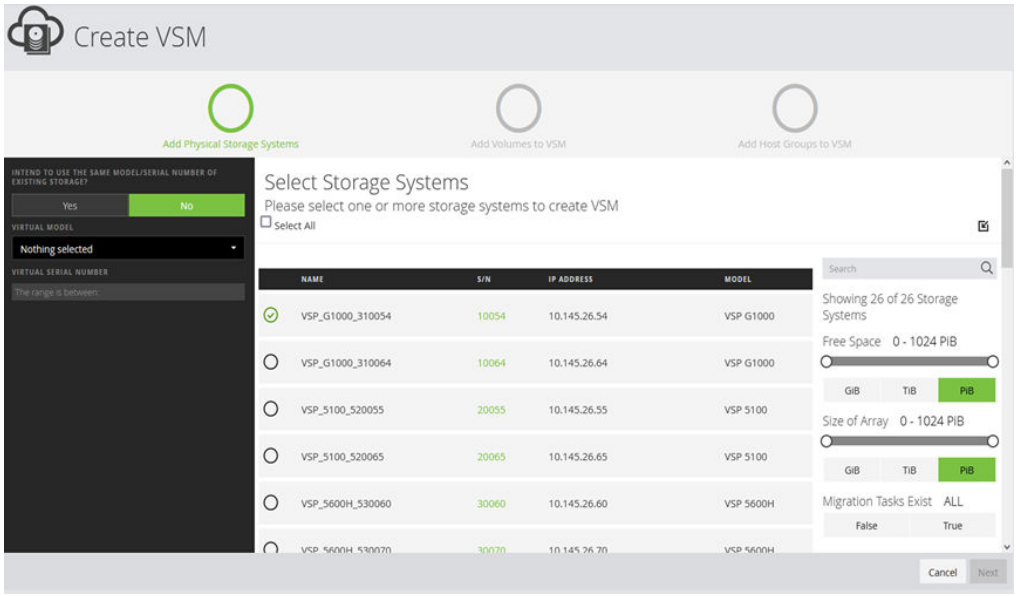
Creating virtual storage machines

You can use Ops Center Administrator to create virtual storage machines.

Each virtual storage machine must have a model number and a serial number. After assigning those, you can add volumes and host groups.

Procedure

1. On the dashboard, click **Virtual Storage Machines** and then click the plus sign (+) on the **Virtual storage machines** window.
2. On the **Create VSM** window, select the storage systems you want to use.



3. Choose whether to use the model and serial number of one of the selected storage systems for the new virtual storage machine.
   - If you choose **YES**, the entire meta_resource group of the storage system will be the virtual storage machine.
   - Click **NO** to select a virtual model and a virtual serial number.

   Note: If a resource group already exists, it will be used and a new one will not be created.
4. Click **Next** to add volumes to the virtual storage machine.

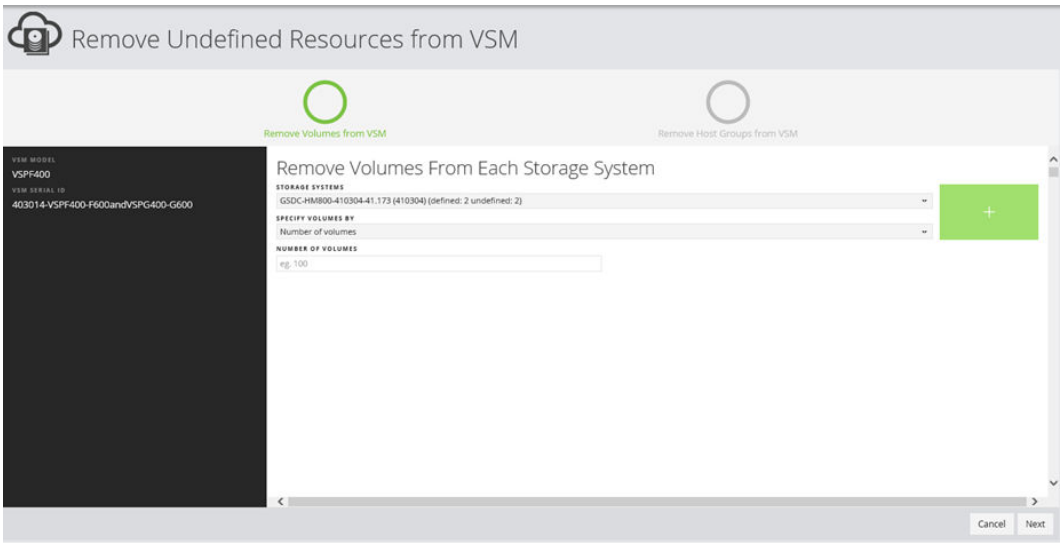
   You can add volumes from any or all selected storage systems, or skip this and the next step and add volumes later.
5. For each storage system you selected, specify undefined volumes you want to add by choosing one of the following from the **Specify Volumes By** drop down:
   - Select **Number of Volumes** and enter a number in the **Number of Volumes** field beneath it.
   - Select **Number of volumes and volume ID range** and enter the **Number of Volumes** and **Volume ID/Range** in the fields beneath it.
   - Select **Volume ID range (add all volumes within the range)** and enter the **Volume ID/Range** in the field beneath it.
6. Click **Next** to add host groups. Add host groups from one storage system at a time, then click the plus sign (**+**) to add them to the list.
7. Click **Submit** to create a job to add the virtual storage machine.

Removing undefined resources from a virtual storage machine

You can remove undefined resources if you no longer need them.

Procedure

1. On the **Virtual Storage Machines** window, click the VSM icon (⊖) and select **Remove Undefined Resource** from VSM from the menu.
2. On the **Remove Undefined Resources from VSM** window, select a storage system from the menu.



3. For each storage system you selected, specify undefined volumes you want to remove by choosing one of the following from the **Specify Volumes By** drop down:
   - Select **Number of Volumes** and enter a number in the **Number of Volumes** field beneath it.
   - Select **Number of volumes and volume ID range** and enter the **Number of Volumes** and **Volume ID/Range** in the fields beneath it.
   - Select **Volume ID range (remove all volumes within the range)** and enter the **Volume ID/Range** in the field beneath it.
4. Click the plus sign (**+**) to display your selections in the lower half of the window. Add more selections if needed.
5. Click **Next**.
6. Remove host groups using the same procedure as for volumes.
7. Click **Submit** to start a job to remove the undefined resources.

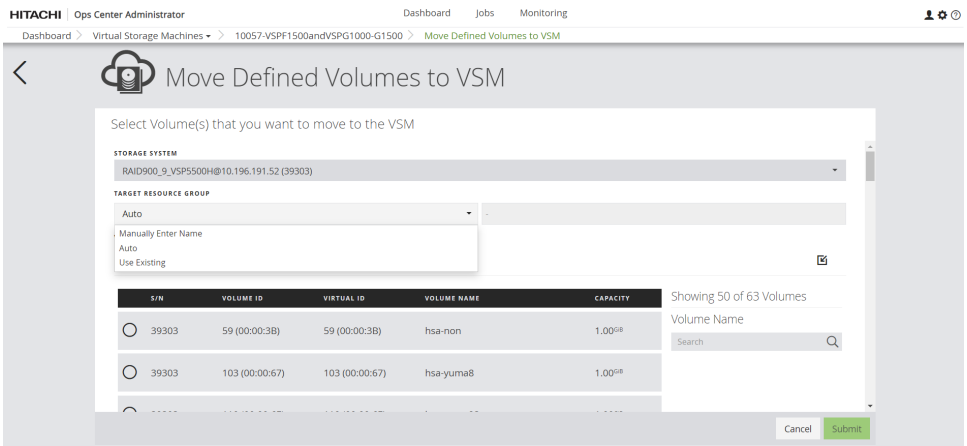
Moving defined volumes to a virtual storage machine

You can move defined volumes from a storage system that is in a virtual storage machine to the virtual storage machine.

Procedure

1. Select a virtual storage machine in the **Virtual Storage Machines** window.
2. Select **Add VSM** then click **Move Defined Volumes to VSM**.

   Note: You can access the **Move Defined Volumes to VSM** window from the **Volumes** tab of the virtual storage machine detail window.
3. Select the volumes to be moved. You can specify the resource group from the **TARGET RESOURCE GROUP** menu. By default, the resource group name is assigned automatically.
4. Click **Submit** to start a job to move the volumes.



Adding resources to a virtual storage machine

You can add additional resources to a virtual storage machine.

Procedure

1. To access the **Add Undefined Resources to VSM** window, select a virtual storage machine on the **Virtual Storage Machines** window.
2. Click the VSM icon ( ) and select **Add Undefined Resources to VSM**.

3. Optionally, select one or more storage systems, then click **Next** to add volumes.
4. For each storage system you selected, specify undefined volumes you want to add by choosing one of the following from the **Specify Volumes By** drop down:
   - Select **Number of Volumes** and enter a number in the **Number of Volumes** field beneath it.
   - Select **Number of volumes and volume ID range** and enter the **Number of Volumes** and **Volume ID/Range** in the fields beneath it.
   - Select **Volume ID range (add all volumes within the range)** and enter the **Volume ID/Range** in the field beneath it.

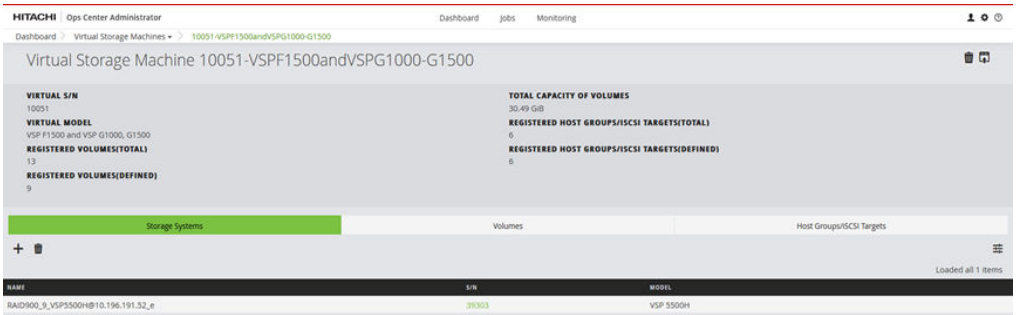
5. Click the plus sign (**+**) to add your selections to the lower window. When you are finished adding selections, click **Next** to add host groups.

   At least one undefined volume must remain in each storage system.
6. Add host groups for each required storage system and port combination. Choose one of the following from the **SPECIFY HOST GROUPS BY** menu:
   - Select **Number of Host Groups**, then click the plus (+) sign to add them to the list.
   - Select **Host Group ID**, then click **HOST GROUP LIST** to specify the host group ID.
7. When all selections are complete, click **Submit** to start a job to add the undefined resources.

Virtual storage machine details

Review the details for a single virtual storage machine.

Click on a virtual storage machine in the **Virtual Storage Machines** inventory window to view details for the virtual storage machine.



The following actions are available:

- Click the Delete icon to delete the virtual storage machine.
- Click the Open HA Pairs icon ( ) to view the global-active device pairs on this virtual storage machine.
- Click a storage system serial number in the list of storage systems under the Storage Systems tab to view the physical storage machine detail.
- Click the Storage Systems tab, Volumes tab, or Host Groups/iSCSI Targets tab to review the resources across physical storage systems and manage resources on the virtual storage machine.

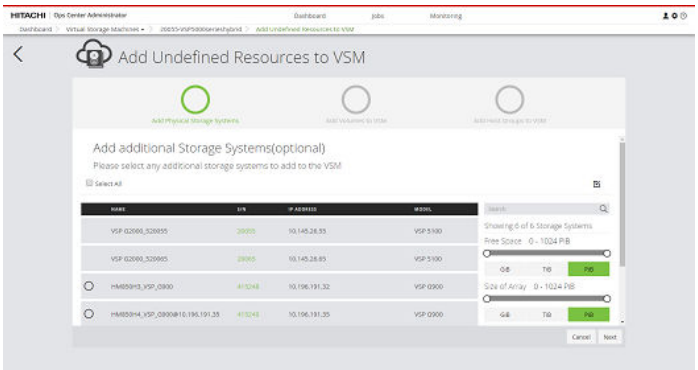
Adding storage systems to a virtual storage machine

You can add physical storage systems to a virtual storage machine (VSM) as follows:

Procedure

1. On the Ops Center Administrator dashboard, click **Virtual Storage Machines**.
2. Click the virtual storage machine listed by ID and model number) on which you want to add a storage system.
3. Under the **Storage Systems** tab, click the **Add Undefined Resources to VSM** ( ) icon.

The **Add Undefined Resources to VSM** window appears.



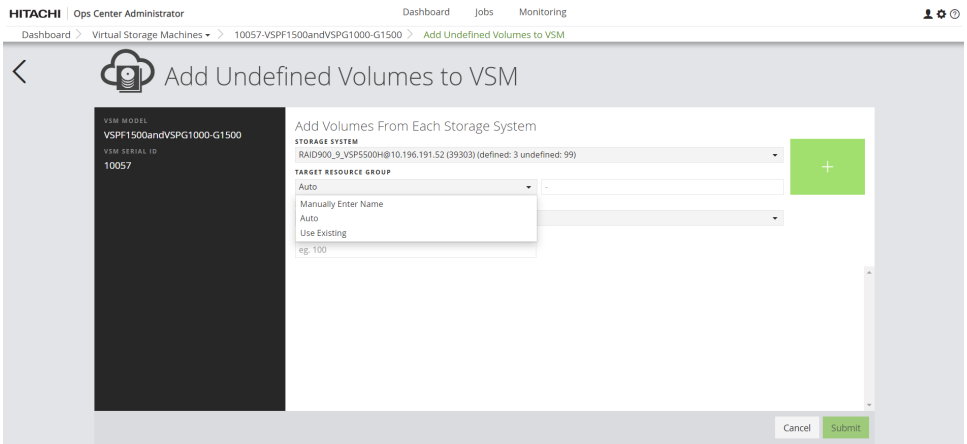
4. Select one or more storage systems to add to the VSM.
5. You can add volumes or host groups to the VSM, or just click **Next** twice, and then click **Submit**.

Adding undefined volumes to a virtual storage machine

You can add undefined volumes from a storage system to a virtual storage machine (VSM) as follows:

Procedure

1. On the Ops Center Administrator dashboard, click **Virtual Storage Machines**.
2. Click the virtual storage machine (listed by ID and model number) on which you want to add a volume.
3. Under the **Volumes** tab, click the **Add Undefined Volumes to VSM** ( ) icon. The **Add Undefined Volumes to VSM** window appears.
4. Specify the resource group from the **TARGET RESOURCE GROUP** menu. By default, the resource group name is assigned automatically.



5. Select the storage system from which you want to add a volume to the VSM from the **STORAGE SYSTEMS** menu.

6. Specify the volumes that you want to add:
   - **Number of volumes**
   - **Volume ID range (add all volumes within the range)**
   - **Number of volumes and volume ID range**
7. Click **Next**. You can then choose to add host groups from a storage system to the VSM or click **Submit**.

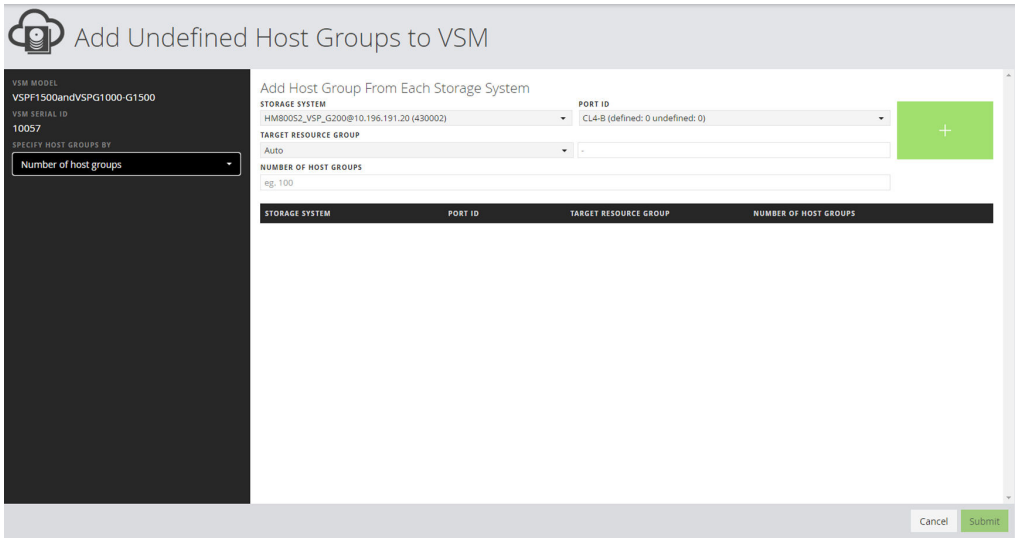
Adding undefined host groups to a virtual storage machine

You can add undefined host groups and iSCSI targets from storage systems to a virtual storage machine (VSM) as follows:

Procedure

1. On the Ops Center Administrator dashboard, click **Virtual Storage Machines**.
2. Click the virtual storage machine (listed by ID and model number) on which you want to add a volume.
3. Under the **Host Groups/iSCSI Targets** tab, click the **Add Undefined Host Groups to VSM** ( ) icon.
   The **Add Undefined Host Groups to VSM** window appears.

   Note: If the **Add Undefined Host Groups to VSM** window does not appear, either add storage systems and volumes to the VSM first, or click **Next** until it appears.
4. Select the storage system from which you want to add a volume to the VSM from the **STORAGE SYSTEMS** menu.
5. Specify the resource group from the **TARGET RESOURCE GROUP** menu. By default, the resource group name is assigned automatically.



6. In the **Add Undefined Host Groups to VSM** window, you can specify the host group you are adding either by **Number of hosts groups** or by **Host Group ID selection**.
7. Click **Submit**.

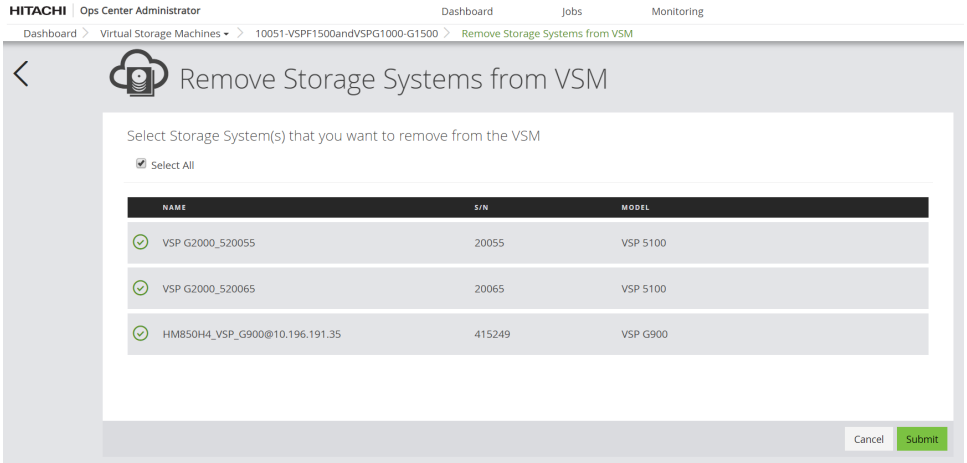
Removing storage systems from a virtual storage machine

You can remove physical storage systems from a virtual storage machine (VSM) as follows:

> **Note:** If there are any existing registered volumes or host groups, Ops Center Administrator tries to remove them before removing the storage systems.

Procedure

1. On the Ops Center Administrator dashboard, click **Virtual Storage Machines**.
2. Click the virtual storage system ID number of the VSM from which you want to remove a storage system.
3. Under the **Storage Systems** tab, click the minus icon (⊖) to remove one or more storage systems from the VSM.
   The **Remove Storage Systems from VSM** window appears.



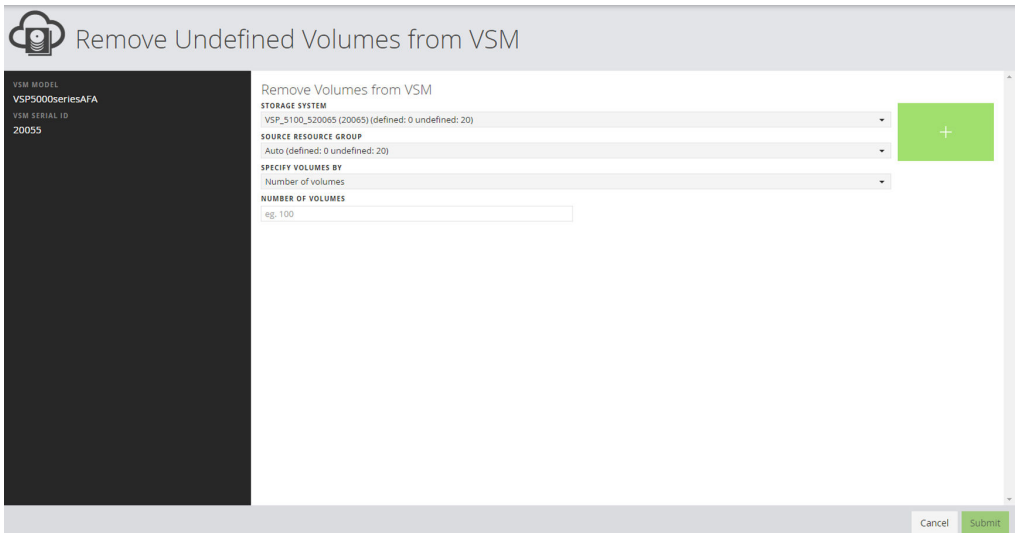
4. Select the storage systems that you want to remove from the VSM, then click **Submit**.

Removing undefined volumes from a virtual storage machine

You can remove undefined volumes from a virtual storage machine (VSM) as follows:

Procedure

1. On the Ops Center Administrator dashboard, click **Virtual Storage Machines**.
2. Click the virtual storage machine (listed by ID and model number) from which you want to remove a volume.
3. Under the **Volumes** tab, click the **Remove Undefined Volumes from VSM** (⊖) icon.
   The **Remove Undefined Volumes from VSM** window appears.



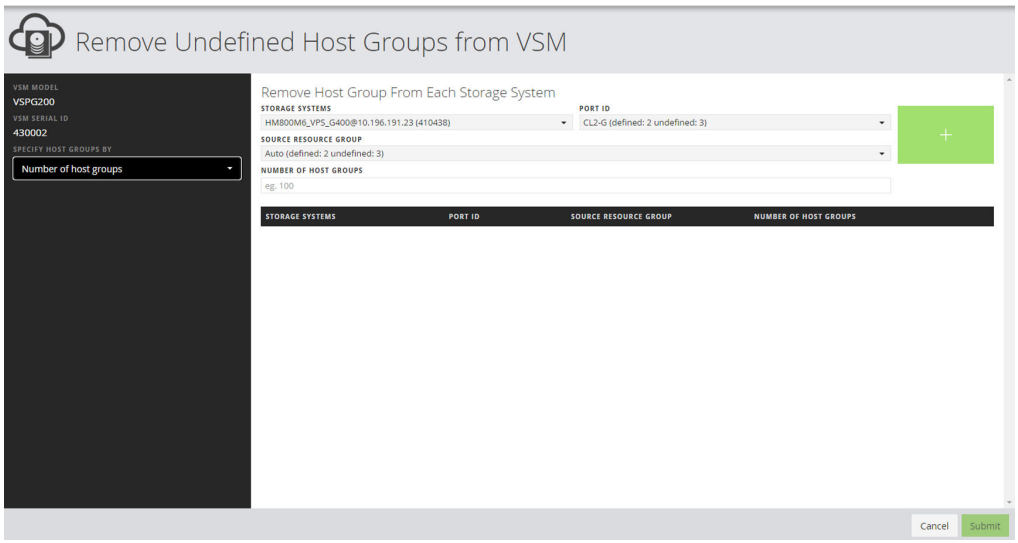
4. Select the storage system from which you want to remove a volume from the VSM from the **STORAGE SYSTEMS** menu.
5. Specify the resource group from the **SOURCE RESOURCE GROUP** menu.
6. Specify the volumes that you want to remove by:
   - **Number of volumes**
   - **Volume ID range (remove all volumes within the range)**
   - **Number of volumes and volume ID range**
7. Click **Submit**.

Removing host groups from a virtual storage machine

You can remove defined or undefined host groups (FC) and iSCSI targets (iSCSI) from a virtual storage machine (VSM) as follows:

Procedure

1. On the Ops Center Administrator dashboard, click **Virtual Storage Machines**.
2. Click the virtual storage machine (listed by ID and model number) on which you want to add a volume.
3. Under the **Host Groups/iSCSI Targets** tab, click the **Remove Undefined Host Groups from VSM** (⊖) icon. The **Remove Undefined Host Groups from VSM** window appears.



4. In the **Remove Undefined Host Groups from VSM** window, you can specify the host group you are adding either by the Number of hosts groups or by the Host Group ID selection.
5. Select the storage system from which you want to remove a host group from the VSM from the **STORAGE SYSTEMS** menu.
6. Specify the host groups that you want to remove by::
   - **Number of host groups**
   - **Number of host groups and host group ID range**
   - **Host Group ID range (add all host groups within the range)**
7. Click **Submit**.

Chapter 4: Provisioning for high availability

You can use Ops Center Administrator to provision P-Vols and S-Vols and create high availability pairs. High availability is supported by global-active device technology.

To set up high availability, configure a virtual storage machine (VSM) in a secondary storage system, and optionally, in a primary storage system. A virtual storage machine can be configured using the actual information of the primary storage system, and the global-active device primary and secondary volumes are assigned the same virtual LDEV number in the virtual storage machine. This enables the server to see the pair volumes as a single volume on a single storage system, and both volumes receive the same data from the server. Alternatively, you can use virtual model and virtual serial numbers.

Prerequisites to provisioning for high availability

Review the conditions required to provision for high availability.

Make sure that the following conditions are met before provisioning for high availability:

- Ops Center Protector v6.9.x or later is registered in Ops Center Administrator.
- The registered Ops Center Administrator must meet the following requirements:
  - Both primary and secondary storage systems are registered with Ops Center Protector.
  - Global-active device licenses for both primary and secondary storage systems are installed in Ops Center Protector.
- At least one Fibre Channel server must be registered.

- The primary and secondary storage systems must have the following configured:
  - Remote paths that are configured bidirectionally.
  - A quorum disk. (The same disk and ID must be assigned in each storage system.)
  - A VSM configured as follows:
    - If the VSM in the primary storage system is using the meta_resource, a VSM with at least one undefined host group must be configured in Ops Center Administrator for the secondary storage system. This is not required if you specify Host Mode Option 88.
    - If the VSM in the primary storage system is not using the meta_resource, a VSM with at least one undefined volume and one undefined host group must be configured for the primary storage system, and a VSM with at least one undefined host group must be configured for the secondary storage system in Ops Center Administrator. This is not required if you specify Host Mode Option 88.
- Make sure that both primary and secondary storage systems:
  - Are onboarded in Ops Center Administrator.
  - Have at least one Fibre port.
  - Have global-active device licenses.
  - For VSP G1x00, F1500 storage systems, firmware version 80-06-6x or later is installed.
  - For VSP G200, G/F400, G/F600, G/F800 storage systems, firmware version 83-04-01-x0 or later is installed.
  - There is enough room to create volumes and remote pairs including CTG.
  - There is a DP or DT pool with enough capacity.

Note: If there are any block storage nodes added before Protector 6.5, re-edit the block storage node in Protector master UI to use it for high availability.

Note: A dummy host group is attached to secondary volumes during pair creation and is detached afterwards. If the job fails before detaching, check that the secondary volumes are attached to correct server and detach volumes from the dummy host group.

Creating, attaching, and protecting volumes with high availability

Ops Center Administrator enables you to create, attach, and protect volumes in a single page.

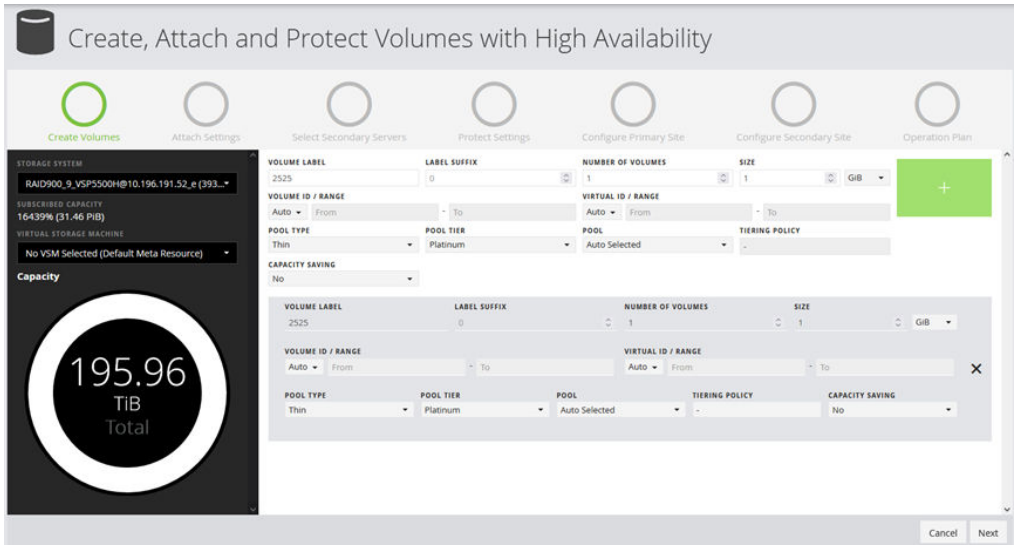
Before you begin

Register Ops Center Protector in Ops Center Administrator.

> **Note:** If you want to align the same volume ID between a primary volume with a secondary volume of a high availability pair, the secondary volume ID must belong to the metadevice or the same virtual storage machine as the primary storage system. If you want to use the same virtual storage machine, ensure it has the same resource group.

Procedure

1. Click **Servers** on the dashboard to open the **Servers** page or navigate to the detail page for a server.
2. Select a server, then select **Create, Attach and Protect Volumes with High Availability.**



3. Configure volumes for the specified storage system.

   You can switch to another storage system by using the **Storage System** list. To add the volume to a virtual storage machine, use the **Virtual Storage Machine** list. If you don't choose a VSM, the meta-resource group is used.

   a. Select the number of volumes.
   b. Enter the volume label and select a suffix for it.
   c. Select the size.
   d. Select the volume unit: **GiB**, **TiB**, or **Blocks**.
   e. Select the pool type: **Thin** or **Tiered**.
   f. For a Thin pool, select the tier: **Platinum**, **Gold**, **Silver**, or **Bronze**.

      If the storage system has available capacity from external storage, you can also select the **External** tier.
   g. (Optional) Select the pool from the list of available pools. The default selection is **Auto Selected**, which means that Ops Center Administrator selects the best pool for provisioning the volume based on utilization and tier requirements.

4. Optionally, select a type of **Capacity Saving**: **Compression** or **Deduplication and Compression**.

> **Note:** You can set capacity saving for volumes based on tiered pools for VSP 5000 series and VSP G1x00, F1500 storage systems with microcode version 80-05-4*x* or later.

> **Note:** If you choose **Deduplication and Compression** and later want to update the volume to **Compression** you must first disable **Capacity Saving**.

5. You can specify a **Volume ID / Range** in decimal or hexadecimal format.
6. (Optional) For a tiered pool, select the **Tiering Policy** from the list. Tiering policy choices available in the list depends on the choice of pool that was made in the previous step. Tiering policy choice is not available for auto-selected pools.
7. When you have made your choices, click the plus sign (**+**) to add the volume row to the list of volumes that being created. Add more rows as needed.
8. Click **Next** to choose attachment settings.

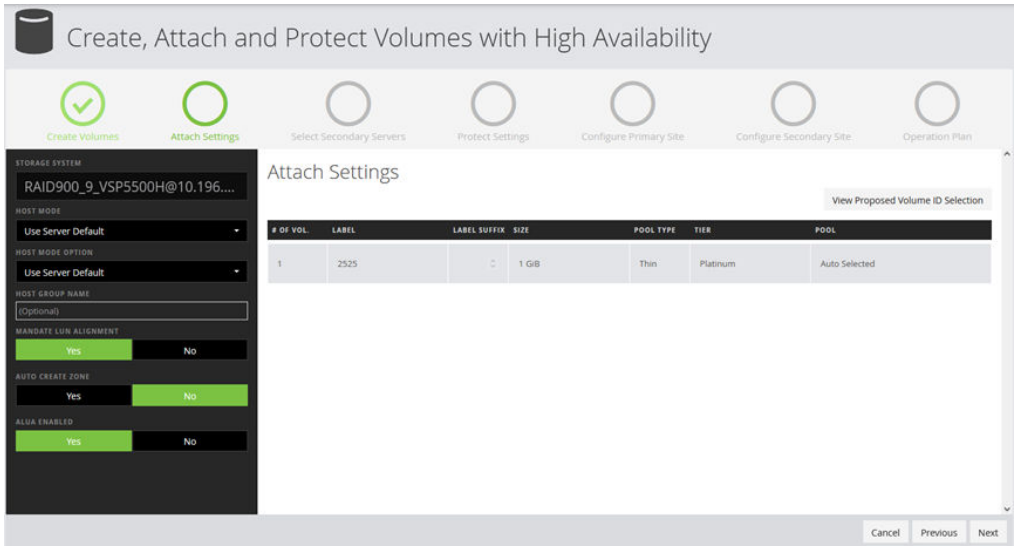
Attaching volumes and selecting secondary servers

Before you begin

- In the Settings menu, access the Ops Center Protector Settings window and register Ops Center Protector.
- Make sure that a quorum disk is available.
- Make sure that a virtual storage machine is available unless you want to use the meta-resource group of the primary storage system. The virtual storage machine you select must have one or more undefined resources available.

Procedure

1. Navigate to the **Servers** window, select a server, and click **Create, Attach, and Protect Volumes with High Availability**.



2. The **Host Mode** is set by default to the server operating system. You can make a selection if needed.

   The server OS Type is provided when the server is added to Ops Center Administrator.

3. The prepopulated **Host Mode Option** depends on the **Host Mode** selection. The default Host Mode Option can be changed manually.

   Default values are set only for **VMWARE EX** and **WIN EX** host modes. The default for all other Host Modes is none.

   Ops Center Administrator identifies all host groups containing any of the server WWNs. If all of those host groups have the same host mode and host mode options, those settings are prepopulated with the same settings in the host groups.

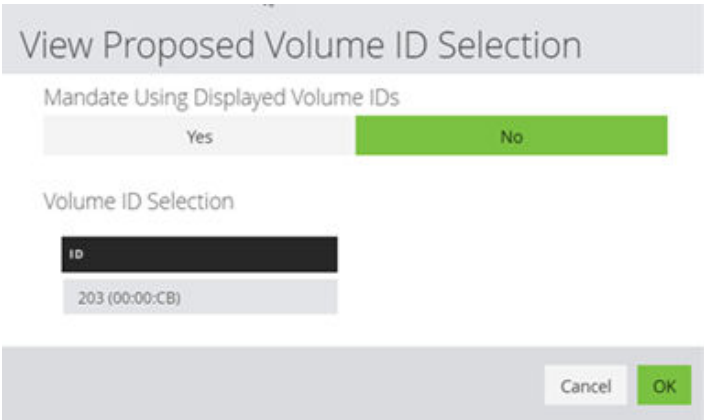
4. Select **Mandate LUN Alignment**.

   This option specifies whether to assign the same LUN number to multiple servers for volumes containing primary and secondary HA pairs. If **Yes** is specified, the same LUN number is always assigned. If **No** is specified, Ops Center Administrator tries to use the same LUN if it is available. If it is not available, Ops Center Administrator selects available LUNs separately for each primary and secondary volume.

5. The **Auto Create Zone** is set to **No** by default. You can set it to **Yes** to automatically create zones.

6. Leave **ALUA** set to **Enabled** to set preferred paths.

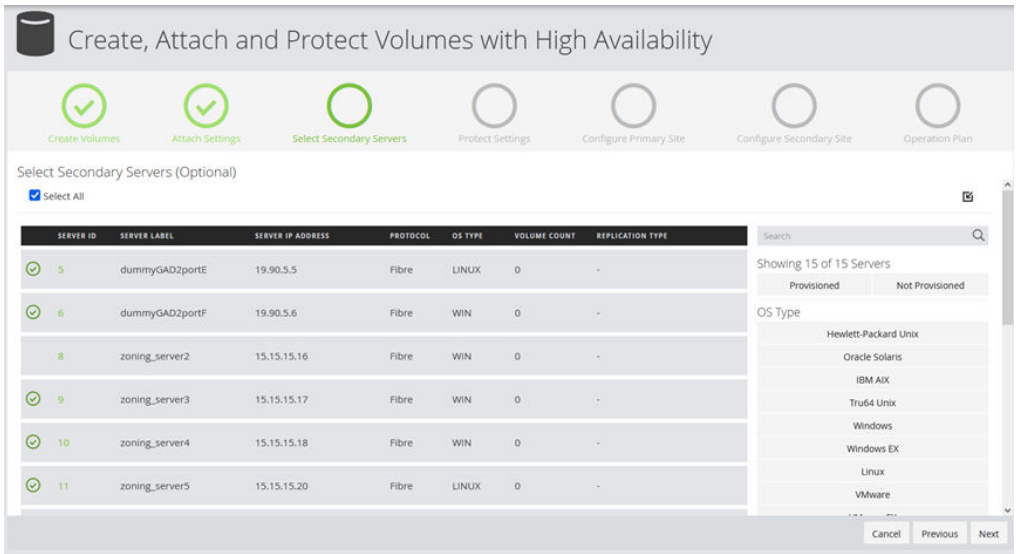
7. You can confirm which Volume IDs will be used by clicking **View Proposed Volume ID Selection**.



   Select **Yes** to mandate using the displayed volume IDs.

   Note: The **Mandate Using Displayed Volume ID** selection will be reset to **No** if you revert to the previous step.

8. Click **Next** to proceed to the **Select Secondary Servers (Optional)** screen.



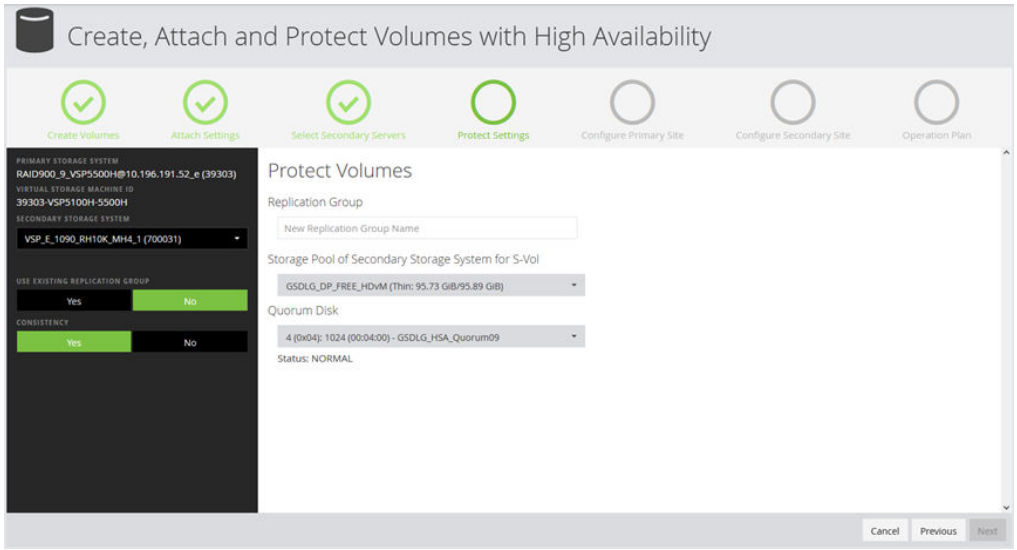
9. Optionally, select a secondary server or servers, then click **Next** to proceed to the **Protect Volumes** screen.

Selecting volume protection options

Select a secondary storage system and other options.

Procedure

1. Select a secondary storage system.
2. Choose whether to use an existing replication group.



3. Select the **Consistency** setting. By default, this is set to **Yes**. Using consistency means that copy processes run on all pairs in the group simultaneously.

4. Select a replication group from the options in the **Replication Group** list or enter a new name. Up to 26 alphanumeric characters, and also hyphens (-) and underscores (_), are allowed. Spaces are not allowed. If you select an existing replication group, the **Storage Pool of Secondary Storage System for S-Vol** and **Quorum Disk** are selected automatically.

> **Note:** Ops Center Administrator can protect volumes with high availability in an existing replication group with the following conditions:
>
> - P-VOL STATUS and S-VOL STATUS of all paired volumes in the replication group is PAIR.
> - Status of the corresponding replication in Ops Center Protector is OK.

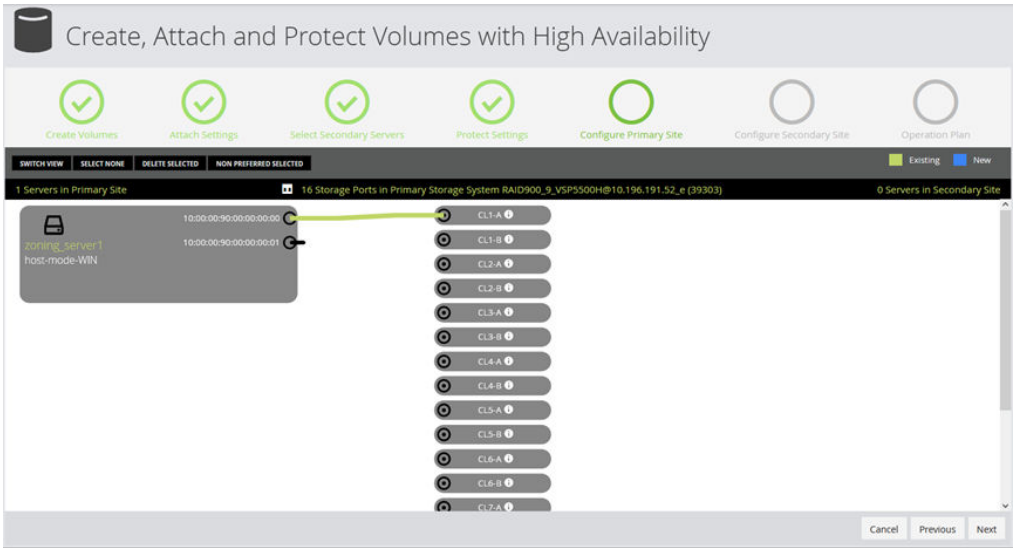
5. Select the pool to use for S-Vols and select a quorum disk.
6. Click **Next** to configure the primary site.

Configuring connections to the primary and secondary sites

You can configure the primary and secondary sites to complete the high availability configuration.

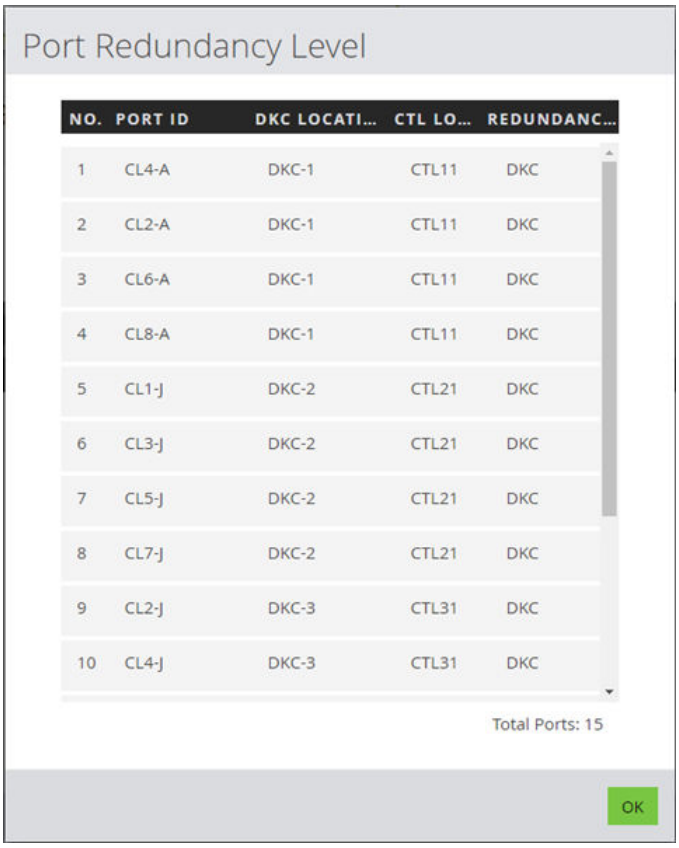
Procedure

1. In the **Configure Primary Site** window, connect ports in the primary storage system to the server in the primary site and to the server in the secondary site, if there is one. You can configure preferred and unpreferred paths.



2. You can view servers and their WWNs, along with ports on the storage system. Ops Center Administrator scan for existing host groups on the storage array and try to reuse them by default.

   For VSP 5000 series storage systems, you can click a port to display a list of ports with their DKC locations, CTL locations, and redundancy levels.



The following options are available for managing LUN paths:

- If you connect more than one server to the same port, the **Share a host group with all servers** box displays. Select the box to add the servers to a single host group.
- **Note:** If host groups already exists on that port and single host group cannot be created, the check box will not appear.

  To prevent the volume from being added to an existing path, click the path to highlight it, then click **Delete Selected**.

  Existing paths are populated as follows: all existing host groups with one or more server WWN and the exact same host mode and host mode options selected on the Attach Settings window are populated as paths.
- Click **Suggest** to populate automatically selected paths. By default, the least-used ports are selected. Suggest paths need both server and storage ports be logged into the fabric switches in the Ops Center Administrator inventory.

  Note: For VSP 5000 series storage systems, the first port suggested has the fewest LUN definitions and the second port suggested has the second fewest LUN definitions.
- To manually create a path, click a WWN and a port to connect them with a blue connector line. Click the connector again and then click **Delete Selected** to delete the connection.
- Optionally, you can click **Switch View** to use tables to create paths by selecting Server Ports to attach to Storage Ports.

3. Click **Next** to configure ports in the secondary storage system to the server in the primary site, and to the server is the secondary site, if there is one.
4. Click **Next** to continue to the optional Operation Plan step, you can confirm settings specified in each window and can confirm the resources to be used in the job, including LUN candidates.

   Note: Internet Explorer 11 does not support the Operation Plan page. Use another supported brower to access this feature.

5. You can specify the LUN range for volumes in the **LUN Settings** pop up window which is launched by clicking LUN Settings button above the Planned Path Configuration table.
6. You can make it mandatory to use the LUNs displayed in the table by specifying Yes to **Mandate Using Displayed LUN**.

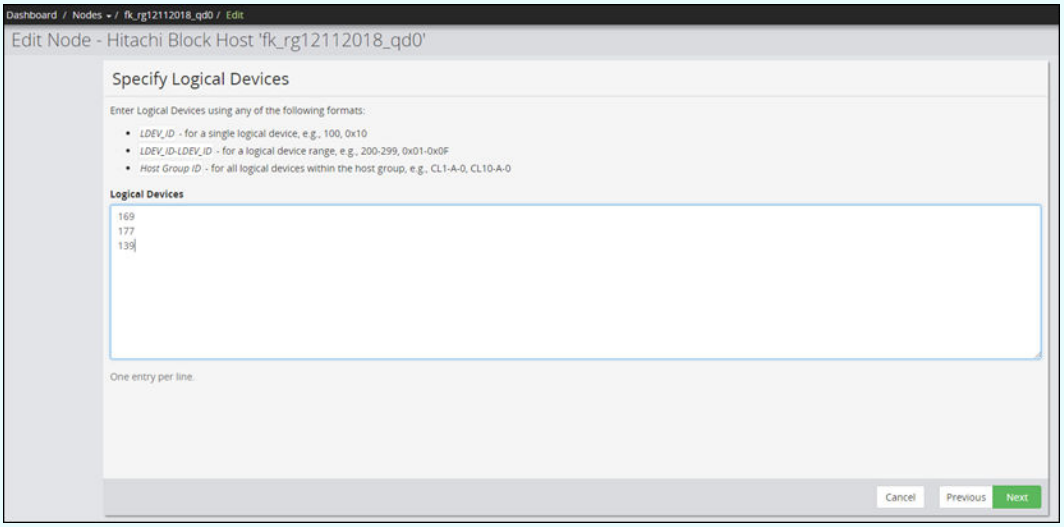
   Note: Please note that if **Yes** is specified to use displayed LUNs, primary and secondary volumes' LUNs may not be aligned even though **Mandate LUN Alignment** is set to **Yes**.

7. When you are satisfied with all the settings, click **Submit**.
8. Click **Submit** to create a job to create volumes, attach to servers and set up data protection.
9. You can monitor the job in the **Jobs** page.

   Note: If the job does not complete successfully, access Ops Center Protector to remove the related resources (Block Host Node, Policy, and Data Flow) with the same name as the selected Replication Group.

   When using an existing **Replication** group, remove added **P-Vol** from **Block Host Node**.

   To edit a Block Host Node created by Ops Center Administrator in Ops Center Protector, specify LDEV IDs in decimal format per line and not in hex format or range format.



Chapter 5: Monitoring high availability operations in Ops Center Protector

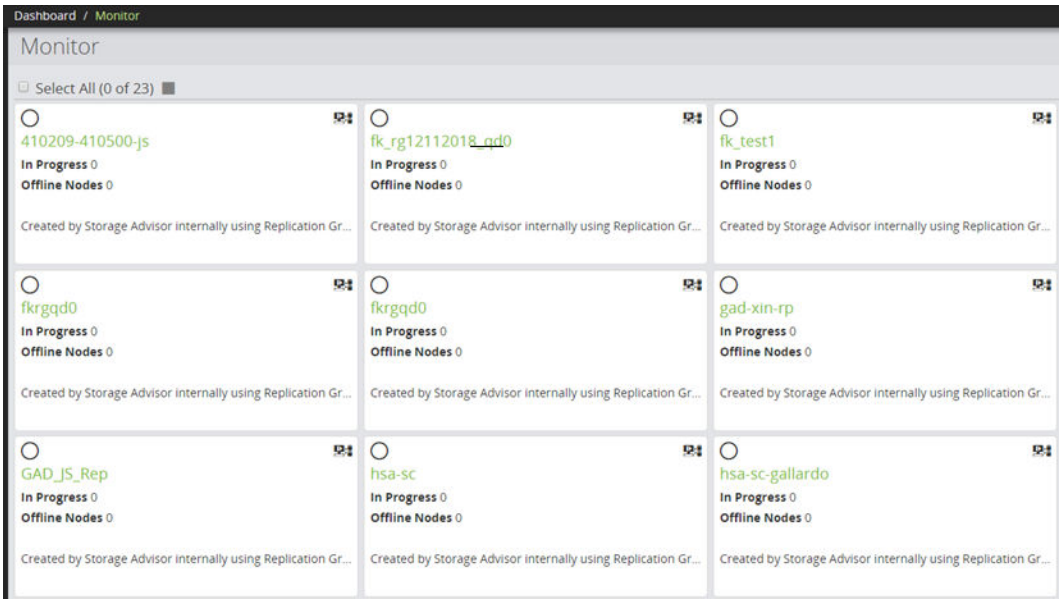
Use Ops Center Protector to monitor high availability operations, HA pairs, and data flows.

Before you begin

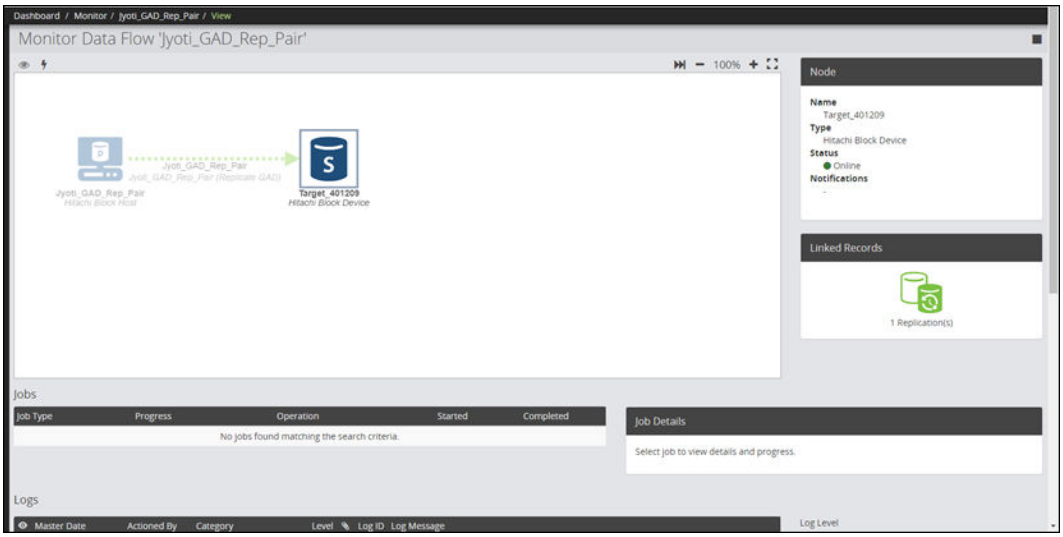
Ops Center Protector must be registered in Ops Center Administrator, and the primary and secondary storage systems must be onboarded in Ops Center Protector.

Procedure

1. Log in to Ops Center Protector and click **Monitoring** in the global navigation menu.
2. In the **Monitor** inventory page, you can see all data flows created by Ops Center Administrator.



3. Click a data flow to open the **Monitor** details page.



4. Click the target block device to expose any related replications in the **Linked Records** panel.
5. Click the **Replications** icon to view the details of related replications and perform operations on them.

6. The following operations are available in this page:
   - **Mount**: Enabled only if one or more Replications are selected. Opens the Hitachi Block Snapshot or Replication Mount Wizard to guide you through mounting the Replication.

     Note: The mount operation can take several minutes to complete.
   - **Unmount**: Enabled only if one mounted replication is selected. Unmounts the selected replication.

     Note: The unmount operation can take several minutes to complete.
   - **Pause**: Enabled only if one or more replications are selected. Pauses the replication.
   - **Resume**: Enabled only if one or more replications are selected. Resumes a paused replication.
   - **Swap**: Enabled only if one or more replications are selected. Opens the Hitachi Block Replication Swap Wizard to guide you through swapping the replication direction.

- **Unsuspend**: If a Swap operation cannot be completed due to a P-VOL or data link fault between the primary and secondary device, the replication will enter the SSWS state (suspended for swapping) indicating that the swap is not yet complete. Unsuspend enables the replication process to be re-established once the cause has been rectified.
- **Transfer RBAC Permissions**: Allows RBAC ownership to be transferred from the current node to another node. Opens the Access Control Transfer Permissions Dialog.
- **Dissociate**: Enabled only if one or more replications are selected. Dissociates a replication that was previously adopted by Ops Center Protector. Removes the selected replications from Ops Center Protector, including state information such as direction and mount location. The replication remains active on the hardware devices. `DISSOCIATE`must be entered before the command is executed.

  Note: Dissociating a replication removes all knowledge of the replication from Ops Center Protector, including state information such as direction and mount location.

Mounting a block snapshot or replication

The steps for mounting a file system path snapshot or replication from a Block storage device to a node other than the one from which it originated using Ops Center Protector are described below.

Procedure

1. Identify the destination where the data set is to be restored. Here we will *mount* a snapshot or replication to a destination machine and volume.

   Depending on the scenario, you can mount the snapshot or replication to its original node as a different volume or to a different node entirely. You can control the level of the mount operation so that the snapshot is added to a host group, through to mounting to the host OS.
2. Ensure that the restore location is prepared to receive the snapshot or replication data set by locating the node in the **Nodes Inventory** and checking it is authorized and online.

   Note:
   - For **Host** and **OS** level mounting, the mount location must have Ops Center Protector Client software installed.
   - **SAN** level mount does not specify a host so Ops Center Protector Client software does not need to be installed.
3. Locate the data set to be mounted for the Block storage device by navigating to the Block Snapshots Inventory or Block Replications Inventory.
4. Select the snapshot or replication that you want to mount, then click **Mount**. The Hitachi Block Snapshot or Replication Mount Wizard is displayed.
   a. Select the mount level (**SAN**, **Host** or **OS**).

b. Choose **Automatically discover** or a **Selected Host Group**.
c. For **SAN** mount click **Finish**, for other mount types click **Next**.
d. Specify the **Host** (i.e. the target machine).
e. For **Host** mount click **Finish**, for **OS** mount click **Next**.
f. Specify the **Mount Location**.
g. For **OS** mount click **Finish**.

The Jobs Inventory is displayed with a mount job that cycles through stages and ending in *Progress - Completed*.

5. Once the mount process is complete, further steps may be needed to fix-up the data set before using it. The amount of fix-up work required depends on the applications accessing the restored data.
6. Mounted snapshots or replications have a mount icon displayed in the **Block Snapshots Inventory** and the **Block Replications Inventory**.

How to swap (takeover/takeback) a replication

The steps below describe how to swap the direction of an Hitachi block GAD replication using Ops Center Protector. In the case of primary site maintenance, application failure, primary volume failure or disaster recovery, it may be necessary to move production to the secondary site, resolve the issue at the primary site and then move production back to the primary site.

Before you begin

When a replication is swapped, the S-VOL takes over the role of the primary volume and the P-VOL takes over the role of the secondary volume. A swapped replication can be swapped back to its normal state with the P-VOL as the primary and S-VOL as the secondary.

When a GAD replication is swapped, the original P-VOL is marked as reserved. If the replication is torn-down while in the swapped state, the reserved flag on the original P-VOL will prevent it from being used and the reserved flag must be manually reset.

If you are swapping an active-active (GAD) replication, additional steps may be required especially if using a cross-path setup.

Procedure

1. Move production from the primary to the secondary site by performing a *Swap* as follows:
   a. Stop any applications that access the primary volumes to be taken over.
   b. Locate the replication to be taken over by navigating to the **Block Storage Replication Details (Storage)** on the secondary device.

      You will see the replication's *Type* (displayed in the **Block Replications Inventory**) is `Active Full Copy` and the *Swapped* state (displayed in the **Block Replication Details (Storage)**) is `No`.

c. From the **Block Replication Details (Storage)** click the **Swap** button.

   The Block Replication Swap Wizard displays a warning that swapping can cause data loss. It is safe to proceed as long as access to the primary volumes has been stopped.

d. Type the word `'SWAP'` into the **Confirm Swap** field and click **OK**.

   The **Jobs Inventory** is displayed and a new job appears indicating that a *Swap VSP Replication* operation is in progress. Click on the *Job Type* in the table to open the **Job Details** which shows the log messages relating to the swap operation.

e. Return to the **Block Replication Details (Storage)** and review the replication's status.

   - If the swap is successful the *Swapped* state is set to `Yes`, indicating that the replication is now reversed (S-VOL to P-VOL) and is back in PAIR status. A *Swapped* status badge appears above the replication's mover on the **Monitor Details**.
   - If the swap cannot be completed due to a P-VOL or data link fault the *Swapped* state is set to `No` and the *Suspend for Swap* state is set to `Yes`, indicating the swap is not yet complete and is in SSWS status. Further action is required on the primary block storage device or data link before the replication process can be re-established, but the secondary is writeable.

   Note: The flow direction of a replication pair should ONLY be determined by referring to the **Summary** - *Swapped* field on the **Block Replications Details (Storage)** for the secondary Block storage device. Primary and secondary volume information shown in the replications **Session Log Details** should not be used to infer the flow direction following a swap.

f. Start any applications that access the secondary volumes that have been taken over and resume production at the secondary site.

2. Perform any maintenance and recovery tasks at the primary site, resolve any faults with the data link between sites, then go back to the **Block Replication Details (Storage)** for the secondary to determine the status of the S-VOLs. Perform one of the following actions as appropriate:

a. If the replication is *Swapped* (S-VOL status = PAIR) then proceed with moving production back to the primary site when ready, as detailed in step 3 below.

b. If the replication is *Suspended for Swap* (S-VOL status = SSWS) then click the **Unsuspend** button. The swap operation will be completed as described above. Production at the secondary site can now continue with replication to the primary site in operation.

c. If the S-VOL status is some value other than PAIR or SSWS then you will need to run the following CCI command sequence from outside Protector to recover the replication pairing: **`pairsplit -R, pairsplit -S, paircreate`**

3. Move production back to the primary site when ready to resume normal operations by performing a *Swap* as follows:

a. Stop any applications that access the secondary volumes to be taken back.

b. Locate the replication to be taken back by navigating to the **Block Replication Details (Storage)** on the secondary device.

   You will see that the replication's *Type* (displayed on the corresponding tile in the **Block Replication Inventory**) is `Active Full Copy` and the *Swapped* state (displayed on the **Block Replication Details (Storage)**) is `Yes`.

c. From the **Block Replication Details (Storage)** click the **Swap** button.

   The Block Replication Swap Wizard displays a warning that swapping can cause data loss. It is safe to proceed as long as access to the secondary volumes has been stopped.

d. Type the word `'SWAP'` into the **Confirm Swap** field and click **OK**.

   The **Jobs Inventory** is displayed and a new job will appear indicating that a *Swap VSP Replication* operation is in progress. Click on the *Job Type* in the table to open the **Job Details** which lists the log messages relating to the swap operation.

e. Return to the **Block Replication Details (Storage)** and review the replication's status.

   When the swap (takeback) is completed the *Swapped* state is set to `No`, indicating that the replication is now normal (P-VOL to S-VOL) and is back in PAIR status. The *Swapped* status badge disappears from above the replication's mover on the **Monitor Details**.

f. Start any applications that access the primary volumes that have been taken back and resume production at the primary site.

Chapter 6: Disabling high availability functions

Disabling high availability functions is a maintenance task that deletes the system configurations used for high availability functions.

Certain functions must be performed in tools other than Ops Center Administrator:

- Replication removal:

  Replications created from the S-VOL of the HA pairs, including any local or remote replications, must be deleted or HA pair deletion will fail.

- Stopping an OS or application:

  In many cases the S-VOL must be disconnected before unprovisioning. If necessary, stop the OS or application.

  The P-VOL is not changed, so the OS or application using the P-VOL should not be stopped.

- The dummy host group created by Ops Center Protector cannot be deleted in Ops Center Administrator.

Notes regarding unprotecting volumes: After removing protection by high availability set to a primary volume, all LUN paths for a secondary volume are deleted. A host group for the LUN path that is created by Ops Center Administrator is deleted when the host group has no LUN path. The dummy host group that is created by Ops Center Protector is not deleted. You can delete it with other storage management software as needed.

Notes regarding replication group deletion: After deleting a replication group whose replication type is high availability, all LUN paths for secondary volumes in the replication group are deleted. A host group for the LUN path that is created by Ops Center Administrator is deleted when the host group has no LUN path. The dummy host group that is created by Ops Center Protector is not deleted. You can delete it with other storage management software as needed.

Notes regarding primary volume removal from a replication group: After removing primary volumes from a replication group whose replication type is high availability, all LUN paths for secondary volumes paired with the removed primary volumes in the replication group are deleted. A host group for the LUN path that is created by Ops Center Administrator is deleted when the host group doesn't have LUN path. The dummy host group that is created by Ops Center Protector is not deleted. You can delete it with other storage management software as needed.

Disable by deleting the replication group and primary volumes

You can disable high availability functions by deleting the replication group and primary volumes.

Procedure

1. Delete all GAD pairs by deleting the replication group:

   On **Replication Groups** page, select the replication group, then click **Delete**.
2. Detach primary volumes in one of the following ways:
   - On the detail page for the server, select all primary volumes, then click **Detach Volume**.
   - On the Volumes page, select all primary volumes, then click **Detach Volume**.
3. Delete primary volumes in one of the following ways:
   - On the **Volumes** page, select the primary volumes, then click **Delete**.
   - One the detail page for each primary volume, click **Delete**.
4. (Optional) Delete the host group created by Ops Center Protector.
5. (Optional) Remove volume IDs and host group IDs in the secondary virtual storage machine.
   a. Open the **Virtual storage machines** page and select the secondary VSM.
   b. Click **Remove VSM** to open the **Remove Undefined Resources from VSM** page.
   c. Specify the number of volumes, the range of volume IDs, or both, then click the plus sign (**+**). Click **Next**.
   d. Specify the number of host group IDs to delete, then click the plus sign (**+**). Click **Submit**.
6. Delete the secondary VSM

   On the **Virtual storage machines** page, select the secondary VSM, then click **Delete**.

Disable by deleting the replication group and retaining the primary volume

You can disable the high availability functions by deleting the replication group and keeping the primary volume.

Procedure

1. Delete all GAD pairs by deleting the replication group:

   On the **Replication Groups** page, select the replication group, then click **Delete**.

2. (Optional) Detach primary volumes from the secondary server:

   On the details page for the server, select all primary volumes, then click **Detach volumes**.

3. (Optional) Set the ALUA status of the primary volumes to **Disabled**.

   On the detail page for each volume, click **Edit** and set **ALUA** to disabled. Click **Submit**.

4. (Optional) Delete the host group created by Ops Center Protector.
5. (Optional) Remove volume IDs and host group IDs in the secondary virtual storage machine.
   a. Open the **Virtual storage machines** page and select the secondary VSM.
   b. Click **Remove VSM** to open the **Remove Undefined Resources from VSM** page.
   c. Specify the number of volumes, the range of volume IDs, or both, then click the plus sign (**+**). Click **Next**.
   d. Specify the number of host group IDs to delete, then click the plus sign (**+**). Click **Submit**.
6. Delete the secondary VSM.

   On the **Virtual storage machines** page, select the secondary VSM, then click **Delete**.

Disable by deleting some global-active device pairs but retaining the replication group

You can disable high availability functions without removing all GAD pairs.

Procedure

1. Delete some, but not all, GAD pairs in one of the following ways:
   - On the **Replication Groups** page, select a replication group, then click **Edit** to open the **Edit Replication Group** page. Select the primary volumes to remove, then click **Submit**.
   - On the **Volumes** page, select a primary volume, then click **Unprotect volume**. Repeat for each primary volume to be deleted.
   - On the details page for the server, select a primary volume, then click **Unprotect volume**. Repeat for each primary volume to be deleted.

   Note: Ops Center Administrator can unprotect volumes with high availability with following conditions:
   - P-VOL STATUS and S-VOL STATUS of all paired volumes in the replication group is PAIR.
   - Status of the corresponding replication in Ops Center Protector is OK.

2. Detach primary volumes in one of the following ways:
   - On the detail page for the server, select all primary volumes, then click **Detach volume**.
   - On the Volumes page, select all primary volumes, then click **Detach volume**.
3. Delete primary volumes in one of the following ways:
   - On the detail page for the server, select all primary volumes, then click **Delete volume**.
   - On the **Volumes** page, select a primary volume, then click **Delete volume**. Repeat for each primary volume.
4. (Optional) Remove volume IDs and host group IDs in the secondary virtual storage machine.
   a. Open the **Virtual storage machines** page and select the secondary VSM.
   b. Click **Remove VSM** to open the **Remove Undefined Resources from VSM** page.
   c. Specify the number of volumes, the range of volume IDs, or both, then click the plus sign (**+**). Click **Next**.
   d. Specify the number of host group IDs to delete, then click the plus sign (**+**). Click **Submit**.

Disable by deleting some global-active device pairs but retaining the replication group and primary volumes

You can disable high availability functions by deleting some GAD pairs and retaining both the replication group and the primary volumes.

Procedure

1. Delete some, but not all, You can disable high availability functions by deleting some GAD pairs and retaining both the replication group and the primary volumes. pairs in one of the following ways:
   - On the **Replication Groups** page, select a replication group, then click **Edit** to open the **Edit Replication Group** page. Select the primary volumes to remove, then click **Submit**.
   - On the **Volumes** page, select a primary volume, then click **Unprotect volume**. Repeat for each primary volume to be deleted.
   - On the details page for the server, select a primary volume, then click **Unprotect volume**. Repeat for each primary volume to be deleted.

   Note: Ops Center Administrator can unprotect volumes with high availability with following conditions:
   - P-VOL STATUS and S-VOL STATUS of all paired volumes in the replication group is PAIR.
   - Status of the corresponding replication in Ops Center Protector is OK.

2. (Optional) Remove volume IDs and host group IDs in the secondary virtual storage machine.
   a. Open the **Virtual storage machines** page and select the secondary VSM.
   b. Click **Remove VSM** to open the **Remove Undefined Resources from VSM** page.
   c. Specify the number of volumes, the range of volume IDs, or both, then click the plus sign (**+**). Click **Next**.
   d. Specify the number of host group IDs to delete, then click the plus sign (**+**). Click **Submit**.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact