

VSP 360

Quick Start Guide

Contents

Book abstract (QSG).....	2
Legal Notices.....	3
Hitachi Legal Notices.....	3
Preface.....	11
Product version	11
Release notes.....	11
Accessing product documentation.....	11
Getting help.....	11
Comments.....	11
Chapter 1: Hitachi VSP 360 Overview.....	13
Chapter 2: Installation and configuration.....	15
System requirements.....	15
Installation requirements.....	15
Port requirements.....	16
Supported browsers.....	19
Installing the VSP 360 platform on VMware ESXi.....	19
Downloading the VSP 360 platform software.....	19
Deploying the VSP 360 platform software operating system on VMware vSphere ESXi.....	20
Installing the VSP 360 platform on VMware vSphere ESXi	21
Setting up the VSP 360 platform for the first time.....	21
Adding users locally.....	22
Log in to the VSP 360 platform for the first time as administrator.....	23
Chapter 3: Getting started with VSP 360 Fleet Management.....	25
VSP 360 Fleet Management overview.....	25
Dashboard.....	25
Analyzing data in the dashboard.....	29
Inventory and resource information.....	31
Schedule jobs.....	32
Scheduling a job.....	33
Monitoring scheduled jobs.....	33
Deleting scheduled jobs.....	33
Searching resources.....	34

Add a Hitachi Block Host Node.....	79
Authorize a node.....	79
Create policies.....	80
Create a policy.....	80
Add a filter to a classification.....	81
Create and activate data flows.....	81
Create a data flow.....	81
Connect nodes on a data flow.....	83
Apply a policy to nodes on a data flow.....	84
Activate a data flow.....	84
Create Hitachi block workflows.....	85
Data protection workflow prerequisites.....	85
Protect your data.....	85
Snapshot a Hitachi Block LDEV with Thin Image.....	87
About Thin Image and Thin Image Advanced differential and refreshed snapshots.....	89
Replicate a Hitachi Block LDEV with ShadowImage.....	93
About ShadowImage replication.....	96
Implement 3DC multi-target with delta UR replication.....	100
About three datacentre multi-target with delta.....	104
Dissociate a replication.....	104
About Hitachi Block replication adoption.....	105
Adopt a replication.....	108
Chapter 5: Get started with Hitachi Virtual Storage Platform 360 Clear Sight.....	111
Product overview.....	111
Initial Setup.....	111
Configure initial settings.....	112
Add probes.....	112
Prerequisites for adding Hitachi Block Storage probes.....	113
Add a Hitachi Block Storage probe.....	114
Add multiple Hitachi Block Storage probes.....	115
Configure the SMTP server.....	116
Define thresholds for monitoring resources.....	117
Quick access to actionable insights.....	118
Analyze overall block storage capacity.....	118
Analyze application capacity utilization.....	120
Analyze workload placement.....	122
Example scenario for workload placement.....	124
Analyze port imbalance.....	125
Identify LUNs with a single path.....	128

Identify ports without LUN security.....	130
Identify unused host groups.....	132
Identify idle applications.....	133
Change application idle status to active.....	135
Troubleshoot block health problems.....	135
Troubleshoot block health.....	135
Troubleshoot data reduction health.....	139
Troubleshoot application performance.....	142
Troubleshoot alerts.....	144
Monitor data reduction.....	146
Data reduction metrics.....	146
Analyze current savings with data reduction	147
Evaluate potential savings and data reduction candidates.....	149
Monitor capacity.....	150
Monitor overall capacity and forecast usage.....	150
Monitor storage capacity and forecast usage.....	152
Monitor application capacity and forecast usage.....	154
Identify pools running out of capacity.....	155
Monitor pool capacity and forecast usage.....	155
Monitor volume capacity usage.....	157
Monitor performance.....	158
Application performance.....	159
About applications.....	159
Application performance metrics.....	160
Identify applications under stress.....	160
Analyze application performance.....	161
Storage system performance.....	165
Analyze storage system health.....	165
Analyze storage performance trends and metrics.....	168
Analyze storage system performance.....	171
Pool performance.....	173
Identify pools under stress.....	173
Analyze pool performance	174
Volume performance.....	176
Identify volumes under stress.....	177
Analyze volume performance.....	177
Port performance.....	181
Identify ports under stress.....	181
Analyze port performance.....	181
Processor performance.....	183
Identify processors under stress.....	183

Analyze processor performance.....	184
Cache performance.....	186
Identify caches under stress.....	186
Analyze cache performance.....	187
Configure alerts.....	189
Define a monitoring time period.....	189
Default alert profiles.....	189
Clone the application alert profile.....	191
Edit default alert profiles.....	193
Manage probes.....	193
Edit a probe.....	193
Delete a probe.....	194
Manage reports.....	194
Add a custom report.....	194
Schedule reports.....	197
Schedule a report.....	197
Edit a scheduled report.....	201
Download scheduled reports.....	201
Delete a scheduled report.....	201
Download reports.....	202
View and edit reports.....	202
Delete reports.....	202

Chapter 3: Getting started with VSP 360 Fleet Management

Hitachi Virtual Storage Platform 360 Fleet Management reduces the complexity of managing storage systems by simplifying the setup, management, and maintenance of storage resources.

VSP 360 Fleet Management overview

VSP 360 Fleet Management reduces infrastructure management complexities and enables a simplified approach to managing storage infrastructures. It has intuitive graphical user interfaces and recommended configuration practices to streamline system configurations and storage management processes.

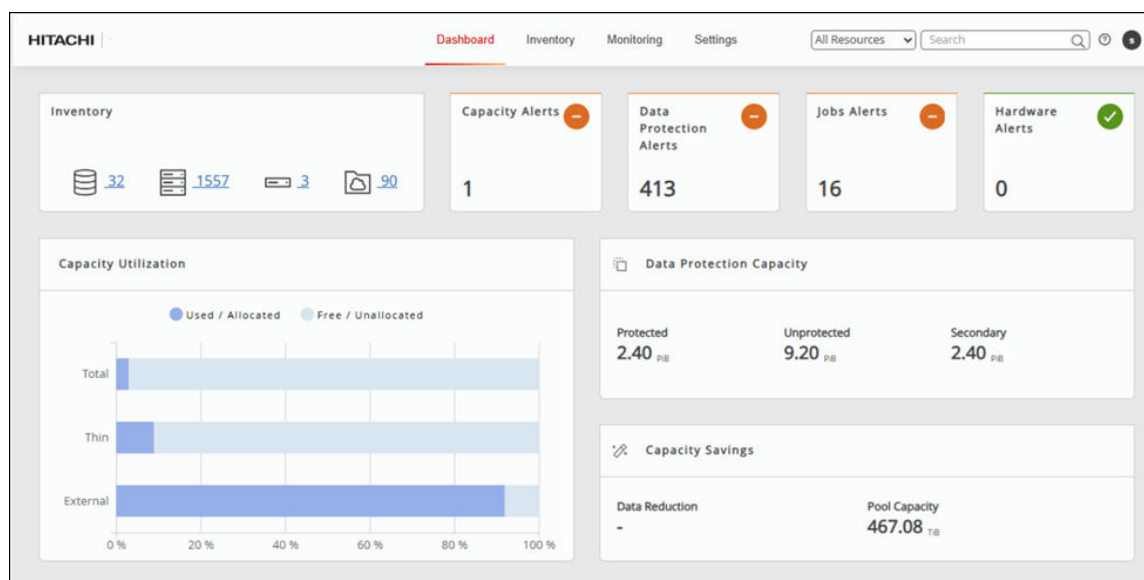
You can use Fleet Management to easily provision new storage capacity for business applications without requiring in-depth knowledge of the underlying infrastructure resource details. It provides centralized management while reducing the number of steps to configure, optimize, and deploy new infrastructure resources.

Some of the key capabilities include:

- Simplified user experience for managing infrastructure resources. Visual aids enable easy viewing and interpretation of key management information, such as used and available capacity, and guide features that help you to quickly determine the next steps for a specific management task.
- Recommended system configurations to speed initial storage system setup and accelerate new infrastructure resource deployments.
- Integrated configuration workflows with Hitachi recommended practices to streamline storage provisioning and data protection tasks.
- Common, centralized management for supported storage systems.
- Automated SAN zoning during volume attach and detach. Optional auto-zoning eliminates the need for repetitive zoning tasks on the switch.

Dashboard

After you onboard a storage system, the dashboard displays as soon as you log in. The dashboard includes the tools for easily configuring, managing, and monitoring storage systems.



From the dashboard, you can access managed resources and provision storage for a specific storage system or server. The templates and configurations enable you to quickly and easily provision a storage system without knowing the details of the underlying hardware and software.

From the top navigation menu, you can access the Inventory, Monitoring, and Settings windows, and you can use the search bar to access resources quickly. The Settings window includes links to the following settings, based on the user role:

- Tier Management
- Security
- SNMP
- Change Local Password
- VSP 360 Data Protection

The dashboard includes the following sections:

Inventory tile

Provides quick access to review the configuration of your storage systems, servers, fabric switches, and virtual storage machines.

Alert tiles





Provides alert tiles that represent various aspects of the storage system health. When the software detects a problem with a storage system environment, a number appears in the tile. The number indicates the number of storage system alerts for the health aspect represented by the tile. Click the alert tile to go directly to a summary of the problems.

Resource summary

Provides an information gauge with a summary of the capacity allocated from the registered storage systems.

Inventory tile

The Inventory tile enables quick access to storage systems and servers.

- Click the Storage Systems () icon to view and add storage systems.
- Click the Servers () icon to view and add servers.
- Click the Fabric Switches () icon to view and add fabric switches.
- Click the Virtual Storage Machines () icon to view virtual storage machines and move volumes to a VSM or add and remove undefined resources.

These options can also be accessed by clicking the Inventory tab in the top navigation menu, and then clicking the side-navigation tree menu.

Alert tiles

The alert tiles are located across the top of the dashboard and display alerts for storage capacity, data protection, jobs, and hardware.

If a tile includes a circled check mark, there are no alerts for that part of the storage system, and everything is functioning normally. If a dash within an orange circle is shown in a tile, it indicates one or more problems with that part of the storage system.

To view a summary for a category of alerts, click the tile for Capacity Alerts, Data Protection Alerts, or Hardware Alerts.

The Jobs Alert tile displays the number of jobs in the last 24 hours with a status of Failed or Success with Errors.

Resource summary

The Resource summary includes Capacity Utilization, Data Protection Capacity, and Capacity Savings panels.

- Capacity Utilization

- Total:

- Allocated: Indicates the sum of all pool capacities available across all block storage systems and all drive capacities, excluding drives in an "Offline" state in software-defined storage systems.
 - Free: Indicates the sum of all parity group capacities that have not yet been allocated to pools across all block storage systems and all drive capacities, including drives in an "Offline" state in software-defined storage systems.

If no pools are created, the "Allocated" value will be zero. As you create pools, this number will increase to eventually reach 100% when all parity groups in block storage systems have been consumed for pool creation and all drives in software-defined storage systems have been utilized for storage pool expansion.



Note: To see the total, which is the sum of "Allocated to Pools" and "Unallocated to Pools", hover your cursor over the total bar chart.

- Thin:

- Used: Indicates the storage utilization. As you create volumes in the pools and start consuming capacity, the utilization of thin pools increases, and the "Used" value increases, eventually reaching 100 % when all pools have filled up.

- External:

- Allocated: Indicates the sum of all allocations to pools across all external parity groups in block storage systems.
 - Unallocated: Indicates the total that is unallocated to pools across all external parity groups in block storage systems.

If you notice the "Total Allocated" and "Thin Used" values approaching 100%, you might be running out of storage on one or more storage systems and need to add disks to increase storage capacity. Review the information gauge for each storage system to identify which one requires additional capacity. In addition, inspect disks for each storage system to determine if there is unused capacity available for parity group creation.

- Data Protection Capacity: Indicates the types of protected, unprotected, and secondary capacity.

- Capacity Savings:
 - Data Reduction: The ratio of logical used capacity to the physical used capacity for all compression and deduplication technologies.



Note: The value displayed as the capacity of data after reduction includes the size of metadata and garbage data generated by the storage system in addition to user data. This value might temporarily be greater than the capacity of data before reduction.

- Pool capacity: The sum of all pool capacities available across all block storage systems and all drive capacities, excluding drives in an "Offline" state in software-defined storage systems.

Analyzing data in the dashboard

The dashboard is a visual display of the important information required to analyze the overall capacity utilization and health of your storage system. It has visual indicators such as total usable capacity, current utilization, a data protection summary, and monitoring alerts.

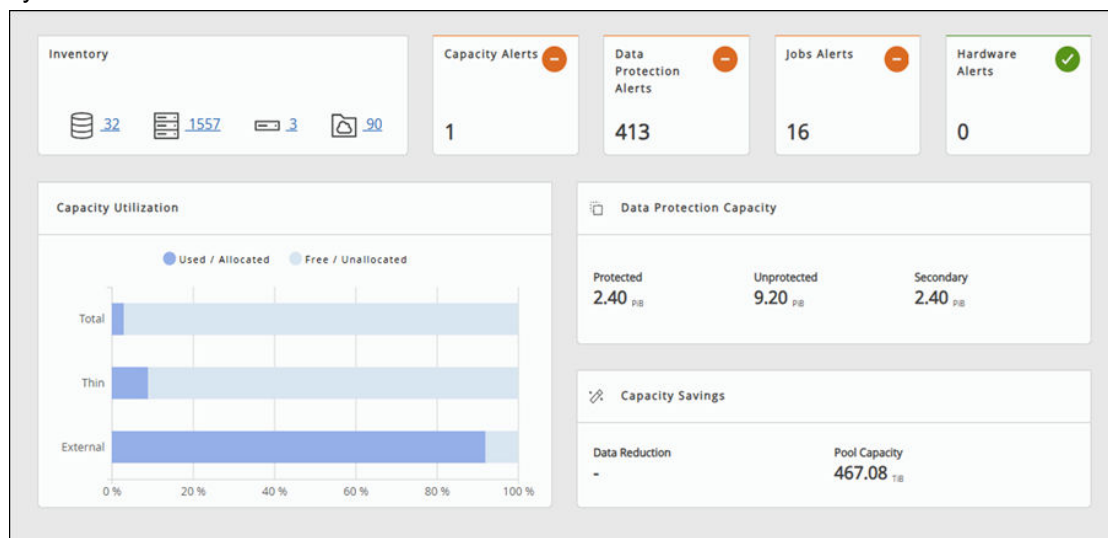
Analyzing data shown in alert tiles

The alert tiles collectively present the health of the storage system environment. With a quick view, you can verify that your storage environment is healthy if you see no alerts on the alert tiles. No alerts indicates that there are no capacity or hardware issues in the environment, no failed jobs in the last 24 hours, and that data protection is working without any issues.

If you see any alerts, you can drill down to the relevant alert window to investigate the cause. There are alerts for capacity utilization, hardware, data protection, and jobs status for block storage.

Analyzing data in the information gauge

The information gauge gives a visual indication of the total capacity of all managed storage systems.



Thin Used indicates the sum of all capacity that is currently used. If the usage is around 70-80% of the total capacity, you might receive capacity alerts based on the thresholds set by your storage administrator for block storage. The default thresholds are 70% and 80% and can be changed during pool creation.

The Total Allocated value representing the sum of the capacities of all pools in the system must be close to 100% capacity. This indicates that you are utilizing your entire parity group capacities for block storage and drive capacities for software-defined storage systems by allocating them to pools. If the Thin Used value nears the Total Allocated value then you might run out of pool capacity soon. In this case, consider expanding the pool to accommodate more capacity.

If you notice that the Total Allocated and the Thin Used values are approaching the total capacity, you might be running out of disk capacity on one or more storage systems and might need to add disk space to increase storage capacity. Before adding disk space, consider the following steps:

- Review the information gauge for each storage system to identify which one needs additional capacity.
- Check for unused disks in each storage system to determine if any raw unused capacity is available for parity group creation in block storage and for storage pool expansion in software-defined storage systems.

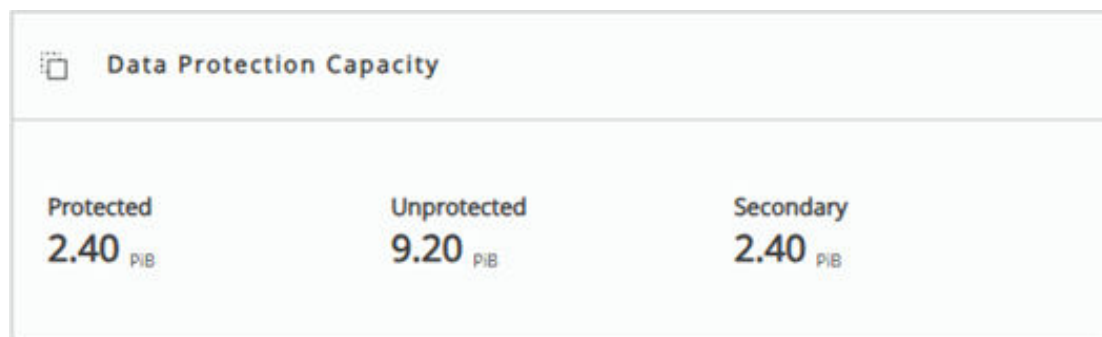
Capacity subscription beyond the total available capacity must not be an issue as long as your thin capacity utilization remains well within the total capacity.

Analyzing data protection metrics

The balance of your protected primary volumes and secondary volumes depends on the number of copies you chose to maintain and on the type of the data protection technology used. If you set aside more volumes for data protection, the overall usable capacity might be affected. However, if you have a large amount of unprotected data, you should consider data protection options.



Note: These data protection capacity numbers are based on oversubscribed allocations and, as a result, correlate with the overall oversubscription percentage, not the usable capacity numbers represented in the rest of the information gauge.



Tier management

As parity groups are created, the various disk types become categorized into tiers. The tiers and corresponding disk types are as follows for block storage.

Table 1 Tier definitions

Tier	Disk type
Diamond	SCM NVMe
Platinum	FMD, FMD DC2, SSD, SSD(RI), FMD HDE, SSD NVMe, and SSD(QLC)
Gold	SAS 15 k
Silver	SAS 10 k
Bronze	SAS 7.2 k



Note: Adding all tier capacities together equals the Total Usable Capacity in the center of the information gauge.

The Tier Management window displays the tier definitions. You can edit the tier names (Diamond, Platinum, Gold, Silver, Bronze, External, and SDS).

Access the Tier Management window by clicking the Settings tab and selecting Tier Management.

Inventory and resource information

The inventory windows display details about the storage system resources. These resources include storage systems, servers, ports, pools, volumes, parity groups, external parity groups (if the storage system has external storage), host groups, NVM subsystems, and replication groups.

The maximum number of items that can be displayed in each inventory is 100,000. You can use the search, filter, and sort functions to display items when it is exceeding the maximum limit in the inventory. Columns that display multiple values in a cell cannot use the sort function. If you use the sort function for these columns, the result of the sort function might be unexpected.

You can complete common tasks from the inventory windows, such as the following:



Note: The software-defined storage resources are only displayed in the storage system inventory.

- You can select one or more resources and delete them.

When you delete a storage system, you disassociate it from the management software. When you delete a pool or volume, the resource is removed from the storage system.

- You can delete the parity group to reconfigure the storage system with some other RAID configuration or simply decommission the array.

When you delete a parity group, it is removed from the storage system and the disks used to create the parity group are no longer in use. If the parity group is in use by a pool, the parity group deletion fails.

- You can select one or more of the same type of resources and update their properties. The properties that you can update depend on the type of resource.
- You can click a specific resource to see more details in the resource detail window.
 - When you delete a block pool, the parity groups used by the pool are no longer in In Use status. The pool volumes on these parity groups are formatted and the parity group will eventually be in Available status.
 - When you delete a volume, the pool subscription goes down. Volume deletion fails if the volume participates in data protection or is attached to a server.
 - When you delete a server, the server is disassociated from the management software. You can no longer provision volumes to the server (or its WWNs). Server deletion fails if it has volumes attached to it.

Schedule jobs

Configuring storage systems, servers, and fabric switches (such as provisioning volumes), involves a series of tasks that are consolidated into jobs. You can create the jobs to run immediately or schedule the jobs to run at a specified date and time. You can schedule jobs during underutilized time slots like midnight to avoid high load time.

You can schedule jobs to configure the following resources:

- Block storage
- Servers/Server groups
- Fabric switches
- Virtual Storage Machines

You can also monitor and delete jobs.

When scheduling jobs, note the following:

- If the storage management service is stopped for some reason, the scheduled jobs will run at the specified date and time after the service starts again. However, if the specified date and time is before the service is restarted, the jobs will fail and not run. If this occurs, reschedule the jobs again.
- If you upgrade the software or back up and restore it to a different environment, scheduled jobs that are scheduled to run at a later date or time will not be migrated and will fail. If this occurs, schedule the jobs again after the upgrade or restore process is complete.
- If too many jobs are run simultaneously, it can exceed the processing capacity of the server. Also, the jobs might hang up in the In Progress state and fail to complete. If this occurs, schedule the jobs at different times.
- When you schedule a provisioning job, if another provisioning job that uses the same path configuration is running or other tools before the scheduled job starts, the scheduled job may fail to use the planned LUN.

For example, if you schedule a Create, Attach, and Protect Volumes with High Availability job with Mandate LUN Alignment enabled, and then submit an Attach Existing Volumes job that specifies the same path configurations as the P-VOL of the HA pair you are creating in the scheduled job, the scheduled job will fail during the Attach Volumes process when the LUNs because the pair cannot be aligned.

If this occurs, delete the created volumes and then submit the job again after specifying a LUN that you know will be available.

Scheduling a job

Procedure

1. Follow the procedures to configure storage systems, servers, fabric switches, or virtual storage machines, and provide the required information.
2. To schedule a job, click the down arrow next to **Submit**, and select **Schedule**.
3. Specify the date and time to run the job in the **Schedule Setting** dialog box, and then click **Schedule**.

Monitoring scheduled jobs

You can monitor the status of scheduled jobs from the Jobs or Job Details window.

For more information on monitoring jobs, see [Monitoring jobs \(on page 59\)](#).

Deleting scheduled jobs

You can only delete or cancel a scheduled job before its scheduled start time.

Procedure

1. To delete a scheduled job, do one of the following:
 - Select the scheduled job and click the trash (🗑️) icon in the **Jobs tab**.
 - Click the scheduled job to open the **Job Details** window, and then click the trash (🗑️) icon in the upper right-hand corner.
2. In the confirmation dialog box, click **OK**.

Searching resources

You can search for resources across by entering a keyword in the search field and clicking the search icon or pressing Enter to view the search results.

You can search all resources or a specific resource type.

Procedure

1. Navigate to the search bar in the upper-right corner, and select **All Resources** or a specific resource.
2. Type a keyword and click the search icon or press Enter.
The **Keyword Search** window opens with the search results. Use the resource types to refine the search results.

Keyword Search

If you cannot find the resource you were looking for, change the search keyword.

All Resources ▾

dpvol_0020

[Volume] S/N: 10054 - ID: 200 (00:00:C8) (DpVol_00200) - Virtual ID: 200 (00:00:C8)

[Volume] S/N: 10054 - ID: 201 (00:00:C9) (DpVol_00201) - Virtual ID: 201 (00:00:C9)

[Volume] S/N: 10054 - ID: 202 (00:00:CA) (DpVol_00202) - Virtual ID: 202 (00:00:CA)

[Volume] S/N: 10054 - ID: 203 (00:00:CB) (DpVol_00203) - Virtual ID: 203 (00:00:CB)

[Volume] S/N: 10054 - ID: 204 (00:00:CC) (DpVol_00204) - Virtual ID: 204 (00:00:CC)

[Volume] S/N: 10054 - ID: 205 (00:00:CD) (DpVol_00205) - Virtual ID: 205 (00:00:CD)

[Volume] S/N: 10054 - ID: 206 (00:00:CE) (DpVol_00206) - Virtual ID: 206 (00:00:CE)

[Volume] S/N: 10054 - ID: 207 (00:00:CF) (DpVol_00207) - Virtual ID: 207 (00:00:CF)

[Volume] S/N: 10054 - ID: 208 (00:00:D0) (DpVol_00208) - Virtual ID: 208 (00:00:D0)

[Volume] S/N: 10054 - ID: 209 (00:00:D1) (DpVol_00209) - Virtual ID: 209 (00:00:D1)

[Volume] S/N: 20055 - ID: 200 (00:00:C8) (DpVol_00200) - Virtual ID: 200 (00:00:C8)

[Volume] S/N: 20055 - ID: 201 (00:00:C9) (DpVol_00201) - Virtual ID: 201 (00:00:C9)

[Volume] S/N: 20055 - ID: 202 (00:00:CA) (DpVol_00202) - Virtual ID: 202 (00:00:CA)

[Volume] S/N: 20055 - ID: 203 (00:00:CB) (DpVol_00203) - Virtual ID: 203 (00:00:CB)

[Volume] S/N: 20055 - ID: 204 (00:00:CC) (DpVol_00204) - Virtual ID: 204 (00:00:CC)

[Volume] S/N: 20055 - ID: 205 (00:00:CD) (DpVol_00205) - Virtual ID: 205 (00:00:CD)

3. Click the result record to view the details.
If you cannot find your resource, change the keyword or resource type, and search again.

Add a storage system

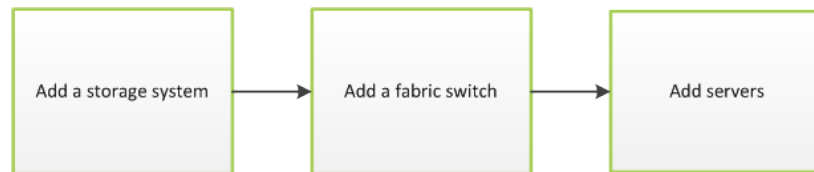
Onboarding a storage system is the process of associating it with the management software. After you onboard the storage system, you can manage it from the dashboard.

Note: Do not onboard the same storage system to multiple management instances. This may exhaust SVP resources, which causes the SVP to slow or become unresponsive.

For details on block storage, see [Adding block storage \(on page 35\)](#).

Onboarding a block storage system workflow

When you onboard a storage system, you associate it with the management software so that you can manage it from the dashboard. Then you can add servers to which you can attach volumes. Optionally, you can add fabric switches to auto-create zones during volume provisioning.



Note: If you use resource groups, make sure that the Service Processor (SVP) username used to onboard storage systems has access to all custom resource groups and meta resource groups.

Adding block storage

You can add multiple storage systems at the same time by specifying an SVP IP address that has multiple storage systems. You cannot add storage systems with different credentials at the same time.

Note: Onboarding a storage system also migrates server information from Hitachi Storage Advisor Embedded. For data integrity purposes, the Hitachi Storage Advisor Embedded provisioning function is turned off after migration.

Before you begin

Verify the following:

- The user name used to onboard a storage system has access to all resource groups on the storage system, including custom resource groups and meta resource groups, so that workflows function correctly.
- The user is a member of the Administration Users Group.
- The storage system is set to SNMPv3 to receive storage systems alerts. If the storage systems have SNMPv1 or SNMPv2c settings configured, you can still onboard the storage systems, but alert information for these storage systems is not shown in the user interface. For alerts to be received from onboarded storage systems, change the SNMP setting to SNMPv3, then restart the server so that the management software is added as an SNMP trap destination.

To launch Storage Navigator under one of the following conditions, the account used for onboarding must be authenticated locally by Storage Navigator:

- The Storage Navigator Launch Setting option is disabled.



Note: Some storage systems support upgrading the controllers by replacing the Controller Board. After replacing the Controller Board, update the storage system data by manually refreshing or waiting for the automatic refresh to complete. You can confirm that the data is successfully updated by verifying the following information:

- The MODEL in the storage system inventory and storage system details is updated.
- The report showing that the storage system model is updated is reported in the Jobs window.

Procedure

1. On the dashboard, click the **Storage Systems** (📁) icon.
2. Click the plus sign (+) to add a storage system.
3. In the **Onboard Storage System** window, enter values for the following parameters:

IP Address:

VSP One Block: Enter the service IP address (IPv4) for the target storage system.

All other VSP storage systems:

- Storage system with an SVP: Enter the IP address (IPv4) of the external SVP for the target storage system.
- Storage system without an SVP: Enter the GUM IP address (IPv4) of the controller for the target storage system.

User name and password:

Enter the credentials for a user who has administrator privileges on this storage system. For example, you can log in with the username `maintenance`.



Note: If the storage system has a virtual SVP, you can specify the SVP access port number following the IP address in the IP address field. The syntax is *IP-address:Port-number*.

4. Click **Submit**.

Result

When you successfully add a 4-node cluster, a message displays requesting that you ensure both storage systems in the global-active device pair are added before performing procedures.

The Jobs window is updated with a job called `Create Storage System`. If you are adding multiple storage systems, there is a job for each one.

Wait a while for the management software to add the storage system. Refresh the Jobs window to verify that the storage system is onboarded.

The dashboard shows that the number of storage systems is incremented by one.

Additionally, when you click the Storage Systems (📁) icon, you are redirected to the storage system inventory window where you can see the newly added storage system.

When a storage system is onboarded, there is an initialization process that gathers information about the current configuration of the storage system. During this time, you see that the ports, volumes, pools, and parity groups in the storage system are "Not accessible". After the initialization is complete, you can see the port, pool, volume, and parity group information in the **Storage System detail** window.

Next steps

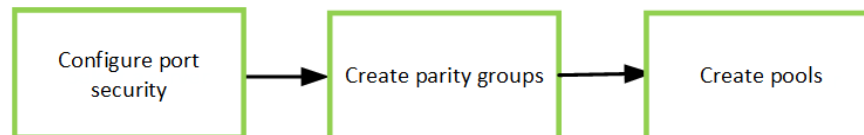
1. From the parity groups inventory window, create parity groups to convert the raw disk capacity into usable capacity.
2. From the Settings tab, access the tier definitions before creating pools.

Configure block storage

Use the management software to configure block storage systems.

Configuring a block storage system workflow

The following workflow shows what you must do before using the provisioning functions.



Note: The software retrieves and displays any resources that already exist in the storage system.

Complete the following to configure a storage system:

- Set port security: Port security must be enabled for a host storage domain (HSD) to be created on the port. If port security is disabled, the port is not selected for HSD creation. If you manually select the security-disabled port, the host group is created.
 - For Fibre/Fibre with SCSI mode ports or iSCSI ports, enable port security to use the provisioning functions.
 - For Fibre with NVMe mode ports, disable port security to use the provisioning functions.
- Create parity groups so you can create pools.



Note: You cannot create or modify parity groups for VSP One Block, but you can view them.

To create or modify parity groups for configuring a pool, you must use VSP One Block Administrator. The pool configuration workflow in VSP One Block Administrator automatically handles the parity groups setup. For a detailed procedure, see [Creating a pool \(on page 45\)](#).

- Create pools so you can create volumes.

Managing port security and settings

Before creating a host storage domain (HSD) on a port, you might need to change the port security and settings like port attributes.

For example, port security must be enabled for Fibre or iSCSI ports. By default, security is disabled on supported storage systems. If port security is disabled, the port is not selected for host storage domain (HSD) creation.

If you select a Fibre or iSCSI port with security disabled, you are limited to the default host group. If you manually select the port with security disabled, the host group is created.

Procedure

1. On the dashboard, click the **Storage Systems** (🗄️) icon to see the inventory of storage systems and capacity information.
2. Click a storage system to see the configuration of pools, ports, volumes, and parity groups.
3. Click **Ports** to see the configured storage ports for the storage system. The Ports window opens:



Note: Ports with NVMe mode are displayed only for storage systems with firmware versions supporting NVMe over FC.

PORT ID	WWN	SPEED	FABRIC CONNECTION TYPE	SECURITY	VSP PORT	ATTRIBUTE
CL1-A	50:06:0E:80:07:27:46:00	Auto	Fabric ON / Point-to-point	Yes	No	Target Port
CL1-B	50:06:0E:80:07:27:46:01	Auto	Fabric ON / Point-to-point	Yes	No	Target Port
CL1-C	50:06:0E:80:07:27:46:02	Auto	Fabric ON / Point-to-point	Yes	No	Target Port
CL1-D	50:06:0E:80:07:27:46:03	Auto	Fabric ON / Point-to-point	Yes	No	Target Port
CL3-A	50:06:0E:80:07:27:46:20	Auto	Fabric ON / Point-to-point	Yes	No	Target Port
CL3-B	50:06:0E:80:07:27:46:21	Auto	Fabric ON / Point-to-point	Yes	No	Target Port
CL3-C	50:06:0E:80:07:27:46:22	Auto	Fabric ON / Point-to-point	Yes	No	Target Port
CL3-D	50:06:0E:80:07:27:46:23	Auto	Fabric ON / Point-to-point	Yes	No	Target Port
CL5-A	50:06:0E:80:07:27:46:40	Auto	Fabric ON / Point-to-point	Yes	No	Target Port

4. To modify ports, do one of the following:
 - Select one or more Fibre Channel ports, then click **Edit Ports** to open the **Edit Fibre Port** window where you can change the port settings.
 - Select an iSCSI port, then click **Edit Ports** to open the **Edit iSCSI Port** window where you can change security settings and IPv4 or IPv6 settings.
5. For VSP 5000 series storage systems, you can select either the **Target** attribute or the **Bidirectional** attribute in the **Edit Fibre Port** window.



Note: The bidirectional port attribute includes all the port attributes (such as Target and External). Ports with this attribute are available on some storage system models.

6. Click **SCSI Mode** or **NVMe Mode** to select the port operation mode.
7. Click **Enable Security** or **Disable Security**, then click **OK**.

A job starts to update the port security.

To provision volumes, set the following:

- For Fibre/Fibre with SCSI mode ports and iSCSI ports: **Enable Security**
- For Fibre with NVMe mode ports: **Disable Security**

Modifying port attributes in Storage Navigator


You can open the **Ports inventory** window in Storage Navigator by clicking Open the Ports/ Hosts Groups/iSCSI Targets window in Storage Navigator to view and modify port attributes.

For more information, see the Storage Navigator online help.




Note: Changes you make in Storage Navigator might take a few minutes to appear in the management software.

Next steps

To view the Login WWN and iSCSI Name details, click  in the upper right-hand corner of the window.

Login WWN and iSCSI Name details

To view the Login WWN and iSCSI Name details, click  in the upper right-hand corner of the Ports window.



Note: Ports with NVMe mode are not displayed.

Login WWN and iSCSI Name

Fibre iSCSI

Search Filter

Loaded all 32 items

WWN	PORT ID	HOST GROUP NAME	STATUS
13:57:08:16:96:00:01:00	CL1-A	HostGroup-1A001	Logged-in
13:57:08:16:96:00:01:01	CL1-A	HostGroup-1A001	Logged-in
13:57:08:16:96:00:01:02	CL1-A	HostGroup-1A001	Logged-in
13:57:08:16:96:00:01:03	CL1-A	HostGroup-1A001	Logged-in
13:57:08:16:96:02:01:00	CL1-C	HostGroup-1C001	Logged-in
13:57:08:16:96:02:01:01	CL1-C	HostGroup-1C001	Logged-in
13:57:08:16:96:02:01:02	CL1-C	HostGroup-1C001	Logged-in
13:57:08:16:96:02:01:03	CL1-C	HostGroup-1C001	Logged-in
13:57:08:16:96:04:01:00	CL1-E	HostGroup-1E001	Logged-in
13:57:08:16:96:04:01:01	CL1-E	HostGroup-1E001	Logged-in
13:57:08:16:96:04:01:02	CL1-E	HostGroup-1E001	Logged-in
13:57:08:16:96:04:01:03	CL1-E	HostGroup-1E001	Logged-in
13:57:08:16:96:06:01:00	CL1-G	HostGroup-1G001	Logged-in
13:57:08:16:96:06:01:01	CL1-G	HostGroup-1G001	Logged-in
13:57:08:16:96:06:01:02	CL1-G	HostGroup-1G001	Logged-in
13:57:08:16:96:06:01:03	CL1-G	HostGroup-1G001	Logged-in
13:57:08:16:96:24:01:00	CL3-E	HostGroup-3E001	Logged-in
13:57:08:16:96:24:01:01	CL3-E	HostGroup-3E001	Logged-in
13:57:08:16:96:24:01:02	CL3-E	HostGroup-3E001	Logged-in

Show 200 items

To see the iSCSI name details, click the iSCSI tab.

Login WWN and iSCSI Name

Fibre iSCSI

Search Filter

Loaded all 280 items

iSCSI NAME	PORT ID	iSCSI TARGET ALIAS	iSCSI TARGET NAME	STATUS
iqn.530070.1b000.0	CL1-B	1B-G00	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b000.1	CL1-B	1B-G00	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b000.2	CL1-B	1B-G00	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b000.3	CL1-B	1B-G00	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b001.0	CL1-B	HostGroup-1B001	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b001.1	CL1-B	HostGroup-1B001	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b001.2	CL1-B	HostGroup-1B001	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b001.3	CL1-B	HostGroup-1B001	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b002.0	CL1-B	HostGroup-1B002	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b002.1	CL1-B	HostGroup-1B002	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b002.2	CL1-B	HostGroup-1B002	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b002.3	CL1-B	HostGroup-1B002	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b003.0	CL1-B	HostGroup-1B003	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b003.1	CL1-B	HostGroup-1B003	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b003.2	CL1-B	HostGroup-1B003	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b003.3	CL1-B	HostGroup-1B003	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b004.0	CL1-B	HostGroup-1B004	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b004.1	CL1-B	HostGroup-1B004	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in
iqn.530070.1b004.2	CL1-B	HostGroup-1B004	iqn.1994-04.jp.co.hitachids.r90.1.30070...	Logged-in

Show 200 items

You can filter the display by:

- Port ID
- Status (Logged-In or Logged-Out)
- Host Group Name (Fibre tab only)
- iSCSI Target Alias (iSCSI tab only)
- iSCSI Target Name (iSCSI tab only)

Editing iSCSI port settings

You can change the settings for port security and for IPv4 and IPv6.

Procedure

1. Navigate to the **Ports** window and select the **iSCSI** tab.
2. Select the port, then click the edit (✎) icon.

Edit iSCSI Port

PORT
CL1-B

SECURITY
Enable Disable

ATTRIBUTE
Bidirectional

IPV6
Enable Disable

IPV4 Information
IPV4 DEFAULT GATEWAY
10.1.1.1

IPV6 Information
LINK LOCAL ADDRESS MODE
Auto Manual

GLOBAL ADDRESS MODE
Auto Manual

IPV6 DEFAULT GATEWAY
..

Cancel Submit

3. Update the port security or the settings for IPv4 and IPv6, then click **Submit**.

Creating parity groups

Parity groups are the basic units of storage capacity. Creating parity groups converts the raw disk capacity in your storage system into usable capacity.

Parity group concepts

The software has a simple one-click method for creating parity groups that is based on best practices applicable to the disks in the storage system.

An advanced method for creating parity groups is also available. You can choose to use the advanced method if there is no need to rely on best practices.



Note:

- You cannot create parity groups on the following storage systems:
 - VSP 5000 series

An authorized service representative must create these parity groups, but you can initialize them in the software. You can enable encryption in Storage Navigator.

- You cannot create or modify parity groups for VSP One Block using the management software, but you can view them.

To create or modify parity groups for configuring a pool, you must use VSP One Block Administrator. The pool configuration workflow in VSP One Block Administrator automatically handles the parity groups setup. For a detailed procedure, see [Creating a pool \(on page 45\)](#).


Creating parity groups also creates LDEVs that can be consumed for pool creation.

Encryption can be enabled during parity group creation if prerequisites are met, including a storage system with an Encryption Disk Board.

The standard practice is to use all available disk capacity when creating parity groups to ensure that all the storage system capacity is usable. There can be exceptions to this practice, for example:

- If the entire capacity of the storage system is not needed.
- If there is a need to create fewer parity groups to reserve more disks as spares.

Viewing parity groups

Access the **Parity Groups** window by clicking the Storage Systems () icon on the dashboard, clicking a storage system ID link, and then clicking the Parity Groups tile.

A summary of parity groups includes disk type, number of parity groups, capacity, and available spares, all sorted by disk type.

- Click Manage Spare Disks to open the Disk Management window and set free disks as spare disks, or spares as free disks.



Note: This feature is not available for the following storage systems:

- VSP 5000 series

- Click any parity group tile to view the details.
- Click the plus sign (+) to open the Create Parity Groups window.

When you open the Create Parity Groups window, choose whether to use the basic method (default) or the advanced method. You can enable encryption using either method.

- Basic option: Creating a parity group using the basic option needs no input, but you can change the RAID type or the number of parity groups. Best practices are used when creating the parity groups.
- Advanced option: You can configure the RAID layout of the parity group by selecting the specific disks to assign for parity group creation.

Enabling parity group encryption in Storage Navigator

To enable parity group encryption, click Open the **Parity Groups** window in Storage Navigator.

For more information, see the Storage Navigator online help.



Note: Any changes you make in Storage Navigator might not be reflected for a few minutes.

Creating parity groups, basic method

The following procedure describes the basic option for creating a parity group and enabling encryption.



Note: You cannot create parity groups on the following storage systems.

- VSP 5000 series

An authorized service representative must create these parity groups using another tool.

Before you begin

- Register the storage system.
- Identify the target storage system name.
- Identify the total capacity that you expect to use. Plan to use all of the available disks in the system when you create parity groups.

Procedure

1. On the dashboard, select the **Storage Systems** (🗄️) icon in the resource side window to see the inventory of registered storage systems.
2. Click a storage system to create and configure the parity groups for it.
3. Click **Parity Groups** to see the inventory of all parity groups in the storage system.
4. Click the plus sign (+) to open the **Create Parity Groups** window and review the list of unused disk types in the storage system. This information is grouped by disk type, disk speed, and disk capacity, and includes the following details:
 - Number of available disks.
 - Available spares detected for each disk type, disk speed, and capacity.
 - Number of new or additional spares to reserve. This calculation is the total spares needed based on best practices, and the number of existing spares in the system.
 - Correct RAID configuration for the disk type.
 - Number of parity groups that you can create.
 - Total usable capacity that is available based on the number of parity groups and the RAID configuration.

Create Parity Groups

Basic | Advanced

STORAGE SYSTEM
420052

DISK TYPE	TOTAL DISKS	AVAILABLE DISKS	AVAILABLE SPARE	ADDITIONAL SPARE	RAID TYPE	PARITY GROUPS	TOTAL CAPACITY	ENCRYPTION
SAS 15k 300.00 GB	48	8	0	2	RAID5 (3D+1P)	1	838.19 GB	Off
SAS 10k 600.00 GB	48	8	0	2	RAID5 (3D+1P)	1	1.64 TiB	Off
SSD 3.80 TB	48	8	0	2	RAID5 (3D+1P)	1	10.37 TiB	Off
SSD(R) 1.90 TB	48	8	0	2	RAID5 (3D+1P)	1	5.18 TiB	Off
FMD DC2 6.40 TB	48	8	0	2	RAID5 (3D+1P)	1	17.46 TiB	Off
FMD 1.60 TB	48	8	0	2	RAID5 (3D+1P)	1	4.37 TiB	Off
SAS 7.2k 10.00 TB	48	8	0	2	RAID5 (3D+1P)	1	27.28 TiB	Off

ENCRYPTION On **Off**

Cancel Submit

5. Decide whether the RAID configuration for each disk type is acceptable. Choose one of the following options:

- Accept the RAID configuration, which uses the full capacity of the installed drives.
- Change the RAID configuration or create fewer parity groups. The software shows the number of parity groups that you can create for the new RAID configuration and the corresponding usable capacity.

6. (Optional) To use encryption, go to Encryption option and click **ON**.

Prerequisites for enabling encryption:

- Storage system must have an Encryption Disk Board.
- Encryption License Key must be installed.
- Key Management Server must be configured on the SVP.



Note: You cannot disable Encryption.

7. Click **Submit**.

Result

A job is started to create the parity group for the storage system. This job includes the following tasks:

- Identifies the appropriate number and position for the spare disk.
- Assigns a spare disk.
- Creates the required number of parity groups for the requested RAID layout.
- Creates and quick formats the necessary volumes on the parity group so that it is ready for pool creation.
- Creates sub-jobs when creating multiple parity groups. Each sub-job shows the status of the parity group creation.

Next steps

Click the Monitoring tab and select Jobs in the side menu to verify the parity group creation status.



Note: Parity group creation might take a long time.

Creating a pool

When creating a pool, use the basic option to take advantage of tiers that are based on best practices.

If you want more flexibility and do not need to take advantage of best practices, you can use the advanced option to select specific parity groups.




Note: You cannot use the basic or advanced options to create a pool for VSP One Block. Instead, you can use an alternative method to create a pool. For more information, see [Pools inventory \(on page 45\)](#).

The pool types are as follows:

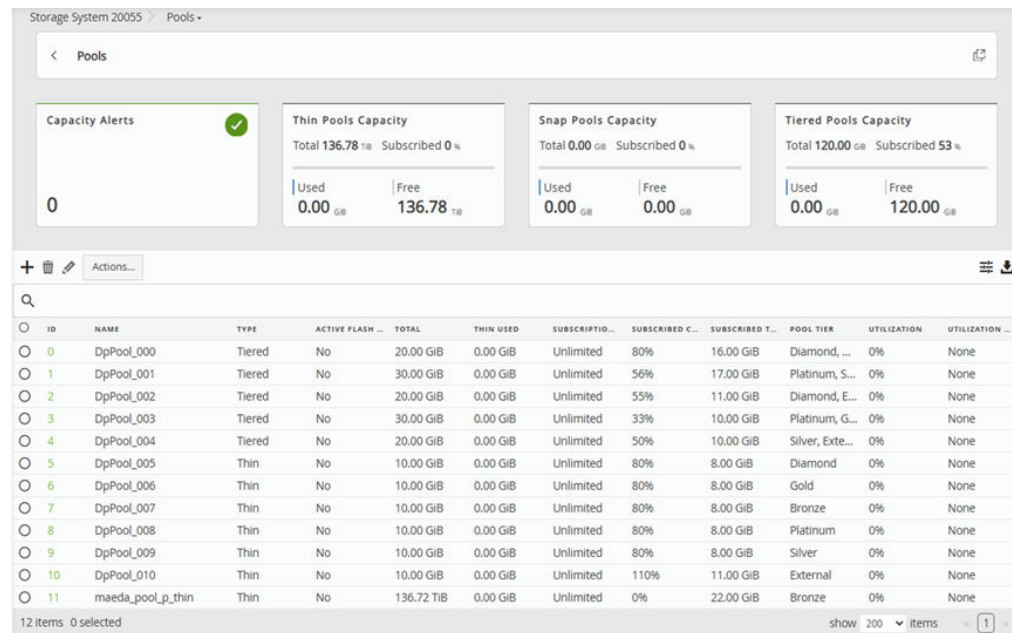
- HDP (Dynamic Provisioning), which allocates virtual volumes to a host and uses the physical capacity that is necessary according to the data write request.
- Tiered, which is used with Dynamic Provisioning and places data in a hardware tier according to the I/O load. For example, a data area that has a high I/O load is placed in a high-speed hardware tier, and a data area that has a low I/O load is placed in a low-speed hardware tier.
- TI (Thin Image), which stores snapshot data in pools. A pool consists of multiple pool-VOLs. The pool-VOLs contain the snapshot data. A pool can contain up to 1,024 pool-VOLs.

Pools inventory

Access the **Pools** window to add, update, and delete pools.

From the dashboard, click the Storage Systems () icon and then click a storage system tile to view parity groups, pools, volumes, and ports.

Click Pools to view the inventory of pools.



You can filter the volumes as follows:

- Free Space: Filter the pools by the amount of free space they have.
- Total: Filter by pool size.
- Pool Type: Filter by the pool type: Thin, Tiered, or Snap.
- Pool Tier: Filter by the pool tier: Diamond, Platinum, Gold, Silver, Bronze, or External.
- Active Flash Enabled: Filter by whether Active Flash is enabled.
- DDM Enabled: If Yes, the pool can be used to migrate volumes greater than 4TiB.
- Encryption: Filter by whether encryption is used. Select YES, NO, PARTIAL, or UNKNOWN.
- FMD Compression: Filter by whether a pool is using a parity group that is enabled for accelerated compression. Select YES, NO, PARTIAL, or UNKNOWN.
- Deduplication Enabled: Select YES or NO.

The following actions are available in this window:

VSP One Block 20:

- Select a pool with parity groups, then click Actions > Manage storage pool in VSP One Block Administrator to update it with VSP One Block Administrator.
- Click Action > Create storage pool with external volume capacity to add a pool with external volume groups in the Create Pool window.
- Select a pool with external volume groups, then click Action > Edit storage pool with external volume capacity to update it in the Update Storage Pool window.
- Select one or more pools with external volume groups, then click Action > Delete storage pool with external volume capacity to delete the pools. Deleted pools are removed from the storage system.

- Click the plus sign (+) to add a pool with parity groups using VSP One Block Administrator.

For more information, see the VSP One Block Administrator documentation

- Click the Export CSV (📄) icon to download the pool details.

All other VSP storage systems:

- Click the Open the Pools page in Storage Navigator icon (🔗) to open the Pools window in a separate browser window.
- Select one or more pools, then click Delete to delete the pools. Deleted pools are removed from the storage system.
- Select a pool, then click the pencil icon to update it in the Update Storage Pool window.
- Select a Tiered Pool, then click Actions > Update Tiering Settings to update it in the Update Tiering Settings window.
- Click the plus sign (+) to add a pool in the Create Pool window.

For more information, see [Creating a pool, basic method \(on page 47\)](#) or [#unique_50](#).

- Click the Export CSV (📄) icon to download the pool details.



Note: Any changes you make in Storage Navigator might not be reflected for a few minutes.

Creating a pool, basic method

To create pools based on best practices use the basic method.



Note: You cannot create a pool with external parity groups using the basic method. You must use the advanced method.

Before you begin

- Create and configure parity groups on the storage system.
- Verify that there is a minimum of four parity groups of the Bronze, Silver, or Gold tiers, or one parity group of the Platinum or Diamond tier. If your environment does not meet this requirement, you can use the advanced method to create pools.
- Verify that you have the following required license:
 - For a Dynamic Tiering pool: Dynamic Tiering
 - For a Thin pool: Dynamic Provisioning
 - For a Thin Image pool: Thin Image
 - For active flash: active flash

Procedure

1. On the dashboard, click the **Storage Systems** (📁) icon to see the inventory of registered storage systems.
2. Click a storage system to create a pool for it.

3. Click **Pools**.
4. Click the plus sign (+) to open the **Create Pool** window.
By default, the **Basic** option is selected.

Create Pool

Basic Advanced

POOL NAME
Pool Name

STORAGE SYSTEM
30060

USE FOR SNAP?
Yes No

BREAKDOWN OF DISKS
Total: 0.00 GiB

Select capacity from Tiers to allocate to Pool

Tier	Capacity
DIAMOND	1.10 TiB Available
PLATINUM	18.75 TiB Available
GOLD	0.00 GiB Available
SILVER	0.00 GiB Available
BRONZE	0.00 GiB Available

Cancel Submit

5. Enter a **Pool Name**.
Pool names can contain alphanumeric characters, hyphens, and underscores only.
Initial hyphens are not allowed.

6. In the **Select capacity from Tiers to Allocate to Pool** pane, you can choose storage from 1, 2, or a maximum of 3 tiers (**Diamond**, **Platinum**, **Gold**, **Silver**, or **Bronze**).
- If you select only one tier, you can use the **USE FOR SNAP?** toggle to decide whether to use Snap pools.
 - Click **Yes** to create Snap pools.
 - Click **No** to create Dynamic Provisioning (DP) pools. These pools can also be used to create snapshots.
 - If you select two or three tiers, the system creates Tiered pools. The following options are available for a Tiered pool:
 - **Tiering:** Select **Automatic** or **Manual** monitoring and tier relocation.
 - **Cycle Time:** Select the cycle for performance monitoring and tier relocation. For automatic tiering, select one of the monitoring cycles from the drop-down. The cycle time can be 0.5, 1, 2, 4, 8 or 24 hours.
 - **Monitoring Period:** When you select 24 hours as the cycle time, specify the time from 00:00 to 23:59 (default value) in which to perform the performance monitoring. Set one or more hours between the start and end time. The start time cannot be later than the end time.
 - **Monitoring:** Specifies the monitoring mode. If you perform the tier relocation weighted to the past period monitoring result, select **Continuous**. If you perform the tier relocation on the specified cycle, select **Periodical**.
 - **Relocation Speed:** Specifies the window relocation speed. You can set the speed to: 1 (Slowest), 2 (Slower), 3 (Standard), 4 (Faster), or 5 (Fastest). The default is 3 (Standard). If the speed specified is slower than 3 (Standard), the data drive load is low when tier relocation is performed.
 - **Buffer Space for Relocation:** Specifies the storage area required for processing tier relocation. Set this as percentage of the tier size. For each tier enter an integer value from 2 to 40 as the percentage to set for that tier. The default value for each tier is 2%.
 - **Buffer Space for New Page Assignment:** Specifies the storage area required for processing new page assignments. Set this as a percentage of the tier size. For each tier enter an integer value from 0 to 50 as the percentage to set for that tier. For tier 1, this value must be between 0 and 50. The default value is 8% for all drive types.



Note: Tiering, Cycle Time, Monitoring Period and Relocation Speed can only be set in environments with an SVP.

Table 2 Tier definitions

Tier	Disk type
Diamond	SCM NVMe
Platinum	FMD, FMD DC2, SSD, SSD(RI), FMD HDE, SSD NVMe, and SSD(QLC)

Tier	Disk type
Gold	SAS 15 k
Silver	SAS 10 k
Bronze	SAS 7.2 k

7. Click a selected tier to view the available storage capacity and select a capacity size.
8. Click **Tier Management** to see the disk type of each pool category.
9. Review the high and low pool utilization thresholds. The thresholds serve as the Warning and Critical thresholds for monitoring capacity. Adjust the thresholds if needed.

If you are creating a Thin (DP) pool, you can choose whether to permanently suspend snapshots when usage exceeds the Critical threshold to reserve capacity for user data. If the threshold is exceeded, the pairs become suspended (PSUE) and the S-VOLs can never accept read-write processes. You can still write to P-VOLs. If this option is selected, a message displays in the Utilization graph in the detail window for the pool.

Thin Image Advanced that uses DRS-VOLs does not support this option. If the threshold is exceeded while this option is enabled, the Thin Image Advanced pair that uses DRS-VOLs does not change to suspended (PSUE).



Note: This option is available for the following storage systems:

- VSP 5000 series
- VSP E series
- VSP G/F350, G/F370, G/F700, G/F900

10. To set the limit to Unlimited, select the **Subscription Limit %** checkbox.



Note: Subscription Limit % is not applicable to Snap pools or to the following storage systems:

- VSP 5000 series with firmware version 90-01-6x
- VSP E990 with firmware version 93-02-02-60/8x or earlier
- VSP G/F350, G/F370, G/F700, G/F900

11. Click **Submit**.

Result

A job is started to allocate the storage capacity and create the pool.

Next steps

- Click the Monitoring tab and select Jobs in the side menu to verify the pool creation job status.
- Create a volume.

Create, attach, and protect volumes

You can create volumes and attach them to servers and then apply data protection in a single workflow by first selecting a server.

Creating and attaching volumes to servers workflow

This workflow shows a single window to create volumes and immediately attach them to servers. Optionally, you can protect volumes as part of the same workflow.

Begin by choosing a server on which you want to create and attach volumes. As part of the workflow, volumes are automatically attached to servers after you select settings. Finally, you are given the option of immediately applying data protection.



Creating, attaching, and protecting volumes with local replication

You can start the create-and-attach workflow by selecting a server and creating volumes.

When you create volumes you can:

- Create multiple volumes of the same size or different sizes at the same time.
- Select the specific pool for volume creation or let the software automatically select the best pool based on utilization.
- Specify a common label and starting label suffix for identical volumes that are the same size and have the same pool requirement.

Creating, attaching, and protecting volumes with local replication for configuring LUN paths

Before you begin

- Create parity groups.
- Create pools.
- Add servers.

Procedure

1. On the dashboard, click the **Servers** (📁) icon to see the inventory of servers.
2. Select a Fibre or iSCSI server, click **Actions** > **Attach Volumes** > **Create, Attach, and Protect Volumes with Local Replication**.

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.

- Select the number of volumes.
- Enter the volume label and select a suffix for it.
- Select the volume size.
- Select the volume unit: **MiB**, **GiB**, **TiB**, or **Blocks**.
- (Optional) Select a **Volume ID Range** to specify one for the new volume for granular management of volumes. For instance, for ease of management, you can assign a certain range of IDs to certain departments in your organization. ID ranges can be specified in Decimal or Hexadecimal. The default selection is **Auto**, which means that the ID is automatically selected for the volume. You can also specify a **Virtual ID / Range**.
- For creating a DRS-VOL, select **Enable** from **Data Reduction Share**.



Note: Do not specify a DRS-VOL and a non-DRS-VOL at the same time when creating a snapshot.

- Select the pool type: **Thin** or **Tiered**.
- For a **Thin** pool, select the pool tier: **Diamond**, **Platinum**, **Gold**, **Silver**, or **Bronze**. If the storage system has available capacity from external storage, you can also select the **External** tier.
- (Optional) Select the pool from the list of available pools. The default selection is **Auto Selected**, which means that the best pool for provisioning the volume based on utilization and tier requirements is automatically selected.



Note: DDM pools are not available and cannot be used to create volumes.

- (Optional) Select a type of **Capacity Saving**: **Compression** or **Deduplication and Compression**.



Note: You can set capacity saving for volumes based on tiered pools for the following storage systems:

- VSP 5000 series

- k. (Optional) For a tiered pool, select the **Tiering Policy** from the list. Tiering policy choices available in the list depend on the choice of pool that was made in the previous step. Tiering policy choice is not available for auto-selected pools.
- l. For creating a T10PI-VOL, select **Enable** from **T10PI**.



Note:

- When creating multiple volumes at the same time, it is not possible to have different T10PI settings enabled and disabled for those volumes.
- To define an LU path between a port and an LDEV with the T10PI attribute enabled, the port must have T10PI mode enabled. To enable T10PI mode on the port, use another storage management tool.

To achieve end-to-end data integrity from components of the server such as application, HBA, and so on to disk drives using T10PI or the combination of T10PI and DIX, see the storage system documentation to verify the supported version of the OS and HBA. To configure the required settings for your servers and HBAs, see the OS documentation.

4. When you have made your choices, click the plus sign (+) to add a volume row to the list of volumes being created. Add more rows as needed.
5. Click **Next** to attach volumes to the selected servers.

STORAGE SYSTEM
VSP_G1000_310054 (10054)

HOST MODE
Use Server Default

HOST MODE OPTIONS
Use Server Default

HOST GROUP NAME
(Optional)

MANDATE LUN ALIGNMENT
Yes No

AUTO CREATE ZONE
Yes No

NUMBER OF VOL...	LABEL	LABEL SUFFIX	SIZE	POOL TYPE	TIER	POOL
1	example_test	—	1.00 GiB	Tiered	—	Auto Selected

View Proposed Volume ID Selection

Cancel Previous Next

6. 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.

7. 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.

The software 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.

8. Select **Mandate LUN Alignment**.

This option specifies whether to assign the same LUN number to multiple servers for a volume. If **Yes** is specified, the same LUN number is always assigned, and if **No** is specified, the same value is not necessarily used. If the volumes is attaching to only one server, this setting has no effect.

9. The **Auto Create Zone** is set to **No** by default, which means that no auto-zone is created. You can set it to **Yes** to automatically create zones.

Physical connections must be available on the switch. If these exist, an auto-zone is created between the ports you selected in the **Attach Volumes** window.



Note: If there was already a zone connected between those two ports, an existing zone is used. (A new one will not be created.)

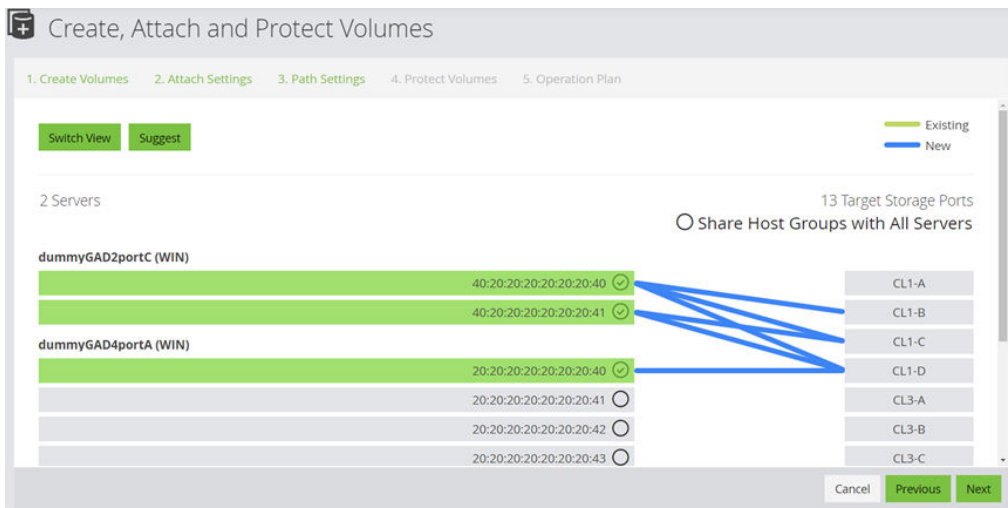
10. You can confirm which Volume IDs will be used by clicking **View Proposed Volume ID Selection**.

To mandate using volume IDs shown in pop-up dialog, select **Yes** under **Mandate Using Displayed Volume ID**.



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

11. Click **Next** to view options for creating and editing LUN paths. The displayed path configuration of the **Path Settings** window depends on the selected **Host Mode** and **Host Mode Option** set in the **Attach Settings** window.



12. In the **Path Settings** window, you can view servers and their WWNs, along with ports on the storage system. The software scans 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.

Port Redundancy Level

NO.	PORT ID	DKC LOCATI...	CTL LOCATION	REDUNDANC...
1	CL1-C	DKC-0	CTL01	CHB
2	CL3-C	DKC-0	CTL01	CHB
3	CL5-C	DKC-0	CTL01	CHB
4	CL7-C	DKC-0	CTL01	CHB
5	CL3-E	DKC-0	CTL01	CHB
6	CL5-E	DKC-0	CTL01	CHB
7	CL7-E	DKC-0	CTL01	CHB

OK

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 exist on that port and a single host group cannot be created, the checkbox will not appear.

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 in the Attach Settings window are populated as paths.

To prevent the volume from being added to an existing path, click the existing path to remove it.

- Click **Suggest** to populate automatically selected paths. By default, the least-used ports are selected. Suggest paths need both server and storage ports to be logged into the fabric switches in the inventory.



Note: For VSP 5000 series storage systems, the first port suggested has the fewest LUN definitions and the second port suggested has the fewest number of LUNs in the highest redundancy level.

- To manually create a path, click WWNs to select them and click a port to connect those with a blue connector lines. To delete the connection, click the connector again.
- Optionally, you can click **Switch View** to use tables to create paths by selecting Server Ports to attach to Storage Ports.

13. When you are satisfied with the paths, click **Next** to view options for protecting volumes.

If you specify a DRS-VOL, you can only select **Auto Selected** for **POOL FOR SNAPSHOT** and the same pool to which the P-VOL belongs is selected automatically.

Create, Attach and Protect Volumes

1. Create Volumes 2. Attach Settings 3. Path Settings 4. Protect Volumes 5. Operation Plan

REPLICATION TYPE

☒ Snap ☐ None

SNAP RETENTION POLICY (MAX 1024)

Snap Retention

CONSISTENCY

☐ Yes ☒ No

Note: For volumes that already contain one or more snapshots, new snapshots will be saved in the same pool as the existing snapshots.

☒ Hourly ☐ Daily ☐ Weekly ☐ Monthly

START MINUTE

0

EVERY

1

Hours

▲ Snap will start every 1 hours of the UTC time. Current time in UTC is 12/04/23 01:42 PM.

USE REPLICATION GROUP

Use New

REPLICATION GROUP NAME

Replication Group Name

POOL FOR SNAPSHOT

STORAGE SYSTEM ID

20079

STORAGE POOL

Auto Selected

VOLUMES

NUMBER OF VOLUMES	LABEL	LABEL SUFFIX	SIZE	DATA REDUCTION SHARE	POOL TYPE	TIER	POOL
1	—	—	1.00 GiB	Enable	Thin	Diamond	Auto Selected

Cancel Previous Next Submit

14. 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: To view the plan summary page, limit the number of LUN Paths to 5000.

15. You can specify the LUN range for volumes in the **LUN Settings** pop up window which is launched by clicking **LUN Settings** above the Planned Path Configuration table.
16. You can make it mandatory to use the LUNs displayed in the table by specifying Yes to **Mandate Using Displayed LUN**.
17. When you are satisfied with all the settings, click **Submit**.

Monitor block storage

Using the management software, you can monitor capacity, data protection, jobs and hardware.

Monitoring capacity

You can monitor block storage capacity so you can tell when physical capacity usage is exceeding thresholds set for your pools.



Note: Capacity alerts for Snap (TI) pools are not supported.

Alerts are represented by the number shown on the right-hand side of the Capacity Alerts tab label. It indicates the number of the capacity components that are monitored and have alerts. The number shown on the right-hand side of the pool tab label represents the number of capacity alerts. The number includes errors and warnings. The Error threshold is set in the "Utilization Threshold (High)" field when the pool is created and the Warning threshold is set in the "Utilization Threshold (Low)" field.

Capacity Alerts for all storage systems are shown on the dashboard and on the Monitoring tab. Click the Capacity Alerts tab to view the number of pools that have alerts and their details. The number of Capacity Alerts cannot be more than 1 because the software monitors at the component level, which is pools.

The alert clearance process runs every 20 minutes for each storage system that has pools with errors. Alerts are only cleared when all pools with errors in the storage system return to normal state. For example, if there are 5 pools with errors in one storage system, then all alerts will display until all the pool alerts are cleared.

Procedure

1. Monitor the alerts for one or more of the following resources:
 - All storage systems: If **Capacity Alerts** on the dashboard has a dash displayed in an orange circle, click it to open the **Monitoring** window with the number of **Pool** alerts exposed in the **Capacity** carousel. Alternatively, you can click the **Monitoring** tab and then click the **Capacity** tile.
 - Storage system detail: In the storage systems inventory, click a storage system tile. If the **Capacity Alerts** tile has a dash displayed in an orange circle, click it to open the **Monitoring** window and display the **Pool** alerts for the selected storage system.
 - Pool inventory: On the storage system inventory window, click a storage system tile to view resources for the storage system. Click **Pools**. Then click the **Capacity Alerts** tile to open the alerts carousel for the storage system pools in the **Monitoring** tab.
2. In the **Capacity** alerts carousel, click **Pools** to populate the table with details of the alerts.

Next steps

If there are pools with alerts displaying the "Error" status, you can expand the pools to increase their capacity.

Monitoring hardware

You can monitor hardware devices to view and investigate warnings and critical alerts.

The software monitors components in your storage systems and displays alerts on resources. You can also see how many components are in normal status.

Alerts are represented by the number shown on the right-hand side of the **Hardware Alerts** tab label. It represents the number of the hardware components that are monitored and have alerts. The number shown on the right-hand side of each hardware component tab label represents the number of the alerts in its component. The number includes errors and warnings.

The alerts are received from the storage array: one alert per component type, for a maximum of eight.

The alert clearance process runs every 20 minutes for each storage system that has components with errors. Alerts are only cleared when all components of a specific type with errors in the storage system return to normal state. The exception is disks other than VSP One Block, each of which can have alerts cleared, even if other disks remain in error. Alerts for ports and processors are cleared together, so alerts are cleared only when all ports and all processors are normal.

For example, if there are five fans with alerts in one storage system, they will be cleared only when every fan alert is cleared. However, for disks, each alert is cleared as and when disk alert clearance is available.

The software monitors the following components:

- Disks
- Fans
- Batteries
- Cache
- Processors
- Power supplies
- Ports
- Shared memory

The software does not report the following types of alerts:

- Alerts generated by storage system maintenance operations
- Alerts not categorized as system failures (for example, recommend replacement)

Procedure

1. Monitor the alerts for one or more of the following resources:
 - Dashboard: Click the **Hardware Alerts** tile or the **Monitoring** tab, select **Alerts**, and then click the **Hardware** tile to display the types of components.
 - Storage system detail: Click a storage system tile, then click the **Hardware Alerts** tile to view hardware alerts for the selected storage system in the **Monitoring** tab.
 - Parity Group inventory: Click a storage system tile and then click **Parity Groups** to open the inventory. Click the **Hardware Alerts** tile to view alerts for disks where parity groups are located.
2. Click a component type to display details in the table. Review the details to resolve the issue.

Monitoring data protection

Data protection monitoring enables you to monitor the status of each data protection task.



You can view jobs alerts for your data protections tasks in a single window. Data protection alerts can be viewed by storage system and by server and are available for the aggregated storage systems.

Alerts for the following operations are available:

- Failed Clone Now operations
- Failed Snapshot operations

A number in a Data Protection tab indicates the number of primary volumes and servers on which data protection tasks have failed. You can click the tab to investigate failed tasks.

Procedure

1. View data protection alerts for the following resources:
 - All data protection alerts:
 - From the dashboard, click the **Monitoring** tab, select **Alerts**, and then click the **Hardware** tile or **Data Protection Alerts** to open the **Monitoring** window.
 - A single storage system: Click the **Storage Systems**  icon and then click a storage system tile. Click the **Data Protection Alerts** tile to open the **Monitoring** window.
 - Volumes attached to a single server: Click the **Servers**  icon from the dashboard, then click a **Server** tile. Then click **Data Protection Alerts** to open the **Monitoring** window.



The volumes inventory for a server includes failed tasks marked by an exclamation point. Click an exclamation point to view all volumes with failed tasks in the **Monitoring** window.
 2. Click the **Data Protection Alerts** tab in the **Monitoring** window and then click **Volumes** to display details that can help you identify the issue. You can click the volume ID to view details for the volume.
- GAD pairs with the status **PSUE** are displayed.
3. Select a volume to perform one of the available functions:
 - Click **Delete** to delete the volume.
 - Click **Edit** to open [Update Volume window \(on page 66\)](#).
 - Click **Unprotect Volumes** to remove data protection.
 - Click **Restore** to open the **Restore Volume** window and restore secondary volumes to a primary volume.

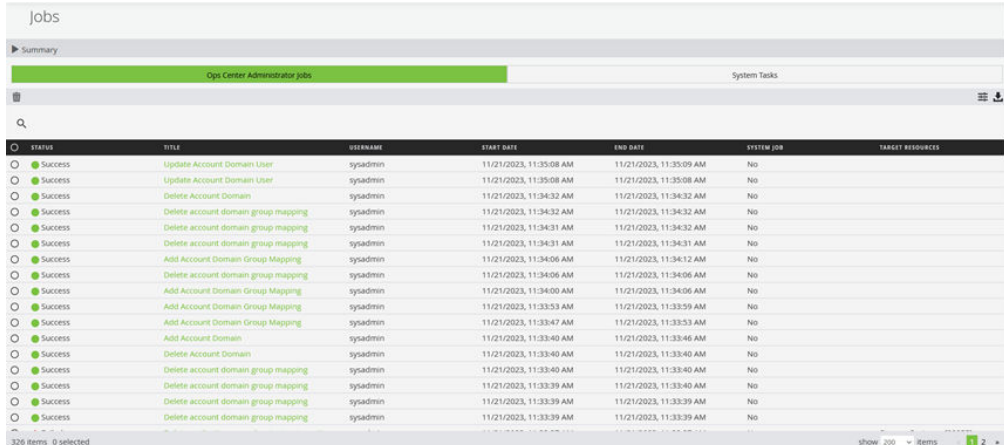
Monitoring jobs

You can view the **Jobs** window to get an update on the status of a task, download the details of a job, perform a job search by keyword, user, or target resource IDs, or view the errors associated with a job.

In this window you see two types of jobs or tasks by switching the displayed tab. In the Jobs window, you can verify submitted jobs and their statuses. In the System Tasks tab, you can verify tasks submitted in Storage Navigator which runs on the onboarded storage system SVP.

Procedure

1. If there is a dash displayed in an orange circle in the **Jobs Alert** tile, it reflects the number of failed jobs and jobs that succeeded with errors. Access the Jobs window in one of these ways:
 - From the dashboard, click **Jobs Alerts** to open the **Jobs** window, or click the **Monitoring** tab and select **Jobs** in the side menu.
 - On the dashboard, click the **Storage Systems**  icon to open the storage systems inventory. If the **Jobs Alert** tile has a dash displayed in an orange circle, click it to view the Jobs window.
2. Click the **Export Jobs in CSV Format** icon () to download the details of a job and its tasks.
3. Use the **Search** function to view job status and search by keyword, start date, end date, resource, or user.








The screenshot shows the 'Jobs' window with a 'Summary' tab selected. Below the tab is a green bar labeled 'Ops Center Administrator jobs' and a 'System Tasks' tab. A search bar is visible. The main table has columns: STATUS, TITLE, USERNAME, START DATE, END DATE, SYSTEM JOB, and TARGET RESOURCE. The table contains 16 rows of job data, all with a status of 'Success'. The bottom of the window shows '326 items, 0 selected' and a 'Show 200 items' button.

STATUS	TITLE	USERNAME	START DATE	END DATE	SYSTEM JOB	TARGET RESOURCE
Success	Update Account Domain User	sysadmin	11/21/2023, 11:35:08 AM	11/21/2023, 11:35:09 AM	No	
Success	Update Account Domain User	sysadmin	11/21/2023, 11:35:08 AM	11/21/2023, 11:35:08 AM	No	
Success	Delete Account Domain	sysadmin	11/21/2023, 11:34:32 AM	11/21/2023, 11:34:32 AM	No	
Success	Delete account domain group mapping	sysadmin	11/21/2023, 11:34:32 AM	11/21/2023, 11:34:32 AM	No	
Success	Delete account domain group mapping	sysadmin	11/21/2023, 11:34:31 AM	11/21/2023, 11:34:32 AM	No	
Success	Delete account domain group mapping	sysadmin	11/21/2023, 11:34:31 AM	11/21/2023, 11:34:31 AM	No	
Success	Add Account Domain Group Mapping	sysadmin	11/21/2023, 11:34:06 AM	11/21/2023, 11:34:12 AM	No	
Success	Delete account domain group mapping	sysadmin	11/21/2023, 11:34:06 AM	11/21/2023, 11:34:06 AM	No	
Success	Add Account Domain Group Mapping	sysadmin	11/21/2023, 11:34:06 AM	11/21/2023, 11:34:06 AM	No	
Success	Add Account Domain Group Mapping	sysadmin	11/21/2023, 11:33:59 AM	11/21/2023, 11:33:59 AM	No	
Success	Add Account Domain Group Mapping	sysadmin	11/21/2023, 11:33:47 AM	11/21/2023, 11:33:53 AM	No	
Success	Add Account Domain	sysadmin	11/21/2023, 11:33:40 AM	11/21/2023, 11:33:46 AM	No	
Success	Delete Account Domain	sysadmin	11/21/2023, 11:33:40 AM	11/21/2023, 11:33:40 AM	No	
Success	Delete account domain group mapping	sysadmin	11/21/2023, 11:33:40 AM	11/21/2023, 11:33:40 AM	No	
Success	Delete account domain group mapping	sysadmin	11/21/2023, 11:33:39 AM	11/21/2023, 11:33:40 AM	No	
Success	Delete account domain group mapping	sysadmin	11/21/2023, 11:33:39 AM	11/21/2023, 11:33:39 AM	No	
Success	Delete account domain group mapping	sysadmin	11/21/2023, 11:33:39 AM	11/21/2023, 11:33:39 AM	No	

Common search terms include:

- Volume
- Pool
- Storage
- Create
- Provision
- Expand
- Delete

The **Status** column displays the job status.

Icon	Description
 Success	The job completed successfully.
 Success With Errors	The job completed successfully, but there were errors.
 * In Progress	The job is still in progress.
 Schedule	The job is scheduled to run at the specified date and time.
 Failed	The job failed.
*: If the job status does not change from "In Progress" for more than 20 minutes, verify that storage system is not locked.	

- Click a job to open the **Job Details** window where you can view any child jobs, reports, target resources, and request information associated with each job. Reports are the messages that the software returns regarding the progress of each job. Child jobs serve to track jobs that start multiple, smaller tasks (such as creating multiple volumes).

Next steps

- If the job failed, review the job reports to determine the cause of the failure.
- If the job completed successfully with errors, click the job to view the error message.

Modifying block storage resources

Using the management software, you can modify storage system resources.

Updating a storage system

Update the storage system name, user name and password for the storage system.

Before you begin

The user must be assigned the System Administrator role.

Procedure

- Log in to Storage Navigator and create a new user.

2. Access the **Update Storage System** window one of these ways:
 - In the **Storage Systems** window, select a storage system, then click **Edit**.
 - In the storage system detail window, click **Edit**.
3. Edit the storage system name, user name or password, then click **Submit**.



Note: When you update the storage system name, the change will be reflected to some views and REST API responses after the next manual refresh. To reflect it, manually refresh the storage system data in the management software.

Updating a server

You can change the parameters for an existing server.

Procedure

1. Access the **Update Server** window in one of these ways:
 - From the dashboard, click the **Servers** (📁) icon to open the inventory of servers. Select a server, then click **Edit**.
 - On the detail window for a server, click the pencil icon.

2. Edit any of the following for a server with the Fibre Channel protocol:
 - **Server Name**
 - **Description**
 - **IP Address**
 - **OS Type**

- **Modify Existing WWNs**

- **Add New WWNs**

- a. If needed, add new WWNs, then click the plus sign to add them to the list.
- b. (Optional) Click **WWN List** to select and update existing WWNs.



Note: If you remove or update all WWNs to which command devices are attached and select the **Apply changes to attached volumes** checkbox, the command device configuration will be disabled.

If you are removing WWNs, update the server without selecting the **Apply changes to attached volumes** checkbox, and then use Storage Navigator to make changes to keep the command device configuration enabled.

If you are updating an existing WWNs, add a WWN to the server first and then remove the existing WWN.

- c. (Optional) You can add and edit user-defined names for WWNs.
- d. You can select a reference WWN to add the new WWN into host groups to which the reference WWN belongs.



Note: If reference WWN is specified, **Apply changes to attached volumes** must also be verified.

- e. Clear the **Apply changes to attached volumes** checkbox if you do not want to make the following changes:
 - If a WWN is updated, all host groups with the old WWN are updated with the new one. All zones created using the software have the old WWN removed and new address populated.
 - If a WWN is deleted, it will be removed from any host group that has it. If the host group is left with no WWNs, the entire host group is deleted. All zones created using the software have the deleted WWN removed.
 - If you add a reference WWN, host groups are edited. If you do not add a reference WWN, no host groups are edited. You can add paths using the new LUN.
 - Changes to name, description, IP address, or OS type do not impact host groups.
3. Edit any of the following for a server with the FC-NVMe protocol:
 - **Server Name**
 - **Description**
 - **IP Address**
 - **OS Type**
 - **Modify Existing Host NQN**

- a. Clear the **Apply changes to attached volumes** checkbox if you do not want to make the following changes:
 - If a Host NQN is updated, all NVM subsystems with the old Host NQN are updated with the new one.
 - Changes to name, description, IP address, or OS type do not impact attached namespaces.
- **Modify Existing WWNs**
- **Add New WWNs**
 - a. If needed, add new WWNs, then click the plus sign to add them to the list.
 - b. (Optional) You can add and edit user-defined names for WWNs.
- 4. Edit any of the following for a server with the iSCSI protocol:
 - **Server Name**
 - **Description**
 - **IP Address**
 - **OS Type**
 - **Modify Existing iSCSI Names**
 - **Add New iSCSI Names**
 - **Enable or Disable CHAP Settings.**
 - a. You can select a reference iSCSI name to add the modified or new iSCSI name into host groups to which the reference iSCSI belongs.
 - b. (Optional) Click **iSCSI List** to select and update existing iSCSI names.



Note: If you remove or update all iSCSI initiator names that command devices are attached to and select the **Apply changes to attached volumes** checkbox, the command device configuration will be disabled.

If you are removing iSCSI initiator names, update the server without selecting the **Apply changes to attached volumes** checkbox, and then use Storage Navigator if you want to keep the command device configuration enabled.

If you are updating existing iSCSI initiator names, add the iSCSI initiator names to the server first and then remove the existing iSCSI initiator names.

- c. (Optional) You can add and edit user-defined names for iSCSI names.
- d. Select **Update CHAP Credential** to add a new CHAP user.

- e. Clear the **Apply changes to attached volumes** checkbox if you do not want to make the following changes:
 - If an iSCSI initiator name is updated, all iSCSI targets with the old iSCSI name are updated with the new one.
 - If an iSCSI initiator name is deleted, it will be removed from any iSCSI target that has it. If the iSCSI target is left with no iSCSI initiator names, the entire iSCSI target is deleted.
 - If an iSCSI initiator name is added, no iSCSI targets are edited. You can add paths using the new LUN.
 - If a CHAP user information changes, the software updates the information on the storage system.
 - Changes to name, description, IP address, or OS type do not impact iSCSI targets.

Updating a server group

You can add and remove servers from a group or update the name and description. You can also attach and detach the volumes when you add and remove servers.

Procedure

1. Access the **Updating a Server Group** window by opening the **Servers** window. Click the **Server Groups** tab.
2. Select a server group, then click **Edit**.
3. Change the other contents accordingly.
 - If you want to change the name and description, change them and click **Submit**.
 - If you want to detach the volumes when removing servers, check the **Apply changes to attached volumes** option and click **Submit**.



Note:

- **Fibre or iSCSI:**
 - If you detach all volumes that comprise a specific host group, the host group is also deleted.
 - The command device configuration will be disabled if all the attached LUN paths are removed.
- **FC-NVMe**
 - If you detach all volumes that comprise a specific NVM subsystem, the NVM subsystem is also deleted.
- If you want to attach the volumes when adding servers, check the **Apply changes to attached volumes** option, click **Next**, and then specify the settings to attach the volumes in the following steps.
- If you want to add or move servers without attaching or detaching the volumes, click **Submit** without checking the **Apply changes to attached volumes** option.

4. In the **Select Volumes to Attach** step, you can select one or more existing volumes attached to the servers in the server group. If the protocol is FC-NVMe, proceed to step 8.
5. In the **Path Settings** step, you can select storage port settings for creating paths. The following options are available:
 - **Use Existing Ports:** The software attaches volumes by copying the paths from an existing server. If select this option, select a single server for copying the paths.
 - **Use New Ports:** The software attaches volumes by creating paths between the added server ports and storage ports not used by existing servers in the server group.
6. In the **Path Mappings** step, you can select storage port settings for creating paths. The following options are available:
 - If you select **Use Existing Ports**, select the selected server ports and the added server ports in a one-to-one relationship.
 - If you select **Use New Ports**, you can create paths by selecting server ports to attach to storage ports.



Note: The software attempts to share a host group among multiple servers' ports if at least one shared host group exists in the server group and shared host group configuration is possible in the specified configuration.

7. The **Create Zone Setting** is set to **No** by default. Set it to **Yes** to automatically create zones.
8. When you are satisfied with all the settings, click **Submit**.



Note: You cannot do the following combinations at the same time. You must do them separately.

- Update the name and description and add/remove servers with attaching/detaching volumes.
- Add and remove servers with attaching and detaching volumes (Without attaching and detaching volumes, you can add and remove servers at the same time).

Updating volumes

You can expand and rename a single volume and enable or disable capacity saving (deduplication and compression), command device setting, and ALUA mode.

You can also rename volumes and enable or disable capacity saving (deduplication and compression) and command device at the same time if you select multiple volumes.

Expanding protected volumes is supported for the following storage systems:

- VSP One B20
- VSP E series
- VSP 5000 series
- VSP G/F350, G/F370, G/F700, G/F900



Note: From the data protection block device advanced system settings, you can set the storage system prerequisite advanced system settings.



Note: For VSP One B20, you cannot disable capacity saving.





Tip: You can change the DRS settings type of the existing volume using the Migrate volumes job.

Before you begin

To expand a protected volume, see the relevant hardware manual to confirm that all prerequisite conditions are met.

Procedure

1. To update a volume, navigate to the volume details by using one of the following options:
 - From the dashboard, click the **Storage Systems** () icon, and then click a storage system tile to view the resources. Click **Volumes**, and then click the volume tile for the volume that you want to update.
 - From the dashboard, click the **Servers** () icon, and then click a server tile to view the volumes. Click a volume tile for the volume that you want to expand.
2. In the **Volume Detail** window, click **Edit** to open the **Update Volume** window.



Note: To reset a volume to the default settings, click **Reset**.

3. You can rename the volume and change the size by clicking the up and down arrows next to the volume size.
4. Under **Change Compression Type**, select **Compression** or **Deduplication and Compression** to change the type. To disable compression, select **No**.



Note: You can set capacity saving for volumes based on tiered pools for the following storage systems:

- VSP 5000 series

5. You can update command device settings by selecting **Change Value** under **Change Command Device Settings**. To keep current settings, select **Keep Current Value**.

**Note:**

- You can enable or disable command devices.
- When changing the command device setting, you must specify the command device security, user authentication, and device group setting.
- If selected command devices have different settings or command devices belongs to a storage system without an SVP, then command device security, user authentication, and device group setting are displayed as empty values. When updating at least one of these attributes, set all three attributes.
- If you have protected, T10 PI, or ALUA volumes, then you cannot enable them as command devices. The ALUA setting and command device settings cannot be updated at the same time.

6. Click Submit.**Note:**

- When you expand HA pair volumes, only those registered with data protection can be expanded. When expanding, note the following:
 - The HA pair may be able to be expanded without suspension for specific storage system models. See the storage system documentation to verify the support requirements.
- To use a new data protection version after an upgrade, wait four hour so that the new version information is correctly updated.
- For HA paired volumes, regardless of whether you change the volume size, this operation expands the capacity if the paired volume capacity is smaller than the target volume capacity. The HA paired volumes will have the same capacity.



Result

A job is started to update the volume.

Editing host groups

Edit host groups as follows:

Procedure

1. From the **Dashboard**, click the **Storage Systems**  icon.
2. Select a storage system from the list.
3. Click the **Host Groups/ISCSI Targets** tile.
The **Host Groups** window opens.
4. Select a host group from the list, then click the Edit  icon and select **Edit Host Group** to edit a host group.
The **Edit Host Group** window opens.

From Edit Host Group, you can edit:

- Host Group Name
- Host Mode
- Host Mode Options
- Preferred Path

5. After you make changes, click **Submit**.

Editing NVM subsystems

Edit the NVM subsystems as follows:

Procedure

1. From the Dashboard, click the **Storage Systems** (🗄️) icon.
2. Select a storage system from the list.
3. Click the **NVM Subsystems** tile.
4. Select an NVM subsystem from the list, then click the Edit (✎️) icon.

The **Edit NVM Subsystem** window opens.

From the **Edit NVM Subsystem** window you can edit the NVM subsystem name.

5. After you make changes, click **Submit**.

Chapter 4: Getting started with VSP 360 Data Protection

VSP 360 Data Protection is an enterprise copy data management software platform designed to automate and orchestrate data protection, recovery, and retention processes.

VSP 360 Data Protection overview

VSP 360 Data Protection provides a modern, holistic approach to data protection, recovery and retention. It has a unique workflow-based policy engine, presented in an easy-to-use whiteboard-style user interface that helps map copy-data management processes to business priorities. A wide range of fully integrated hardware storage-based and host-based incremental-forever data capture capabilities are included that can be combined into complex work flows to automate and simplify copy-data management. With these you can:

- Choose the right technology for each workload, based on service level requirements, but manage them from one place.
- Drag-and-drop a range of protection, retention and repurposing capabilities to easily create and manage complex work flows.
- Automate and orchestrate Hitachi storage-assisted snapshots, clones and replications to eliminate backup windows.
- Automate the mounting of Hitachi storage based snapshots, clones and replications for proxy backup and repurposing.

Features and benefits

VSP 360 Data Protection enables you to:

- Meet operational recovery, disaster recovery and long-term recovery challenges in a single, unified platform.
- Drive the backup window, recovery point objective (RPO) and recovery time objective (RTO) to near zero.
- Employ incremental-forever data capture at the block level helping to reduce secondary storage requirements by 90% or more.
- Use intuitive, drag-and-drop workflow creation, node and policy management wizards for administrative agility.
- Use Hitachi Thin Image snapshot orchestration for your critical data and applications.
- Easily create or adopt ShadowImage, TrueCopy[®], Universal Replicator, Global-Active Device and File Replication without scripting, on a scheduled or ad-hoc basis.

- Orchestrate application-consistent snapshot and clone management for Oracle.
- Orchestrate application-consistent snapshots and clones across other applications and file systems.
- Combine automated local snapshot and off-site replication for an end-to-end modern data protection and recovery solution.
- Automatically trigger snapshots and clones of remote replica data for secondary operations, such as test and development.
- Mount and unmount snapshots and clones automatically as part of an orchestrated policy workflow.
- Further reduce network and storage costs through source and target data deduplication.
- Protect VMware hypervisors and virtual machines.
- Support a broad range of storage types, including repositories and block storage.

Understanding data protection

Data protection involves building structured workflows that automate and manage backup, recovery, and retention tasks across complex IT environments.

About nodes

The *Client* software must be installed on each server participating in the data protection environment. The VSP 360 Data Protection application serves as the *Master* and acts as the central controller and the connection point for the user interface. Active data protection policies will continue to function with or without the Master being available because the participating Clients operate autonomously using rules distributed from the Master.

Physical storage devices and hypervisors interface with the software through servers with the *Client* software installed. One *Client* can be used to communicate with more than one storage device, however when doing this, many factors must be considered, including server hardware performance and the impact on system availability should that server go down.

The physical environment is represented as nodes that represent data sources and destinations as follows:

- *OS Host* nodes are automatically added to the inventory. These represent every server that has Master or Client software installed. A basic OS Host node can only be used as a file system data source on a data flow and can only support path and disk type classifications.
- *Block Device* nodes require a Client with block prerequisites installed to act as an ISM. Block Device nodes act as both data sources and destinations on data flows, enabling users to specify block specific policies with snapshot and replication operations to other Block Device nodes. Note that Block Host and Logical Block nodes can only be used as data sources.

About data flows

A *Data Flow* is a diagrammatic representation of the nodes involved in a data protection scenario where each node is represented by an icon. Data flow diagrams identify both physical and logical entities and the connections between them. The data that is to be protected flows from a *Source Node* to a *Destination Node* during the data protection process by way of a *Mover*; the direction of movement being indicated by an arrow on the connector between nodes. Data is transferred in scheduled batches indicated by a solid *Batch* mover. For host based backups, data transmitted across a network can be compressed to reduce bandwidth utilization and bandwidth throttling schedules can be applied to movers, to ensure that data protection activity does not degrade normal network performance.

Each node in a data flow plays a part in implementing the data protection scenario by having a *Policy* assigned to it. After a data flow is constructed, it must be *Activated* before it becomes operational.

The process of compiling a data flow performs validity checks on the data flow and assigned policies, then generates a set of rules for each node in the data flow. The compiled rules are distributed to the affected nodes and activated; the participating nodes use these rules to act autonomously. The operation of a data flow can be monitored in real-time using the same data flow diagram rendered as a mimic display.

About policies

A *Policy* consists of *Classifications* that specify what data to protect and *Operations* that specify how to protect the data.

Physical classifications specify the data by directly naming the path, logical device/volume or disk type to be protected, whereas *Application classifications* specify the data indirectly by naming the application instance such as databases or virtual machines to protect. The software uses this information to discover the volumes on which the application data resides.

The *Operations* in a policy define the methods to use when creating backups of the primary data. Operations can be implemented using software methods (for example, Backup), or by orchestrating the hardware storage devices (such as Hitachi Block) to implement operations in the hardware (for example, Thin Image and Universal Replicator).

The following table shows which operations can be used in conjunction with a particular type of source or destination node.

Operations defined in a *Policy* work in conjunction with *Movers* placed on a *Data Flow*. When a policy is assigned to a source node, all the operations in that policy are assigned to that node. The policy is then routed by a mover and the contained operations assigned to one or more destination nodes.

Installing the client software

You must install the data protection client software on all nodes that participate in a backup data flow.

The instructions to install the client software are as follows:

Procedure

1. Locate and run the required installer for the target OS.

The installer filename has the following format:

Data Protection-*m.n-m.n.n.nnnnn-ostype-proctype*

where:

- *m.n-m.n.n.nnnnn* - is the version and build number
- *ostype* - is the target operating system type:
- *proctype* - is the target processor type:
 - **x64**
- **Windows:** Data Protection-7.x.x.x+20231124-094611-d960e0b3-windows-x64.exe
- **Linux:** Data Protection-7.x.x.x+20231124-094611-d960e0b3-linux-x64.run
- **AIX:** Data Protection-7.x.x.x+20231124-094611-d960e0b3-aix-x64.run

The **Setup** wizard is launched if a GUI shell is available. If no, the same information is presented using the text mode shell.

2. When the **Setup** wizard appears, a welcome message is displayed. Click **Next** to begin the installation.
3. Read the License Agreement, select **I accept the agreement** if you are ready to proceed, and click **Next**.
4. Accept the default location or install in a different location by entering the path or using the folder browser, and then click **Next**.
5. For installation type, select **Client** and click **Next**.

The Client option installs all node types. The specific roles assumed by Client nodes are defined from the Nodes page after completing the installation. These roles include:

- Data Sources (basic hosts, VMs, and application servers)
- ISMs (for controlling Hitachi Block and File storage hardware)
- Repositories (acting as host-based backup storage destinations)

6. Specify a node name and click **Next**.



Note: Node names are limited to a maximum of 64 characters. By default, the name is set to the machine host name. This name is only used internally, and will not change the name set by the operating system.

7. Enter the **Master Hostname or IP** address for the Master node. If the node will be running over a non-secure network, then we recommend enabling the **Internet connected node** option. This will encrypt transmitted data as an extra security precaution.

8. When prompted to begin the installation, click **Next**.
The files are copied to the designated directories and the necessary components are installed.
9. When the installation is complete, you have the option to open the UI in a web browser. Click **Finish**.



Note: You do not need to restart the machine. The installer starts all the necessary components on the system.

If a third party firewall is installed on the network, the software generates firewall warnings when it starts running.

Create and authorize nodes

Before nodes can be used in data protection operations such as backup, restore, or replication, they must first be added to the system and authorized.

Hitachi Block prerequisites

The following prerequisites are for snapshotting and replicating Hitachi Block volumes:

- A machine (known as an ISM) must be assigned that controls the Block storage device. This node is a Windows or Linux machine with the client software installed.
- All primary data (paths or application data) to snapshot or replicate within the same data protection policy must exist on the same storage device.
- The block storage system must:
 - Support the data protection technologies you intend to use.
 - Have the correct firmware version installed.
 - Have the correct SVOS version installed.
- For all replication types, the P-VOLs must be set up in the host group.
- To resize logical devices represented by the Block Host node that are part of a replication or snapshot pair, the array account must have the Support Personnel permission.
- For GAD, the quorum disks or quorum-less disks must be provided. In most cases, one quorum device between participating storage systems is satisfactory. For best practices see the *Global-Active Device User Guide*.
- For GAD, configure the storage system to allow virtualized LDEVs if they are required (where supported by the storage system).
- Port security must be enabled.
- Primary volumes must be set up using other Hitachi management tools.
- For application consistent snapshots, the application must be installed and configured to use P-VOLs on a storage system. For details on the application configuration, see the associated application guide.

- The password for authorizing a Block Device node must contain only useable CCI command characters: A-Za-z0-9'-./: @\ _
- The device must have adequate shared memory (see Provisioning and Technical Guides).
- Pools must be created in another tool before selecting a data protection target storage system:
 - For standard mode (non-cascading) TI, the TI Pools must be set up.
 - For cascade mode TI, the Dynamic Provisioning Pools must also be set up as a hybrid pools, otherwise a TI pool is also required.
 - For SI, TC, UR and GAD, the Dynamic Provisioning Pools must be set up.
- The following licensed features may be required depending on the features being used:
 - Dynamic Provisioning.
 - Storage Navigator.
 - Thin Image (for TI snapshot and RTI replication scenarios).
 - ShadowImage (for SI replication scenarios).
 - TrueCopy (for TC replication scenarios).
 - Universal Replicator (for UR replication scenarios).
 - Global-Active Device (for GAD replication scenarios).
 - Remote Replication Extended (for 3DC scenarios).
- The ISM node controlling the block storage device must have:
 - The correct version of Hitachi CCI installed.
- A dedicated user for use with the data protection software (specified when creating the Hitachi Block Device node) must be created on the storage device with a minimum of the following roles:
 - Storage Administrator (Provisioning)
 - Storage Administrator (Local Copy)
 - Storage Administrator (Remote Copy)
 - Security Administrator (View and Modify)

The user must also have access to Resource Group 0 on the storage device.

- Fibre connectivity (including zoning) or iSCSI connectivity and pre-configured RCU paths between storage systems for remote replication technologies is required.
- If physical and software block devices are being configured in a single environment, it is essential that they do not share an ISM node.

Add a Hitachi Block Device Node

Before you begin

Verify the prerequisites before adding the node. For more details, see [Hitachi Block prerequisites \(on page 74\)](#).

You can add a Hitachi block storage device as a node as follows:

Procedure

1. From the navigation pane, select **Nodes**.
2. In the Nodes page, click the **Create a new item** tile.
3. From the **Storage** node type, select **Hitachi Block Device**, and then click **Next**.
4. Enter the **Node Name** and add **Tags** to associate relevant metadata with the node.
5. Select the confirmation checkbox and click **Next**.
6. By default, nodes are automatically allocated to the default resource group. Select additional resource groups if required, and click **Next**.
7. Select a proxy node and click **Next**.
8. Browse and select the metadata directory for placing the metadata files related to block snapshots and replications and click **Next**.



Note: The proxy and all storage nodes on this proxy will use this directory path. You can change the directory path after initial configuration.

9. Specify the storage device using one of the following options and click **Next**:
 - Specify the storage device by serial number. Storage device serial numbers available to the proxy node selected in the previous step for your storage device are displayed in the dropdown list.

If there are no serial numbers of your choice, it implies that the proxy node might not have an in-band command device. In this case, you can specify the storage device by IP address or hostname with a port.

- Specify the storage device using the IP address or hostname and port number of an IP command device on the storage device. Additional in-band and out-of-band command devices can be added in a later step.



Note: For VSP One B20 storage devices, use the IP address of CTL01 or CTL02. Do not use the ESM or Service IP address.

As you continue through the steps, you can add the second controller as an alternative address for failover purposes.

When performance is important or where high workloads are expected, the use of in-band channel command devices is highly recommended. Using out-of-band command devices will result in slower performance.

10. Enter the **Username** and **Password** for the selected storage device and click **Next**.
The username must belong to the Storage Administrator roles (Provisioning, Local Copy, and Remote Copy) and the Security Administrator roles (View Only, View, and Modify) on the block device. Additionally, the Support Personnel role is required for changing the storage system SOM settings that allow LDEV resizing for replications. If the block device cannot be accessed or the credentials are invalid, the node authorization will fail.



Note: The password for authorizing a block device must contain only usable CCI command characters. For example: A-Za-z0-9'-./: @\ _

11. Specify the **LDEV Range** by choosing one of the following options and clicking **Next**:

- If you want the software to automatically detect the LDEV range from which snapshots and replications must be allocated, select **All**.
- If you want to manually specify the LDEV range from which snapshots and replications must be allocated, select **User defined**.

Enter the **Start** and **End** LDEV range to use for allocation.



Note:

All replication and snapshot S-VOLs must be created using free LDEV IDs that are mapped to the *meta_resource* group, and have virtual LDEV IDs matching the corresponding physical LDEV IDs.

For fully provisioned snapshots and all replications, this applies to the operation that creates that snapshot or replication.

For floating device snapshots and snapshots mounted using cascade mode, this applies to the mount or restore operation.

For fully provisioned snapshots mounted using cascade mode, this applies both to the operation that creates that snapshot and to the mount or restore operation.

If an operation tries to create one or more LDEVs, that operation will fail if there are not enough free LDEV IDs that meet the above conditions.

12. Create and configure in-band or out-of-band command devices.

If one or more command devices are specified, the software will attempt to control the hardware storage device through a command device in the order specified by the user. If the first command device fails, the software will progress to the next. If all specified command devices fail, the operation fails. No attempt is made to use any command devices that are not specified, even if they are available.

If no command devices are specified, the software will attempt to control the hardware storage device through any connected command device, available to the **Proxy Node** specified in an order specified by HORCM.

For example, it is possible to specify a specific In-band command device, followed by any In-band command device, followed by a specific out-of-band command device.

To add a command device, complete the following details:

- a. Click the **Create a new item** icon.

- b. Depending on the command device type, choose from the following options:
 - For an **In-band** command device, choose from the following options:
 - To insert an entry in the command device list that allows the software to use any available In-band command device such as fibre or iSCSi, select the **Use any available in-band command device** option.
 - To insert a specific In-band command device in the list. The decimal LDEV IDs of the detected In-band command devices are displayed in the list, select the **Select from detected in-band command devices** option
 - For an **Out-of-band** command device, enter the **IP address or Hostname** and **Port Number** of the command device.
 - c. Click **Apply**.
 13. Click **Next**.
 14. Configure LDEV ranges for each virtual storage machine (VSM) as follows:
 - a. Click the **Create a new item** icon.
 - b. Enter the **VSM Serial Number** to use within the software.
 - c. Enter the start and end of virtual LDEV range to use for allocation and click **Apply**.



Note: GAD replications require P-VOLs and S-VOLs to have matching virtual serial numbers and virtual LDEV IDs. To avoid virtual LDEV ID collisions between GAD volumes and non-GAD S-VOLs (created by the data protection software for other types of replications and snapshots), it is possible to define virtual LDEV ID ranges for use by those non-GAD operations. Virtual LDEV ranges can be specified for each VSM (Virtual Storage Machine).



Caution: These ranges control the virtual LDEV IDs used for non-GAD replications and snapshots. They must be defined to exclude the IDs of any GAD volumes. Failure to provide such a range (or providing an incorrect range) may result in ID clashes when attempting to set up GAD replications.

15. Click **Next**.
16. Configure the ports for provisioning as follows:
 - a. Click the **Create a new item** icon.
 - b. Enter the **Port** identifier in the following format and click **Apply**:
CL_{C-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 is used.

17. Click **Next**.

18. Review the node configuration summary and click **Finish** to create the node.
The node details are displayed in the Nodes page.

Add a Hitachi Block Host Node

Before you begin

Verify the following prerequisites before adding the node:

- [Hitachi Block prerequisites \(on page 74\)](#)
- A physical block device node must be created before creating block host nodes. For more details, see [Add a Hitachi Block Device Node \(on page 75\)](#).

The Hitachi block host represents a collection of Hitachi storage volumes. You can add a Hitachi block host node as follows:

Procedure

1. From the navigation pane, select **Nodes**.
2. In the Nodes page, click the **Create a new item** tile.
3. From the **Host** node type, select **Hitachi Block Host**, and then click **Next**.
4. Enter the **Node Name**, add **Tags** to associate relevant metadata with the node, and then click **Next**.
5. By default, nodes are automatically allocated to the default resource group. Select additional resource groups if required, and click **Next**.
6. Select a **Hitachi Block Device** node and click **Next**.
7. Enter LDEVs or host groups that you want to include or exclude from the block host in any of the following format:
 - LDEV_ID: A single logical device. For example, 100, 0x10.
 - LDEV_ID-LDEV_ID: A logical device range. For example, 200-299, 0x01-0x0F.
 - Host Group ID: All logical devices within the host group. For example, CL1-A-0, CL10-A-0, CL10-A-0xA.
 - nvme: All logical devices within the NVMe subsystem ID. For example, nvme:1





Note: Spaces and colons must not be present in the entries. If a space or colon is encountered on a line, the remaining text on that line from the space or colon is disregarded. This allows entries that contain the LDEV name after a space or colon to be present in the list.

8. Click **Next**.
9. Review the node configuration summary and click **Finish** to create the node.
The node details are displayed in the Nodes page.

Authorize a node

The node must appear in the Nodes page and must be authorized before they can participate in a data flow.

Procedure

1. From the navigation pane, select **Nodes**.
2. In the Nodes page, select the node you want to authorize.
Unauthorized nodes display a  icon in the top right corner
3. Click the **Authorize** icon.
4. Wait a few moments for the authorization process to finish.
Authorized nodes display a  icon in the top right corner.



Note: For extra security, you can verify the SSL/TLS fingerprint of the client node prior to authorization.

Create policies

Policies define how and what data is protected across the environment. A policy consists of classifications, which specify the data to be protected, and operations, which define how that protection is carried out. These operations can include backups, snapshots, replication, and more.

Create a policy

Before you begin

Ensure that the nodes acting as sources and destinations for your backup data are added to the software.

Create a policy as follows:

Procedure

1. From the navigation pane, select **Policies**.
2. In the Policies page, click the **Create a new item** tile.
3. Enter the **Name**, **Description**, **Tags**, and then click **Next**
4. By default, the policy is added to the default resource group. Select additional resource groups if required, and click **Next**.
5. Click the **Create a new item** icon to add a classification to the policy, and click **Next**.
6. Select a classification category and click **Next**.
7. Specify the classification attributes and click **Apply**.
The configured classification is listed in the Add one or more Classifications page.
8. Click **Next**.
9. Click the **Create a new item** icon to add an operation to a policy, and click **Next**.
10. Specify the operation attributes and click **Apply**.
The configured operation is listed in the Add one or more Operations page.
11. Click **Finish** to create the policy.
The policy details are displayed in the Policies page.

Add a filter to a classification

Before you begin

It is recommended to review data flows with policies to understand the effect of filters.

Add a filter to a classification as follows:

Procedure

1. In the Policies page, select the required policy.
2. Click the **Edit** icon.
3. In the Policy page, go to **Add one or more Classifications**.
4. Click the **Edit Filters** link on the required classification. For example, Path classification.
5. In Add one or more Classification Filters page, click the **Create a new item** icon.
6. Select the required filter from the list, and then click **Next**.
7. Specify the filter attributes, and then click **Apply**.
The configured filter is listed in the Add one or more Classification Filters page.

Create and activate data flows

Data flows define how data is transferred and protected between nodes. After creating a data flow, you must activate it to ensure it is valid and ready for use in data protection operations such as backup, replication, or snapshot.

Create a data flow


Before you begin

Ensure that the policies that you want to assign are defined. For more details, see [Create a policy \(on page 80\)](#).


The following procedure describes how to create a simple one-to-one data flow. You can create complex data flows involving one-to-many and cascaded topologies by following the same approach:

Procedure

1. From the navigation pane, select **Data Flows**.
2. In the Data Flows page, click the **Create a new item** tile.
3. Enter the **Name**, **Description**, and **Tags**, and then click **Next**.
4. By default, the data flow is added to the default resource group. Select additional resource groups if required, and click **Next**.
5. Drag a source node from the **Nodes** or **Node Groups** list to the data flow canvas. The node is displayed on the canvas with a gray box around showing that it is selected. The available policies appear next to the canvas. If a policy contains operations that can be performed locally to the node, without requiring a separate destination node (for example, local snapshots), it is shown directly below the policy.

6. Select the policies and local operations that you want to assign to the source node by selecting those that apply from the **Policies** section:
 - If you select a policy that requires a destination node and corresponding operation assignment to complete it, a warning triangle icon  appears next to the source node, indicating that the node has an incomplete policy assigned to it. Completing the policy assignment is described in the steps that follow.
 - If you select an operation, the operation properties dialog opens. Enter the required operation properties in the dialog and click **OK**.

After the operation properties are applied, you can edit them by clicking the **Edit** icon.

If a node has a snapshot operation assigned, a snapshot icon  appears in the bottom right corner of the node.

7. Place and connect the destination node by using one of the following methods:
 - Drag the destination node from the **Nodes** list, passing over the source node to which you want to connect, then drop the destination node where you want to place it. A connection is created between the destination and source node. Now, select the destination node.
 - Place the destination node on the canvas.

The destination node is displayed on the canvas with a gray box around showing it is selected. The available policies appear to the right of the canvas. If a policy contains operations that can be performed by the destination node (for example, remote replication operations), then these are displayed below the policy.

8. With the selected destination node, choose the operations that you want to assign by selecting those that apply from **Policies**. Note that you cannot select the policy checkbox. When you select an operation, an operation properties dialog opens. Enter the required properties and click **OK**.
 If an operation is selected that completes a policy previously selected on the source node, then the warning triangle icon is removed from the source node, indicating that the node has a completed policy assigned to it. The following image shows a source node with a remote policy assigned (*myReplication*) that is completely specified (the operation *Mirror (Replicate)* is assigned to the destination node). A local operation (*mySnapshot*) is also assigned to the source node.

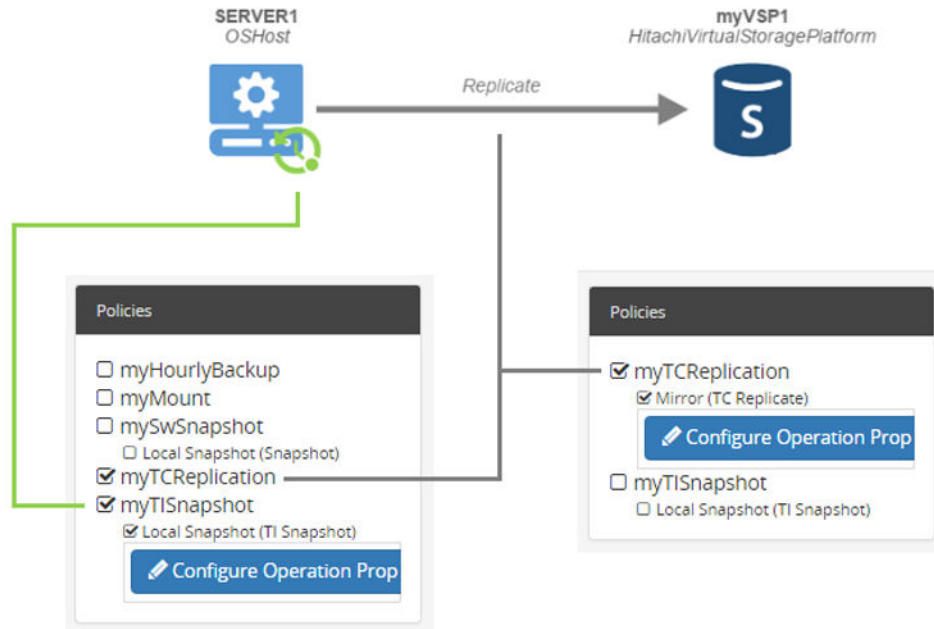


Figure 1 Source node with a remote policy assigned (completed assignment)

9. Select the connection between the source and destination nodes to display **Routed Policies** and **Mover Settings**.

The **Routed Policies** section lists policies being routed along the selected connector.

- a. In **Mover Settings**, select the mover **Transfer Type**.



Note: The Data Flow Wizard only prevents some incorrect mover and operation combinations from being constructed. However, the *Rules Compiler* will generate warnings or errors for incorrect combinations. Ensure to use correct mover type for the specific operation when creating data flows.

- b. (Optional) Enter a **Label** for the connection.
 - c. Turn network compression on or off with **Enable network data compression**.
 - d. For *Host Based* policies only, click **Bandwidth Settings** to open the Mover Bandwidth Settings dialog, then set the times and days for **Default Speed**, **High Speed** and **Low Speed** network utilization by clicking the required options.
10. When drawing the data flow and assigning policies, click **Finish**.

Connect nodes on a data flow

Before you begin

Create a data flow as described in [Create a data flow \(on page 81\)](#).

Nodes can be connected on a data flow as follows:

Procedure

1. Drop the two nodes that you want to connect on the data flow canvas.
2. Select the node from which the data will flow.
3. Click the **Connect To** icon.
A dashed line appears connected to the selected node at one end and the mouse cursor at the other.
4. Move the mouse cursor to the node to which data must flow and click to connect the two nodes.
A line is drawn from the first node to the second node with an arrowhead indicating the data flow direction.
5. Click the connection between the first and second node to view and set **Routed Policies** and **Mover Settings**.

Apply a policy to nodes on a data flow

Before you begin

Create a data flow as described in [Create a data flow \(on page 81\)](#).

Policies are applied to nodes on a data flow as follows:

Procedure

1. Select the source node on the data flow canvas.
2. In the **Policies** section, select the policy you want to apply to the source node.
3. Click the mover that routes the policy to the destination node to view **Routed Policies**.
4. Select the destination node on the data flow canvas.
5. In **Policies** section, select the operation you want to apply to the destination node.
Only individual operations can be applied; not the policy.
An **Operation Properties** dialog based on the destination node and operation type opens. For example, when applying a *Replication* operation to a Hitachi *Block* node, the Hitachi Block Replication Configuration Wizard opens.
6. Configure the operation properties as required, and then click **OK**.
7. Click **Finish** to progress to the next page of the Data Flow wizard.

Activate a data flow


Before you begin

Ensure the data flows that you want to compile are correctly defined, the required policies are assigned, and no significant warning icons¹ are displayed on nodes in the data flow diagrams.

1. There is no reason why all policy operations must be applied in all cases. Warning icons may therefore be present, but they may indicate a warning, not an error.

To compile a data flow and activate the resulting rules:

Procedure

1. From the navigation pane, select **Data Flows**.
 2. In the Data Flows page, select the data flows that you want to compile.
Although it is possible to compile multiple data flows same time, it may be easier to initially compile one at a time and fix any compilation errors, before compiling all data flows and distributing rules in one operation.
-  **Note:** Activate data flows in batches not exceeding 20 data flows at a time. Activating more than this simultaneously can result in longer activation times.
3. Click the **Activate** icon.
The Activate Data Flow dialog is displayed and the selected data flows start compiling. After a short time the results of the compilation process are displayed with a message indicating whether the compilation process succeeded or failed.
 4. Complete the following compilation process:
 - If the compilation succeeds, click **Activate** to update the rules on the affected nodes.
 - If the compilation fails, **Activate** is disabled. Examine the compiler output to locate the cause of the failure, fix the data flow and policy, and recompile.

Create Hitachi block workflows

Hitachi block workflows are a series of tasks and subtasks that are created for snapshotting and replicating Hitachi Block volumes.

Data protection workflow prerequisites

Before you begin

The following prerequisites are for creating data protection workflows:

- The Client software is installed on the source nodes and proxy nodes.
- The Client software and prerequisites are installed on the destination nodes and proxy nodes.
- Destination storage devices are set up based on the requirements and prerequisites described in the [Hitachi Block prerequisites \(on page 74\)](#) section.
- Role-based access permissions are granted at the platform level.
- Any applications being backed up have been installed based on the requirements and prerequisites.

Protect your data

Before you begin


This generic workflow describes the steps for protecting your data.

Ensure you have completed the prerequisites listed in [Data protection workflow prerequisites \(on page 85\)](#).

This task describes the general steps to follow when protecting your data:

Procedure

1. Create the required source nodes and then check that they are authorized and online.
Source nodes represent the places where the data you are protecting resides in your system.

 **Note:** Source Hardware Storage Device nodes must be created even if they do not appear on the data flows for snapshot and replication operations.
2. Create the required destination nodes and then check that they are authorized and online.
Destination nodes represent the places where the data will be backed up.
3. Define the data protection policies.
Policies define the data sets you want to protect and the methods to use. See [Create a policy \(on page 80\)](#).
4. Draw the backup data flows.
Data flow diagrams show the participating source and destination nodes and the data paths interconnecting them. See [Create a data flow \(on page 81\)](#).
5. Assign the policies to the participating nodes on the data flows.
Policy assignments define precisely how the data flows from each source node to the respective destination nodes. See [Apply a policy to nodes on a data flow \(on page 84\)](#).
6. Compile and activate the data flows.
The source and destination nodes work autonomously by implementing rules locally. These rules are generated by the master node and disseminated to the participating nodes. See [Activate a data flow \(on page 84\)](#).
7. Trigger the policies if required.
Policies are invoked according to a user-defined schedule or RPO. In some cases, you might want or need to trigger policies manually.
8. Monitor the data flows, logs, and so on to ensure policies are running as expected.
9. Review the storage nodes to ensure backups are being created.
You must continue to monitor the storage devices to ensure that they are running correctly and sufficient resources are available to store your data securely.

Snapshot a Hitachi Block LDEV with Thin Image

Before you begin

Verify the following prerequisites before creating the workflow:

- [Data protection workflow prerequisites \(on page 85\)](#).
- The Client software is installed on the source node that will act as a proxy for the Hitachi Block storage device.



Note: For a Thin Image snapshot, the source and destination LDEVs are located on the same device.

This task describes the steps to follow when protecting an LDEV allocated from a Hitachi Block storage device. This is useful when the software has no way of interacting with the application or OS that is using the LDEV. The snapshot will be crash consistent because the software is not able to orchestrate the snapshot operation in conjunction with applications using the LDEV. Thin Image hardware snapshots of the P-VOL are created as S-VOLs residing within the same storage device. For more information, see [About Thin Image and Thin Image Advanced differential and refreshed snapshots \(on page 89\)](#).

The data flow and policy are as follows:



Figure 2 Hitachi Block Snapshot Data Flow

Procedure


1. In the Nodes page, locate the node that controls the Hitachi Block Device through a command device interface and verify that it is authorized and online.
This node is used to orchestrate snapshot creation and is identified as the **Proxy Node** when creating the Hitachi Block Device node. This node is known as an ISM node. The ISM node does not appear in the data flow.
2. Create a new Hitachi Block Device node (unless one already exists) and check that it is authorized and online. This node is where the production LDEV to be snapshotted is located.
For a snapshot using a Hitachi *Block* classification, a Hitachi *Block Device* node is required.
3. Define a policy as shown in the following table using the **Hitachi Block** classification and **Snapshot** operation:


Table 3 Hitachi Block Snapshot Policy

Classification Type	Parameters	Value
Hitachi Block	Specify additional selections	Selected
	Logical Devices	10323/10

Operation Type	Parameters	Value	Assigned Nodes
Snapshot	Mode	Hardware	Hitachi Block Device
	Hardware Type	Hitachi Block	
	RPO	10 mins	
	Retention	1 hour	
	Run Options	Run on RPO	
	Quiesce...	Not selected	

4. Draw a data flow that shows only the Hitachi *Block Device* source node using data flows. For more details, see the Data Protection User Guide.

At this stage the snapshot icon  is not shown. See [Create a data flow \(on page 81\)](#).

5. Assign the *Snapshot* operation to the Hitachi *Block Device* source node. The *Block-Snapshot* policy will then be assigned automatically.
The Snapshot Configuration page is displayed.
6. Select the **Snapshot Pool** by selecting one of the available Thin Image or hybrid pools.
7. Leave the remaining **Advanced Options** at their default settings, then click **OK**.
The snapshot icon  is now shown superimposed over the source node.
8. Compile and activate the data flow. Make sure there are no errors or warnings.



Note: If the **Quiesce configured applications before backup** option is not deselected during the snapshot operation configuration, then a compiler warning message is generated because the data protection software is not be able to quiesce applications using the LDEV.

9. In the Monitor page, locate and open the active data flow.
The policy is invoked repeatedly according to the specified RPO. The policy can also be manually triggered from the source node in the monitor data flow. You might want to manually trigger to create an initial snapshot.
10. In the Monitor detail page, watch the active data flow to ensure the policy is operating as expected.

For a healthy data flow you will periodically see:

- Snapshot jobs appearing in the **Jobs** area below the data flow that cycle through stages and ending in *Progress - Completed*.
- Information messages appearing in the **Logs** area below the data flow indicating rules activation, storage handler and sequencer events.
- Attachments to storage handler log events confirming which volumes are being snapshotted.

For a problematic data flow you may see:

- Permanent **Node Status** icons appear over nodes and associated warning messages displayed to the right of the data flow area.
- Backup jobs appearing in the **Jobs** area below the data flow that cycle through stages and terminating in *Progress - Failed*.
- Warning and error messages appearing in the **Logs** area below the data flow indicating failed events.

11. Review the status of the Hitachi *Block Device* and snapshots to ensure snapshots are being created.

Hitachi Block Devices require ongoing surveillance to ensure that they are operating correctly and sufficient resources are available to store your data securely. If required, you can modify the retention period of individual snapshots.

New snapshots will appear in the Snapshot page periodically as dictated by the *RPO* of the policy. Old snapshots will be removed periodically as dictated by the *Retention Period* of the policy.

About Thin Image and Thin Image Advanced differential and refreshed snapshots

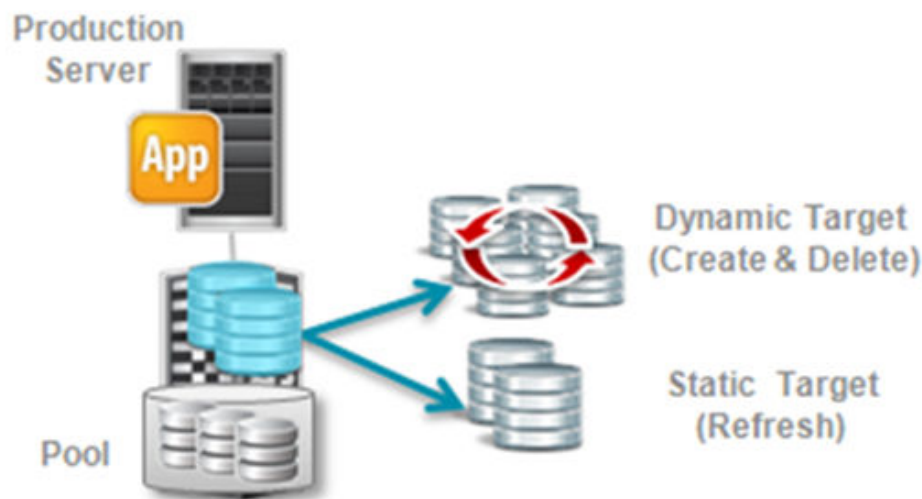


Figure 3 Differential and Refreshed Thin Image Snapshot

Thin Image and Thin Image Advanced enables rapid creation of in-system, space efficient, read/write, volume-consistent snapshots and subsequent rollback of entire volumes.

When handling multiple primary volumes, the storage system takes a snapshot of each volume sequentially. This means that a slight difference can be seen across the snapshot timestamps. If exactly the same timestamp is required among the snapshot set (for crash-consistent backup), the snapshot set should be created using Consistency Groups (CTGs).

When taking a snapshot, there are two options for the target volumes:

- **Differential Snapshot:** Creates a new snapshot for each backup and deletes it when the retention time expires. This simplifies the management of numerous snapshots and is suitable for backup operations. Data Retention Utility (DRU) protection can be applied to the snapshot's LDEV so that it can be used as a read-only volume or to protect it against both read and write operations.
- **Refreshed Snapshot:** Creates a new snapshot for the first backup, and then resynchronizes it on the following backups. This enables static target volumes (Port, Host Group and LUN, although the LUN may not remain constant depending on the mount host OS) and is suitable for repurpose operations.

Floating Device is an improved snapshot capability, used in conjunction with Thin Image and Thin Image Advanced, that simplifies snapshot management. With this capability snapshots can be created without creating target volumes upfront. This means that the limit on the number of snapshots in the entire storage system is increased (the number of snapshots of a specific primary volume is 1024). To revert the snapshot it is only necessary to select the required timestamp. To mount the snapshot for re-purposing, it must be mapped to a specific LDEV/LUN. After the snapshot is un-mounted, the volumes will be deleted as part of the unmount process.

The storage system supports two types of snapshots. Thin Image and Thin Image Advanced, the storage system will automatically decide the type of snapshot used. For Data Reduction Shared (DRS) volumes Thin Image Advanced snapshots will always be used and for all other types of volumes Thin Image snapshots will be used.

About Thin Image Snapshots:

Snapshots of a volume in the storage system are stored in a dedicated area called the Thin Image pool. For floating snapshots, where no LDEV is assigned until it is mounted, no data movement occurs and thus creation of a snapshot is near instantaneous. For non-floating snapshots, the auxiliary tasks of creating an LDEV and a LUN will take some time.

Once a snapshot is created, subsequent updates to the primary data causes the storage system to move the data blocks being updated to the TI pool. TI pool usage thus increases as the primary data changes and snapshots are retained.



Caution:

Filling a Thin Image pool to capacity will invalidate all snapshot data contained within that pool. All snapshots in the pool will have to be deleted before snapshotting can be resumed.

When accessing a snapshot, the storage system presents the virtualized contents by merging the primary volume with its differentials held in the TI pool.

When deleting a snapshot, the storage system releases the differentials held in the TI pool. When multiple snapshots are involved, the delete operation may take some time. The differentials are reference counted and will only be deleted when no remaining snapshot requires them.



Note: Once snapshots have been released back into the pool, that space can only be reused by the same primary volume. This hardware limitation means that this space cannot be used by a different volume. The only way to completely free the space to the pool for any volume is to delete all the snapshots on that primary volume.

When handling multiple primary volumes, the storage system takes a snapshot of each volume sequentially. This means that a slight difference can be seen across the snapshot timestamps. If exactly the same timestamp is required among the snapshot set (for crash-consistent backup), the snapshot set should be created using Consistency Groups (CTGs).

When taking a snapshot, there are two options for the target volumes:

- **Differential Snapshot:** Creates a new snapshot for each backup and deletes it when the retention time expires. This simplifies the management of numerous snapshots and is suitable for backup operations. Data Retention Utility (DRU) protection can be applied to the snapshot's LDEV so that it can be used as a read-only volume or to protect it against both read and write operations.
- **Refreshed Snapshot:** Creates a new snapshot for the first backup, and then resynchronizes it on the following backups. This enables static target volumes (Port, Host Group and LUN, although the LUN may not remain constant depending on the mount host OS) and is suitable for repurpose operations.

Floating Device is an improved snapshot capability, used in conjunction with Thin Image, that simplifies snapshot management. With this capability snapshots can be created without creating target volumes upfront. This means that the limit on the number of snapshots in the entire storage system is increased (the number of snapshots of a specific primary volume is 1024). To revert the snapshot it is only necessary to select the required timestamp. To mount the snapshot for re-purposing, it must be mapped to a specific LDEV/LUN. After the snapshot is un-mounted, the volumes will be deleted as part of the unmount process.

About Thin Image Advanced Snapshots:

Snapshots of a volume in the storage system are stored in the same pool as the primary. When a snapshot is taken the data mapping of the primary volume is copied. Once a snapshot is created, subsequent updates to the primary data cause the storage system to redirect the new data blocks to new storage in the primary pool. Primary pool usage will increase as the primary data changes and snapshots retain the old data blocks.

**Note:**

- When using a snapshot, intensive read/write access to the snapshot may impact the performance of the primary volume, due to the way the snapshot volume is virtualised. If this is of concern then consider using ShadowImage or ShadowImage-Thin Image in cascade, where the Thin Image primary volume becomes the ShadowImage secondary volume instead of the original source.
- Long-term retention increases the number of differentials held in the TI pool once writes are distributed across all data blocks. Thus, for long-term backups, it is recommended to use ShadowImage.
- Thin Image requires the primary data in order to present a virtualised snapshot volume. This means that snapshots will be lost if a disk failure occurs on the primary volumes. To protect the data from such hardware failure use ShadowImage to create a clone and take snapshots of the clone instead.

About cascaded Thin Image and Thin Image Advanced snapshots

Thin Image and Thin Image Advanced snapshots of a P-VOL can be cascaded, the first layer being referred to as L1 S-VOLs. Cascading can be recursive so as to form a snapshot tree to a depth of up to 64 layers (L64 S-VOLs), consisting of the *root* P-VOL, intermediate *node* S-VOLs and terminal *leaf* S-VOLs. The total number of S-VOLs in a tree is limited to 1024.

To create cascadable snapshots, the L1 snapshot volumes must be created in cascade mode as a floating device or fully provisioned. Cascade mode snapshots must be provisioned, either at creation or mount time from a dynamic pool. From v 6.5 onwards, L1 snapshots are created in cascade mode by default, and are dynamically provisioned, although standard mode can still be specified if the storage device does not support cascading.

For Thin Image Advanced snapshots, the pool of the source P-VOL is always used for the cascade mode snapshot. However, for Thin Image snapshots, it uses a number different of pools for cascade mode snapshots as follows:

- **Snapshot Pool** - a Thin Image or hybrid pool where the P-VOL/L1 and L1/L2 snapshot pair data is held. If a hybrid pool is specified then the snapshot S-VOLs may also be created here.
- **Cascade Pool** - a dynamic or hybrid pool where snapshot S-VOLs are created if they are fully provisioned.
- **Mount Pool** - a dynamic pool where snapshot S-VOLs are created if the **Snapshot Pool** is a Thin Image pool or if a floating device was specified for the snapshot operation. If a **Mount Pool** is specified as an option then it will be used in preference.

For Thin Image both standard and cascade mode snapshots require a **Snapshot Pool** to be specified regardless of the mode. If fully provisioned cascade mode is selected then a **Cascade Pool** must be specified when configuring the operation.

When mounting a cascade mode snapshot, you have the option to mount the original (L1) or a duplicate (L2) snapshot. The duplicate (L2) snapshot can be modified without changing the original (L1) snapshot data. When the duplicate (L2) snapshot is unmounted, it is deleted and any changes made to it are lost. For Thin Image snapshots original and duplicate mount modes for cascade mode snapshots may or may not require a **Mount Pool** to be specified, as per the following table:

Snapshot Pool Type	Provisioning Type	Mount Mode	Specify Mount Pool?
Thin Image	Floating Device	Original (L1)	Required
Thin Image	Floating Device	Duplicate (L2)	Required
Thin Image	Fully Provisioned	Original (L1)	N/A
Thin Image	Fully Provisioned	Duplicate (L2)	Optional
Hybrid	Floating Device	Original (L1)	Optional
Hybrid	Floating Device	Duplicate (L2)	Optional
Hybrid	Fully Provisioned	Original (L1)	N/A
Hybrid	Fully Provisioned	Duplicate (L2)	Optional

Replicate a Hitachi Block LDEV with ShadowImage

Before you begin

Make sure to complete the following tasks:

- Verify the prerequisites listed in the [Data protection workflow prerequisites \(on page 85\)](#) section.
- The Client software is installed on the destination node that will act as a proxy for the Hitachi Block storage device. Note that for a ShadowImage replication, the source and destination LDEVs are located on the same device.
- In this example, all nodes are in the default resource group, so there is no need to allocate nodes to user defined resource groups.

This task describes the steps to follow when protecting an LDEV allocated from a Hitachi Block storage device. This is useful when the software has no way of interacting with the application or OS that is using the LDEV. The replication will be crash consistent, because it is not able to orchestrate the replication operation in conjunction with applications using the LDEV. A ShadowImage hardware replication of the P-VOL is created as an S-VOL residing within the same storage device. For more information, see [About ShadowImage replication \(on page 96\)](#).

The data flow and policy are as follows:



Figure 4 ShadowImage Replication Data Flow

Procedure

1. In the Nodes page, locate the node that controls the Hitachi Block Device through a command device interface and verify that it is authorized and online.
This node is used to orchestrate replication and is identified as the **Proxy Node** when creating the Hitachi Block Device node in the next step. This node is known as an ISM node. The ISM node does not appear in the data flow.
2. Create a new Hitachi Block Device node (unless one already exists) and verify that it is authorized and online. This node is where the production LDEV to be replicated is located.
For a replication using a Hitachi *Block* classification, a Hitachi *Block Device* node is required.
3. Define a policy as shown in the following table using the **Hitachi Block** classification, **Replication** operation, and trigger schedule:

Table 4 Hitachi Block Replication Policy

Classification Type	Parameters	Value
Hitachi Block	Specify additional selections	Selected
	Logical Devices	10323/10

Operation Type	Parameter	Value	Assigned Nodes
Replicate	Run Options	Run on Schedule (See below)	Hitachi Block Device (source),
	Quiesce...	Not selected	Hitachi Block Device (destination)

Schedule Item Type	Parameter	Value	Policy Operations
Trigger	Days	Select All	Replicate (See above)
	Weeks	Select All	
	Time	Scheduled Time	
	Start Time	15:00	
	Duration	00:00	

4. Draw a data flow that shows the Hitachi *Block Device* source node connected to the same Hitachi *Block Device* through a *Batch* mover.
ShadowImage is an in-system replication technology, so the Hitachi *Block Device* node is where both the source (P)VOL) and destination (S)VOL) volumes are located.
5. Assign the *Block-Replicate* policy to the Hitachi *Block Device* source node.
6. Assign the *Replicate* operation to the Hitachi *Block Device* destination node.
The Hitachi Block Replication Configuration page is displayed.
7. Set the replication type to **In System Clone**, and choose a **Pool** from one of the available *Dynamic Pools*. Leave the remaining parameters at their default settings and click **OK**.
8. Compile and activate the data flow, checking carefully that there are no errors or warnings.
If the **Quiesce configured applications before backup** option was not deselected in the Replicate Operation wizard, then a compiler warning message will be generated because the software will not be able to quiesce applications using the LDEV.
9. In the Monitor page, locate and open the active data flow.
The policy is invoked automatically to create a replication according to the schedule specified in the policy. The policy can also be manually triggered from the source node in the monitor data flow.



Note: No replication will be created until it is first triggered manually or by the schedule.

10. In the Monitor detail page, watch the active data flow to ensure the policy is operating as expected.
For a healthy data flow you will periodically see:
 - Replication jobs appearing in the **Jobs** area below the data flow that cycle through stages and ending in *Progress - Completed*.
 - Information messages appearing in the **Logs** area below the data flow indicating rules activation, storage handler and sequencer events.
 - Attachments to storage handler log events confirming which volumes are being replicated.

For a problematic data flow you may see:

- Permanent **Node Status** icons appear over nodes and associated warning messages displayed to the right of the data flow area.
 - Backup jobs appearing in the **Jobs** area below the data flow that cycle through stages and terminating in *Progress - Failed*.
 - Warning and error messages appearing in the **Logs** area below the data flow indicating failed events.
11. Review the status of the Hitachi *Block Device* and replications to ensure the replication is being created and refreshed.
- Hitachi Block Devices require ongoing surveillance to ensure that they are operating correctly and sufficient resources are available to store your data securely.
- The replication process can be paused and resumed from here if required.
- A new ShadowImage replication is displayed in the Hitachi block replications page and is updated periodically as dictated by the schedule for the policy operation. The previous replication will be overwritten upon each refresh.

About ShadowImage replication

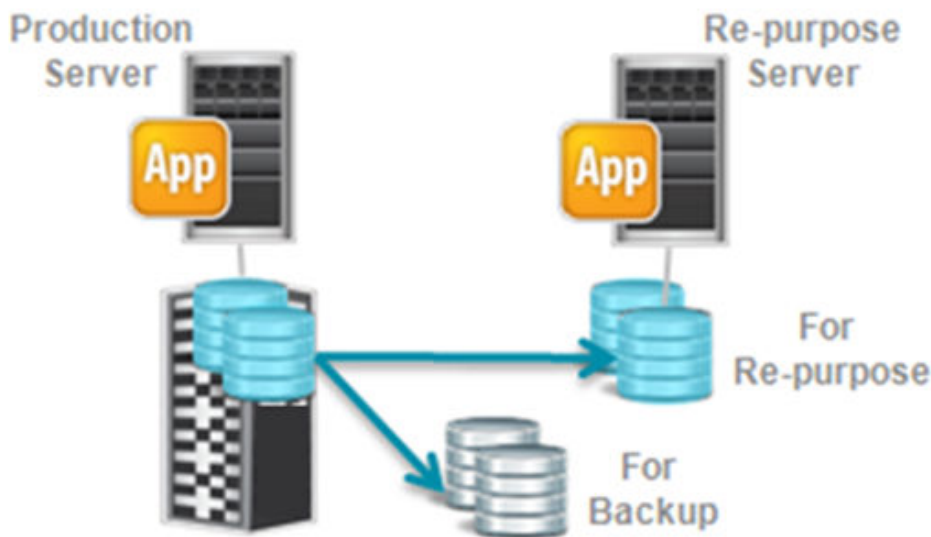


Figure 5 Full clone using batch mode ShadowImage

ShadowImage enables the creation of in-system, RAID-protected, read/write, volume-consistent, full clones.

As with TI snapshots, consistent clones can be created using Consistency Groups (CTGs).



Note: ShadowImage has a limitation on the maximum number of clones that can be created at one time. There can be up to three 1st level (L1) clones and then two L2 clones per L1 clone, giving a potential total of six L2 clones. Including the L1 clones, the potential total is nine clones. If more copies are required beyond this then use Refreshed Thin Image snapshots.

When taking a clone of a primary volume the storage system copies all of the data to the secondary volume. The point at which this is done depends on the split type selected:

- *Quick Split* - copying from primary to secondary is performed in the background so that the secondary is immediately available for reading/writing. The performance of the primary may be affected if access the secondary references data that has not yet been copied from the primary. In this case, on-demand copying of that data from the primary is required.
- *Steady Split* - copying from primary to secondary is performed in the foreground before the secondary is made available for reading/writing. The creation of the secondary takes time depending on volume size.

If using Dynamic Provisioning (DP) volumes for both primary and secondary volumes, the copy is applied only for the allocated area; the unallocated area is ignored.

Once the clone is created, the storage system updates the bitmap for the primary, which records which blocks have been modified. Pair resynchronization can be performed in one of the following ways:

- *Quick Resync* - resynchronization is performed in the background and on-demand. The secondary is briefly made read only (for less than 1 second), after which it becomes available for reading/writing (i.e it enters the PAIR state in less than 1 second). The performance of the primary may be affected if access to the secondary requires on-demand resyncing from the primary.
- *Normal Copy* - the secondary is made unavailable while the resynchronization is performed. The resync takes time depending on the size of differentials between the primary and secondary.

When the secondary is accessed, behaviour depends on the mode of operation as follows:

- *Steady Split* and *Normal Copy* - the storage system presents the actual contents of the secondary volume. This is in contrast to TI snapshots, where a merging process is required between the primary and secondary volumes to reconstruct the data.
- *Quick Split* and *Quick Resync* - the storage system presents the actual contents of the secondary volume. However a merging process may be required between the primary and secondary volumes to reconstruct the accessed block of data, if the background copy of that block has not yet been performed.

The following table shows how *Quick Split* and *Quick Resync* (indicated by the suffix q) are affected by upstream and downstream operations in an SI data flow:

Data Flow	Behaviour
SIq	The SI is performed using quick operations. The SI secondary is immediately available for manually mounting.
SIq with auto-mount of secondary	The SI is performed using quick operations. The SI secondary is auto-mounted immediately.
SIq with downstream replications/snapshots	SI is performed using quick operations. However: <ul style="list-style-type: none"> ▪ The downstream replications/snapshots will wait until the SI secondary is completely copied. ▪ The SI secondary will only be available for manually mounting once it is completely copied. See note below.
SIq with auto-mount and downstream replications/snapshots	SI is performed using quick operations. However: <ul style="list-style-type: none"> ▪ The downstream replication/snapshot will wait until the SI secondary is completely copied. ▪ The SI secondary will only be auto-mounted once it is completely copied. See note below.
Upstream replications with downstream SIq	SI is performed using quick operations. The SI secondary is immediately available for manually mounting. There is no impact on upstream replications.



Note: In cases where the SI replication must be fully evaluated, *Quick Resync* and *Quick Split* will take as long as *Normal Copy* and *Steady Split*. However the use of *Quick Resync* will have a beneficial affect on when and for how long the production application is quiesced.

When the clone is deleted the storage system releases the bitmap.

Steady Split/Normal Copy and *Quick Split/Quick Resync* is supported.



Figure 6 Full clone using continuous ShadowImage with protected, isolated, multiple TI snapshots

Continuous ShadowImage can be used to:

- Protect access to local TI snapshots if the production volumes fail.
- Isolate production volumes from performance impacts caused by heavy I/O on local TI snapshots.
- Allow multiple scheduled mount operations (beyond the limits imposed by SI mirror counts) without affecting the original backup, through the use of Refreshed TI.



Note:

Continuous SI can be combined with all hardware operations (i.e. TI, RTI, SI, TC, UR or GAD), with the exception that a continuous SI S-VOL cannot also be the P-VOL of a remote replication (i.e. TC, Universal Replicator or GAD).

i.e. It is not possible to chain a remote replication from a continuous SI target.

The typical use cases for continuous ShadowImage include:

- Repurpose on Demand - using continuous SI, keeps a close copy of the primary volume and allows pause and mount for repurposing.
- Protected Backup - using continuous SI to TI snapshots, retains snapshots in the event that the primary volume fails.
- DRU Protected Backup - using continuous SI to TI snapshots with DRU, retains snapshots with DRU lock in the event that the primary volume fails.
- Repurposing (TI) - using continuous SI to RTI snapshots, provides multiple repurposing copies, possibly in excess of the SI limit.
- Repurposing (SI) - using continuous SI to batch SI, provides a repurposing copy.
- Repurposing (SI) with Backup - using continuous SI to batch SI to TI snapshots, provides a repurposing copy with snapshots for protection.
- Repurposing (SI) with DRU Backup - using continuous SI to batch SI to TI snapshots with DRU, provides a repurposing copy with snapshots for protection with DRU lock.

Implement 3DC multi-target with delta UR replication

Before you begin

It is assumed that the following tasks have been performed:

- Ensure you have completed the prerequisites listed in [Data protection workflow prerequisites \(on page 85\)](#).
- The Client software is installed on the source node where the Hitachi Block LDEV is mounted. Note that the LDEV is actually located on the primary Hitachi Block storage device.
- The Client software is installed on the nodes that will act as proxies for primary, secondary and tertiary Hitachi Block storage devices. Note that for GAD, TC and UR replications, the source and destination LDEVs are located on different devices.
- The primary, secondary and tertiary storage devices have been set up based on the requirements and prerequisites. See [Hitachi Block prerequisites \(on page 74\)](#).

This task describes the steps to follow when protecting data that resides on a file system created on an LDEV allocated from a Hitachi Block storage device. A GAD or TC replication of the P-VOL at the primary site is created as an S-VOL at the secondary site. A UR replication of the P-VOL is created as an S-VOL at the tertiary site. A Delta UR replication is created between the S-VOLs at the secondary and tertiary sites (this remains suspended unless primary site failure occurs). For more information, refer to [About three datacentre multi-target with delta \(on page 104\)](#).



Note: The software currently only supports the setup of *3DC Multi-target with Delta Replication*. In the event of a primary, secondary or tertiary site failure, the data flow in the Monitor detail page displays notifications indicating any problems with the corresponding movers, and appropriate messages appear in the Logs page.

- For primary site failure:
 1. The *Delta* UR failover link will be invoked automatically by the underlying hardware storage devices to provide near immediate protection of the secondary site.
 2. The data flow should be dissociated from the software before the hardware storage devices are recovered, following procedures defined in the relevant storage device operating manuals. See [Dissociate a replication \(on page 104\)](#).
 3. The data flow for the recovered replication should be re-adopted and re-activated. See [Adopt a replication \(on page 108\)](#).
- For secondary or tertiary site failure, the data flow should remain active. Once the hardware storage devices are recovered, the software will clear its notifications and resume.

The data flow and policy are as follows:

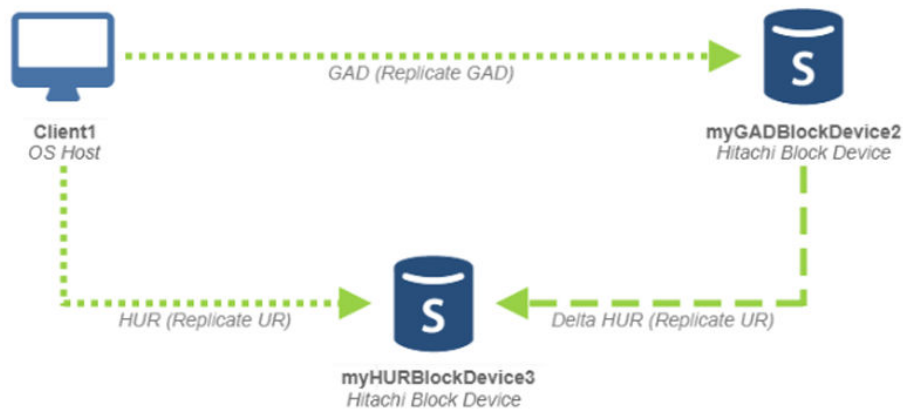


Figure 7 3DC Multi-target with Delta Replication Data Flow

Procedure

1. In the Nodes page, locate the source node and verify that it is authorized and online. This node is where the primary LDEV to be replicated is mounted.
For a file system replication using a *Path* classification, a basic *OS Host* node is required. It is not necessary to create the source node in this case since all Data Protection client nodes default to this type when installed.
2. In the Nodes page, locate the nodes that controls the primary, secondary and tertiary Hitachi Block Devices through command device interfaces and check that they are authorized and online.
These nodes are used by Data Protection to orchestrate replication of the primary LDEV to the secondary and tertiary sites, and are identified as the **Proxy Node** when creating the primary and secondary Hitachi Block Device nodes in the next step. These nodes are known as ISM nodes. The ISM nodes do not appear in the data flow.
3. Create new primary, secondary and tertiary Hitachi Block Device nodes (unless ones already exists) and verify that they are authorized and online.
The secondary and tertiary Hitachi Block Device nodes appear in the replication data flow as the destination nodes. The primary Hitachi Block Device node is represented in the data flow by the *OS Host* node where the primary LDEV is mounted.
4. Define a policy as shown in the following table using the **Path** classification type and **Replicate** operation:

Table 5 Path Replication Policy

Classification Type	Parameter	Value
Path	Include	E:\testdata (E: is where the Hitachi Block LDEV is mounted)

Define three *Replicate* operations (these represent the primary to secondary GAD or UR, primary to tertiary UR and secondary to tertiary Delta UR replications). GAD and UR replications run as continuous operations and thus no schedule needs to be defined.

Operation Type	Parameter	Value	Assigned Nodes
Replicate	Run Options	N/A (GAD is a continuous replication, so the Run option is ignored)	Secondary Hitachi Block Device (from the primary)
Replicate	Run Options	N/A (UR is a continuous replication, so the Run option is ignored)	Tertiary Hitachi Block Device (from the primary)
Replicate	Run Options	N/A (Delta UR is a continuous replication, so the Run option is ignored)	Tertiary Hitachi Block Device (from the secondary)

5. Draw a data flow that shows the *OS Host* source node connected to the secondary and tertiary Hitachi *Block Devices* via *Continuous* movers, and the secondary connected to the tertiary Hitachi *Block Device* via a *Failover* mover.

GAD and UR are remote replication technologies, so the Hitachi *Block Device* nodes shown on the data flow are where the secondary and tertiary destination (S-VOL) volumes are located.
6. Assign the *Path-Replicate* policy to the *OS Host* source node.
7. Assign the first *Replicate* operation to the secondary Hitachi *Block Device* node. The Hitachi Block Replication Configuration page is displayed.
8. Set the replication type to **Active-Active Remote Clone**, then:
 - a. Choose a **Pool** from one of the available *Dynamic Pools*.
 - b. Choose a **Target Quorum** from one of those listed.
 - c. Leave the remaining parameters at their default settings and click **OK**.
9. Assign the second *Replicate* operation to the tertiary Hitachi *Block Device* node.
10. Set the replication type to **Asynchronous Remote Clone**, then:
 - a. Choose a **Pool** from one of the available *Dynamic Pools*.
 - b. Choose a **Source Journal** from one of those listed for the primary node.
 - c. Choose a **Destination Journal** from one of those listed.
 - d. Leave the remaining parameters at their default settings and click **OK**.

11. Assign the third *Replicate* operation to the tertiary Hitachi *Block Device* node.
12. Set the replication type to **Asynchronous Remote Failover**, then:
 - a. Choose a **Pool** from one of the available *Dynamic Pools*.
 - b. Choose a **Source Journal** from one of those listed for the tertiary node.
 - c. Leave the remaining parameters at their default settings and click **OK**.
Data Protection will automatically use the same **Destination Journal** as selected for the **Asynchronous Remote Clone** replication configured in the preceding steps.



Note: If you specify a **Mirror Unit** for this **Asynchronous Remote Failover** replication, then it must differ from the one selected for the **Asynchronous Remote Clone** replication in the preceding steps.

13. Compile and activate the data flow, checking carefully that there are no errors or warnings.
14. In the Monitor page, locate and open the active data flow.
The policy is invoked automatically to create and then maintain the replication accordingly.
15. In the Monitor detail page, watch the active data flow to ensure the policy is operating as expected.

For a healthy data flow you will periodically see:

- Initial replication jobs appearing in the **Jobs** area below the data flow that cycle through stages and ending in *Progress - Completed*.
- Information messages appearing in the **Logs** area below the data flow indicating rules activation, storage handler and sequencer events.
- Attachments to storage handler log events confirming which volumes are being replicated.

For a problematic data flow you may see:

- Permanent **Node Status** icons appear over nodes and associated warning messages displayed to the right of the data flow area.
- Backup jobs appearing in the **Jobs** area below the data flow that cycle through stages and terminating in *Progress - Failed*.
- Warning and error messages appearing in the **Logs** area below the data flow indicating failed events.

16. Review the status of each Hitachi *Block Device* and replications to ensure the GAD and UR replications are being created and maintained.

Hitachi Block Devices require ongoing surveillance to ensure that they are operating correctly and sufficient resources are available to store your data securely.

The replication processes can be paused and resumed from here if required.

There will be three replication records in the Hitachi block replication page corresponding to the GAD, the active UR and the suspended failover UR replication.

About three datacentre multi-target with delta

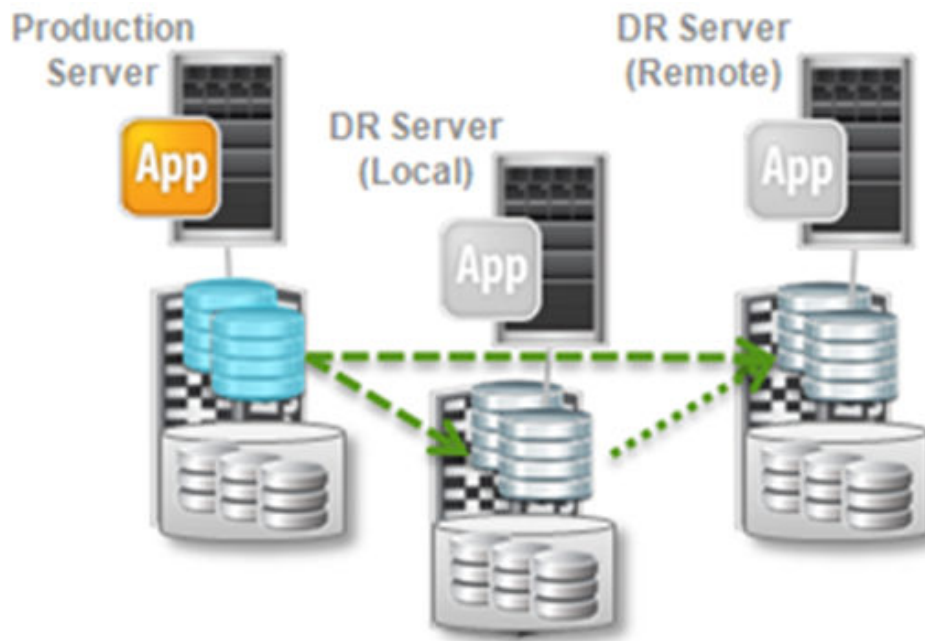


Figure 8 Three datacentre multi-target with delta

Three datacentre (3DC) multi-target with delta is an improvement on 3DC multi-target that provides on-going protection even in the event of a failure at the primary site.

A replication from the production site to the local secondary site is configured using Universal Replicator. A replication from the production site to the remote secondary site is configured using Global-Active Device or TrueCopy. Additionally, a suspended, asynchronous Universal Replicator (delta-UR) replication is established between the local and remote secondary sites. The local and remote secondary sites will be near identical once pairing with the primary site is complete. Differences that appear between the secondary sites over time, due to a number of factors, are tracked by the suspended delta-UR replication.

Failure of the local or remote secondary site is handled in the same way as for 3DC multi-target, in that the primary site remains protected by the surviving secondary site.

In the event that the production site fails, the local secondary site can take over. The local secondary site is then rapidly brought under the protection of the remote secondary site by resuming the suspended delta-UR replication. Because only the deltas between the local and remote secondary sites need to be resynchronized, this pairing takes only a short time to achieve, meaning that the local site only remains unprotected for a brief period. Without the pre-existing, suspended delta UR between the local and remote secondary sites, it could take hours or even days to establish a replication between the secondary sites, leaving the local secondary site vulnerable for an extended period while this takes place.

Dissociate a replication

A Hitachi block replication can be dissociated without it being removed from the underlying hardware.

Procedure

1. Go to the Hitachi block replications page or Hitachi block replication details (storage) page and locate the adopted replication that you want to dissociate.
2. Select the replication and select **Dissociate** from the context menu.
A warning dialog is displayed.
3. If you are sure you want to proceed then type the word 'DISSOCIATE' then click **OK**.
The replication entry is immediately removed from the list. However the dissociated data flow and policy definition will remain and must also be removed.
4. Go to the Data Flows page and delete the dissociated data flows.
5. Go to the Policies page and delete the policies for the dissociated replications.

About Hitachi Block replication adoption

The software can adopt and manage ShadowImage, TrueCopy, Universal Replicator and Global-Active Device replications that already exist on Hitachi Block storage hardware. An adopted replication can then be managed using the GUI.

To adopt a replication, you must specify a replication policy that identifies the required source LDEV or Host Group, draw an appropriate data flow that identifies the source and destination storage devices, replication type (and mirror number for SI and UR), mark the policy for adoption, and then activate the rules.



Note: Any classification can be used to specify the source LDEV, including *Application* and *Filesystem Path*. The software will attempt to resolve and adopt them. This is subject to existing limitations.

Adopted replications can be augmented with user defined replication and snapshot operations.

A replication can be dissociated without being removed from the storage hardware.



Caution: Be aware of the difference in semantics between dissociating and removing replications from data flows:

- Dissociating a replication will leave that replication intact on the hardware.
- Removing a replication from a data flow and redistributing the rules will cause that replication to be torn down on the hardware.




Note: The following apply when adopting replications:

- Replications can be adopted from any supported block storage systems.
- In-system, 2DC and 3DC replications are supported.
- All valid replication data flows including cascades and multi target are supported.
- The user must understand and create the data flow prior to adopting.
- The user needs to know the type of replication that is to be adopted in addition to the Mirror Unit Number. The remaining properties will be discovered from storage.
- At least one existing replication pair must exist on the selected mirror.
- The replication being adopted must be in the in the same direction as the one defined in the data flow, i.e. it cannot be in the reversed flow state.
- Refreshed Thin Image replications cannot be adopted.
- The source and destination journals specified must match those of the Universal Replicator replication being adopted.
- Primary volumes replicating on different mirror unit numbers are not supported.
- Adopting by copy groups or device groups is not supported.
- There is no check for attempting to adopt the same hardware pairs on multiple, active, coexisting data flows.
- Limitations for other features still apply if they are relevant to the adopted replication.

Adopted replications will behave in the following ways depending on the policy and data flow attributes supplied by the user when attempting to perform the adoption process:

Replication Policy and Data flow Configuration	Behaviour
Any	<ol style="list-style-type: none"> 1. Primary volumes that are not being replicated on the specified mirror will have a secondary volume provisioned and that pair is added to the replication set while respecting the replication type, journal, CTG, and fence level options.

Replication Policy and Data flow Configuration	Behaviour
	<ol style="list-style-type: none"> Adopted replications are flagged as such in the hardware resource information along with their CTG ID, journals, mirror unit numbers, and fence levels.
Any	<ul style="list-style-type: none"> If the replication is found to be in PAIR and the mover type is <i>Batch</i> then the replication will be suspended. If the replication is found to be in PSUS/SSUS and the mover type is <i>Continuous</i> then the replication will be resumed.
The user does not select a pool, but does select a mirror unit number	<ol style="list-style-type: none"> If the mirror unit is assigned, adopt the replication pairs on the mirror. If the mirror unit is assigned but there are one or more P-VOLs not replicating on that mirror, create S-VOLs for those P-VOLs, in the pool used by the existing S-VOLs (or error if the S-VOLs exist in more than one pool). If the mirror unit is unassigned, log the error "Cannot provision, no pool selected".
<p>The user selects a mirror number that is not supported for the selected replication type. Valid mirrors numbers are:</p> <ul style="list-style-type: none"> ShadowImage: 0, 1 or 2 TrueCopy: 0 only Universal Replicator: 0, h1, h2 or h3 Global-Active Device: 0, 1, h1 or h2 	<p>Log the error "Could not determine pool/journal/quorum to use. Ensure that there is at least one existing pair of matching replication type"</p> <div>  Note: When attempting to adopt a TC or GAD replication, UR pairs are deleted on mirror number 0 and, if present, log the error: <pre>Handler 'HitachiVirtualStoragePlatform' call failed: [TrueCopy GAD] mirror for one or more adopted pairs already in use by UR.</pre> See above for more limitations relating to mirror unit and replication type combinations. </div>
The user changes the mirror number after initial data flow activation	<p>The user will be warned via the GUI that the following actions will be taken before they reactivate the rules:</p> <ol style="list-style-type: none"> Volumes and relationships that have been adopted will be unadopted Volumes and relationships that have been created by the user will be destroyed

Replication Policy and Data flow Configuration	Behaviour
	3. Replications will be re-adopted and created based on the new mirror number

Adopt a replication

Before you begin

- Ensure you have completed the prerequisites listed in [Data protection workflow prerequisites \(on page 85\)](#).
- The Client software is installed on the nodes that will act as proxies for both primary and secondary Hitachi Block storage devices.
- The primary and secondary storage devices have been set up based on the requirements and prerequisites. See [Hitachi Block prerequisites \(on page 74\)](#).
- Read [About Hitachi Block replication adoption \(on page 105\)](#) to understand how adoption works, its prerequisites, limitations, and behaviour.

This task describes the steps to follow when adopting an outside replication that is set up on the underlying hardware. The data flow and policy in this example are as follows:



Figure 9 Adopted TrueCopy Replication Data Flow

Table 6 Hitachi Block Replication Policy

Classification Type	Parameter	Value
Hitachi Block	Logical Devices	212418/100 212418/101



Note: If you want to add source volumes to a replication policy after it is adopted, then the Adopt existing replication option in the Hitachi block replication configuration page must remain selected when you subsequently reactivate the data flow with the modified policy settings.

Operation Type	Parameter	Value	Assigned Nodes
Replicate	Run Options	N/A (TrueCopy is a continuous replication, so the Run option is ignored)	Primary Hitachi Block Device, Secondary Hitachi Block Device

To adopt a replication, perform the following steps:

Procedure

1. In the Nodes page, locate the nodes that controls the primary and secondary Hitachi Block Devices through command device interfaces and check that they are authorized and online.
These nodes are used by Data Protection to orchestrate replication of the primary LDEVs to the secondary LDEVs and are identified as the **Proxy Node** when creating the primary and secondary Hitachi Block Device nodes in the next step. These nodes are known as ISM nodes. The ISM nodes do not appear in the data flow.
2. Create new primary and secondary Hitachi Block Device nodes (unless ones already exists) and verify that they are authorized and online.
The primary and secondary Hitachi Block Device nodes appear in the replication data flow as the source and destination nodes.
3. In the Policies page, create a new policy.
 - a. Add a Hitachi Block classification, select **Specify additional selections** and specify the LDEVs or Host Group of the primary volumes in the **Logical Devices** field.
 - b. Add a **Replicate** operation. Select **Run on Schedule** and define a suitable schedule if a batch replication is being adopted.
 - c. Click **Finish** to create the policy.
4. In the Data Flow page, create the replication data flow corresponding to the one you want to adopt.
 - a. Place the corresponding Hitachi *Block* source and destination nodes in the Data Flow workspace.
 - b. Connect the two nodes using a **Batch** or **Continuous** mover, as appropriate to the replication type being adopted.
 - c. Select the source node and assign the Hitachi *Block-Replicate* policy defined above.
 - d. Select the destination node and assign the *Replicate* operation.
 - e. Select the type of replication on the left hand side of the dialog and then the **Adopt existing replication** option on the right.



Note: Refreshed Snapshot replications using Thin Image cannot be adopted.