Hewlett Packard
Enterprise

GUI Administration Guide

HPE Alletra 6000 Series

HPE Nimble Storage Flash Arrays

Published April, 2023
Version 6.0.x

Legal Notices

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Hewlett Packard Enterprise believes in being unconditionally inclusive. If terms in this document are recognized as offensive or noninclusive, they are used only for consistency within the product. When the product is updated to remove the terms, this document will be updated.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

All third-party marks are property of their respective owners.

Publication Date

Thursday April 20, 2023 21:26:39

Document ID

tsi1616003769744

Support

All documentation and knowledge base articles are available on HPE InfoSight at https://infosight.hpe.com. To register for HPE InfoSight, click the *Create Account* link on the main page.

Email: support@nimblestorage.com

For all other general support contact information, go to https://www.hpe.com/us/en/services/nimble-storage.html.

Contents

The GUI

The HPE array provides an easy-to-use, intuitive graphical user interface (GUI). To access the GUI, open any supported browser and enter the management IP address of the array. You then see the login page. Enter the password that you set during the array setup and log in.

This document deals with procedures to manage the array and to automate common tasks using the GUI. If you want to manage your array with the CLI, refer to the *CLI Administration Guide*. Not all procedures can be performed with both the GUI and the CLI.

Accepting a Self-Signed Certificate When Logging in to the Array OS Using Firefox

This procedure describes using the Firefox browser to accept a self-signed (untrusted) certificate when logging in to the array GUI for the first time, or when logging in after the certificate on the array has changed. If pop-ups are disabled in Firefox, you must accept the certificate, then enable pop-ups and accept the certificate a second time.

> **Note:** For more information about managing certificates, refer to the "Secure Sockets Layer Certificates" section in the *CLI Administration Guide*.

Procedure

1. From Firefox, do one of the following:
   - Enter the array URL in the address bar and press **Enter**.
   - Click a bookmark to the array.

   An error message displays, indicating that your connection is untrusted.
2. Depending on your version of Firefox, click one of the following:
   - **Advanced**
   - **I Understand the Risks**
3. Click **Add Exception**.
4. Click **Confirm Security Exception**.
   If pop-ups are enabled, you are redirected to the array OS logon screen. However, if pop-ups are disabled, an error message is displayed indicating that you must update the Firefox preferences to enable pop-ups.
5. To enable pop-ups and complete the log-in process, do the following:
   a) Click the **Options** button below the menu bar.
   b) Choose **Allow pop-ups for *array-url***.
   c) Repeat steps 2 through 4.

Using the GUI

There are six main spaces on the GUI dashboard, including Performance, Alarms, Space, Recent Events, Protection and Hardware. Use the menu items to move to any location of interest.

Spaces include:

- **Performance:** Displays latency, IOPS, and MiB/s statistics over time.
- **Alarms:** Displays configuration warnings and information about hardware faults.
- **Space:** Displays the number of volumes that are full and that are under and over threshold. Also displays group and saving statistics, including Thin-Provisioning Savings, Data Reduction Savings, Clones and Compression.

- **Recent Events:** Displays the latest loggable events.
- **Protection:** Displays the percentage of volumes that are protected and the number of local, remote, and unprotected volumes.
- **Hardware:** Displays the number of arrays in a group, hardware errors and warnings, and software status.

Menus include:

- **The Logo:** Click the logo from anywhere in the GUI to return to the dashboard.
- **Manage:** Use the Manage submenus to access pages where you can create and manage volumes, storage pools, volume collections, protection, replication partners, folders, and ACL setup. Each submenu selection opens a more details area for the selection. For example, selecting **Manage** > **Data Storage**, then clicking the **Volumes** tab displays a list of existing volumes, volume replicas, and snapshots those volumes retain.
- **Hardware:** Allows you to view a GUI representation of the array and monitor the status, edit the array and group name, and add and array to and remove an array from a group.
- **Monitor:** Monitor displays all aspects of the array, grouped into intuitive selections such as space, performance, connections, and replication. See the section on Monitoring for details.
- **Events:** Events can be filtered by category, severity, and time frame. Patterns within events can improve your ability to predict problems and correct them before they become critical.
- **Administration:** Administer the system configuration including networking, email alerts, software updates, DNA, time zones, SNMP, and general management. See the section on Administration for details.
- **Help:** Access online help, contact support, or see the About page, which shows the configuration model number and software version.

Each submenu provides links for drilling down and right-click commands for most actions. For example, to see detailed information at the volume level, you would move from *Volume Summary* to *Volume Details*.

GUI Icons

The following icons are used in the array GUI:

Icon	Meaning
+	Add
✎	Edit
✖	Delete
📷	Take Snapshot
➡	Move Volumes
···	More
🗀	Folder
≋	Volume
▦	Group
📅	Schedule
✻	Fan: Green = OK, Orange = Warning, Red = Error
🌡	Temperature: Green = OK, Orange = Warning, Red = Error

Icon	Meaning
🔌	Power Supply: Green = OK, Orange = Warning, Red = Error
🟩	Fibre Channel Connection: Green = OK, Orange = Warning, Red = Error
🟩	Ethernet Connection: Green = OK, Orange = Warning, Red = Error
🟩	SAS HD: Green = OK, Orange = Warning, Red = Error
🟩	SAS Regular: Green = OK, Orange = Warning, Red = Error
✓	Status Checkmark
❗	Critical
⚠	Warning
ℹ	Notice: (Black)
ℹ	Information: (Blue)Hovering the pointer over the icon gives you more information about an item. For charts and graphs, hovering the pointer gives you details based on the area on which the pointer hovers. A circle shows the exact location being displayed on a graph.
🔧	Configuration
☰	Hardware
🛢	Replication
🔒	Security
📄	Service
⬆	Update

Array Overview

The array seamlessly merges high-performance, compressed storage with capacity-optimized snapshot storage and WAN-efficient replication while it also serves the following functions:

- Provides a seamless combination of storage and backup with efficient disaster recovery
- Enables data restoration based on snapshots
- Offers data protection through Recovery Point Objective (RPO) and Recovery Time Objective (RTO) metrics
- Simplifies storage and snapshot management
- Binds multiple arrays into a single management group

The Array

The arrays are engineered for high performance using flash, for low cost using dense, capacity-optimized disks, and for easy installation and administration.

The array OS is built on the patented Cache Accelerated Sequential Layout (CASL™) architecture. CASL leverages the lightning-fast random read performance of flash and the cost-effective capacity of hard disk drives. Data written to the array is compressed and then stored in the disk-drive layer. The arrays take advantage of multi-core processors to provide high-speed inline variable-block compression without introducing noticeable latency. CASL also incorporates efficiency features like cloning and integrated snapshots to store and serve more data in less space.

Data that is frequently accessed is tracked in the array index, which ensures that frequently and recently accessed data is also held in the large adaptive flash layer. A copy of all data in the flash layer also remains safely in the disk-drive layer to ensure reliability, but now it can be accessed with the high performance and low latency made possible by flash technology.

Storage arrays provide:

- Accelerated performance for higher throughput or I/Os per second and sub-millisecond latencies
- Higher storage efficiency to reduce the storage footprint by 30 to 75 percent
- Non-disruptive scaling to fit changing application needs through increased performance, or capacity, or both
- Maximized data and storage availability with integrated data protection and disaster recovery
- Simplified storage management and reduced day-to-day operational overhead

Array Features

Arrays provide features to enhance performance, value, and ease of use. The all-inclusive features described in this documentation do not require extra licensing.

Feature	Function	Benefit
Core Functionality		
Dynamic Caching	Reads active data from flash cache, which is populated on writes or first read	Accelerates read operations, with sub-millisecond latency
Write-Optimized Data Layout	Coalesces random writes and sequentially writes them to disk as a full stripe	Accelerates writes as much as 100x, and gets sub-millisecond latency and optimal disk utilization
Universal Compression	Always-on inline compression for all workloads	Reduces capacity needs by 30-75%, depending on the workload, with no performance impact

Feature	Function	Benefit
Thin Provisioning	Allocates disk space to a volume only as data is written; thin provision "stun" is supported to add greater flexibility	Pools storage, shares free space, and maximizes utilization
Offloaded Data Transfer (ODX) for Windows	Interacts with storage devices to move data through high-speed storage networks	Improves file copy speed
Scale Performance	Non-disruptively upgrade controllers or swap in higher capacity SSDs	Scales performance to manage large amounts of active data
Scale Capacity	Non-disruptively add external disk shelves	Increases storage capacity to 100s of TB per system
Instant Snapshot and Recovery	Backs up and restores data using point-in-time, space-efficient snapshots taken at regular intervals	Retains months of frequent snapshots, which improves RPO with no performance impact. Eliminates backup windows and speeds up restores, which improves RTO.
WAN-efficient Replication	Replicates the compressed data changes to the secondary site for disaster recovery	Deploys affordable and verifiable disaster recovery and efficiently backs up remote sites over the WAN
VLAN Tagging	Part of the 802.1Q frame header containing a VLAN ID between 1 and 4094 that identifies the VLAN to which the frame belongs	Allows a switch to forward that frame only to the appropriate VLAN
Zero-Copy Clones	Creates copies of existing active volumes without needing to copy data	Creates clones in seconds and saves disk space, which is ideal for VDI and test/development environments
Host and Application Integration		
Custom Application Profiles	Predefined policies for block size, caching, compression, and data protection for Microsoft applications and VMware virtual machines	Eliminates the need to manually tune storage and data protection configurations
Windows VSS Enablement	HPE Storage Driver for the Microsoft VSS framework for consistent backup	Takes application-consistent backups and simplifies data protection for Exchange and SQL Server
VMware Integration	Monitors, provisions, and takes snapshots from VMware vCenter	Manages storage from vCenter and takes consistent backups of virtual machines
VMware Site Recovery Manager Adapter	Supports disaster recovery automation for VMware including failover/failback	Simplifies disaster recovery, including testing failover/failback
Management and Support		
Proactive Wellness and DNA	Real-time monitoring and analysis; sends alerts on critical issues	Spots and remedies potential issues to maximize uptime, performance, and utilization (no user data is accessed or collected by DNA)
Secure Remote Support	Allows remote troubleshooting, configuration, and problem resolution	Reduces burden on IT staff and quickly resolves problems

Feature	Function	Benefit
Non-Disruptive Upgrades	Upgrades software with no disruption to applications	Maximizes uptime and user productivity through continuous availability

Note: Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are among the most important parameters of a disaster recovery plan.

- RPO: The point-in-time to which systems and data must be recovered after an outage. The interval reflects the amount of data loss a business can survive.
- RTO: The amount of time it takes to recover systems and data after an outage. The interval reflects the amount of downtime a business can survive.

For RPO and RTO, a shorter time interval is better.

Array Management

Arrays are easy to install and manage. Consolidation of storage, backup, automatic failover, reusable schedules based on application usage, and application integration are combined with clean, intuitive management interfaces that improve the ease of administration. Use one of the following interfaces to manage array features:

Management Interface	Description
Data Services Cloud Console	An application running on the HPE Cloud that lets you manage storage resources regardless of where those resources are deployed. The Data Services Cloud Console is supported on HPE Alletra 6000 arrays when you have a valid subscription. The array registers with Data Services Cloud Console automatically when initialized. Data Services Cloud Console is also supported with HPE Storage Flash Arrays with valid subscriptions. You must manually enable the connection between the array and Data Services Cloud Console. **Note:** Data Services Cloud Console is supported with HPE Flash Arrays running array OS 6.0.0.300 or later. The supported models include AF20, AF20Q, AF40, AF60, AF80, HF20, HF20H, HF20C, HF40, HF40C, HF60, and HF60C. Both HPE Alletra 6000 arrays and HPE Storage Flash Arrays require that you set up a cloud account before you configure the array for DSCC. For more information, see the *Installation Guide for HPE Alletra 6000*, which is available on the HPE Alletra, Nimble Storage documentation portal on HPE InfoSight.
GUI	An on-array graphical user interface (GUI) interface that lets you manage arrays with an easy-to-use and intuitive interface.
CLI	An on-array command line interface (CLI) that lets you automate common array management.
REST API	An on-array REST API that lets you manage arrays programmatically.

Cloud Accounts and Arrays Using Data Services Cloud Console

To use Data Services Cloud Console, you must have a cloud account set up with HPE GreenLake (https://common.cloud.hpe.com). This account consists of both an HPE GreenLake user account and an HPE GreenLake organization account. You use the cloud account to connect with Data Services Cloud Console.

> **Note:** Information about setting up a cloud account for Data Services Cloud Console can be found in the *Data Services Cloud Console Getting Started Guide*, which is available on the HPE InfoSight documentation portal (https://infosight.hpe.com/resources/nimble/docs). The path to this guide is **HPE InfoSight** > **HPE Alletra, Nimble Storage** > **Documentation** > **Getting Started**.

The procedure for setting up an array with Data Services Cloud Console varies depending on whether you are using an HPE Alletra 6000 array or an HPE Flash Array with a valid subscription to Data Services Cloud Console.

HPE Alletra 6000 Series Arrays

The HPE Alletra 6000 series arrays require that you set up the cloud account and enter the software subscription key before you initialize the array. Doing this enables the array to automatically connect to Data Services Cloud Console. The HPE Alletra 6000 series arrays require Data Services Cloud Console to perform operations, such as creating a volume, pool, partner, or snapshot.

> **Note:** This subscription key was emailed to you in a **Electronic Software Delivery Receipt** that included a link to **Access Your Products**. If you cannot locate the key, contact support.

HPE Flash Arrays

HPE Flash Arrays that have a subscription to Data Services Cloud Console use the array OS GUI to get the subscription key. After you perform the steps necessary to get the GUI to retrieve the key, you must log in to the cloud account where you manually enter the key and perform other steps necessary to enable Data Services Cloud Console.

> **Note:** HPE Flash Arrays can perform operations such as creating a volume, pool, partner, or snapshot regardless of whether Data Services Cloud Console is enabled.

Enable HPE Alletra 6000 Arrays to Work with Data Services Cloud Console

HPE Alletra 6000 series arrays with valid subscriptions and existing cloud accounts automatically register with Data Services Cloud Console when you initialize the array.

To ensure that the array initialization process goes smoothly, you should set up your HPE GreenLake cloud account before you initialize the array. You enter the subscription key for Data Services Cloud Console in the cloud account.

> **Note:** The subscription key was emailed to you in a **Electronic Software Delivery Receipt** that included a link to **Access Your Products**. If you cannot locate the key, contact support.

For information about a setting up cloud account and getting started with Data Services Cloud Console, see *Data Services Cloud Console Getting Started Guide*, which is available on the HPE InfoSight documentation portal (https://infosight.hpe.com/resources/nimble/docs). The path to this guide is **HPE InfoSight** > **HPE Alletra, Nimble Storage** > **Documentation** > **Getting Started**.

Enable HPE Flash Arrays to Use Data Services Cloud Console

HPE Storage Flash Arrays running array OS 6.0.0.300 or later are supported with Data Services Cloud Console when you have a valid subscription.

Connecting with Data Services Cloud Console is optional. You can create volumes, snapshots, pools, and replication partners on the arrays both without Data Services Cloud Console and with Data Services Cloud Console enabled.

To use the array with Data Services Cloud Console, you must perform setup steps in the array GUI and in the Data Services Cloud Console section of your cloud account.

Note: You can also enable Data Services Cloud Console on the array by using the array CLI.

Before you begin

You must have the following:

- An HPE Flash Array running OS 6.0.0.300 or later.

  The supported models include AF20, AF20Q, AF40, AF60, AF80, HF20, HF20H, HF20C, HF40, HF40C, HF60, and HF60C.

- A valid subscription for Data Services Cloud Console.

  To get the key associated with your subscription, you must complete the steps in this task.

- A cloud account.

  It is a good practice to set up your account with HPE GreenLake before performing this procedure. To enable the array to work with Data Services Cloud Console, you must perform steps in the cloud account.

  Note: *Data Services Cloud Console Getting Started Guide*, which is available on the HPE InfoSight documentation portal (https://infosight.hpe.com/resources/nimble/docs), contains information to help you set up a cloud account. This guide is in the section **Document Type** > **Getting Started Guide**.

Procedure

1. If you have not already set up your cloud account for your HPE Storage Flash Array, do it now.
2. **(Array)** After the array has initialized, select **Administration** > **Customization** > **Data Services Cloud Console** from the array GUI.

   This screen displays the current status of the array with Data Services Cloud Console. If it displays the connection status as **Not Connected**, complete the following steps to connect the array to Data Services Cloud Console.

3. **(Array)** Enable the option **Connect to Data Services Cloud Console** and select **Save**.

   The array OS retrieves the key you need to use to connect to Data Services Cloud Console.

   It can take 20 seconds or more before the array OS retrieves the key. Refresh the GUI window until it displays the subscription key.

4. **(Array)** Copy the subscription key and array serial number so you can enter this information in Data Services Cloud Console.

   Note: The GUI displays an alarm stating that the array could not be activated. This is because you must manually enter the array information in Data Services Cloud Console.

5. **(Data Services Cloud Console)** Log in to your cloud account and go to the Data Services Cloud Console section.
6. **(Data Services Cloud Console)** Select **Menu** > **Manage** > **Device Management** > **Add Devices**.
7. **(Data Services Cloud Console)** In the pop-up box, select **Storage Devices** from the drop-down list and choose **Continue**. Now enter the array serial number and subscription key.
8. **(Data Services Cloud Console)** Select **Enter**.
9. **(Data Services Cloud Console)** Select **Add Devices**.
10. **(Data Services Cloud Console)** In the pop-up window, select **Close**.
11. **(Data Services Cloud Console)** Assign a Data Services Cloud Console instance to the device by selecting the array and clicking **Assign to Application**.
12. **(Data Services Cloud Console)** Select both the application and the application instance it is assigned to from the drop-down lists.
13. **(Data Services Cloud Console)** Select **Finish**.
14. **(Data Services Cloud Console)** In the pop-up window, select **Close**.

15. **(Array)** In the array GUI, select **Administration** > **Customization** > **Data Services Cloud Console**. The page shows that the array is connected to Data Services Cloud Console. It also displays the Data Services Cloud Console instance in addition to the subscription key and the array serial number.

Disable HPE Flash Arrays from Data Services Cloud Console

You can disable an HPE Flash Array's connection with Data Services Cloud Console from the array GUI.

Note: This procedure can only be used with HPE Flash Arrays running array OS 6.0.0.300 or later that have Data Services Cloud Console enabled.

Procedure

1. Select **Administration** > **Customization** > **Data Services Cloud Console** from the array GUI.
2. De-select the option **Connect to Data Services Cloud Console Connect to** by moving the button to the left.

   Note: If you want to enable Data Services Cloud Console again, all you need to do is enable the **Connect to Data Services Cloud Console** button and select **Save**.

3. Click **Save**.

Addressing Possible Data Services Cloud Console Connection Issues

Occasionally, you might experience a problem accessing Data Services Cloud Console. If this happens, the array retries the initiation activation process every 30 seconds. In the meantime you should verify that the network connectivity for your configuration is set up correctly.

The following alarms have been seen sometimes. If you encounter one of these alarms, take the recommended action to resolve it:

Alarm	Action
fail-prov-no-device	Array *x* can connect to Data Services Cloud Console, but the storage system is not in the inventory. Contact support to add the storage system to the inventory.
fail-prov-no-rule	Array *x* can connect to Data Services Cloud Console, but cannot find an application instance for this storage system. Log in to HPE GreenLake (https://common.cloud.hpe.com) and confirm that this storage system is assigned to the proper application instance.

IOPS and MiB/s Limits on Volumes and Folders

You can set both IOPS (input/output requests per second) and MiB/s (mebibytes per second) limits when you set up a Quality of Service policy for a volume or Storage Policy-Based Management (SPBM) for Virtual Volumes.

You specify the IOPS and MBps limits separately. The input/output requests are throttled when either the IOPS limit or the MBps limit is met.

The default upper bound value for both the IOPS and the MiB/s is unlimited. The lower bound for IOPS is 256 requests. The lower bound for the MiB/s value is calculated as greater than or equal to the IOPS limit multiplied by the volume block size. This way the MiB/s value does not throttle the IOPS for the volume.

If the volume contains folders, then the IOPS and MiB/s limits work as an aggregate. The input/output requests to the volumes under the folder are throttled when the cumulative IOPS of all the volumes under that folder exceeds the folder IOPS limit or when the cumulative throughput of all the volumes under that folder exceeds the folder MiB/s limit. When this happens, all the volumes are throttled equally.

You can set these limits when you create or edit either a volume or a folder. You can set separate limits for both volumes and folders. You can view the limits for volumes and folders on the Performance tab at:

Manage > **Data Storage** > **Performance**

If you are creating or editing a folder, you can set the limits at the folder level that are in addition to the volume-level limits. The default limits are at the volume level. You can view the limits on the Folder tab at:

Manage > **Data Storage** > **Folder**

You can monitor the throughput and bandwidth for the array, the volumes, and the folders by selecting:

Monitor > **Performance**

Horizontal Scaling

Scale-out, often referred to as horizontal scaling, means adding arrays to a *group*. Performance and capacity scale linearly as you add arrays to the group. Grouping multiple arrays so that they can be managed as one entity provides significant manageability benefits, because it appears as if you are managing a single large array. Scale-out simplifies load balancing and capacity management, as well as hardware and software life-cycle management.

From an organizational standpoint, scale-out establishes a group of merged systems upon which storage pools can be developed. Volumes are created within pools that can span multiple physical arrays. A volume might exist on one array or span multiple arrays in a group by virtue of how the pool is configured.

Scale-out is a *peer-to-peer* technology where each array can operate independently, but can be managed as a single pool of storage. With scale-out, you not only add more disk and flash memory, but also CPU, system memory, network links, and so on.

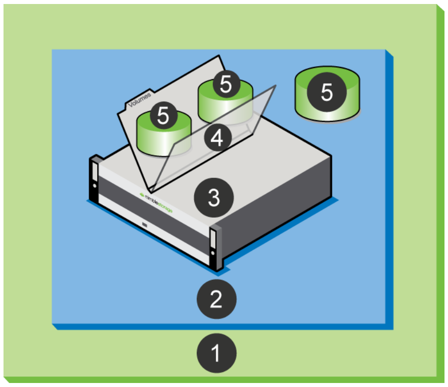
Scale-out requires that all arrays in a group have the same version of array software installed.

Relationship of Groups, Pools, Arrays, Folders, and Volumes

A *group* is a collection of one to four arrays that are physically connected. Logically, they represent a single storage entity to aggregate performance and capacity, and to simplify management. Arrays in the group can be iSCSI, Fibre Channel, or multiprotocol (iSCSI and Fibre Channel). A group contains one or more disjoint pools. For groups of arrays, data can be striped across the arrays in the same pool. For most administrative tasks, a group looks and feels like a single array. You administer the group by connecting to its management IP address, hosted by one of the arrays in a group.

A single-array group is formed when you configure a array.

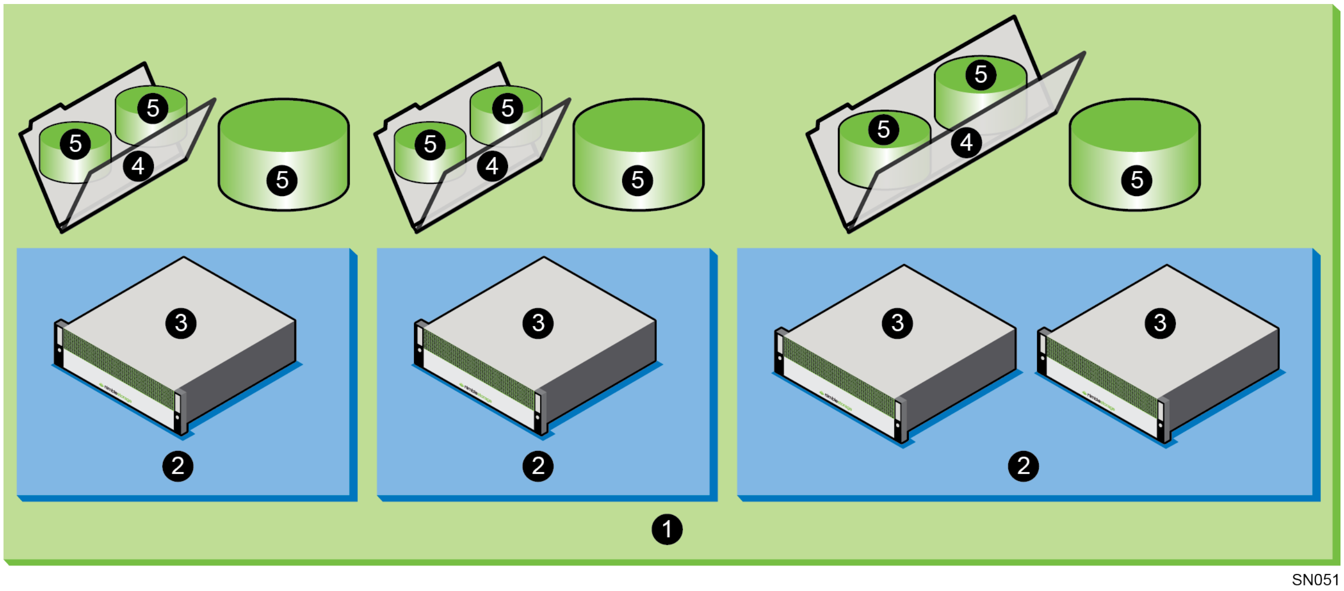
Figure 1: Relationships of Groups, Pools, Arrays, Folders, and Volumes in Single-array Groups



1	Group
2	Storage Pool
3	Array
4	Folder
5	Volume

A group is scaled-out, or expanded to a multi-array group, by adding unconfigured or configured arrays to the group. Adding a configured array to a group is also known as a *group merge*.

Figure 2: Relationships of Groups, Pools, Arrays, Folders, and Volumes in Multi-array Groups



1	Group
2	Storage Pool
3	Array
4	Folder
5	Volume

You can remove an array that is part of a storage pool by evacuating the data from the array and then removing the array from the pool. When you need to remove an array from a group, you can evacuate the data to another array in the group (for example, moving a volume), provided there is enough space for the data that is stored on the array being removed.

Pools

A storage pool confines data to a subset of the arrays in a group. A storage pool is a logical container that contains one or more member arrays in which volumes reside. The system stripes and automatically rebalances data of resident volumes over the members across the pool. Storage pools dictate physical locality and striping characteristics. A member array can only be a part of one storage pool. Note the following:

- Volumes and their respective snapshots and clones reside within a pool and are tied to a specific pool.

  Volumes are also referred to as logical units (LUNs). On an array, LUNs are exposed as volumes.
- You can migrate (move) volumes between different pools.
- Volume collections are not tied to pools and can contain volumes that reside in different pools.

Use single-array pools under the following conditions:

- Fault isolation is a priority
- Linux hosts, or any hosts that do not have a supported HPE Storage Connection Manager available, can access the arrays

Consider using multi-array pools under the following conditions:

- Scaling performance and capacity, as well as consolidating management, are priorities
- Windows and ESX hosts that have a supported Connection Manager available can access the arrays

> **Note:** If your host system is not running an MPIO module, you experience a decrease in I/O performance when connected to a volume that spans multiple arrays. The drop is caused by the data paths among the arrays being redirected. Install the Connection Manager, which sets up the optimum number of iSCSI sessions (only iSCSI) and finds the best data connection to use under MPIO.

Feature Support on iSCSI and Fibre Channel Arrays

HPE Storage Fibre Channel arrays have slight differences in feature compatibility compared to HPE Storage iSCSI arrays.

The following table lists specific features and identifies whether each feature is supported on an iSCSI array and a Fibre Channel array. For additional details, see the documentation specific to each feature.

Feature	Supported in an iSCSI Array	Supported in a Fibre Channel Array
Multi-array pools	Yes	Yes
Multi-array groups	Yes	Yes
Pool merge	Yes	Yes
Volume move	Yes	Yes
Array add	Yes	Yes
Discovery IP address	Yes	No
CHAP users	Yes	No

Integration

For optimal integration, you must familiarize yourself with the Windows and VMware environments. Both Microsoft and VMware provide conceptual and practical information in the form of knowledge base articles, online manuals, and printed books.

About Storage Windows Integration

The HPE Storage Toolkit for Windows contains the necessary components to use Microsoft Volume Shadow Copy Service (VSS) to provide the backup infrastructure for Microsoft Exchange and SQL servers. It also enables you to initialize and configure a array from your Windows host.

Table 1: HPE Storage Toolkit for Windows Components

Component	Description
HPE Storage Protection Manager	Provides the HPE VSS requester and the HPE VSS hardware provider. These features enable you to use the Microsoft VSS to take application-consistent snapshots on an array.
Connection Manager	Sets up the optimum number of iSCSI sessions and finds the best data connection to use under MPIO.
HPE Storage Setup Manager	Identifies uninitialized arrays and initializes them. Then it takes you to the array GUI to finalize the configuration.

About Array Integration with VMware

Many array integration features with VMware are preinstalled in the array OS. There are some features, such as Storage Replication Adapter (SRA) and HPE Storage Connection Manager for VMware, that you must install.

Table 2: HPE Storage VMware Integration Components

Component	Description
HPE Storage Connection Manager for VMware	Manages connections from the host to volumes on HPE systems. The Connection Manager optimizes the number of iSCSI sessions and finds the best data connection to use under MPIO. It includes an HPE DSM that claims and aggregates data paths for the array volumes.
vStorage APIs for Array Integration (VAAI)	Provides hardware acceleration by enabling the WRITE SAME, UNMAP, ATS,Thin Provisioning Stun, and XCOPY features.
vCenter Plugin	Allows you to create and manage datastores on the array as well as use the vCenter Server to create vCenter roles and edit protection schedules. You must register the HPE vCenter Plugin that is provided with the array OS with the vCenter Server
VMware Synchronized Snapshots	Enables application-consistent snapshots within VMware environments.
Storage Replication Adapter	Allows a array to support VMware Site Recovery (SRM) to perform array-based disaster recovery. You must install the HPE SRA on the Windows server that runs SRM.
VMware Virtual Volumes (vVols)	Enables you to use VMware virtual disks mapped to volumes on the array without requiring that you know the implementation details of the underlying storage. You must have vSphere 6.0 or later, ESXi 6.0 or later and VASA Provider to use vVols. The array eOS provides VASA Provider as part of the vCenter plugin.

Wellness and DNA

DNA is a diagnostic tool that supports array wellness, increases storage uptime, and keeps arrays running at peak performance and efficiency. Based on how you set up your array, there are support tools that can monitor *heartbeats* and logs produced by your system and analyze a variety of parameters in real time. Any anomalies such as configuration errors or abnormal operating conditions are reported, and you are alerted before a failure occurs.

These tools automatically resolve over 75 percent of issues and decrease escalations. That means faster resolution of customer issues. If needed, the support staff can also perform secure remote troubleshooting, configuration, and problem resolution, all of which help resolve issues while maintaining data security. Non-disruptive upgrades mean you can upgrade your array and all new features and software releases with no planned downtime.

You should enable DNA when you first configure the array.

Access Controls

On your Windows server or ESXi host, you must configure iSCSI or Fibre Channel connections with your volumes on the array in order for your server or host to access those volumes. By using certain features of iSCSI or Fibre Channel, the arrray OS can control who has access to your volumes. *Access control list (ACL)* is another term for access control.

The array OS supports multiple methods of access control: user permissions, CHAP accounts, iSCSI initiator groups, Fibre Channel initiator groups, and VLAN segmentation and tagging. You can apply access controls when you create a volume or at any later time.

User Permissions

Each individual accesses the array through a user account, which is created by an Administrator. Users log into the array with their user name and password. The Administrator has two methods of access control for each user account:

- Role or permission level
- Enabling or disabling the user account

CHAP Accounts

Challenge-Handshake Authentication Protocol (CHAP) is an authentication method that servers use to verify the identity of remote clients. CHAP verifies the identity of the client by using a *handshake* when establishing the initial link and at any time afterwards. The handshake is based on the exchange of a random number known to both the client and server.

CHAP accounts are not required to establish a functional data connection between an array and a Windows server or ESXi host.

Note: CHAP works only with iSCSI; it is not supported on Fibre Channel.

iSCSI Initiator Groups

An iSCSI initiator group is a collection of one or more iSCSI initiators, with each initiator having a unique iSCSI Qualified Name (IQN) and IP address. Each IQN represents a single Network Interface Card (NIC) port on an iSCSI-based client in the form of a Windows server, ESXi or Linux host. Configure iSCSI initiator groups on the array; configure client-side iSCSI initiators according to the vendor's recommendations.

Note: By default, iSCSI volumes deny access to initiators. To allow initiators in an initiator group to access a volume, you must configure an ACL that includes the desired initiators and attach it to the volume.

Fibre Channel Initiator Groups

A Fibre Channel initiator group is a collection of one or more initiators, with each initiator having a unique World Wide Port Name (WWPN). Each WWPN represents a single Host Bus Adapter (HBA) port on a Fibre Channel-based client in the form of a Windows server, ESXi or Linux host. Configure Fibre Channel initiator groups on the array; configure client-side Fibre Channel initiators according to the vendor's recommendations.

Note: By default, Fibre Channel volumes deny access to initiators. To allow initiators in an initiator group to access a volume, you must configure an ACL that includes the desired initiators and attach it to the volume.

VLAN Segmentation and Tagging

VLANs provide logical segmentation of networks by creating separate broadcast domains, which can span multiple physical network segments. Arrays support VLANs, after the initial array setup has been completed. VLANs can be grouped by departments, such as *engineering* and *accounting*, or by projects, such as *release1* and *release2*. Because physical proximity of the end-stations is not essential in a VLAN, you can disperse the end-stations geographically and still contain the broadcast domain in a switched network. You can also use a Target Subnet List to limit the number of VLAN-tagged subnets that can access an end-station. VLANs provide a number of advantages such as ease of administration, confinement of broadcast domains, reduced network traffic, and enforcement of security policies.

VLAN tagging simplifies network management by allowing multiple broadcast domains or VLANs to be connected through a single cable. This is done by prepending a header to each network frame, which identifies the VLAN to which the frame belongs. Switches can be configured to route traffic for a given VLAN through a certain set of ports that match the VLAN tag.

VLANs and Initiator Groups

An initiator group is a group of one or more initiator names (iSCSI IQNs or Fibre Channel WWPNs) that can be used to grant access to volumes or LUNs in a SAN, or to assign those volumes or LUNs to a VLAN.

The array OS supports the configuration of multiple initiator groups with access control. Access can be added to or removed from a volume by configuring initiator groups. By default, iSCSI volumes are set up with full access, while Fibre Channel volumes are set up with no access.

The array OS also supports the configuration of an initiator group with no access control, by entering "*" in both the IQN and IP fields in the Edit an Initiator Group screen. This configuration allows the initiator group to control access through the Target Subnet List, if selected.

VLANs allow you to have multiple subnets per interface. By selecting the Target Subnet List, you can limit the number of subnets that have access to a volume. This is useful when there are so many subnets that timeouts may occur, for example when subnets need to be scanned on volume restart. It can also be used for security, to prevent certain subnets from accessing the volume.

Major Workflows

The following major workflows tables describe the steps necessary to complete commonly performed end-to-end, multi-task configurations. Each workflow table provides:

- A hyperlinked list of steps (tasks) required to complete each workflow
- Descriptions and guidelines for each step in the workflow

Updating the Array OS Workflow

The array OS is the software that runs on the array. HPE Storage provides regular maintenance releases and periodic updates to the array OS. Before you configure your array, be sure you have the latest version of the array OS installed.

If an array OS update is available for your array, you can download it now and install it later. The GUI has an automated procedure to install updates.

The following table describes the workflow for updating the array OS software on an array:

Step		Notes
1.	Find the Array OS Version on page 30	You must note the version of the array OS currently running on your array to help you select the right update.
2.	(Optional) Download and Update the Array OS without Internet Access on page 31	If your array has Internet access, skip to Step 3. If your array does not have Internet access, you must manually download the array OS update from the support site. To perform this task, you must have access to HPE InfoSight from a PC or other workstation with an Internet connection.
3.	Download and Update the Array OS with Internet Access on page 31	Installs the array OS software update on the array.
4.	Verify the Array OS Update on page 32	After the array OS update has finished, verify that the update was successful.

Provisioning Storage Volumes and Performance Policies Workflow

After an array has been configured, the next step is to create volumes and associate them with one of the performance policies that is included in the array OS package, or create your own performance policy.

The following table describes the workflow for provisioning volumes and performance policies on your array:

Step	Notes
1. Create a Volume on page 65	Use the new volume wizard to create either iSCSI or Fibre Channel volumes on your array.
2. Create a Performance Policy on page 76	A performance policy helps optimize the performance of the volume based on the characteristics of the application using the volume.

Setting Up Replication Workflow

The following table describes the workflow for setting up replication on your volume collections using the GUI:

Step		Notes
1	Create a Replication Partner on page 117	Create a replication partner and add it to the volume collection.
2	Configure Bandwidth Limitations for a Replication Partner on page 141	
3	Test the Connection between Replication Partners on page 119	
4	Add Replication to a Volume Collection on page 120	(Optional) You can add replication to both the upstream and downstream volume collections if replication is not already enabled. If replication is already enabled on both volume collections, you can skip this step.
5	Perform a Volume Collection Handover on page 185	(Optional) You perform this task in a disaster recovery situation. It allows you to copy the current volume collection, move the copy to the downstream replication partner, and make that partner the upstream partner.

Creating a vVol Datastore Workflow

VMware uses virtual volumes (vVols) to manage virtual machines (VMs) and their data (such as VMDKs and physical disks). Supporting vVols enables a volume to reside in a vVol datastore that maps to a folder on an array. A folder can contain both vVols and regular volumes.

vVols are visible in the GUI as regular volumes, where you can monitor their capacity and performance. However, you must use the vCenter UI to manage vVols.

> **Note:** Before configuring vVols, you must have vCenter Server installed and the HPE vCenter Plugin registered with the server. For more information, refer to the VMware vCenter installation documentation.

The following table describes the workflow for creating a vVol datastore.

Keep the following in mind as you perform the steps in the table.

- The database and log files need to be on a separate VMDK.
- You cannot use the VMware synchronous replication feature for volume collections.
- The VSS option to quiesce the operating system is a Microsoft VSS function, not an HPE Storage VSS function.

Step		Interface	Notes
1	Register a vCenter Plugin with vCenter Server on page 81	Array OS	Check the **VASA Provider (vVols)** check box to register the vCenter extension for a VASA provider.
2	Create a Folder on page 83	Array OS	Choose the **VMware virtual volumes (vVols)** from the Management pulldown, then choose a vCenter Server from the VCenter Server pulldown.
3	Create a vVol Datastore	vCenter	For more information about creating a vVol datastore in a folder, refer to the *VMware Integration Guide*.

Restoring Snapshot Data from Clones Workflow

In the rare case that an entire dataset is corrupted, you can restore the entire volume. Restoring a volume from a snapshot replaces the data in the volume with the data that existed when you created the snapshot. Restoring a volume does not destroy the existing snapshot.

The following table describes the workflow for restoring snapshot data from a clone:

Step		Notes
1.	Change the State of a Volume on page 70	Before restoring data from a snapshot, the volume to be restored needs to be taken offline.
2.	Take a Manual Snapshot on page 107	Taking a manual snapshot of the volume saves its most recent state.
3.	Clone a Volume from a Snapshot on page 71	Clone a volume from the snapshot you want to use to restore the data.
4.	Restore a Volume from a Snapshot on page 71	Restoring the volume from the snapshot restores the snapshot data to the volume.
5.	Change the State of a Volume on page 70	After the volume is restored from the clone, you need to set the volume back online.

Hardware and Software Updates

There are several ways to keep an array up-to-date, to improve its performance, and to increase data storage capacity. (The term *upgrade* refers to array hardware.) The term *update* refers to the software.

Upgrades and Updates

There are multiple upgrade paths for hardware, as well as software updates available that you can perform on the array, depending on your array model. If you want to increase data storage capacity, you can add expansion shelves without having to perform an update or upgrade.

Hardware Upgrades

Depending on which model of storage array you have, there are multiple upgrade paths available. Cache, controllers, PCI devices, and capacity can be upgraded independently from each other.

Details about possible upgrades can be found in the compatibility matrix, which can be accessed on InfoSight.

Contact your sales rep when you want to upgrade.

See the applicable upgrade quick start guide that ships with the upgrade component. The Hardware Guide for your array model also covers upgrades.

Updates

There are regular maintenance releases and periodic updates to the array OS. Maintenance releases typically correct bugs and enhance features. Updates involve a major new release of the array OS with new features and capabilities.

If an array OS update is available for your array, you can accomplish the update in less then an hour for each array in the group. (If you want to combine your arrays as members of a group, each of them must have the same array OS version installed.) The update procedure works on one controller at a time and results in a controller failover. To avoid any data service disruption, make sure that the initiators connected to the array have proper MPIO timeouts configured before performing the software update.

If the HPE Storage Toolkit for Windows is not installed on the Windows hosts, be sure to configure timeout values appropriately. See System Limits and Timeout Values on page 200.

The array OS has an automated procedure to download and install updates. Or, you can download the array OS software from InfoSight™ at https://infosight.nimblestorage.com. If you do not have a user account, you can create one on your first visit.

Find the Array OS Version

Complete these steps to determine the array OS version installed on your array.

Procedure

1. In the GUI, choose **Help** > **About Array Group**.
2. Look for the Version number just below the logo.
3. Click **OK** to dismiss the dialog box.

Download and Update the Array OS without Internet Access

Important: This task is required if your storage array has no Internet access.

Procedure

1. In the array GUI, choose **Administration** > **Software**.

   In the Group Software Version area, note the Current version package number. This is the software currently installed on your storage array.

2. From your PC or local host, verify that the array has not been deny listed from the corresponding release.
   a) In a browser window navigate to https://infosight.hpe.com/InfoSight.
   b) Choose **Infrastructure** > **Arrays** > **Select an array** > **Software Recommendations**.
   c) Ensure that the release is not marked as deny listed.

3. Contact support or your local Sales Engineer, who will provide you with a hidden link to the appropriate update file.
4. Use the hidden link to download update file.

   You are required to log in to HPE InfoSight to download the array OS update file.

5. Save the update to a convenient location on your PC or host.
6. In the array GUI, choose **Administration** > **Software**.
7. Click the **Upload** button, then click **Choose File** > **Navigate to**, select the update package saved on your PC or host, and click **Open**.
8. After the upload has completed, choose **Administration** > **Software**.
9. When you see the uploaded array OS file in the Software pane, click **Update**.
10. When the End User License Agreement (EULA) appears, scroll to the bottom of the EULA, check the box, and click **Agree**.

    Note: Installation does not continue until you click **Agree**.

11. Read the Software Update message and click **OK**.
    The array OS update process takes about 70 minutes per array. During that time, a controller failover and a browser reload occur automatically. The array itself remains online and available throughout the update.

    If you have multiple arrays in a storage group, all group arrays are updated, one at a time, to the same array OS version.

    Note: If your connection to the array drops during the update, you might not be able to re-establish connection until the update is done.

    When the update is finished, the new array OS version is listed as the *Current* version and the previous version is listed as *Previous*.

Download and Update the Array OS with Internet Access

Use this task to update your array OS software when the array has an internet connection.

Before you begin
If you have not tested failover recently, you should perform a failover in each direction prior to updating the software to ensure that the software update process is successful.

Procedure

1. Choose **Administration** > **Software**.

2. In the Software pane, click **Download**.
3. In the list of Updates, check the update to install and click **Download**.
4. When you see the update file in the Software pane as *Downloaded*, click **Update**.
5. When the End User License Agreement (EULA) appears, scroll to the bottom of the EULA, check the box, and click **Agree**.

   Note: Installation does not continue until you click **Agree**.

6. Read the Software Update message and click **OK**.
   The update process takes about 70 minutes per array. During that time, a controller failover and a browser reload occur automatically. The array itself remains online and available throughout the update.

   If you have multiple arrays in a storage group, all group arrays are updated, one at a time, to the same array OS version.

   Note: If your connection to the array drops during the update, you might not be able to re-establish connection until the update is done.

   When the update is finished, the new version is listed as the *Current* version and the previous version is listed as *Previous*.

Verify the Array OS Update

Verify that the array OS update installed successfully.

Procedure

1. In the array GUI, click **Events**.
2. In the left pane, scroll down to **Category**, and select **Update**.

   All events in the Category Update are listed.

3. Verify the array OS update by looking in the Events list for two update events.

   A successful software update is indicated by two update events, one each for controller A and B. The Description of the update includes the software version installed.

Network Configuration

A network configuration enables an array to be accessed and managed from the network, communicate with other arrays in a group, carry data traffic, and replicate volumes. It contains all the network parameter settings on an array, including:

- Network configuration profiles
- IP addresses
- Subnets
- Routes
- Network interfaces
- iSCSI connection
- Fibre Channel connection
- VLANs and VLAN tagging

For more information about network considerations during array installation (depending on your topology), refer to the Installation Guide or Hardware Guide for your array model.

Network Configuration Profiles

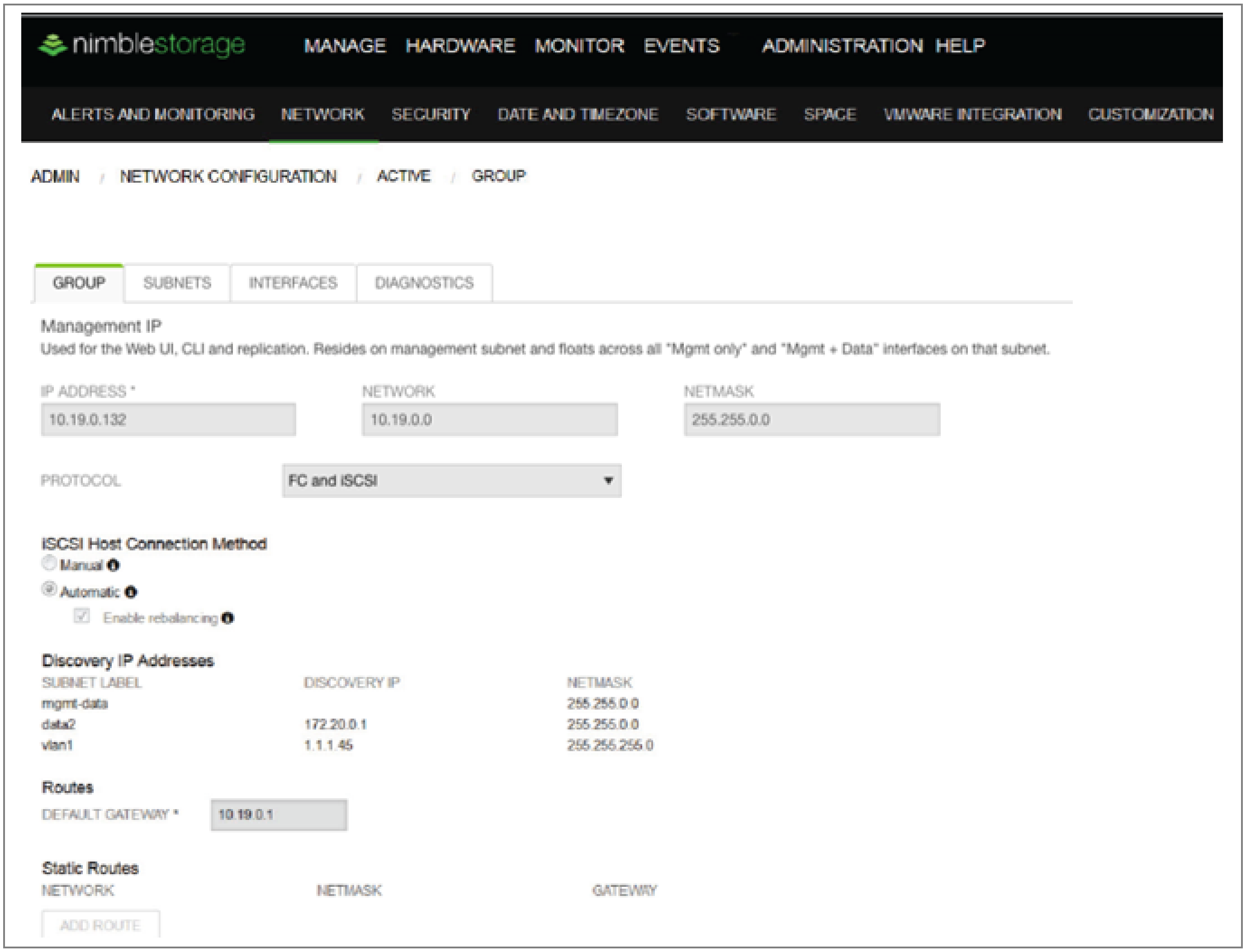
You assign network settings to one of three network configuration profiles: Active, Backup, and Draft. You can make changes to (edit) all three profiles while the array is running.

You can create a Draft profile from an Active or a Backup profile. After you have finished creating a new network configuration using the Draft profile, you can promote it to be the Active profile.

When the Active profile is revised, by being edited or replaced by the Draft configuration, the previous Active profile becomes the Backup profile.

Create a Draft Network Configuration Profile

You can create a Draft network configuration profile from either the Active or Backup profile.



Management IP

Used for the Web UI, CLI and replication. Resides on management subnet and floats across all "Mgmt only" and "Mgmt + Data" interfaces on that subnet.

IP ADDRESS *	NETWORK	NETMASK
10.19.0.132	10.19.0.0	255.255.0.0

PROTOCOL: FC and iSCSI

iSCSI Host Connection Method

○ Manual

● Automatic

☑ Enable rebalancing

Discovery IP Addresses

SUBNET LABEL	DISCOVERY IP	NETMASK
mgmt-data		255.255.0.0
data2	172.20.0.1	255.255.0.0
vlan1	1.1.1.45	255.255.255.0

Routes

DEFAULT GATEWAY *: 10.19.0.1

Static Routes

NETWORK	NETMASK	GATEWAY

SN044

Procedure

1. Choose **Administration** > **Network**.
2. Click **General** for the Settings Summary.
3. Click either **Configure Active Settings** or **View Backup Settings**.
   a) Modify settings on the Group, Subnets, Interfaces, and Diagnostics tabs.
4. Click **Save as Draft**.
   A Draft network configuration profile is created if one does not already exist. If one does exist, a warning is displayed, and you must click **Update** to continue creating a new Draft profile.

Activate a Network Configuration Profile

You can activate the Backup or Draft network configuration profile. When you activate a Draft profile and it becomes Active profile, a Backup profile is automatically created.

If the new Active profile settings are undesirable, you can activate the newly created Backup profile to be the Active profile, which changes the network configuration back to your original settings.

Procedure

1. Choose **Administration** > **Network**.

2. On the General page, click one of the following:
   - **Configure Draft Settings** or
   - **View Backup Settings**
3. Click **Make Active**.
   The Activate draft configuration dialog box is displayed.
4. Click **Make Active**.

   The confirmation dialogs for the Backup configuration and the Draft configuration are different. Choose either:

   - Click **Revert** to make the Backup configuration the new Active profile.
   - Click **Make Active** to make a Draft configuration the new Active profile.

   The selected network configuration profile is activated and becomes the Active profile. The previous Active configuration now becomes the new Backup profile.

Delete a Draft Network Configuration Profile

You can delete an existing Draft network configuration profile.

Procedure

1. Choose **Administration** > **Network**.
2. On the General panel, click **Configure Draft Settings**.
3. Click **Delete**.
   The Draft network configuration profile is deleted.

IP Addresses

An IP address is a 32-bit identifier for devices on a TCP/IP network. IP addresses allow devices on a network, such as servers, switches, and arrays, to communicate with each other. Arrays use IP addresses for the following purposes:

Table 3: Types of IP addresses

IP Address	Purpose
Management	Typically defined on eth1 or on eth1 and eth2 interface, the management IP address provides access to the array OS management interface (GUI, CLI, or API) for the array group. It is also used for volume replication. It resides on the group management subnet and floats across all management only (Mgmt only) and management + data (Mgmt + Data) interfaces.
Secondary	This is a secondary management IP address that is associated with the backup group leader array. In the event of a group leader migration or manual takeover, you can use this IP address to enable the backup group leader to take over the group leader functions. This IP address resides on the group management subnet and floats across all management only (Mgmt only) and management + data (Mgmt + Data) interfaces. While setting up a secondary management IP address is a best practice, it is optional.
Discovery	For iSCSI arrays, each subnet has its own discovery IP address. It enables the iSCSI initiator to discover iSCSI targets for the volumes on the array. You can use this IP address for data as well as management in a single shared network. **Note:** Discovery IP addresses are not required for Fibre Channel arrays.

IP Address	Purpose
Data	One or more IP addresses can be configured to carry data traffic. One data IP address can be configured for each interface pair (corresponding interfaces on the two controllers). Both controllers use the same IP address but never at the same time because only one controller is active at a time. Other data IP addresses can be configured on different subnets. **Note:** In a dedicated network topology, the data IP addresses cannot be the same as the management/iSCSI discovery IP addresses.
Support	Each controller on an array must have a dedicated support IP address, which can be used for troubleshooting and technical support purposes in the event that a controller is not reachable through the management IP address. The support IP addresses must be placed on the group management subnet.

Configure IP Addresses

You can configure management, secondary management, data, and support IP addresses.

Note: You are not required to configure all IP addresses at the same time or to configure them in the order shown in this task.

Procedure

1. Choose **Administration** > **Network**.
2. Click **Configure Active Settings** to make configuration changes in the Active network configuration profile.

   Note: You can also click **Configure Draft Settings** or **View Backup Settings** to make configuration changes in the Draft or Backup network configuration profile, respectively.

3. Click **Edit**.
4. Configure the management and secondary management IP addresses on the **Group** tab in the Management IP section.
   a) On the Primary row, enter the management IP address and subnet netmask. This IP address is used by the group leader array.
   b) (**Optional**) On the Secondary row, enter the secondary IP adddress, which is used by the backup group leader.
5. Configure the management and secondary management IP addresses on the **Subnet Configuration** tab.
   a) On the Primary row, enter the management IP address and subnet netmask. This IP address is used by the group leader array.
   b) (**Optional**) On the Secondary row, enter the secondary IP adddress, which is used by the backup group leader.
6. Configure the data IP address when adding a subnet.
   a) Click the **Subnets** tab.
   b) Specify the parameters to create a new subnet.
   c) In the Assign Interfaces to this subnet section, click an available interface.
   d) In the Interface Assignment section, enter the data IP address in the **Data IP Address** field.
   e) Click **Done**.
7. Configure a data IP address when editing a subnet.
   a) On the **Subnets** tab, select a subnet that is carrying data trafic, and click **Edit**.
   b) In the Interface Assignment section, enter the data IP address in the **Data IP Address** field.
   c) Click **Done**.
8. Configure a data IP address when you configure an interface.
   a) Click the **Interfaces** tab.
   b) Select an interface assigned to a subnet carrying data traffic, and click **Edit**.

c) Check the checkbox to select the interface that you want to configure.
d) Click **Configure**.
e) Select the Subnet from the dropdown menu if it is not already selected by default.
f) If necessary, specify the data IP address for the subnet to which the interface is assigned.
g) Click **Done**.

9. Configure the Support IP addresses.

a) Click the **Diagnostics** tab.
b) Specify the IP addresses for Controller A and Controller B.

10. Click **Save**.
The array OS validates the configuration, and commits the configuration if no error exists. If an error does exist, array OS returns an error message.

Subnets

A subnet is logical subdivision of a network. It is defined by the first IP address in the network and a netmask that specifies a contiguous range of IP addresses within that network. A subnet can be assigned to one or more network interfaces.

The maximum Transmission Unit (MTU) can be set for a subnet so that it uses either a standard, jumbo, or custom frame size. If you choose to use a custom frame size, you must specify the size in bytes.

Specifying a VLAN ID on a subnet allows an interface to be assigned to more than one subnet using IEEE 802.1Q tagged frames. Switch port configuration must match the VLAN IDs configured on the subnets for tagged assignments. For more information, refer to the procedure to Configure VLAN Tagging in the *GUI Administration Guide* or *CLI Administration Guide*.

Note: The arrays in a group communicate with each other on the “native vlan”. The native vlan can be enabled on any subnet; however, there needs to be at least one subnet in which “untagged” traffic is allowed. This native vlan is used when merging a group, adding and removing an array, updating a group configuration, and updating network configurations.

Subnet Traffic Types

Traffic types are used to segregate network traffic into different subnets. A subnet can carry one of the following traffic types.

Table 4: Traffic Types

Traffic Type	Description
Management (Mgmt only)	The subnet carries only management traffic.
Data (Data only)	The subnet carries only data traffic.
Management and Data (Mgmt + Data)	The subnet carries both management and data traffic.

Subnet Traffic Assignments

Traffic assignments determine what type of iSCSI traffic a subnet carries. A subnet can have one of the following traffic assignments.

Note: Traffic assignments are not required for Fibre Channel arrays.

Table 5: Traffic Assignments

Traffic Assignment	Description
iSCSI + Group	The subnet carries both iSCSI data traffic and intra-group communication (traffic between arrays in a group).
iSCSI only	The subnet carries only iSCSI data traffic.
Group only	The subnet carries intra-group communication traffic.

IP Address Zones in Subnets

An IP address zone is a group of host IP addresses and array data IP addresses in a subnet. When using two switches for iSCSI traffic, hosts can achieve better performance by establishing iSCSI connections with data IP addresses inside the same zone, as opposed to establishing iSCSI connections with data IP addresses in a different zone.

Note: IP address zones are not required for Fibre Channel arrays.

The IP addresses within a subnet can be divided into the following IP address zone types:

Table 6: IP Address Zones Types

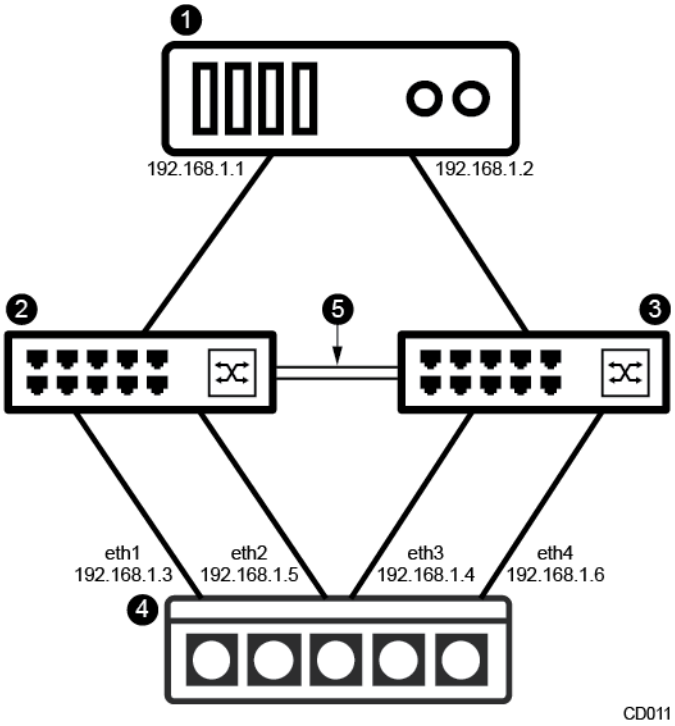
Zone Type	Description
None	Used for non-iSCSI enabled subnets.
Single	All IP addresses are in one zone. This is the default zoning setting. With two network switches, iSCSI connections can be routed over the inter-switch link.
Bisect	One zone includes the IP addresses from the top half of the subnet; for example, 192.168.1.128 to 192.168.1.254. The other zone takes the IP addresses from the bottom half of the subnet; for example, 192.168.1.1 to 192.168.1.127
Even/Odd	The IP addresses are grouped by their last bit. One zone includes the even-numbered IP addresses, such as 192.168.1.2, 192.168.1.4, 192.168.1.6, and so on. The other zone includes the odd-numbered IP addresses, such as 192.168.1.1, 192.168.1.3, 192.168.1.5, and so on.

IP address zones are useful for configurations that use two switches, where you want to establish connections that avoid the Inter-Switch Link. For IP address zones to work, the host and the array must have its data IP addresses configured with half of its IP addresses from one zone connected to one switch and the other half of its IP addresses from the other zone connected to the other switch. For example, assume that:

- There is single subnet, 192.168.1.0/24.
- There are two zones, defined as Red and Blue.
- Red zone consists of:
  - Host IP 192.168.1.1
  - Array Data IP 192.168.1.3
  - Array Data IP 192.168.1.5
- Blue zone consists of:
  - Host IP 192.168.1.2
  - Array Data IP 192.168.1.4
  - Array Data IP 192.168.1.6

In the IP Address Zone, the host IP addresses in the Red zone only establish connections with the data IP addresses in the Red zone. And the host IP addresses in the Blue zone only establish connections with the data IP addresses in the Blue zone. In this way, iSCSI connections do not use inter-switch link and thereby maximize I/O performance.

Figure 3: IP Address Zones



1	Host	**4**	Array
2	Switch 1	**5**	Inter-switch link
3	Switch 2		

Configure a Subnet

You can configure one or more subnets.

Procedure

1. Choose **Administration** > **Network**.
2. Click **Configure Active Settings** to make configuration changes in the Active network configuration profile.

   Note: You can also click **Configure Draft Settings** or **View Backup Settings** to make configuration changes in the Draft or Backup network configuration profile, respectively.

3. Click **Edit**, then click the **Subnets** tab.
4. Do one of the following:
   - Click **Add** to configure a new subnet.
   - Check the checkbox nest to an existing subnet and click **Edit** to change its settings.
5. Configure the subnet settings.

   Note: If you choose the Custom frame size, you must specify the size in the Bytes field.

   If you want to specify a VLAN ID, you can find more information in Configure VLAN Tagging on page 45.

6. Click an available interface to assign to the subnet, specify the data IP address (if required), then click **Done**.
7. (Optional) Repeat the steps to configure more subnets.
8. Click **Done**.
   The array OS validates the configuration change and commits the configuration if no error exists. If an error does exist, the array OS returns an error message.

Delete a Subnet

You can delete one or more subnets.

Procedure

1. Choose **Administration** > **Network**.
2. Click **Configure Active Settings** to make configuration changes in the Active network configuration profile.

   > **Note:** You can also click **Configure Draft Settings** or **View Backup Settings** to make configuration changes in the Draft or Backup network configuration profile, respectively.

3. Click **Edit**.
4. Click the **Subnets** tab.
5. Check the checkbox nest to an existing subnet then click **Delete**.
   A warning is displayed. Click **OK** to continue.
6. Repeat Step 5 to delete more subnets.
7. Click **Update**.
   The array OS validates the configuration change and commits the configuration if no error exists. If an error does exist, the array OS returns an error message.

Routes

Routes are paths from one network location to another; static routes are paths that do not dynamically change with changing network conditions. You can add static routes to a network configuration. For example, if you want an array to use a specific path through the network to reach a gateway, you can create a static route to the gateway.

To create a static route, you specify a subnet (network address and netmask) and the gateway IP address within the subnet.

> **Note:** The default gateway IP address is in the same subnet as the management IP address.

Configure a Static Route

You can onfigure one or more static routes.

Procedure

1. Choose **Administration** > **Network**.
2. Click **Configure Active Settings** to configure IP addresses in the Active network configuration profile.

   > **Note:** You can also click **Configure Draft Settings** or **View Backup Settings** to configure IP addresses in the Draft or Backup network configuration profile, respectively.

3. Click **Edit**.
4. On the Group tab, in the Routes section, click **Add Route**.
5. Specify the IP address and netmask of a configured subnet.

   The route will run on the specified subnet.

6. Specify the gateway IP address.

   Note: The gateway IP address must must be in the specified subnet.

7. Click **Save**.
   The array OS validates the configuration change, and commits the configuration if no error exists. If an error does exist, the array OS returns an error message.

Delete a Static Route

You can delete one or more existing static routes.

Procedure

1. Choose **Administration** > **Network**.
2. Click **Configure Active Settings** to configure IP addresses in the Active network configuration profile.

   Note: You can also click **Configure Draft Settings** or **View Backup Settings** to configure IP addresses in the Draft or Backup network configuration profile, respectively.

3. Click **Edit**.
4. On the Group tab, in the Routes section, click the delete icon next to an existing static route.

   The static route is deleted.
5. Click **Save**.
   The array OS validates the configuration change, and commits the configuration if no error exists. If an error does exist, the array OS returns an error message.

Configure the Default Gateway

You can configure the default gateway for the array.

Procedure

1. Choose **Administration** > **Network**.
2. Click **Configure Active Settings** to configure IP addresses in the Active network configuration profile.

   Note: You can also click **Configure Draft Settings** or **View Backup Settings** to configure IP addresses in the Draft or Backup network configuration profile, respectively.

3. Click **Edit**.
4. On the Group tab, in the Routes section, specify the default gateway IP address.
5. Click **Save**.
   The array OS validates the configuration change, and commits the configuration if no error exists. If an error does exist, the array OS returns an error message.

Network Interfaces

Network interfaces are logical representations of physical ports on Ethernet Network Interface Cards (NICs) or Fibre Channel Host Bus Adapters (HBAs). For iSCSI traffic, each Ethernet interface must be assigned a configured subnet, and the same subnet can be assigned to multiple interfaces. You can also enable or disable VLAN tagging for each subnet on each Ethernet interface.

Fibre Channel arrays have both Ethernet and Fibre Channel interfaces. The Ethernet interfaces on a Fibre Channel array are used only for management, intra-group communication, and replication traffic; Fibre Channel interfaces are used for data traffic only. Fibre Channel interfaces do not require an assigned subnet. Instead, WWPNs are automatically assigned to them.

Configure an iSCSI Interface

You can add or remove an iSCSI interface to or from one or more subnets.

Procedure

1. Choose **Administration** > **Network**.
2. Click **Configure Active Settings** to configure an interface in the Active network configuration profile.

   Note: You can also click **Configure Draft Settings** or **View Backup Settings** to configure an interface in the Draft or Backup network configuration profile, respectively.

3. Click **Edit**.
4. Click the **Interfaces** tab.
5. Check the checkbox next to the interface to be configured then click **Configure**.
6. Add or remove the interface to or from subnets as follows:
   - Click **Add to another Subnet** and choose a subnet on which to add the interface. If you choose a data subnet, you must specify the data IP address. If the subnet has a VLAN ID, VLAN tagging is automatically enabled. You can uncheck **Tagged** to disable VLAN tagging.
   - Click the delete icon to remove the interface from a subnet.
7. Click **Done**, then click **Save**.
   The array OS validates the configuration change, and commits the configuration if no error exists. If an error does exist, the array OS returns an error message.

Unconfigure an iSCSI Interface

You can unconfigure an iSCSI interface by removing it from all subnets.

Procedure

1. Choose **Administration** > **Network**.
2. Click **Configure Active Settings** to configure an interface in the Active network configuration profile.

   Note: You can also click **Configure Draft Settings** or **View Backup Settings** to configure an interface in the Draft or Backup network configuration profile, respectively.

3. Click **Edit**.
4. Click the **Interfaces** tab.
5. Select the interface to be unconfigured, then click **Unconfigure**.
6. Click **Done**, then click **Save**.
   The array OS validates the change. If an error exists, the array OS returns an error message.

Set a Fibre Channel Interface Administrative State

You can set the administrative state for one or more Fibre Channel interfaces to either online or offline.

Procedure

1. Choose **Administration** > **Network**.
2. Click **Configure Active Settings** to configure an interface in the Active network configuration profile.
3. Click **Edit**.
4. Go to the **Interfaces** tab, then click the **Fibre Channel** tab.
5. Check one or more interfaces.

6. Click **Set Online** or **Set Offline**, then click **Save**.
   The array OS changes the administrative state for the selected Fibre Channel interface(s) to online or offline. Interfaces connected to initiators will drop their connection when set to offline.

Fibre Channel Interfaces

Each storage system with Fibre Channel interfaces has a unique 64-bit WWNN of the form `56:C9:CE:90:xx:xx:xx:00`, where the `xx:xx:xx` is generated pseudo-randomly as part of the setup process. Each interface has a unique 64-bit WWPN where the last octet is numbered sequentially starting from 01. Unlike iSCSI interfaces, the WWPN is not shared between controllers. Rather, the WWPNs are numbered in order from the lowest interface to the highest interface (for example, fc1.1, fc2.1, fc5.1, etc.) starting first with controller A, and then controller B. If you add an additional card or cards of Fibre Channel interfaces in the future, the original cards will keep their WWPNs, and the new cards will get the next available sequence of WWPNs after the rescan is initiated with the CLI command fc update_config.

This predictable WWN scheme allows you to do things like plan a maintenance window to switch zoning before a new storage array arrives. To do this, use the `fc regenerate_wwn wwnn_base` command to alter the WWNN base. The WWNN base can be any value between 00:00:01 and FF:FF:FF (inclusive). When the WWNN base is changed, the WWPNs are also renumbered back to their default order as described above.

Note: All Fibre Channel interfaces must be both administratively and operationally offline before proceeding. After the regenerate completes, all interfaces will be brought back online.

Note: It is the customer’s responsibility to avoid having duplicate WWWN’s. For high availability, HPE Best Practices recommend having dual fabrics with hosts connected to both. Similar to the Even/Odd IP address zone used by iSCSI network interfaces, HPE Best Practices recommend having all odd numbered ports (01, 03, 05...) connected to one fabric and all even numbered ports (02, 04, 06...) connected to the other fabric.

See the fc command in the *Command Reference* for more details.

iSCSI Host Connection Methods

The iSCSI initiators on the host system connect with targets on the array through the data ports on each controller. Each port is identified by its IP address. Normally, the array OS selects the IP address for each connection automatically. Hosts connect to the Virtual Target IP addresses, then the connection is automatically redirected to an appropriate iSCSI Data IP address.

The default iSCSI host connection method for the array OS releases earlier than 2.0 is *Manual*, but the default iSCSI host connection method for the array OS 2.0 and later releases is *Automatic*. However, after upgrading from a pre-2.0 release, hosts will continue to connect manually to iSCSI data IP addresses. To remedy this, install the Host Integration Toolkit on supported hosts and then change the iSCSI host connection method from Manual to Automatic. The Connection Service (CS) changes the iSCSI connections to connect to discovery IP addresses instead of data IP addresses, and NCS maintains the optimal number of connections. On the remaining hosts, change the iSCSI connections to connect to discovery IP addresses instead of data IP addresses. After all iSCSI connections are changed to connect to Virtual Target IP addresses, enable iSCSI connection rebalancing in order for the array OS to automatically rebalance iSCSI connections when distribution of connections becomes unbalanced.

If a Layer 2 inter-switch link that cannot handle the volume of iSCSI traffic is present, set up IP address zones before enabling the Automatic iSCSI host connection method. Generally speaking, a Layer 2 inter-switch link is used when traffic to different iSCSI data IP addresses goes through different switches on the same subnet.

Automatic iSCSI Host Connections

The Automatic iSCSI connection method uses data subnet discovery IP addresses for host connection. The array then automatically redirects the connection to an appropriate iSCSI data IP address. The Automatic method is the better choice for most applications.

Use a data subnet discovery IP address to connect from the host to the array.

Note: The iSCSI host-to-array connection process is faster and simpler when you install and use HPE Connection Manager on your Windows or VMware host.

See the *Windows Integration Guide* and the *VMware Integration Guide*.

Manual iSCSI Host Connections

For pre-array OS 2.0 releases, hosts connect manually to iSCSI data or discovery IP addresses. The same is true for array OS 2.0 and later releases when the iSCSI connection method set to *Manual*. The Manual method is provided for legacy applications to upgrade to array OS 2.0 or later, make configuration changes, and switch to the automatic method.

Use a data subnet discovery IP address to connect from the host to the array.

Note: The iSCSI host-to-array connection process is faster and simpler when you install and use HPE Connection Manager on your Windows or VMware host.

For more information, refer to the *Windows Integration Guide*, and the *VMware Integration Guide*.

Set the iSCSI Host Connection Method to Manual

The manual iSCSI host connection method is intended primarily so that you can configure legacy applications to use the automatic connection method after upgrading to array OS 2.0 or later. (Neither option applies to Fibre Channel arrays.)

Procedure

1. Go to **Administration** > **Network**.
2. Click **Configure Active Settings** to configure an interface in the Active network configuration profile.
3. Click **Edit**.
4. On the **Group** tab, in the iSCSI Host Connection area, click **Manual**.
5. Click **Save**.

VLAN Support and VLAN Tagging

The array supports the configuration of VLANs, and provides a way to tag/untag frames on iSCSI or Fibre Channel arrays for specified VLANs.

Note: VLANs can only be configured for use with an array after the array setup has been completed.

About VLANs

VLANs provide logical segmentation of networks by creating separate broadcast domains, which can span multiple physical network segments. They can be grouped by departments, such as *engineering* and *accounting*, or by projects, such as *release1* and *release2*. VLANs provide a number of advantages:

- Ease of administration — VLANs enable logical grouping of end-stations that are physically dispersed on a network. This aids in speed, efficiency, and accuracy of provisioning the right LUN to the right client.
- Access control — VLANs enforce security policies by separating different environments for security and compliance.
- Reduction of network traffic — By confining broadcast domains, VLANs reduce the need to have routers deployed on a network to contain broadcast traffic. In addition, end-stations on a VLAN are prevented from listening to or receiving broadcasts not intended for them. If a router is not connected between the VLANs, the end-stations of a VLAN cannot communicate with the end-stations of other VLANs.

VLANs have IDs from 1 to 4094. The array allows a single VLAN ID to be assigned to a single subnet. A subnet without a VLAN ID belongs to the default VLAN. In a group of arrays, certain restrictions apply:

- A subnet must be assigned to at least one interface on each array in the group.
- A group can have a maximum of 60 subnets, including the management subnet.

- Each array in a group can have a maximum of 120 subnet-to-NIC assignments.

Target Subnet List

Because VLANs allow you to have multiple subnets per interface, you may want to limit the number of subnets that have access to a given volume. You do this using the Target Subnet List. This is useful when there are so many subnets that timeouts may occur, for example, when subnets need to be scanned upon volume restart. It can also be used for security, to prevent certain subnets from accessing the volume.

You access the Target Subnet List when creating initiator groups.

About VLAN Tagging

Multiple VLANs can be connected through a single cable using the VLAN tagging feature. A VLAN tag is a unique identifier (between 1 and 4094) included in the 802.1Q frame header that corresponds to the ID of the VLAN to which the frame belongs. When a switch receives a tagged frame, it forwards that frame to the appropriate VLAN. A tagged frame belongs to the VLAN specified by the tag. An untagged frame belongs to the default VLAN. The array supports both tagged and untagged traffic on the same interface.

Tagged and Untagged VLAN Subnets

The VLAN tag attribute of an interface determines whether the subnet to which that interface belongs is tagged or untagged. Interfaces that have VLAN tagging enabled are exposed to the network with that subnet's VLAN ID. While a subnet can accept both tagged and untagged traffic, all tagged interface assignments must use the same VLAN ID. For each subnet, the interfaces at both ends of the network link (switch end and device end) must be assigned either tagged or untagged.

For more information, see Move an Array from One Tagged VLAN to Another on page 46.

VLAN tagging is supported on both iSCSI and Fibre Channel subnets. For Fibre Channel, VLAN tagging is supported on management subnets only. For iSCSI, VLAN tagging is supported on both management and data subnets.

Configure VLAN Tagging

To enable VLAN tagging, first be sure a subnet has been created with a valid VLAN ID. (Subnets without a VLAN ID can only accept untagged traffic.) Then, assign network interfaces on an array to this subnet, and specify the interfaces as tagged. For more information on how to do this, see Configure a Subnet on page 39.

The procedure below describes how to configure an existing subnet from the **Subnets** tab. You can also perform the same subnet configuration from an interface-centric view using the **Interfaces** tab.

> **Note:** Do not use the same network for both back-end and front-end traffic. Heavy usage on one side will cause latency or congestion issues on the other side, and there will be a cascading impact to the overall environment.

Before you begin

You must already have VLANs created on your network.

Procedure

1. Go to **Administration** > **Network**.
2. Click **Configure Active Settings**, and then click the **Subnets** tab.
3. Click **Edit**.
4. Select a subnet to configure.
   - If no subnets are listed, create one by clicking **Add** and filling out the fields at the top of the screen.
   - If subnets are listed, check the subnet you want to configure and then click **Edit**.
5. In the **Edit** section, assign a valid VLAN ID to the subnet.

   If a valid VLAN ID is already assigned to this subnet, you can skip this step.

6. In the **Assign interfaces to this subnet** section, click on the interfaces to assign them to the subnet for the specified VLAN. The interfaces you select are listed as **Tagged** in the **Interface Assignment** section. Note that you can still uncheck the **Tagged** checkbox if the interface has not been assigned to other subnets for untagged traffic.
7. In the **Interface Assignment** section, review the data IP address for the interfaces you have assigned to ensure they are correct.. Review the **Tagged** checkboxes to ensure VLAN tagging is enabled on the appropriate interfaces.
8. Click **Done**.

Remove VLAN Tagging

The procedure below describes how to remove VLAN tagging from an existing subnet from the **Subnets** tab. You can also perform the same task from an interface-centric view using the **Interfaces** tab.

Procedure

1. Go to **Administration** > **Network**.
2. Click **Configure Active Settings**, and then click the **Subnets** tab.
3. Click **Edit**.
4. Check the subnet containing the interfaces for which you want to remove VLAN tagging, and then click **Edit**.
5. In the **Interface Assignment** section, uncheck the Tagged checkboxes next to each interface for which you want to remove VLAN tagging.
6. Click **Done**.

Move an Array from One Tagged VLAN to Another

The workflow below describes how to successfully move an array from one tagged VLAN to another without losing connectivity to the array. Using this method, there is always at least one path to the host, and downtime is avoided.

Procedure

1. Be sure there are at least two links between the host and the array.
2. Untag one of the links.
3. Move that link from the old host to the new host. The array is still visible on the old host using the tagged link, and is now also visible on the new host using the untagged link.
4. Untag and move the second link from the old host to the new host. Repeat this until all links have been untagged and moved.
5. Tag the links with a new VLAN ID, if desired.

Array Groups

Array groups are collections of up to four arrays that are managed as a single entity. Grouped arrays allow you to aggregate for increased performance and capacity. For iSCSI arrays, grouping makes multi-array storage pools possible.

Note: If you have configured synchronous replication and want to enable the Automatic Switchover feature, the array group can only consist of two arrays. For more information, see Synchronous Replication on page 121.

Once an array is initialized, it becomes a group of one. When a group contains only one array, the GUI simplifies the presentation by hiding some group and pool features that apply only to multi-array groups.

If other arrays are added to this group, that first array becomes the group leader. You can then access the added arrays using the management IP address of the group leader.

Multiprotocol Array Groups

Version 5.1.x and later supports multiprotocol array groups, providing the ability to present volumes to iSCSI or Fibre Channel (FC) hosts from the same array.

The multi-protocol feature enables you to use both iSCSI and FC protocols simultaneously on a single array or group to access different volumes.

A volume can be accessed via FC on an array where other volumes are accessed via iSCSI. This feature provides flexibility in environments with both iSCSI and FC hosts, and it facilitates migrating from one protocol environment to the other.

Note the following prerequisites and limitations for multiprotocol support:

- Every array in the group must have similar hardware capabilities. At least one FC HBA or one iSCSI NIC is required per controller.
- Protocols are enabled on the entire group. Every array in the group has the same protocols enabled.
- When Peer Persistence is deployed, only one protocol is permitted on the arrays in the group, and both arrays must use the same protocol.
- A volume can only be accessed via one protocol at a time.
- An initiator group cannot contain a mix of iSCSI and FC hosts.
- SMI-S does not support using multiprotocols.

Note: See the *CLI Administration Guide* for information about enabling or disabling both iSCSI and FC on an array.

Group Leader Array

In a multi-array group, the array serving as the group leader maintains configuration data and hosts the management IP address. In a group of iSCSI arrays, all communication received at the discovery IP address is sent to the leader of the group. Fibre Channel arrays do not use the discovery IP address.

Note:

If an array is the group leader, it cannot be removed from the group. You can use the CLI command **group --status** to determine whether there is a backup group leader array, and if it is in sync with the group leader array.

The backup group leader array stores configuration data that is a replica of the data on the group leader. You can migrate the group leader functions from the group leader array to the backup group array by executing the CLI command **group --migrate** from the group leader array.

After the migration task is completed, the backup group leader becomes the group leader and you can remove the array that was previously the group leader.

Backup Group Leader Array

The backup group leader array helps you maintain service and ensure high availability if the group leader array becomes unresponsive or there is a planned outage that affects the group leader. The backup group leader stores replicated configuration data. It keeps this data in sync with the group leader data.

Each group can have one backup group leader.

A backup group leader enables you to:

- Migrate the functions of the group leader array to the backup group leader array.

  When you have a backup group leader set up, you can migrate the current group leader to the backup group leader. Doing this lets you seamlessly accommodate any scheduled issues that require you to halt or remove the group leader array.

  You initiate a migration from the group leader array using either the GUI or the CLI:

  - **GUI method**: Attempt to shutdown the group leader array from the GUI. The system displays a message stating that the array is performing management services and asking if you want to migrate the group leader to the backup group leader before halting the array. If you select this option, the array OS automatically performs the migration.
  - **CLI method**: From the group leader array, run the following commands:
    - **group --check_migrate** to confirm that it is OK to perform the migration. You can perform a migration operation only if the backup group leader array is in synch with the group leader array.
    - **group --migrate** to migrate the group leader functions to the backup group leader.

  After your backup group leader becomes the group leader, you can specify a different secondary management IP address to designate another backup group leader.

- Set up Automatic Switchover (ASO) to enable the backup group leader to automatically take over the group leader role if it detects that the group leader is unresponsive. ASO automatically creates a backup group leader.

  If the backup group leader can no longer get a response from the group leader, ASO promotes the backup group leader array to the group leader array.

  To use ASO, you must either install and configure a Witness daemon on a Linux server, or run the daemon in a separate VM. For information about ASO, see Automatic Switchover (ASO) on page 125.

- Perform a manual takeover using the OS CLI **group --takeover** command to promote the backup group leader array to group leader. You must run this command from the backup group leader. You cannot perform this operation if you have ASO enabled and a witness installed.

  Note: You should take down your cluster before you perform a manual takeover. This enables you to have a predictable recovery and avoid having host interactions while changes are being made on the array side. If Peer Persistence (synchronous replication and ASO) is not configured when the group leader goes down, the host generally loses access to all Group Scoped Target (GST) LUNs.

  Before you can perform a takeover, the following two conditions must be true:

  - The OS CLI **group --check_takeover** command says it is OK to perform a takeover.
  - The group leader array is unresponsive and cannot be reached by the backup group leader array.

Secondary Management IP Address and Backup Group Leader

You have the option of setting up a secondary management IP address that is used for the backup group leader array. Like the management IP address, the secondary management IP address is a floating address that floats to where the background group leader goes. The secondary management IP address enables you to quickly access the backup group leader in the event that the group leader becomes unresponsive.

Note: While adding a secondary management IP address is optional, it is a good practice to set one up. If there is not a backup group leader, this address is not used.

The secondary management IP address must be a unique IP address that is on the management subnet reserved for the backup group leader array.

Methods for Setting Up a Secondary Management IP Address to Use for a Backup Group Leader

Creating a secondary management IP address is a best practice; however, it is not required. The advantage of having a secondary management IP address is that it lets you quickly and easily identify the backup group leader array.

If you decide to configure a secondary management IP address, you can use one of the following methods. You can set up a secondary management IP address:

- During the the array configuration process. See the hardware installation guide for instructions.
- Using the CLI command **setup --backup_mgmt_ipaddr** **<***ipaddr***>** on the backup group leader array.
- Using the CLI command **ip –add** **<***backup_mgmt_ipadd***>**.
- From the GUI. Select **Administration** > **Network** > **Configure Active Settings** > **Group**. Click **Edit** to add or modify a secondary management IP address.

Note: The backup group leader secondary management IP address is not accessible until the backup group leader becomes active.

Adding Arrays to a Group

You can add a configured (initialized) or unconfigured (uninitialized) array to an existing group.

Add an Unconfigured Array to a Group

Note: The operation can take several minutes.

Before you begin

Every unconfigured array that is added to the group must:

- Use the same Layer 2 network as the group leader array
- Run the same version of the OS as the group leader array
- Use a compatible access protocol, iSCSI, Fibre Channel, or both (multiprotocol). All arrays in a group must use the same protocol.

If the destination group has a backup group leader with a secondary management IP address, you will not be able to modify that IP address.

Procedure

1. Log into the group leader array (the array to which you will be adding the unconfigured arrays).
2. Click **Hardware**.
3. Choose **Actions** > **Add Array to Group**.

   A list of arrays is displayed. The GUI displays error icons for incompatible arrays. Mousing over an error icon displays a list of errors that must be resolved before you can add the array to the group.

4. Note the version of each array.

If the array OS version of the array you want to add matches the array OS version on the configured array, you can add the array. Otherwise, you must update the version of array OS on the array before you can add it.

> **Note:** You are not able to install updates on an unconfigured array. You must complete the array setup to perform software updates. For more information, see Hardware and Software Updates on page 30.

5. Enter a name for the array in the field under Array Name.
6. Under Interface Assignment, add the Data IP address for each NIC interface (eth or tg port) for interfaces set to Data only or Management + Data.
7. Under Diagnostics, type the support IP addresses for Controller A and Controller B.
8. Under Storage Pool, complete one of the following actions:
   - (Default) Create a new storage pool and assign it to the array. Enter the name of the new pool in the field provided.

     or

   - Assign an existing storage pool to the array. Choose the pool name from the drop-down list.
9. Click **OK**.

   The array is added to the group.

Add a Configured Array to a Group (Group Merge)

A configured array is a group of one. Therefore, adding a configured array to a group is the same procedure as merging two groups of arrays. You can merge two groups of arrays that are accessed with either iSCSI, Fibre Channel, or multiprotocol (both iSCSI and Fibre Channel). The array that is being merged into the target is the *source* group, and the target array is the *destination* group.

> **Note:** There is no way to unmerge groups. To undo a merge, you must remove the arrays from the merged group. You can then create a new group for those arrays, if desired.

Before you merge two groups, verify the following requirements.

Platform Compatibility Notes:

- You cannot merge two groups of arrays that have different access protocols. Both groups must use iSCSI, Fibre Channel, or iSCSI and Fibre Channel (multiprotocol).
- You can add multiple FC arrays to the same group.
  - Array OS 3.x.x.x or later is required.
  - Fibre Channel WWPNs will change for the array added to the group. You must adjust zoning appropriately to reflect this.
- All Flash (AFA), Hybrid Flash (HFA), and Secondary Flash (SFA) arrays can be merged into the same multi-array group.
  - Pools of different array types (AFA, HFA, and SFA) cannot be merged into a single multi-array pool.
  - Only pools from the same array type can be merged into a multi-array pool.
- To move data from one array to another, you can add an AFA to an existing HFA or SFA group, migrate to the AFA using volume move, and remove the old array non-disruptively.
  - Array OS 4.x.x.x or later is required.
  - For more information, see KB-000277 Array Data Migration
- To move data from one array to another, you can add an HFA or SFA to an existing AFA group, migrate from the HFA or SFA to AFA, and remove the HFA or SFA array.
  - This process is disruptive to host I/O since this iSCSI arrays will undergo a discovery IP change.
- If the same CHAP username is configured on both the source and destination groups, only the CHAP user on the destination array will be used after the merge.

- If secure shell (SSH) keys exist for users of the same name on source and destination groups, the SSH keys for the destination group will be used. SSH keys for the user in the source group will be discarded.

Verify the following:

- Both groups use the same data and management subnets.
  - All array groups to be merged must have the same subnets defined using the same subnet names
  - All interfaces assigned to a given subnet must be able to reach each other, regardless of which array they are located on.
  - All interfaces within a given subnet must be within the same broadcast domain (the L2 or layer 2 network segment).
  - All interfaces in a particular subnet must be in the same VLAN, and any inter-switch links that exist between those interfaces must be configured to allow the same VLAN
  - The array will have one or more subnets tagged as Allow Group. For any subnet where Allow Group is set to Yes, the switch ports connected to those arrays need to also be in the same native VLAN.
  - No more than four data subnets can exist.
- Both groups use the same data protocol (iSCSI, Fibre Channel, or multiprotocol) and the data ports must be connected.

> **Note:**
>
> If necessary, you can modify the management subnet to carry data and management traffic.
>
> Data Discovery IP addresses must be added for group traffic between the arrays.

- All arrays to be merged that have Active Directory integration enabled must be configured to use the same Active Directory domain for authentication.
- Both arrays are in an active or standby state.
- Both arrays have the same array OS version.
  - If they do not, update one or both arrays. To learn more about updating the array OS, see Updates on page 30.
- Not more than one of the groups contains partners with synchronous replication.
- Throttle levels are the same for both groups.
  - Group-level throttles from the joining group are automatically discarded and the hosting group throttles are automatically applied. If the throttle levels are set differently on the two arrays that are associated with the source and destination groups, adjust the throttle level on the destination group based on your environment and requirements.
- Arrays must have the same maximum transmission unit (MTU) setting on configured subnets.
- Switches and inter-switch links must have their MTUs set to a value equal to or greater than the MTU used on group members.
  - Note that some switches require that the MTU be set higher than the value on the array, due to differences in how they calculate the value of the MTU.
  - There are no consequences to setting the switch MTU to the largest reasonable value, often as high as 9214 or 9216 bytes.
- Both groups must be on the same L2 network or broadcast domain

  Both groups must also be in the same VLAN, on the same switch or switch-stack, or on switches connected via an inter-switch link or trunk.

Notes on Names:

- All array names in your environment must be unique.
- iSCSI subnet label names on both arrays must be the same.
- Group names must be unique and short enough to avoid truncation when merged.
- The group name must be different from the name of the array being added.
- Volume names cannot be re-used on the source and destination groups.

- All initiator group names must be unique.
  - Initiator IQNs on the source and destination, if matching, must also use the same case.
- All protection schedule names must be unique.
- The names for all new pools must contain fewer than 64 characters, if you intend to merge two groups.
  - If the name of the source group is short enough to form a new pool name that is less than 64 characters, then truncation does not occur. However, if the source group has a long name, such as a 63-character name, then the new pool name results in more than 64 characters. In this case, the name is automatically truncated to the limit of 64 characters.
- Other than the default pool, pool names on the source and destination groups must be unique.
  - The default pool on the source group will be renamed `default-source_group_name`.
  - A group named `default-source_group_name` cannot exist on the destination group.

Pre-Merge Tasks

Note:

- Array OS 4.X is required.
- Merging an iSCSI array and a FC array together in the same group is not supported.
- You cannot perform a pool merge between different array types, for example AFA, HFA and SFA.
  - To add an AFA to an existing HFA or SFA group and keep both (with their own pools), you must migrate to the AFA and remove the old array non-disruptively.

    For more information, see *KB-000277*.
  - To add an HFA or SFA to an existing AFA group, you must migrate from the HFA or SFA to AFA, and remove the HFA or SFA array.
  - This process is disruptive to host I/O and not recommended for iSCSI arrays which will undergo a discovery IP change.
  - Deduplication Domains cannot be merged, see Domains on page 88 for details.

Verify the following factors:

- Both arrays are in an active or standby state and are running the same array OS version.

  If not, update one or both arrays. To learn more about updating the array OS, refer to the Installation Guide or Hardware Guide for your array model.
- Switches and inter-switch links must have their MTU's set to a value.
- One or more subnets must be set to include group traffic in the **Traffic Assignment** menu. For any subnet where Allow Group is set to Yes, the switch ports connected to those array interfaces must be in the same Native VLAN. Arrays must have the same MTU setting on configured subnets.
- Verify that the following factors are the same for both groups:
  - The data and management subnet
  - The data protocol

    The data ports must be connected.

    Note:

    A data subnet is required so the management subnet must be modified for use for management and data. The management and data ports must be in the same VLAN (L2 network, broadcast domain) as the other interfaces in that subnet.

    Data IPs must be added for group traffic between the arrays.

- The L2 network or broadcast domain

  Both groups must also be in the same VLAN, on the same switch or switch-stack, or on switches connected via an inter-switch link or trunk.

- The replication throttle levels

  Group-level throttles from the source group are automatically discarded and the destination group throttles are automatically applied.

  If the throttle levels are set differently on the two arrays that are associated with the destination and source groups, adjust the throttle level on the destination group based on your environment and requirements.

  The joining group inherits the destination group settings. You might see replication delays for the joining group if the throttle was set higher than its destination group. If the destination group has no throttle then the joining group no longer uses a throttle

- When accessing the arrays using HPE CSI Driver for Kubenetes, make sure that the names of the tenant users are not the same on both arrays. In this configuration, the merge will fail if there is a user in both arrays with the same name.

Complete the following tasks if applicable:

- Configure source and destination groups to have matching subnets in the Active network configuration.
  - Delete any draft network configs from source and destination groups.
  - On source and destination groups, “Edit” and “Save” the network configuration in order to over-write the “backup” network configuration.
- Configure the joining group (the group being merged) as a single-array configuration.
  - You can merge only two groups at a time. Make sure that the joining group consists of a single array.
- Perform the following replication tasks if you intend to merge replication partners into the same group:
  - Stop all replication and group merge processes in your environment.
  - Remove the hosting and joining groups from any replication configurations.
- Unregister the HPE vCenter plugin, if you previously registered it.
  - Unregister the plugin at the source (joining) array because the destination group will service the plugin under its group management services. This does not cause downtime.
  - To learn more about unregistering the plugin, see the *VMware Integration Guide*. If you are using vVols, refer to the "Supported Features" section to determine if your vVol environment is impacted by the group merge.
- Set offline all volumes associated with the joining group.

  Note: It is recommended that you perform this task using the GUI.

For Fibre Channel arrays:

- After the volumes are offline, then offline all Fibre Channel interfaces on the source group. These tasks are easier using the GUI.
- A data subnet is still required
  - The management subnet can be modified to be used for Mgmt+Data
  - Alternately, an unused Ethernet interface can be configured as a “data” interface, and a data IP added for group traffic between the arrays.
- An alias is a human-friendly name associated with a WWPN. An alias may be defined on the switch (as a fabric-assigned alias) or using the array OS (as a user-assigned alias). For any two disjoint groups with user-assigned aliases, two potentially problematic situations can occur:
  - Different initiators with the same WWPN must use the same alias for that WWPN
  - Different initiators cannot be using the same alias for different WWPNs

- In either case, you are presented with this information on the validation screen, and must manually perform the rename operation.

Merge Two Groups

Before you begin

- Check array cabling. For more information about cabling, refer to the *Storage Quick Start Guide* for your arrays.
- Ensure that the network configuration is correct.

Procedure

1. Log into the group leader array for the group into which you will merge a second group.

   The group that you log into is the *destination group*. It has the group leader array and up to two other arrays, one of which might be the backup group leader. This group will merge with a second group, which is the *source group* and has only a single array.

   > **Note:** The merge operation takes the following actions with regard to backup group leaders and the destination group and source group.
   >
   > - If the destination group includes a secondary management IP address, the merge operation ignores any secondary management IP on the source group.
   > - If the destination group does not have a secondary management IP address, but the source group has one, the merge operation gives you the option to use the source group secondary management IP address.

2. Go to **Hardware**.
3. Click **Actions** > **Add Array to Group**.
4. In the Add Array to Group dialog box, locate the array that you want to add to the group and check it.

   The group to add (source) must contain an array that runs the same array OS version and the same iSCSI or Fibre Channel data protocol as the group leader array (destination).

   A list of arrays is displayed. The GUI displays error icons for incompatible arrays in the groups. Hovering over an error icon displays a list of error that must be resolved before you can add the array to the group.

5. Type the Administrator password in the **Password** field, then click **Connect**.
6. Click **Add**.

   A dialog is displayed to validate what is needed to successfully complete merging the two groups. The dialog also identifies the consequences of the merge. Be sure to read this information carefully and take all recommended actions. Some of the notifications include:

   - Any merge conflicts, such as common initiators with user-assigned alias conflicts.
   - Logical Unit (LU) number conflicts — For the same initiators accessing volumes on both the source and destination groups, it is possible that the same LU number could be assigned to volumes on both the source and destination groups. Because different volumes cannot be exposed to the same initiator using the same LU number, the merge validation will fail. The validation report will show the conflicting LU numbers, and these must be changed manually before the merge can be successful.

7. In the Validation successful dialog box, click **Finish**.

   A progress bar identifies the progress of the merge process. If the process completes successfully, a subsequent message provides status about the successful completion of the group merge.

8. Click **Close**.

Both arrays appear in the Arrays panel as members of the destination group. Make sure that you now use the management IP address of the Group Leader array.

9. Select **Manage** > **Array** to verify that the two groups have been merged.
10. If applicable, register the HPE vCenter Plugin again.

> **Note:** If you unregistered the HPE vCenter Plugin before completing the merge of the two groups, you must register the HPE vCenter Plugin again.

To learn more about registering the HPE vCenter Plugin, see the *VMware Integration Guide*.

Post-Merge Tasks

After you merge two groups, perform the following tasks.

Procedure

1. Online all volumes that were previously in the source group.
2. Update any SNMP clients to contact the group leader's (destination group's) management IP rather than the source group's, and the group leader's SNMP community name (rather than the source group's).
3. For iSCSI groups, update initiators with the new discovery IP for these volumes and then reconnect.
4. Re-arrange pool and volume assignments as needed. For example, merge the default source group into the default pool on the destination group.
5. If there was replication going to the source group, change it to now go to the destination group.
   a) On any group (other than the destination group) that was previously replicating to the source group, create a partner to the destination group.
   b) Edit all schedules previously using the source group so that the destination group is used instead.
   c) Delete the source group as a partner.
6. If there was replication going from the source group, change it to now come from the destination group.
   a) On any group (other than the destination group) that was previously being replicated from the source group, create a partner to the destination group.
   b) Promote all volume collections that were replicated from the source group (making the new group the owner).
   c) Demote to the destination group.

      This makes the destination group the new owner for these volume collections.
   d) On the destination group, all partners that were paused on the source group before the merge must be resumed.
7. Rezone.

   If you had zoning set up, then re-zone due to changes to WWPNs for what was previously the source group.

Group Information

When you select **Hardware** in the GUI, a summary of the arrays in a group and a summary of the group itself appears. For single-array groups, the Hardware Details page opens.

The following information for each array is displayed, as well as the total aggregate for the group:

Item	Description
Group and Arrays	The name of the group and all member arrays
IOPS	The IOPS measured in 5-minute increments
MiB/s	The performance as measured in 5-minute increments

Item	Description
Usage	Array usage and group capacity
Used (capacity)	Amount of capacity used for each array and for the group
Storage Pool, if applicable	Storage pools to which each member is assigned and totals

Default Group Settings

Because you manage group members as a single entity, you perform many administrative actions for the group instead of an individual arrays. You can modify the following default group settings:

- Password for the Admin user
- Global Security Policies
- Period of inactivity before an array logs users out
- Default space reservation
- Date, time, and time zone
- DNS settings

Note: You must have an Administrator role to make these settings.

Modify Global Security Policies

You can modify the following session policies, account policies, and password policies for a group.

- Maximum number of user sessions for a group. The default is 0.
- Number of failed authentication attempts allowed before an account is locked. The default is 0.
- Minimum number of characters required for a valid password. The default is 8.
- Minimum number of uppercase characters required for a valid password. The default is 0.
- Minimum number of lowercase characters required for a valid password. The default is 0.
- Minimum number of numerical characters required for a valid password. The default is 0.
- Minimum number of special characters required for a valid password. The default is 0.
- Minimum number of characters that must be different from the previous password. The default is 1.
- Number of times that a password must change before you can reuse an old password. The default is 1.

Before you begin
You must have Administrator permission to change the default global security policies for the group.

Procedure

1. Select **Administration** > **Security** > **Security Policy**.
2. Modify a security policy.
3. Click **Save**.

Modify the Default Inactivity Timeout

In the GUI, all users must observe the group inactivity timeout interval unless you specify a user-specific timeout interval when creating or editing a user account.

By default, users are logged out after a specified amount of time with no activity. You can change the default inactivity timeout value up to a maximum of 720 minutes (12 hours). The initial default value is 30 minutes.

⚠ **CAUTION:** Before you change the default inactivity timeout interval, consider all security issues.

Before you begin

You must have Administrator permission to change the default inactivity timeout interval for the group.

Procedure

1. Select **Administration** > **Security** > **Inactivity Timeout**.
2. Type the number of minutes that must pass with no activity before users are logged out.

   The maximum value is 720 minutes.

3. Click **Save**.

Modify the Default Space Reservation

You can set the default space reservations for new volumes or replicas. If needed, you can specify different settings when creating volumes.

Procedure

1. Select **Administration** > **Space**.
2. Define the Volume Limit setting that you want to use as the *volume space* default when you create volumes.

   This setting becomes the default value for all future volumes. However, you can modify the setting at any time. This setting only determines the value that is automatically used when you start the Create Volume wizard.

3. Click **Save**.

Modify the Date, Time, and Timezone

The date and time are set when the array is created. However, you can change the date, time, and time zone at any time.

Procedure

1. Select **Administration** > **Date and Timezone**.
2. Set the time by selecting one of the following options:
   - Select **Use NTP server** and type the IP address or hostname of the NTP server to use.
   - Select **Enter Date & Time** and type the current date and time in the appropriate fields.
3. Select the appropriate time zone from the drop-down lists.
4. Click **Save**.

Modify DNS Settings

You can use a DNS server to map a hostname to an IP address. The service enables users to type host names that can be translated into an IP address usable by networking software. You can modify the DNS server settings for the group as needed.

Procedure

1. Select **Administration** > **Network** > **DNS**.
2. Type the domain name in the **Domain Name** field.
3. Type the IP addresses of up to three DNS servers on separate lines in the **DNS Servers** field.
4. Click **Save**.

Initiator Groups

An initiator is a port on a server or computer that "initiates" a connection with "target" ports on a storage array. It can be an Ethernet Network Interface Card (NIC) port that initiates a connection over an iSCSI fabric to one or more target ports, or a Fibre Channel Host Bus Adapter (HBA) port that initiates a connection over a Fibre Channel fabric to one or more target ports.

An initiator group is a collection of either iSCSI initiators or Fibre Channel initiators that are managed as a single unit.

iSCSI Initiator Groups

An iSCSI initiator group is a collection of one or more iSCSI initiators, with each initiator having a unique iSCSI Qualified Name (IQN) and IP address. Each IQN represents a single Network Interface Card (NIC) port on an iSCSI-based client in the form of a Windows server, ESXi or Linux host. Configure iSCSI initiator groups on the array; configure client-side iSCSI initiators according to the vendor's recommendations.

Note: By default, iSCSI volumes deny access to initiators. To allow initiators in an initiator group to access a volume, you must configure an ACL that includes the desired initiators and attach it to the volume.

Create an iSCSI Initiator Group

Before you begin

To create an iSCSI initiator group, you must know either the iSCSI Qualified Name (IQN) or IP address, or both for each initiator being added to the group.

Procedure

1. Choose **Manage** > **Data Access** > **Initiator Groups**.
2. Click the + icon to create a new initiator group.
3. Enter a name for the initiator group.

   For multi-protocol array groups, you must also specify Fibre Channel or iSCSI in the Protocol dropdown list.
4. From the **Subnets** dropdown list, choose one of the options:
   - Use all configured subnets
   - Use selected subnets

   If you chose **Use selected subnets**, a list of available subnets appears.

   a) (Optional) Highlight the available subnets you want to associate with this initiator group and click **Add**.
5. To add initiators, click **Add** under Initiators.
6. Enter a Name, the IQN of the client system, and the IP Address of the client system for the first initiator.

   Repeat this step to create the number of initiators that you want.
7. Click **Create**.

Results

The new iSCSI initiator group is ready to be applied to a volume.

Edit an iSCSI Initiator Group

Procedure

1. Choose **Manage** > **Data Access** > **Initiator Groups**.
2. On the central panel, select the initiator group you want to edit.
3. Go to **More Actions** > **Edit** to edit the initator group.
4. Edit the initiator name and subnets as desired.

   You can add and remove subnets to associate them with the initiator group.
5. Click **Save**.

Delete an iSCSI Initiator Group

Procedure

1. Choose **Manage** > **Data Access** > **Initiator Groups**.
2. On the Initiator Group screen, check the initiator group or groups you want to delete.
3. Click **Delete**.
4. In the confirmation dialog box, click **Delete**.

   Note: You cannot delete an initiator group if the ACL is associated with one or more volumes

Add an Initiator to an iSCSI Initiator Group

Procedure

1. Choose **Manage** > **Data Access**.
2. On the Initiator Group screen, click the name of the initiator group to which you want to add initiators.
3. Click **More Actions** > **Edit**.
4. In the Edit Initiator Group dialog box, click Add.
5. (Optional) Enter a name for the initiator.
6. Copy and paste the IQN of the client system into the IQN field.

   Note: If you cannot copy and paste the IQN, enter it very carefully.
7. Enter the IP Address of the client system.
8. Click **Add**.
9. Repeat steps 4-7 for each initiator you want to add.
10. When you are done adding initiators, click **Save**.

Delete an Initiator from an iSCSI Initiator Group

Procedure

1. Choose **Manage** > **Data Access** > **Initiator Groups**.
2. On the center panel, select the name of the initiator group from which you want to delete initiators.
3. Click the pencil icon to edit the initiator group.
4. Click the X icon next to the name of the initiator that you want to delete.
5. In the confirmation dialog box, click **Save**.

Fibre Channel Initiator Groups

A Fibre Channel initiator group is a collection of one or more initiators, with each initiator having a unique World Wide Port Name (WWPN). Each WWPN represents a single Host Bus Adapter (HBA) port on a Fibre Channel-based client in the form of a Windows server, ESXi or Linux host. Configure Fibre Channel initiator groups on the array; configure client-side Fibre Channel initiators according to the vendor's recommendations.

> **Note:** By default, Fibre Channel volumes deny access to initiators. To allow initiators in an initiator group to access a volume, you must configure an ACL that includes the desired initiators and attach it to the volume.

Target Driven Zoning

Target Driven Zoning (TDZ) is a feature that enables storage arrays to automatically create Fibre Channel fabric zones. This feature obviates the need for storage administrators to manually configure Fibre Channel zones for each initiator-target port pair, which can make it easier to configure Fibre Channel zones in large Fibre Channel environments.

To enable Target Driven Zoning on an array, go to **Administration** > **Network** > **General**, click **Configure Active Settings**, and then check the **Enabled** box under **FC Target Driven Zoning**.

TDZ Enablement Considerations

FC Target Driven Zoning automatically creates peer zones for each supported initiator group. When TDZ is enabled, the host ports (WWPNs in the initiator groups) are associated with these peer zones. The host ports can then log into the target ports without manually configuring Fibre Channel zones.

If you have a large number of target ports, check your initiator group configuration to ensure that you have an optimal number of paths per LUN before enabling TDZ.

Create a Fibre Channel Initiator Group

Before you begin

To create a Fibre Channel initiator group, you must know the Fibre Channel World Wide Port Name (WWPN) for each initiator being added to the group.

Procedure

1. Choose **Manage** > **Data Access**.
2. Click the **Add** icon (+).
3. Enter a name for the initiator group.

   For multiprotocol array groups, you must also specify Fibre Channel or iSCSI in the Protocol dropdown list.
4. (Optional) To use Target Driven Zoning, choose **Select Manually** in the **Target Ports** drop down list. Then do the following:
   a) Select ports from the Available Target Ports list.
   b) Click the **Move** button to move the selected ports to the Associated Target Ports list.
   c) Click **Save**.
5. (Optional) If you want to add an initiator to the initiator group, click **Add**.
6. (Optional) Enter an initiator alias for the WWPN.

   > **Note:** If a defined initiator alias is detected in the Fibre Channel fabric, you can type the first few characters of the alias and the auto-complete feature provides a list of suggested initiator aliases and associated WWPNs; choose an alias from the list.
7. Enter the WWPN for the initiator group.

   A WWPN is 16 hexadecimal characters (case insensitive) in XX:XX:XX:XX:XX:XX:XX:XX or XXXXXXXXXXXXXXXX format.

> **Note:** Type the first few characters of the WWPN and the auto-complete feature provides a list of available WWPNs; choose one from the list.

8. (Optional) If you want to remove an initiator from the initiator group, click the X icon to the right of the WWPN field.
9. After all initiators have been added to the initiator group, click **Create**.

Edit a Fibre Channel Initiator Group

Procedure

1. Choose **Manage** > **Data Access**.
2. On the Initiator Group screen, click the initiator group you want to edit.
3. Click **More Actions** > **Edit**.
4. Edit the initiator group name, or add or remove initiators as desired.
5. Click **Save**.

Delete a Fibre Channel Initiator Group

Procedure

1. Choose **Manage** > **Data Access**.
2. On the Initiator Groups screen, check the initiator group or groups you want to delete.
3. Click **More Actions** > **Delete**.
4. In the confirmation dialog box, click **Delete**.

> **Note:** You cannot delete an initiator group if the ACL is associated with one or more volumes

Add an Initiator to a Fibre Channel Initiator Group

Procedure

1. Choose **Manage** > **Data Access**.
2. On the Initiator Groups screen, click the name of the initiator group to which you want to add initiators.
3. Click **More Actions** > **Edit**.
4. Enter an alias for the initiator.
5. Enter the WWPN for the initiator group.

   A WWPN is 16 hexadecimal characters (case insensitive) in XX:XX:XX:XX:XX:XX:XX:XX or XXXXXXXXXXXXXXXX format.

   > **Note:** Type the first few characters of the WWPN and the auto-complete feature provides a list of available WWPNs; choose one from the list.

6. Click **Add**.
   Repeat the steps for each initiator you want to add.
7. Click **Save**.

Delete an Initiator from a Fibre Channel Initiator Group

Procedure

1. Choose **Manage** > **Data Access**.
2. On the center panel, select the name of the initiator group from which you want to delete initiators.

3. Click the pencil icon to edit the initiator group.
4. Click the X icon next to the name of the initiator that you want to delete.
5. In the confirmation dialog box, click **Save**.

Initiator Group Access Control Lists

All initiators in an initiator group are granted access to a volume when the access-control list (ACL) for an initiator group is added to the volume. An ACL can be added to multiple volumes, granting the initiators in the group access to those volumes.

When you create or edit a volume, you can add one or more initiator group ACLs to it.

Note: If you do not add any ACLs to a volume, no initiators will be able to connect to the volume.

Add an Initiator Group ACL to a Volume

Procedure

1. Choose **Manage** > **Data Storage**.
2. Click the name of the volume to which you want to add the initiator group group access control list (ACL).
3. Click **Edit**.
4. From the Edit Volume pane, click **Access** on the progress bar.
5. Click **Add**.
6. Choose to apply access to Volume & Snapshots, Volume Only, or Snapshots Only.
7. Choose the initiator group you want to add to the volume.
8. Perform one of the following steps:

Option	Description
For a Fibre Channel array	Enter a LUN number. A LUN value that is not currently in use is automatically filled in. You can change this value but the new value must be unique in the set of LUNs associated with the specific initiator group. The valid range of LUN values is 0-2047, inclusive.
For an iSCSI array	Enter a CHAP account or Unrestricted Access.

9. Click **Add**.
10. Click **Save**.

Remove an Initiator Group ACL from a Volume

Procedure

1. Choose **Manage** > **Data Storage**.
2. Click the name of the volume from which you want to remove an initiator group access control list (ACL).
3. Click **Edit**.
4. From the Edit Volume pane, click **Access** on the progress bar.
5. Click the X button to the right of the initiator group or groups you want to remove from the volume.
6. In the confirmation dialog box, click **OK**.
7. Click **Save**.

Volumes

Volumes are the basic storage units from which the total capacity of an array is apportioned. The number of volumes per array depends on how the storage is allocated.

Hosts connect to volumes using iSCSI or Fibre Channel. A volume appears to a host as a single disk drive, which can be used as a file system, a raw disk, or a virtual disk.

When you delete a volume, the snapshots that are associated with that volume are also deleted. If the volume has online snapshots, they must be taken offline before you can delete them.

Clones, Replicas, and Snapshots

The array OS lets you manage the objects in a storage system: volumes and their associated clones, replicas, and snapshots.

Clones are writable, highly space-efficient copies of volumes which you can create from snapshots. When you create a clone from a snapshot, you create a new volume with a new name and iSCSI or Fibre Channel target with the same settings. Clones share identical blocks and are often used to test applications before putting them into production.

Replicas are copies of volumes stored on a different array, called a replication partner. Replicas are most often used for disaster recovery. For more information about replicas and replication, see Replication on page 113.

Snapshots are point-in-time copies of volumes. Snapshots are often used as backups, and to preserve the state of volumes at specific points. By creating a clone from a snapshot, snapshots can also be used as starting points to which applications can write and read data. For more information about snapshots, see Snapshots on page 105.

Logical versus Physical Space

When working with volumes, it is important to understand the difference between logical space and physical space.

Physical storage resources are aggregated into storage pools from which the logical storage is created. It allows you to have a logical space for data storage on physical storage disks by mapping space to the physical location. Physical space is the actual space on the hardware that is used.

Logical space is space that the system manages, such as the volume size. In this case, the volume size is not necessarily the actual amount of space on a physical disk, but the amount of space defined for a volume, which may span multiple physical disks.

Space Management

The array OS has built-in capacity saving mechanisms such as inline compression and thin provisioning. The following considerations help you plan your space configuration for volumes and snapshots.

The simplest form of space management is to not use reserves at all. This means that there is no dedicated (prereserved) space per volume taken from the general storage pool, so all volumes can consume what they need as it is needed. This method requires that you monitor space usage to ensure that there is always space available.

However, for critical volumes, such as those hosting business-critical data, it may be more important for you to reserve space to ensure that the volume will always have enough. Reserved space is immediately taken from the storage pool.

When you create a volume, you define a certain amount of space for that volume. The volume space is the size that is reported to your application.

Volume Reserve

Volume reserve is guaranteed physical space that is reserved for a volume. Reserved space is set aside for the volume and is immediately withdrawn from the general storage pool. Set the volume reserve to Thin Provisioning (no physical space is reserved) or Thick Provisioning (the entire physical space is reserved). As new data is written to a thickly provisioned volume, free space within the volume reserve decreases.

One consideration when setting volume sizes and reserves is the level of compression you get for a particular application or data set. For example, most volumes should see 50-75% compression, so a volume reserve of 10 GB will be able to store far more than the actual 10 GB space if it were uncompressed. In other words, 10 GB space of application data will only use between 2.5 GB and 5 GB when compressed.

Thin Provisioning

Thin provisioning is a storage virtualization technology that uses physical storage only when data is written instead of traditional provisioning, which reserves all the capacity up-front when an application is configured. This method addresses over-provisioning and its associated costs. Frequently, volumes reserve excessive space against expected growth. Often this growth does not materialize, or materializes much later than expected. With thin provisioning, you create volumes and assign them to servers and applications, but the physical resources are only assigned when the data is written. Physical storage that is not being used remains available to other volumes. No unnecessary storage is reserved for use by any single application.

For example, like most SANs, your array must support several applications. Projections show that eventually the total storage needed by all applications will reach 3 TB. However, for the first few quarters of the year, these applications should only use about 300 GB. Instead of creating the volumes using the total 3 TB that you expect to need, with thin provisioning you can create three 1 TB volumes, but set the reserve to only 150 GB for each volume. When you factor in compression savings, the applications should not use the full 3 TB until the next purchasing window, minimizing the cost of buying more capacity until it is needed.

Volume Usage Limits

Volume usage limits determine how much of a volume can be consumed before an alert is sent to the administrator. When the usage limit is reached, the performance policy associated with the volume determines the next action (for example, whether to make the volume read-only or take the volume offline). An alert is also sent.

Thickly-provisioned volumes have a default volume limit of 100 percent. For thinly-provisioned volumes, you can set the volume limit to a value between 0 and 100 percent. Some applications do not tolerate changes to volume sizes. Limits address this issue. Volume limits let you set a limit but leave room in case more space is needed.

For example, if you have an application that you do not want to fill all the space on the volume before more space is available for expansion, set a limit for the volume. You now have a safety factor, and when the limit is met, you can reset the limit, giving more space to the application. You can then plan for further expansion if necessary.

If the volume is approaching the limit, an event is logged. If enforcement is enabled, the administrator can access the system log to determine what follow-up actions to take, such as preventing the user from accessing more disk space or allocating additional disk space to the user.

Note: Volume usage limit must be greater than or equal to the volume reserve.

A Note on Defragmentation

Do not defragment volumes on an array. The value of defragmentation is mainly on a local physical disk to keep files contiguous so the disk heads do not require unnecessary physical seeks across the platters, and slow down file I/O.

There is no such value about the effectiveness of this in a networked iSCSI environment, especially where files are stored on storage devices that have their own layers of virtualization.

Defragmenting files in a storage array environment results in changed blocks, even though the files did not change, and can have unnecessary impacts, such as snapshots being larger than they should.

Cloning Space Considerations

Clones are space-efficient copies of a volume that can be used independently of the source volume. When created, they have the same settings as the volume from which they were created. Clones share blocks that are identical with the source volume, and only begin to use space when changes are made.

HPE recommends that you lower the reserve settings for clones. When determining the reserve settings, factors to consider include how long-lived the clone will be and how much the clone will vary from its source. For example, the reserve settings may not need to be very high if the clone is being run to test a new application against, will not be changed much, and will be deleted after the testing is complete.

Note: You cannot delete the source volume of a clone unless you first delete the clone.

Protecting Data Using Snapshots

Snapshots ensure that data stored in volumes is always recoverable.

Note: If a volume is deleted, all associated snapshots are also permanently deleted.

Merging primary and backup storage makes snapshots an efficient method to protect data. Because no data needs to be copied outside the array, snapshots can be created and used to restore data almost instantaneously.

You can restore a volume from either the local recovery point or the remote recovery point. The local recovery point is the last local snapshot taken for the volume. The remote recovery point is the last snapshot taken through replication.

Because snapshots are part of the converged storage and backup, and because they are so efficient, consider the implications when creating snapshots. For some applications, the amount of storage used for snapshots may equal or exceed the storage needed for the source volume.

Volume collections let you automate snapshot schedules based on common usage scenarios. Create your own sets, using the predefined collections provided as templates.

Even if you plan to manually take snapshots of volumes or use a third-party program to create backups, create a volume collection without schedules for volumes that are being manually snapshotted.

Create a Volume

Volumes are also referred to as logical units (LUNs). They are the building blocks of any storage system. A host connects to the volume and the volume appears to the host as a single disk drive, which can be used as a file system, a raw disk, or a virtual disk.

Note: A volume that is configured for synchronous replication does not support volume pinning and cannot be resized.

You can use the Create Volume wizard to create either an iSCSI or a Fibre Channel volume (maximum size 127 TiB).

Note: For a Fibre Channel array, the CHAP account fields are replaced with LUN fields.

Procedure

1. Choose **Manage** > **Data Storage**.
2. Click the plus icon to add a new volume.
   The Create Volume dialog box opens.
3. Configure the general properties of the volume.

   In multi-protocol array groups, you must specify either Fibre Channel or iSCSI protocol before creating the volume.

Option	Description
For iSCSI volumes	Identify CHAP accounts that can access the volume and its snapshots. Choose either: • Unrestricted Access • A previously defined CHAP account
For Fibre Channel volumes	Indicate a LUN to be added to the ACL

Note: You can also modify access control to the volume at a later time.

a) (Optional) For iSCSI volumes only, check the box to allow multiple initiator access.

⚠ **CAUTION:**

Enable multiple initiator access only on iSCSI volumes that are optimized for simultaneous access by multiple initiators, such as VMware VMFS or Microsoft Cluster Server.

Non-coordinated access by multiple initiators can result in data corruption.

4. (Optional) Click **More Options** to configure space, protection, and performance settings.
The Create Volume page opens. There is a progress bar at the top of the page.

5. (Optional) Click **Space** on the progress bar to configure space settings.

a) In the Deduplication area, check the box to **Enable** deduplication.

Note: If you enable deduplication on the volume, you cannot enable cache pinning in the Performance page, even if you disable deduplication at a later time.

b) In the Thresholds area, allocate space for the following:

Space	Description
Volume Reserve	Amount of space prereserved for the volume usage. If deduplication is enabled when creating the volume, the reserve is set to Thin Provisioning. If deduplication is enabled on the volume, you cannot set a volume reserve, even if deduplication is later disabled.
Volume Limit	Maximum allowed usage for the volume, defined as a percent of volume size. If the volume usage exceeds this value, the volume is taken offline or made read-only, based on how the associated performance policy is configured. For a thickly provisioned volume, the volume limit is 100%.

6. (Optional) Click **Next** to configure the protection settings.

a) Choose the type of volume protection that you want.

No volume collection: No protection	Click **Next**.
Join a volume collection	Choose the volume collection from the drop-down and click **Next**. If you cannot find the volume collection that you are looking for, begin typing the name until it appears in the drop-down list. Click the X icon to remove your choice.
Create a new volume collection	Continue with the steps that follow.

Protect as a standalone volume	The difference between protecting a volume with a volume collection and standalone volume protection is that the standalone volume collection is intended to be associated only with the one volume. So when the volume is deleted, the standalone volume collection is also deleted Other volumes cannot be associated with the volume collection that is associated with a standalone volume. Continue with the steps that follow. The new volume collection name is automatically generated.

b) In the Create Volume Collection page, complete the fields.

c) Choose a method of application synchronization. Select one of the following:

- None
- Microsoft VSS – Type the hostname or IP address of the application server and choose an application from the drop-down list.
- VMware vCenter – Type the hostname or IP address of the vCenter host, and the corresponding user name and password.

d) For the Synchronization Service, select one of the following options.

This quiesces application I/O when snapshots are created to ensure application-consistent backups and replicas.

Option	**Description**
None	Create snapshots that do not need synchronization.
Microsoft VSS®	Create application-consistent snapshots for applicable types of Microsoft applications, including Hyper-V. Synchronization quiesces volume traffic before a snapshot is taken. This ensures that your application never has a snapshot with incomplete data. Select the appropriate application and provide further information such as the application server address. For detailed information, see the *Windows Integration Guide*.
VMware vCenter®	Create snapshots through a VMware vCenter Server. This ensures that snapshots are VMFS-consistent. The first time you create a volume collection with schedules that use this synchronization setting, you need to provide the vCenter host name or IP address, user name, and password. For detailed information, see the *VMware Integration Guide*.

To help eliminate possible performance issues for snapshot schedules that synchronize with Microsoft Exchange®, schedule the snapshot verification to run no more than once daily.

e) In the Schedules section, create a custom protection schedule.

Default values are provided for many of the fields

- You can create multiple schedules for the volume collection.

  For example, you can create one schedule for working hours, one for peak hours, and one for weekends. Schedules can overlap, but they cannot span midnight. If you need a schedule that takes hourly snapshots from 10 PM to 4 AM, you need to create two schedules. The first schedule covers the time period from 10 PM to 11:59 PM and the second schedule covers the time period from 12 AM to 4 AM.

- If you chose replication, specify how frequently (or after how many snapshots) replication of the volumes in the volume collection should be triggered.

Note: If the replication is not complete within the time specified, the replication partner sends an alert.

f) After you define all the protection schedules you need, click **Next**.

7. (Optional) Configure the settings for performance on the Performance page.

   For Volume Caching, you should use the **Pinned** setting only for volumes that require a 100% cache hit rate.

   Note: If you enabled deduplication on the Space page, you cannot enable cache pinning for the volume.

8. Click **Create**.

What to do next

- Configure the connections (iSCSI or Fibre Channel) on your volumes to connect to the group leader array.
- Configure the connections (iSCSI or Fibre Channel) for your server or host to access those volumes.
- The IQN or WWPN and serial number are available by hovering over the disk icon to the left of the volume name on any tab.
- Configure your client initiator according to the vendor's recommendations.

Edit a Volume

Some notes about editing a volume:

- You can modify most volume configuration options, such as access restrictions, volume limit, performance policy, and the volume collection assignment after you have created the volume.
- You cannot change the location of a volume with the Volume Edit command. You must use the Volume Move command to change the folder or pool in which a volume resides.
- You cannot modify the following settings after the volume has been created.
  - Encryption settings
  - Block size

    You can only change the performance policy to another performance policy that has the same block size.
  - Application category, if the volume was ever deduplicated
- If you are editing a volume with reserved space (thick provisioned) and you enable deduplication, the reserve will be reset to 0 (thin provisioned).
- If the volume is replicated, any allowable attribute changes are propogated to both the upstream and the downstream volumes.

  Note: For information on volume restrictions with synchronous replication, see Synchronous Replication Prerequisites and Limitations on page 121.

When you edit a volume, you can navigate directly to any page using the progress bar at the top of the page. You do not need to perform any steps on the intervening tabs. After you make the desired edit or edits, you can click **Save** without navigating to the last tab.

Procedure

1. Choose **Manage** > **Data Storage**.
2. Click the link of the volume you want to modify.
3. Click **Edit**.
4. On the General page, make the changes to the following:
   - Name
   - Description

- Performance Policy

  If you choose **Create Performance Policy**, complete the information requested in the Create Performance Policy dialog box.

5. Click **Next**.
6. (Optional) Configure the size of the volume on the Space page.
   a) (Optional) In the Deduplication area, deselect **Enable**.
   b) In the Thresholds area, allocate space for the following:

Space	Description
Volume Reserve	Amount of space prereserved for the volume. If deduplication is enabled when creating the volume, the reserve is set to Thin Provisioning. If deduplication was ever enabled on the volume, you cannot set a volume reserve, even if deduplication is disabled.
Volume Limit	Maximum allowed usage for the volume, defined as a percent of volume size. If the volume usage exceeds this value, the volume is taken offline or made read-only, based on how the associated performance policy is configured. For a thickly provisioned volume, the volume limit is 100%.

7. Click **Next**.
8. (Optional) On the Protection page, select one of the following:

Option	Description
No volume collection: No protection	Click **Next**.
Join a volume collection	Choose the volume collection from the drop-down and click **Next**.
Create a new volume collection	Continue with the steps that follow.
Protect as a standalone volume	The difference between protecting a volume with a volume collection and standalone volume protection is that the standalone volume collection is intended to be associated only with the one volume. So when the volume is deleted, the standalone volume collection is also deleted. Other volumes cannot be associated with a volume collection that is associated with a standalone volume. Continue with the steps that follow. The new volume collection name is automatically generated.

   a) In the Create Volume Collection page, complete the fields.
   b) Choose a method of application synchronization. Select one of the following:

   - None
   - Microsoft VSS – Type the hostname or IP address of the application server and choose an application from the drop-down list.
   - VMware vCenter – Type the hostname or IP address of the vCenter host, and the corresponding user name and password.

   c) For the Synchronization Service, select one of the following options.

   This quiesces application I/O when snapshots are created to ensure application-consistent backups and replicas.

Option	Description
None	Create snapshots that do not need synchronization.

Option	Description
Microsoft VSS®	Create application-consistent snapshots for applicable types of Microsoft applications, including Hyper-V. Synchronization quiesces volume traffic before a snapshot is taken. This ensures that your application never has a snapshot with incomplete data. Select the appropriate application and provide further information such as the application server address. For detailed information, see the *Windows Integration Guide*.
VMware® vCenter™	Create snapshots through a VMware vCenter Server. This ensures that snapshots are VMFS-consistent. The first time you create a volume collection with schedules that use this synchronization setting, you need to provide the vCenter host name or IP address, user name, and password. For detailed information, see the *VMware Integration Guide*.

To help eliminate possible performance issues for snapshot schedules that synchronize with Microsoft Exchange®, run the snapshot verification no more than once daily.

d) Click **Next**.

9. (Optional) Make the desired changes on the Access page.

   a) Click **Add** to add ACLs.

10. Click **Next**.
11. (Optional) Make the desired changes on the Performance page.

    For Volume Caching, you should use the **Pinned** setting only for volumes that require a 100% cache hit rate.

    Note: If deduplication was enabled on the volume when it was created, cache pinning cannot be enabled, even if you deselected deduplication on the Space page.

12. Click **Save**.

Change the State of a Volume

Taking a volume offline makes that volume unavailable to initiators. When you set a volume to offline, all current connections are closed.

Note: Snapshots are not affected by the online state of a volume.

Procedure

1. Choose **Manage** > **Data Storage**.
2. Click the name of the volume to change its status.
3. Click the ellipsis and select the status that you want to apply to the volume.

   The option that is visible depends upon the current state of the volume or volumes.

What to do next

After you change the state of the selected volumes, the volumes remain selected. If you do not want to perform an additional operation on these volumes, you should deselect them.

Clone a Volume from a Snapshot

Clones of snapshots are useful for restoring individual files instead of a complete volume.

Cloning a volume from a snapshot creates a new volume with a new name, but keeps all other settings of the original, including the data at the time the snapshot was taken.

When you clone a volume, settings such as reported size, volume limit, and security are cloned. Clones are set online by default, and are writable.

> **Note:** When a volume configured for synchronous replication is cloned, the cloned volume will not automatically be configured for synchronous replication.

Procedure

1. Choose **Manage** > **Data Storage**.
2. Click the name of the volume you want to clone.
3. Click the Data Protection tab to determine if there are any snapshots for the volume.

   If there are no existing snapshots for the volume, manually create a snapshot. See Take a Manual Snapshot on page 107 for the steps.
4. Select the snapshot you want to clone a volume from, then click **Clone**.
5. Provide a Volume Name for the clone, then click **OK**.

   > **Note:** Names are case sensitive, can contain between 1 and 215 characters, dashes (-), dots (.), and colons (:) but cannot start with a dot, a dash, or a colon, and cannot contain underscores (_), spaces, or any other special characters.

   The clone is created and appears in the list of volumes on the Data Storage page.

What to do next

A clone is not automatically assigned to a volume collection. Edit the clone to assign it to the desired volume collection to ensure that snapshots and replicas will be made according to the desired schedule.

Restore a Volume from a Snapshot

> **Note:** For synchronously-replicated volumes, you must first unconfigure synchronous replication before you attempt to restore the volume.

You can restore a volume from one of its snapshots. Before it is restored, a new snapshot is automatically taken of the existing state of the volume, even if third-party software is used.

You can restore a volume from either the local recovery point or the remote recovery point. The local recovery point is the last local snapshot taken for the volume. The remote recovery point is the last snapshot taken through replication.

After a volume is restored from a snapshot, the automatically created snapshot appears in the list of snapshots for the volume, and is identified with the original snapshot's name appended with a timestamp of the date and time it was taken.

> **Note:** When restoring a volume, it is recommended that you unmount the volume from the host before putting the restored snapshot online. Restoring a volume without stopping all host access can cause data corruption and system errors.

Procedure

1. Choose **Manage** > **Data Storage**.

2. Select the volume that you want to restore.
3. On the volume details page, click the Data Protection tab.
4. Check the snapshot that you want to use to restore the volume.
5. Click **Restore**.

   A warning displays asking if you want to take the volume offline (if it is online). You should check **Set volume offline**, otherwise the operation fails.
6. Click **OK** to acknowledge the warning.

What to do next

Set the volume online. See Change the State of a Volume on page 70.

Delete a Volume

There are some important points to keep in mind when you plan to delete a volume:

- You cannot delete a volume if it has snapshots that are online.

  Deleting a volume also deletes any snapshots of the volume.
- You cannot delete a volume that has a clone.

  Clones share the original data with the source volume.
- When an upstream replicated volume is deleted, the downstream volume is not automatically deleted, in order to provide protection from accidentally deleting a volume.
- A downstream volume cannot be deleted when replication to it is configured.

CAUTION: When you delete a volume, all data stored on the volume and all of the associated snapshots will be destroyed.

Procedure

1. Choose **Manage** > **Data Storage**.
2. Check the volume or volumes you want to delete.
3. (Optional) Go to the ellipsis icon and click **Set Offline** , then click **Yes**.
4. Click the X icon to delete the volume or volumes.

Delete a replicated volume from downstream

Replica volumes are owned by the parent volume collection. To delete a replica volume, you must break the replication relationship by promoting the replica volume collection.

Procedure

1. Select **Manage** > **Data Protection**.
2. Select the volume collection for the replica volume you want to delete.
3. Select **Actions** > **Promote**.

   The volumes will be automatically set online as the volume collection is promoted.
4. Select **Actions** > **Edit**.
5. On the **Volumes** tab, remove the replica volume, and then click **Save**.
6. Select **Manage** > **Data Storage**.
7. Select the replica volume.

8. Select **More Actions** > **Set Offline**.
9. Select **More Actions** > **Delete**.
10. If there are no more volumes in the volume collection, and you want to delete the volume collection:

    1 Select **Manage** > **Data Protection**.
    2 Select the volume collection.
    3 Select **Actions** > **Delete**.

11. If there are volumes remaining in the volume collection, and you are done deleting volumes:

    1 Select **Manage** > **Data Protection**.
    2 Select the volume collection.
    3 Select **Actions** > **Demote**.
    4 Select the upstream partner.

Volume Pinning

Note: Volume pinning is not supported with synchronous replication.

Volume pinning allows you to keep active blocks of a volume in the cache, as well as writing them to disk. This provides a 100% cache hit rate for specific volumes (for example, volumes dedicated to critical applications), and delivers the response times of an all-flash storage system.

A volume is "pinned" when the entire active volume is placed in cache; associated snapshot (inactive) blocks are not pinned. All incoming data after that point is pinned. The number of volumes that can be pinned is limited by the size of the volumes and amount of available cache. However, only one volume in a volume family (a volume and the associated snapshots and clones) can be pinned.

Note: Pinning a volume may affect the cache hit rate of other volumes. It is a best practice to avoid unnecessary cache pinning.

Pinnable Flash Capacity

Only a portion of the array's total flash capacity can be used for pinning. The amount of pinnable capacity is determined by the amount of usable cache in the system and the amount of usable disk capacity in the system. The array OS performs these calculations.

The formula for determining pinnable capacity depends on whether you are using a deduplication:

- A hybrid array without deduplication:

  pinnable capacity = 66% * (usable cache capacity - (4% * usable disk capacity))

  For example, an array without deduplication enabled that has a usable disk capacity of 100 TB and a total flash capacity of 12 TB, the total pinnable capacity of the array is 66% of ((12 TB - (4% * 100 TB)) = 5.28 TB.

- A hybrid array with deduplication enabled:

  pinnable capacity = 66% * (usable cache capacity - (4% * usable disk capacity) – (4% * maximum-enabled deduplication capacity))

For striped pools, the pinnable capacity is

(minimum value of (pinnable capacity/usable disk capacity) on any individual array) * (total usable disk capacity across all arrays in the stripe)

If you are unable to pin a volume, you may need to adjust the flash capacity. For more information, see Unable to Pin a Volume on page 76.

Volume Pinning Caveats

Note: Volume pinning is not supported with synchronous replication.

When performing certain operations related to volume pinning, keep these caveats in mind.

Table 7: Volume Pinning Caveats

Condition	Solution
Volume Pinning Enablement	To be able to pin the volume, the cache must be enabled on the performance policy for the volume.
Limit and Volume Size Changes	When changing a pinned volume's space limits, the amount of cache reserved for the volume will also change. You will not be able to pin volumes until sufficient cache is available.
Moving a Volume	When moving a volume, the pinnable capacity on the destination array or pool must be sufficient to pin the moving volume. Before moving the volume, ensure there is enough cache on the destination array or pool. The cache usage on the source will be freed on the completion of the move. If you attempt to pin a volume during a volume move, pinning will not be guaranteed until a scan has finished on the destination. This could take some time (up to several hours) depending on how much content is in the volume, and how much other activity there is.
Replicating a Volume Using Snapshot Replication	If you replicate a pinned volume, the volume will not be pinned downstream. **Note:** You cannot synchronously replicate a pinned volume.
Adding Shelf Capacity	When adding a shelf to an array, if the total of the new pinnable capacity is less than the size of the pinned volumes, the shelf activation will fail.
Failed, Removed, or Upgraded SSD	When an SSD fails or is removed, if the amount of pinnable capacity is less than the current size of the pinned volumes, then all volumes may become unpinned, because there is not enough free cache to pin the blocks. A message is displayed recommending that you consider adding capacity or unpinning some volumes to restore performance to cache pinned volumes. If the SSD is replaced with one of the same capacity, volume pinning continues normally. If the SSD is replaced with one of a different capacity, the amount of pinnable cache is recalculated. One consolidated alert is sent for all volumes when the free usable cache drops below the acceptable level, and another alert is sent once the free usable cache returns to an acceptable level for the rescan to be completed.
Pinning an Existing Volume	If you are using the Edit function to specify that a volume is to be pinned, this initiates a scan of the volume. Pinning will not be guaranteed until the scan of the volume is finished. This could take some time (up to several hours) depending on how much content is in the volume, and how much other activity there is. Alerts are sent both when pinning begins and ends, on a per-volume basis.
Performing a Bin Migration or Pool Merge	If you have performed a bin migration (for space balancing, for example), or if you attempt to pin a volume during a bin migration or pool merge, pinning will not be guaranteed until a rescan has been completed on the bin's new destination. This could take some time (up to several hours) depending on how much content is in the volume, and how much other activity there is. For a bin migration, one consolidated alert is sent for all volumes once the rescan is finished. For a pool merge, one consolidated alert is sent for all the volumes before and after the merge.

Condition	Solution
Performing a Volume Snapshot Restore	If you want to do a volume snapshot restore (unpin an old volume and pin a new volume) to re-establish the heat map (cache hit information), pinning will not be guaranteed until a scan of the new tip has finished. This could take some time (up to several hours) depending on how much content is in the volume, and how much other activity there is. **Note:** A snapshot restore can only be performed after unpinning the volume.
Performing a Software Upgrade	In case of a software upgrade, pinning will not be guaranteed until a rescan is performed to determine whether any blocks that were in memory were evicted as a result of the software upgrade. This could take some time (up to several hours) depending on how much content is in the volume, and how much other activity there is. One consolidated alert is sent for all the volumes regarding possible loss of pinning, and another alert is sent once the rescan has completed.
Unmanaged Shutdown	In the case of an unmanaged shutdown (where a few segments of pinned data are not flushed and can show up as cache misses), pinning will not be guaranteed until a rescan of the system is finished. One consolidated alert is sent for all the volumes before and after the rescan.
Volume Promotion/Demotion	Demoting a pinned volume will automatically unpin the volume. The volume can be pinned again after promoting it.

Pin and Unpin a Volume

You can pin a volume to cache as part of the volume creation process, or you can pin an existing volume in the **Data Storage** page.

> **Note:**
>
> If you enable deduplication when creating a new volume, or if an existing volume had deduplication enabled, you cannot enable volume caching (pinning) for the volume.
>
> Before you pin a volume, the performance policy associated with that volume must have caching enabled.

Procedure

1. Go to **Manage** > **Data Storage**.
2. Check the name of the volume you want to pin or unpin.
3. Click the pencil icon to edit the volume.
   The Edit Volume dialog opens.
4. On the Edit Volume page, click **Performance** on the progress bar.
5. Perform one of the following two actions:
   - To pin a volume, select **Pinned** in the Caching pane.
   - To unpin a volume, select **Normal (default)**.
6. Click **Save**.
   If you tried to pin a volume and the volume can be pinned, you will see additional capacity information for that volume. If the volume cannot be pinned, you may see a "not enough cache in the pool" message. For more information, see Unable to Pin a Volume on page 76.

Unable to Pin a Volume

If you try to pin a volume and receive a "cache capacity exceeds available capacity" message, you have insufficient usable cache to pin the volume. There are two options:

- Use another pool - you can use the array OS to display a list of other pools with sufficient cache. You have the option to switch your volume to that pool.
- Unpin other pinned volumes - you can view the pinning capacity of other volumes by hovering over their names listed on the Caching dialog. A tooltip is displayed with the pinning capacity information for that volume. If your volume is already pinned but you want to free more usable cache, you can use the Caching facet on the volume's information page to view a list of pinned volumes.

Performance Policies

Performance policies define how data is stored on the array to achieve optimal performance for a specific application. There are several predefined performance policies to choose from based on the application assigned to the volume.

Note: The default performance policy for a Secondary Flash array is Backup Repository.

Create a Performance Policy

Performance policies are intended to be the optimal performance settings for the specific application. The performance policy helps optimize the performance for a volume based on the expected characteristics of the application using the volume. The performance policy defines the behavior of its associated volumes when their limit is exceeded.

You can associate a volume with an existing performance policy or create a new one.

Important:

During replication synchronization, a custom performance policy on the upstream partner is created on the downstream partner, if needed. If a performance policy already exists that is not identical, the partners might fail to synchronize.

This applies only to snapshot replication. Synchronous replication does not use performance policies.

Procedure

1. Choose **Manage** > **Performance Policies**.

   A list of all performance policies and the number of volumes associated with them is displayed.
2. Click the + sign to create a new performance policy.
3. Enter a name that reflects the best use of the policy.
4. Choose an Application Category from the drop-down list.
5. (Optional) Choose a block size to match the application block size from the **Storage Block Size** drop-down list.

   Choices range from 4 KiB to 32 KiB. If in doubt, use the default of 4 KiB.

   Note: After the performance policy is created, the block size cannot be changed.
6. (Optional) Deselect the check boxes to disable the compression or caching options.

   Note: Leave compression and caching enabled for most applications.

   - Disable compression when the application using the volume precompresses data before storing it or when compression slows write times for an application that requires above-average sequential write throughput.
   - Disable caching for applications that use a sequential access to the volumes, such as an exchange log file. Exchange log files are typically stored on different volumes from the database files so caching is unnecessary.

7. (Optional) Check **Enable deduplication on newly created volumes using this policy** if you want to enable deduplication.
8. Choose a **Limit Exceeded Behavior** option to set the volume offline or non-writable if the limit of the volume is exceeded.

   Note: Volumes with a no-cache policy cannot be pinned.

9. Click **Create**.
   The performance policy appears in the selection list when you create or edit a volume.

Create a Performance Policy with Deduplication Enabled

Performance policies are intended to be the optimal performance settings for the specific application. The performance policy helps optimize the performance for a volume based on the expected characteristics of the application using the volume. The performance policy defines the behavior of its associated volumes when space or capacity limits are exceeded.

You can associate a volume with an existing performance policy or create a new one.

Note:

- Deduplication can be enabled only on All Flash, Secondary Flash, and select models of Adaptive Flash arrays.
- If a particular group does not support deduplication, the checkbox to enable deduplication is not visible.
- If a particular group consists only of All Flash or Secondary Flash arrays, the checkbox to enable caching is not visible.

Procedure

1. Choose **Manage** > **Performance Policies**.

   A list of all performance policies and the number of volumes associated with them is displayed.
2. Click the + sign to create a new performance policy.
3. Type a name that reflects the best use of the policy.
4. Choose an Application Category from the drop-down list.
5. (Optional) Choose a block size to match the application block size from the **Storage Block Size** drop-down list.

   Choices range from 4 KiB to 32 KiB. If in doubt, use the default of 4 KiB.

   Note: After the performance policy is created, the block size cannot be changed.

6. (Optional) Uncheck the boxes to disable the compression or caching options.

   Note:

   Leave compression and caching enabled for most applications.

   - Disable compression when the application using the volume precompresses data before storing it or when compression slows write times for an application that requires above-average sequential write throughput.
   - Disable caching for applications that use a sequential access to the volumes, such as an exchange log file. Exchange log files are typically stored on different volumes from the database files so caching is unnecessary.

7. Check **Enable deduplication on newly created volumes using this policy** to enable deduplication.
8. Choose a **Limit Exceeded Behavior** option to set the volume offline or non-writable if its capacity or space quota is exceeded.

   Note: Volumes with a no-cache policy cannot be pinned.

9. Click **Create**.
   The performance policy appears in the selection list when you create or edit a volume.

Results

Important: When you replicate a volume using this policy, use an identical policy for the volume on the replication partner.

Disassociate a Volume from a Performance Policy

Note: Before you can delete a performance policy, you must ensure that there are no volumes currently associated with it.

Every volume must have a performance policy associated with it.

Procedure

1. Go to **Manage** > **Performance Policies**.

   Volumes that are associated with a policy are listed on the Performance Policy details page.
2. Click the link to the volumes that are associated with a particular performance policy.
3. Check the volume for which you want to remove the association to the performance policy.
4. Click the pencil icon to edit the volume details.
5. On the Edit Volume page, select the new performance policy to associate with the volume from the **Performance Policy** dropdown list or create a new performance policy.

   For more information on creating a new performance policy, see Create a Performance Policy on page 76.
6. If that is the only change that you want to make to the volume, click **Save**.

Edit a Performance Policy

Note: You cannot edit or delete any of the predefined performance policies.

Procedure

1. Choose **Manage** > **Performance Policies**.

   A list of all performance policies and the number of volumes associated with them is displayed.
2. Select the policy that you want to edit.
3. Click the pencil icon to edit the policy parameters.

   Note: You cannot modify the block size of a performance policy.
4. Click **Save**.

   The performance policy updates and new volumes that are assigned to the policy will use the new settings.

Delete a Performance Policy

Note: Before you can delete a performance policy, you must ensure that there are not any volumes currently associated with it.

To find the list of volumes associated with a particular performance policy, click the link under the performance policy name in the Performance Policies list. The Data Storage page opens displaying the list of volumes.

Note: You cannot delete any out-of-the-box performance policies.

Procedure

1. Choose **Manage** > **Performance Policies**.

   A list of all performance policies and the number of volumes associated with them is displayed.
2. Check the policy that you want to delete.
3. Click the X icon to delete the performance policy.
4. If prompted, confirm that you want to delete the policy.

Group Scoped iSCSI Target

The array OS 5.1.x and later supports iSCSI Group Scoped Target (GST) on iSCSI arrays. GST reduces the number of individual host connections you need to configure and manage, which saves you time.

For example, with Volume Scoped Target (VST), if you need to connect four iSCSI volumes to the host, you would need to connect each target to the host individually. With GST, if you want to connect those same four volumes, you only need to connect to the one target.

> **Note:** When you perform a new installation of the array 5.1.x or later, your default target will use GST. If you upgrade to 5.1.x or later, your default target will continue to use VST.

The benefits of GST over VST include:

- Full mesh connections enable optimal performance and resiliency.
- LUNs can be added to or removed from the host at the array level, so there is no need connect them to or disconnect them from the host one at a time.
- Volumes under GST are managed using Access Control List (ACL) records, similar to Fibre Channel (FC) targets.
- With GST, you connect the single group scoped target, and volumes can be added or removed through the array GUI.
- GST is supported in environments where Synchronous Replication is enabled, but VST is not. A synchronously replicated volume collection exposes the GST ACL information to the downstream pool.

> **Note:** If the group leader array goes down and HPE Peer Persistence (also referred to as synchronous replication and Automatic Switchover) is not enabled, the host will lose access to all GST LUNs. Before you perform a manual takeover, you should take down the cluster. You can bring the cluster up again after the takeover completes.

Table 8: Comparison of VST and GST

	Volume Scoped Target	**Group Scoped Target**
Target IQN	Contains the volume name	Contains the group name
Number of IQNs per target	One per volume	One per group
SendTargets response	Contains discovery IP as portal	One target per data IP, same IQN, different portal
Open Access	Allowed, can use * to add ACLs to initiator group for a volume	Disallowed, must use an actual initiator group
Connections	Host connects to discovery IP and is redirected to the target	Host issues **sendtargets** to the discovery IP, but connections are made using the data IP.

GST volumes have these characteristics:

- The IQN is the name of the array group and its ID, and is the same for all GST volumes.
- Each volume has multiple LUN numbers.

- Instead of logging in to each volume, the hosts log in to the group, so the number of connections can be substantially decreased.
- Access is managed by adding or removing ACL records to or from the CHAP user, similar to FC.

Note: SMI-S does not support GTS.

In contrast VST volumes have these characteristics:

- Each volume has a unique iSCSI Qualified Name (IQN).
- The volume name is part of the IQN.
- Each volume is LUN-0.
- Hosts log in to each volume as separate entities, which affects your ability to scale.
- If CHAP authentication is desired, each volume must be configured for CHAP access using the host IQN or an IP to multiple ACLs.

VMware Virtual Volumes

VMware virtual volumes (vVols) allow you to manage virtual machines (VMs) and their data (such as VMDKs and physical disks) without having to know details about the underlying storage. The ability to manage vVols using VMware virtual disks mapped to native storage containers is a new feature in vSphere 6.0.

Support for vVols means that an HPE array volume can reside in a VASA Provider *storage container*. Each folder with a vVol agent type is exported to the vCenter Server as a storage container. A *capability profile*–a group of storage capabilities–is applied to the storage containers. Each storage container supports all VM workflows (create, clone, snapshot, migrate, delete, HA/DRS).An HPE array supports up to 64 storage containers.

Both vVols and regular volumes can exist on the same array or set of arrays (group or pool). vVols appear in the CLI and GUI as regular volumes. You can monitor their capacity and performance from the array. However, you **must** use the vCenter Server UI to manage vVols.

Multiple VASA Provider services can register with multiple vCenter Servers on the array.

> **Note:** vCenter Server registration is different from the HPE vCenter Plugin registration, which can be registered with multiple vCenters.

HPE supports as many vVols as volumes per group. Analytics for these vVols are provided using HPE InfoSight.

> **Note:** Refer to the *Volume* entry in the *System Limits* for volume limits per array model.

vCenter Server

VMware vCenter Server is a data center management server application developed by VMware Inc. to monitor virtualized environments. vCenter Server provides centralized management and operation, resource provisioning and performance evaluation of virtual machines residing on a distributed virtual data center. A vCenter Server is used to manage volumes and Virtual Volumes (vVols) configured on an array.

An array must register the *HPE vCenter Plugin* with vCenter Server before it can be displayed in the list of arrays that can connect to vCenter Server.

> **Note:** You can use the array GUI only to add a vCenter Server to an array, or register a vCenter Plugin. To edit or remove a vCenter Server from the array, or unregister a vCenter Plugin, you must use the array OS CLI. For more information, refer to the *CLI Administration Guide*.

Register a vCenter Plugin with vCenter Server

To manage volumes or Virtual Volumes (vVols) through vCenter Server, you must register the HPE vCenter Plugin with vCenter Server.

Procedure

1. Select **Administration** > **VMware Integration**.
   You see the Register vCenter dialog box.
2. Enter the vCenter Server name.
3. Enter the hostname or IP address of the vCenter Server and the port to be used.
4. Enter a description for the vCenter Plugin.
5. Enter the username and password for the vCenter Plugin.
6. Check one of the following extension types to register the vCenter Plugin with vCenter Server:

- **Web Client** for a web client
- **Thick Client** for a desktop client
- **VASA Provider (vVols)** for a VASA Provider, which is used for vVols

7. Click **Save**.

Folders

Folders are containers for holding volumes. They are used most often for organization, management, and further delegation. Folders provide simple volume grouping for ease of management.

You can monitor the performance of folders by going to the **Monitor** > **Performance** tab.

External management agents such as VASA Storage Containers (Virtual Volumes) and SMI-S storage pools, map to folders and can leverage them directly.

A folder can have a usage limit, a provisioned limit, or no limit.

- Usage limit – Limits the amount of space used by volumes and clones in the folder. The usage includes the compressed size of both the volumes and the snapshots. For virtual volumes, the usage limit is the size that will be reported for the datastore in vCenter. Note that the usage limit will cause new volume creation to fail when the usage limit is reached.
- Provisioned limit – Limits the amount of space that can be provisioned in the folder.

Relationship of Folders, Pools, and Volumes

It is important to know the characteristics of folders and volumes and their relationship to each other and to pools. Some of the characteristics are outlined in the following table.

Folders	Volumes
Folders are provisioned within pools, and can contain volumes.	A volume can belong to a pool without being part of a folder.
Folder names must be unique within the pool that contains them.	Volume names, even those within folders, must be unique across a group.
Pools containing folders can be merged after name conflicts are resolved. However, the folders themselves cannot be merged.	Volumes and their clones can be spread across multiple folders. Volumes can be moved across folders in the same pool or in multiple pools.

Create a Folder

Procedure

1. From **Manage** > **Data Storage**, click **Folders**.
2. Click the plus sign to create a new folder.
3. In the **Create Folder** dialog box, enter the folder name and description.
4. Select the pool from the **Pool** dropdown.
5. From the **Management Type** dropdown, choose **None**, **VMware virtual volumes**, or **Microsoft SCVMM (SMI-S)**.
   - If you choose vVols, choose a vCenter from the **vCenter Server** dropdown. For multi-protocol array groups, you must also specify Fibre Channel or iSCSI in the **Protocol** dropdown.
   - If you choose Microsoft SCVMM (SMI-S), choose a policy from the **Performance Policy** dropdown.
6. From the **Space Limit** dropdown, choose **No limit**, **Based on usage** or **Based on provisioning**.
   - If you choose Based on usage, enter a limit and select **MiB**, **GiB**, or **TiB** from the dropdown.

     To enable existing volumes in the folder to exceed the usage limit, select the **Allow overdraft limit** checkbox and set a percent. The overdraft limit is the percentage by which the folder can exceed the usage limit.

- If you choose Based on provisioning, enter a limit and select **MiB**, **GiB**, or **TiB** from the dropdown.

7. From the **IOPS Limit** and **MIB/S Limit** dropdowns, choose **No Limit** or **Set Limit**.

   When either the IOPS limit or the MBP/S limit is met, input/output requests are throttled.

   - If you choose Set Limit for IOPS, enter a value of 256 or greater.
   - If you choose Set Limit for MBP/S, enter a value equal to or greater than the IOPS limit multiplied by the volume block size.

8. Click **Create**.

Edit a Folder

Procedure

1. From **Manage** > **Data Storage**, select the **Folders** view.
2. Check the name of the pool containing the folder you want to edit.
3. Select the pencil icon to edit the folder.
   Make any of the following changes, as desired.
4. Enter a new folder name.
5. Enter a new description for the folder.
6. From the **Space Limit** dropdown, choose **No limit**, **Based on usage** or **Based on provisioning**.

   - If you choose Based on usage, enter a limit and select **MiB**, **GiB**, or **TiB** from the dropdown.

     To enable existing volumes in the folder to exceed the usage limit, select the **Allow overdraft limit** checkbox and set a percent. The overdraft limit is the percentage by which the folder can exceed the usage limit.

   - If you choose Based on provisioning, enter a limit and select **MiB**, **GiB**, or **TiB** from the dropdown.

7. From the **IOPS Limit** and **MIB/S Limit** dropdowns, choose **No Limit** or **Set Limit**.

   When either the IOPS limit or the MBP/S limit is met, input/output requests are throttled.

   - If you choose Set Limit for IOPS, enter a value of 256 or greater.
   - If you choose Set Limit for MBP/S, enter a value equal to or greater than the IOPS limit multiplied by the volume block size.

8. Click **Save**.

Delete a Folder

You cannot delete a folder that contains any volumes.

> **Note:** Occasionally, in environments using HPE CSI Driver for Kubernetes, if you delete the folders for a tenant user, all the folders are removed from that tenant user without a warning message. When this happens, the tenant user is orphaned.

You can use the Volumes Move function to move or delete volumes.

Procedure

1. From **Manage** > **Data Storage**, select the **Folders** view.
2. Check the name of the folder you want to delete.
3. Click the "x" icon to delete the folder.
4. Click **OK**.

Note: You cannot delete a folder with volumes in it. You must first move or delete the volumes.

Deduplication

Deduplication is a form of data reduction that saves storage space. The deduplication process identifies duplicate content within a domain, and stores only one copy of that content.

The HPE storage array implementation of deduplication works at the volume block level on the following arrays:

- All Flash arrays running release 3.x or later
- Secondary Flash arrays running release 4.2.0 or later
- Select models of Adaptive Flash arrays running release 5.0.1 or later

When deduplication is enabled, identical content stored on the array is deduplicated using inline deduplication. Inline deduplication involves arrays deduplicating data in real-time, as data is received.

The deduplication process uses a two-level fingerprint system, with short fingerprints for speed of detection and long cryptographically secure fingerprints to ensure reliability. The deduplication process optimizes for “flocks” of duplicate data, consecutive runs of blocks that are duplicated. This multi-layer deduplication process allows for near-perfect duplication detection, while dramatically reducing the amount of main memory required to efficiently deduplicate large capacity SSDs.

If data has already been written to the array with deduplication disabled, the data on the disk cannot be deduplicated unless you migrate the data either using array-side functionality (for example, move the volume to another deduplication-enabled pool in the group) or host tools to migrate to a new deduplication-enabled volume or pool.

Note: Volume (and snapshot) limits and reserves are based on pre-deduplication usage.

Deduplication on Hybrid Arrays

Deduplication is supported on the following hybrid arrays:

- CS500, CS700
- CS1000, CS3000, CS5000, CS7000
- HF20, HF20H, HF40, HF60

These restrictions apply to deduplication on hybrid arrays:

- Pinned volumes cannot be deduplicated.
- Deduplication cannot be enabled across striped pools.
- Replicated data is not deduplicated; the data is replicated without any deduplication savings.
- The array must include the number of SSD drives indicated in the following table:

Array Model	Required Number of SSDs
HF20H	2 SSDs
HF20H fully populated	4 SSDs
HF20H fully populated and upgraded to HF40H	4 SSDs
HF20, HF40, HF60	6 SSDs
CS500, CS700	4 SSDs
CS1000	3 SSDs
CS3000, CS5000, CS7000	6 SSDs

Note: See the *Array Configuration Matrix* available on HPE InfoSight at https://infosight.hpe.com/ for more information.

Note: If a hybrid platform contains volumes with deduplication enabled, any extra flash capacity that results from unpinning a volume is used to increase deduplication capacity.

Note:

Arrays that are updated from release 5.0.2.0 and 5.0.1.0 might have volumes with deduplication enabled. Any arrays that are updated to release 5.0.3.0 or later with deduplicated volumes will operate as a deduplication capable array, regardless of the number of installed SSDs. Such configurations are *not* recommended by HPE.

The following tables provide information about the Maximum Deduplication Capacity (MDC) on supported hybrid arrays and the additional Flash to Disk Ratio (FDR) required to support MDC.

MDC and pool deduplication capacity outputs apply to hybrid arrays in the CS series only. On HF series and later models, the entire array capacity can be deduplicated.

Note:

You must have a four percent FDR to enable deduplication on the hybrid models. For MDC, you must have an additional four percent FDR for a total of eight percent FDR.

To see the deduplication capacity (TiB), log in to the array OS CLI as an administrator and run the **pool --info** *pool_name* command. On the HF20H, HF20, HF40, and HF60 models, this command returns **N/A** as the value for dedupe capacity (MiB). This is because you can enable deduplication for the entire array.

Table 9: Effective Capacity and Additional Flash Required to Support MDC

Platform	Maximum Deduplication Capacity (MDC)	Effective Capacity with 3x Deduplication	Additional Flash Required to Support MDC
CS500	40 TiB	120 TiB	1.6 TiB
CS700	100 TiB	300 TiB	4 TiB
CS1000	10 TiB	30 TiB	0.4 TiB
CS3000	40 TiB	120 TiB	1.6 TiB
CS5000	100 TiB	300 TiB	4 TiB
CS7000	200 TiB	600 TiB	8 TiB

Note: Before you enable deduplication on hybrid arrays, review the product documentation for complete details.

Pool-Level Deduplication (Default)

The default setting varies depending on the array type. These are the default settings:

- For pools consisting of a single All Flash array, and Secondary Flash array or Adaptive Flash array (HFxx): The pool-wide deduplication capability is turned on. All newly created volumes in the pool are created with deduplication enabled. If you turn the setting off, all newly created volumes in this pool inherit the deduplication setting defined by their performance policy.
- For pools consisting of a single Adaptive Flash array (CSxxxx, CSxxx): The pool-level deduplication setting is not available. All newly created volumes in this pool inherit the deduplication setting defined by their performance policy.

Managing Deduplication Capacity

Deduplication cannot be enabled on a storage pool if, at the time the storage pool is created, the current deduplication capacity (CDC) is less than or equal to zero.

Deduplication can be enabled on the storage pool if, after the storage pool is created, the CDC becomes greater than zero. This setting persists regardless of the CDC.

A pool can only be marked deduplication-enabled if the following four factors are present:

- The array type supports deduplication
- The array is a Secondary Flash Array
- The FDR is greater than 4% (the CDC is greater than zero)
- The array has enough SSDs to support deduplication

A volume created in a deduplication-enabled storage pool can have deduplication set to Yes, regardless of the CDC level, provided the FDR is at least 4%. Newly written blocks will be deduplicated if the CDC is greater than zero and the capacity of deduplicated data is less than the CDC.

If the CDC is equal to zero, or the capacity exceeds the CDC, deduplication of new writes stops.

If you increase the CDC, deduplication will resume; however the data that was written while deduplication was disabled will not be deduplicated. When old data is overwritten the newly written data will be deduplicated.

The following are suggestions of how to manage deduplication capacity:

Condition	Suggested Action
If the CDC is equal to the maximum deduplication capacity (MDC)	Perform a controller upgrade, if possible
If the CDC is less than the disk capacity	Add flash or unpin volumes
If the CDC exceeds the previous levels	Add a shelf that has a flash deduplication requirement (FDR) of at least 4%

Domains

A deduplication domain is the area where deduplication takes place. It is defined by three settings: intersection of containers (same pool, or folder hierarchy), performance policy, and block size.

Volumes that share blocks are grouped together in the same deduplication domain. Two characteristics help determine which volumes can be grouped together: application category and block size. An application category is an attribute indicating that the volumes store data from the same type of application. Application categories are predefined, and cannot be changed. They are selected when creating or updating a performance policy. Volumes with the same block size are able to be deduplicated, and can be part of the same deduplication domain. Volumes with different block sizes, performance policies or pools cannot be part of the same deduplication domain.

Cloned volumes inherit the parent deduplication domain; you cannot create a clone in another domain. To move a clone to another domain, you use the volume move operation.

Deduplication domains cannot be merged. Also, deduplication is not supported where the volumes are striped across a pool. Pools containing deduplicated volumes cannot be merged with other pools. You cannot add an array to a pool containing an All Flash array that has volumes with deduplicated blocks.

Enable All-Volume (Pool-Level) Deduplication

Procedure

1. Choose **Administration** > **Space**.

In the Deduplication section, you see a list of pools. Eligible pools (pools that contain a single all flash or secondary flash array) are available for selection. All other pools are grayed out.

2. Check the box for each eligible pool for which you want to enable deduplication.
   All volumes created in that pool from now on will have deduplication enabled. Volumes that already exist in that pool will not be affected.

Enable Deduplication Determined by Performance Policy

Procedure

1. Choose **Administration** > **Space**.
   In the Deduplication section, you see a list of pools. Eligible pools (pools that contain a single all flash or secondary flash array) are checked and available for deselection. All other pools are grayed out.
2. Uncheck the box for each eligible pool for which you want to disable deduplication.
   All volumes created in that pool from now on will use the deduplication setting from the performance policy of the pool. When new volumes are created, they inherit the deduplication setting defined in the performance policy. Volumes that already exist in that pool will not be affected. Deduplication on existing volumes can be changed by editing the volume attributes.

Enable Per-Volume Deduplication

Procedure

1. Go to **Manage** > **Data Storage**.
2. Check the volume or volumes for which you want to enable deduplication.
3. Click the ellipsis (More) icon.
4. Choose **Enable Deduplication**.

Disable Per-Volume Deduplication

Procedure

1. Go to **Manage** > **Data Storage**.
2. Check the volume or volumes for which you want to enable deduplication.
3. Click the ellipsis (More) icon.
4. Choose **Disable Deduplication**.

Storage Efficiency Reporting

The array GUI interface provides storage efficiency metrics in several places, to assist in monitoring and managing the capacity of HPE storage arrays. For volumes, this information includes the following:

- The assigned size of a volume
- The mapped size of a volume (the unreduced, or logical usage)
- The compression ratio of the data in the volume

For pools and groups, this information includes the following:

- Aggregate space savings, including data reduction savings and thin provisioning savings
- Data reduction savings, including zero-block, compression, deduplication, and clone savings)

Note: Clone and compression savings ratios are based on all volumes. Deduplication savings ratio is based on volumes that participate in deduplication.

You can see the reported metrics in the following places:

- Monitor Capacity Home Page — shows the total data reduction ratio (total logical usage / total physical usage) for all pools in the group, as applicable. The total data reduction ratio includes savings from zero-blocks, clone-sharing, compression and deduplication. It also shows the overall savings that includes data reduction savings and thin provisioning savings (total size/total logical usage).
- **Monitor** > **Capacity** with All pools and All volumes selected — shows savings reports on the total savings ratio for the pool/group, and the total bytes saved. Also shows the total physical space in use, the unused physical space reserved to thickly provisioned volumes, and the free space.
- **Monitor** > **Capacity** with one pool and All volumes selected — shows the total physical usage, unused reserve, and total size of the pool. Shows the total logical usage, unused reserve, and total size of the pool.
- **Monitor** > **Capacity** with one volume selected — shows size, usage, unused reserve, and overall compression ratio for the volume, and indicates whether deduplication is enabled or disabled.
- **Monitor** > **Capacity** with one folder and All volumes selected — shows size, usage, unused reserve, and overall compression ratio for the volume.
- Volume Summary — shows size, usage, unused reserve, and overall compression ratio for the volume, and indicates whether deduplication is enabled or disabled. Also shows volume and snapshot usage as logical space.

Storage Pools

You can divide the storage in multi-array groups into multi-array storage pools. For example, you might have a segregated storage pool for certain applications, users, or workloads. Arrays can be members of only one pool at a time. However, volumes assigned to storage pools can span multiple arrays.

The difference between groups and storage pools is that groups aggregate arrays for management, while storage pools aggregate arrays for capacity and performance. Storage pools provide automatic load balancing and migration capability, if all the other prerequisites for pools are met.

Pool Considerations

In appropriate environments, you can add or remove group members from a storage pool or you can combine storage pools.

A single-array storage pool provides fault isolation. Volumes whose pools are on one array keep data placement simple and snapshots truly local. All host operating systems identified in the *Validated Configuration Matrix* and array data protocols support single-array pools.

A multi-array pool lets you consolidate capacity and scale performance. Volumes striped across multiple array pools can have larger capacity, pool-wide resources, and more even growth with less rebalancing later. Some host operating systems support multi-array pools.

Consider the following points when planning whether and how to implement storage pools.

- Operating system on host machines

  Windows, ESX, and Linux hosts for which a supported Connection Manager is available can use multi-array storage pools. Any hosts for which a supported connection manager is unavailable require single-array pools.

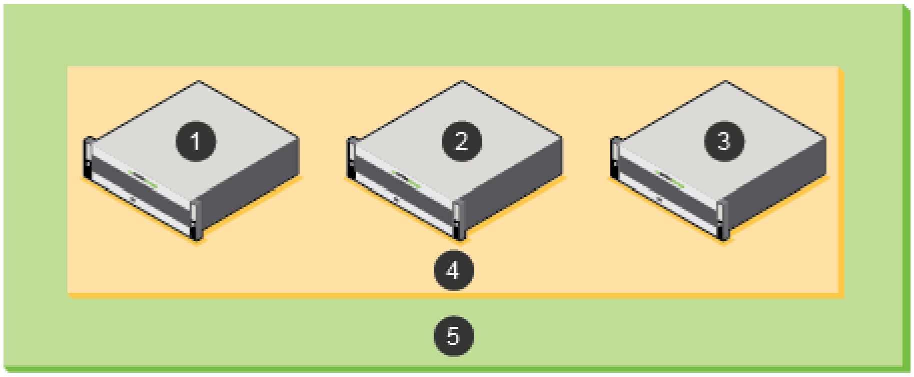
- Disk speed
- Disk capacity
- Network bandwidth
- Application using the storage pool
- Load balancing requirements
- Volumes that will reside on the storage pool

If you are planning on pooling arrays across dissimilar models, consider the following caveats.

- Coupling a lower performance model array with a higher performance model could degrade the performance of the pooled system.
- Performance can be affected when you merge arrays into a single pool when the arrays have different performance caps, cache configurations, and storage capacity.
- Consider using a multi-array pool to migrate data from an older array to a newer array, as this method can be less disruptive than using replication to migrate data.

Storage pools can include some or all of the arrays in a group. When you add an array to a group, you must also add this array to one of the existing storage pools for that group or you can create a new storage pool and add the array to the new pool.

The first implementation example shows a group that includes three HPE arrays that are all in the same group in the default pool.



1 Array 1

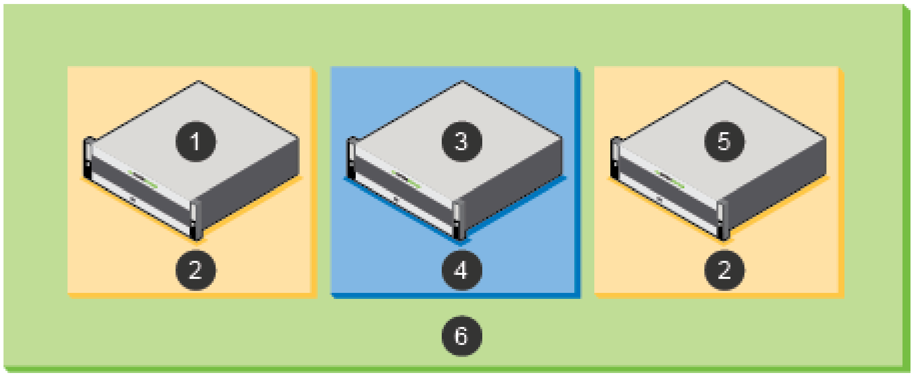
2 Array 2

3 Array 3

4 Default pool

5 Multi-array group that includes arrays 1, 2, and 3

The second implementation example shows two pools that allow a specific application, such as Microsoft Exchange, to use volumes that are spread across two of three arrays in the group, but not use the storage on a third array. In this scenario, the storage on the array labeled 3 is in the default pool. To configure this example, remove the arrays labeled 1 and 5 from the default pool, and then create an Exchange storage pool by adding only the arrays labeled 1 and 5 to the pool.



1 Array 1

2 Exchange pool

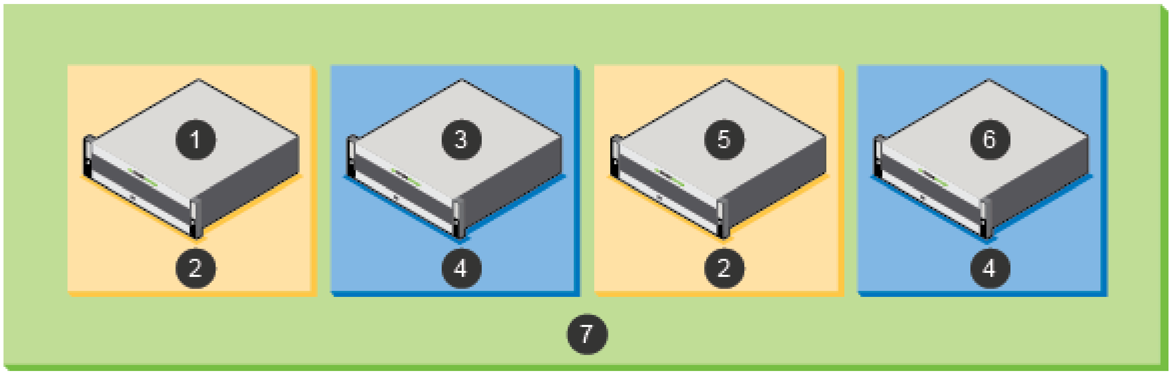
3 Array 3

4 Default pool

5 Array 5

6 Multi-array group that includes arrays 1, 3, and 5

The third implementation example shows adding a new array that is labeled 6 to the group that is assigned to the default storage pool. In this scenario, you have other alternatives. One alternative is to move array 6 to the previously created Exchange pool. Another alternative is to create a new storage pool for array 6 and leave only array 4 in the default pool.



1 Array 1

2 Exchange pool

3 Array 3

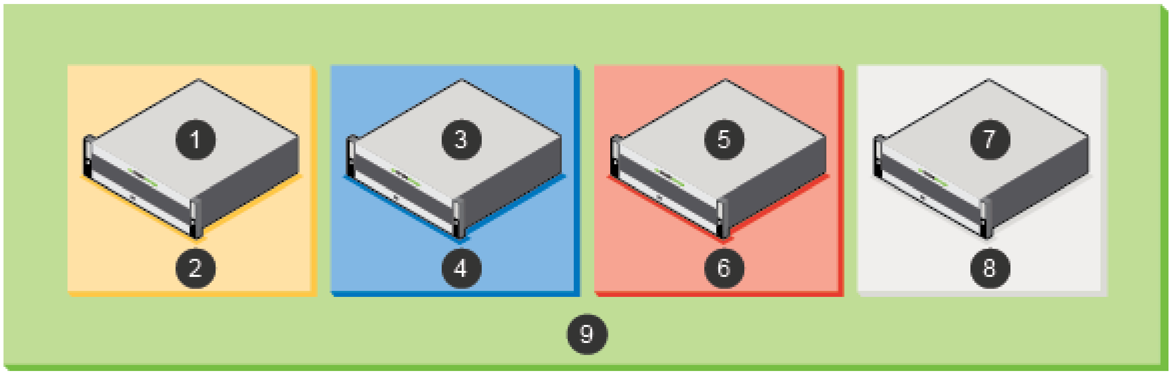
4 Default pool

5 Array 5

6 Array 6

7 Multi-array group that includes arrays 1, 3, 5, and 6

The fourth implementation example shows having one group with four HPE arrays, where each array is in a separate storage pool.



1 Array 1

2 Exchange pool

3 Array 3

4 Default pool

5 Array 5

6 SQL Server pool

7 Array 7

8 VDI pool

9 Multi-array group that includes arrays 1, 3, 5, and 7

Create a Storage Pool

You cannot change the default storage pool, but you can add additional storage pools and you can move volumes between the pools.

A pool confines data to a subset of the arrays in a group. Data of resident volumes is striped and automatically rebalanced across all members of a pool. Pools dictate physical locality and striping characteristics. Think of a pool as a logical container that includes one or more member arrays in which volumes reside. A member array and all of its expansion shelves can only be part of one pool.

Before you begin

Note: You can view the list of storage pools on the Data Storage page.

- You must have at least one unassigned array to put into the new storage pool.

- You can also create a new storage pool when adding an array to a group.

Procedure

1. From **Manage** > **Data Storage**, and select the **Group** view at the top of the facets panel.
2. Click **Group Actions** > **Create Pool**.

   Note: This option requires having at least one array that is not yet assigned to a pool.

3. In the Create Pool dialog box, type the name for the new storage pool.
4. Select all arrays to include in the new pool.
5. Click **OK**.
   The new storage pool now appears in the list of pools.

Add or Remove Arrays from a Storage Pool

You can modify storage pools to add or remove arrays. Only one pool can be assigned to a given array. Multiple arrays can be assigned to the same pool.

You cannot add an array to an existing pool that has synchronous replication enabled.

Note: A pool must always have one member array.

CAUTION: Exercise caution when you change a storage pool assignment because it may result in a large migration of data.

Procedure

1. Go to **Manage** > **Data Storage**.
2. Select the pool name from the navigation tree.
3. Go to **Pool Actions** > **Edit**.
4. In the Edit Pool dialog box, click the green arrow next to any arrays to add them or click the red arrow next to any arrays to remove them.

   CAUTION: Removing an array from a storage pool causes any data in volumes that use the array in the storage pool to be moved to the remaining storage pool members.

5. Click **Save**.

Merge Storage Pools

You can merge two storage pools to combine the contents of both pools. To merge multiple pools, merge two pools at a time until the desired storage pool is created.

Note: A pool merge operation is blocked when one of the pools contains synchronously replicated volumes.

Important: Deduplication Domains cannot be merged, see Domains on page 88 for details.

Procedure

1. Select **Manage** > **Data Storage**.

Note: The Storage Pools menu option only appears if you have more than one array in your environment.

2. In the list of storage pools for the group, click the name of the storage pool into which to merge another pool. This is the target pool.
3. On the details page for the selected storage pool, go to **Pool Actions** > **Merge Pools** .
4. In the Merge Pools dialog box, select the storage pool to merge into the target pool.
5. Click **Merge Pools**.
   The storage pools are merged and the changes appear in the Storage Pools summary page.

Volume Moves

Volume move operations allow you to move volumes between folders or between pools.

Important notes about volume moves:

- Volume moves are **not** supported for volumes configured for synchronous replication.
- You should **always** use storage vMotion to move VMware virtual volumes (vVols) from the vCenter. Moving vVols using the GUI can be a highly disruptive operation and can lead to a loss of data or VM accessibility

When you move a volume from one pool to another, parts of the volume might exist on either the pool or a folder of that pool. When the move is complete, the data exists only on the destination pool or folder. It is not preserved on the source pool or folder.

The two most common reasons to move data are to increase performance by moving a volume from a single-array pool to a multi-array pool or to manually balance space usage between pools.

When you move a volume between pools, you also move all of its snapshots and clones. User access permissions and encryption settings move with the volume.

During a move, the change from one pool to another is transparent. There is no disruption of service, and, during the move process, any write is made to the current location of that part of the volume. A move between pools can require some time, depending on the amount of data in the volume, the number of clones, and the pools being migrated to and from. A move to or from a folder is almost immediate.

Important: During a move, some volume data will reside partially on both pools; consequentially, when performing a move, you must use the HPE Storage Connection Manager on the host to facilitate the move. You should also use Connection Manager to check hosts for old connections to targets that connect directly to data IPs.

If these connections exist, then for each target, perform **one** of the following tasks:

- Confirm that other connections to the corresponding group discovery IP exist.
- Establish new connections that point to the corresponding group discovery IPs before disconnecting these old connections.

In addition, make sure you perform the same checks for any defined static, favorite, or persistent targets and update any connections as necessary.

Volumes can be moved independently or simultaneously with other volume-move operations. However, while in the process of a move, you cannot start another move on the same volume.

Note: For Fibre Channel groups, in order to avoid losing data paths between the host and the volume being moved, it is recommended that you check that Fibre Channel connectivity exists between the host and the arrays in an FC group prior to initiating a volume move operation.

Move a Volume from One Storage Pool to Another

Moving a volume also moves its snapshots and clones from one storage pool to another. Because a folder is confined to a pool, a move between pools will affect the folder assignment. The destination pool must have sufficient space to accommodate the current use and reserve space for all volumes being moved.

Depending on the size of the volume and the amount of data, it could take some time to complete a move from one storage pool to another. During this time, writes are allowed. Some forwarding of I/O requests from arrays in the source pool to arrays in the destination pool can occur during the move. This can result in temporarily reduced I/O throughput.

At any point during a move, an administrator can stop the move. When a volume move is stopped, all data that has already moved onto the destination pool moves back to the source pool. This may take some time, depending on the size of the pools and how much data has been moved.

Procedure

1. From **Manage** > **Data Storage**.
2. On the Volumes summary page, check the name of the volume to move to another storage pool.
3. Click the arrow icon to move the volume.
4. In the Move Volumes dialog box, select the Destination Pool into which to move the selected volume, its snapshots, and its clones.
5. Click **Move**.

   Optionally, you can track the status of the move by moving to the Volume view.

Move a Volume from One Folder to Another

For volume moves within a single pool, only the volume is moved from one folder to another. The data is not moved in the process, which is virtually instantaneous. Due to the rapid nature of the move, the process cannot be stopped after it is started.

Procedure

1. Go to **Manage** > **Data Storage**.
2. On the Volume summary page, check the box associated with the volume or volumes to move to another folder.
3. Click the right pointing arrow icon.
4. In the Move Volumes dialog box, select the destination folder.
5. Click **Move**.
6. Verify that the volume was added to the folder.
   a) Go to **Manage** > **Data Storage**.
   b) Select the folder from the Group list.
   The volume should appear in the list for the folder you moved it to.

End a Volume Move in Progress

You can end an in-progress volume move at any point before completion. All data already moved onto the destination pool moves back to the source pool.

Ending a volume move can take some time, depending on the size of the pools and how much data has been moved.

If you need to undo a volume move after the move is completed, you must perform a second volume move back to the original pool.

Procedure

1. From **Manage** > **Data Storage**, and select the **Volumes** view.
2. Select the volume that is currently being moved so that you can see details about the volume.
3. Click the **X** icon to stop the process.
4. In the confirmation dialog box, click **Abort**.

Delete a Storage Pool

You can delete a storage pool that is obsolete or no longer used after you add its member arrays to other storage pools.

Note: The default pool cannot be deleted.

Before you begin

- Before you delete a storage pool on an array, you must move its associated volumes to another pool or remove the volumes. If you do not, the pool delete action will disconnect the pool from the array, leaving the volumes unassigned.
- An alternative to deleting a pool is to merge it into another pool on different array. The result is that the source pool no longer exists and the destination pool contains any volumes that were in the source pool.

Procedure

1. Select **Manage** > **Data Storage**.
2. Click the name of the storage pool to delete.
3. Click **Delete**.
4. When prompted to confirm the deletion, click **OK**.

Data Protection

Ensuring that your data is protected is a critical part of managing arrays. Volumes that hold multiple components of an application, such as databases and transaction logs, can be grouped into *volume collections*. A volume collection includes a set of protection schedules that create snapshots of each associated volume at specified intervals.

The protection schedule specifies the downstream partner where the volume and snapshot data is replicated as well as information about how often the snapshots are taken and how long the snapshots are retained.

A volume collection can have up to ten protection schedules and up to two downstream partners when you select the replication type of **Periodic Snapshot**. Generally, each application uses a different volume collection.

Arrays ships with several predefined protection templates. These templates include information that is based on best practices for commonly used applications. You can copy the predefined templates and modify the copies, or you can create new protection templates to best match the requirements of applications used in your environment.

All volumes assigned to the volume collection use the same protection schedules, which specify downstream partners, scheduled snapshots, replication, and retention settings. After the volume collection is created, it can be modified as needed.

If you plan to take snapshots of volumes manually, you can create a volume collection without schedules on those volumes. This capability is available in the command-line interface (CLI).

Volume Collections

Volume collections are sets of volumes that share data protection characteristics, such as protection schedules for snapshots and replication.

Snapshots for all volumes in a collection are captured simultaneously to ensure that the data across these volumes is mutually consistent. All the volumes in a volume collection use that collection's protection schedules. Each schedule specifies the downstream partner, when snapshots are taken, and the retention policies for the snapshots.

For disaster recovery, all volumes in a volume collection can simultaneously fail over to a replication partner. You can also manually switch to a replication partner.

Volume collections can have up to two replication partners when you select the replication type **Periodic Snapshot** in the protection template.. These can be two on-site, downstream replication partners or one on-site downstream replication partner and one HPE Cloud Volume partner.

You can create a volume collection for each application. Each volume collection can contain up to ten schedules. These schedules are additive, so when schedules overlap, snapshots and replicas are created for every schedule. You can create volume collection schedules that are specific to some Microsoft applications or VMware virtual machines to ensure consistency.

When configuring protection schedules, be sure that you allow enough time for one schedule to complete before another starts. For example, if Exchange protection schedule 1 has DB verification and replication enabled and runs every hour, and Exchange protection schedule 2 has DB verification turned off and no replication and runs every five minutes, it is possible that, without enough time between snapshots in schedule 2, schedule 1 will not be able to start.

Careful planning can enhance a backup strategy. For example, you might want to set the retention period for hourly snapshots to a few days so you can back up quickly and precisely if necessary. Then you might want to retain daily snapshots for longer periods, such as several weeks. You can define retention periods for snapshots. The protection schedule templates provided by storage arrays have default values that keep volumes in the normal retention range, which is 150 snapshots or fewer, retained either locally or on the replication partner. Although you can configure volumes with a high snapshot retention schedule, it is not recommended. As you define protection schedules, a meter identifies when you reach the high retention range. A mouse-over tooltip identifies the issues with defining protection schedules that exceed the normal retention range.

Note: Volumes that have a high snapshot retention schedule count in the snapshot limits for the volume, group, and pool.

Volume Collections and Multiple Replication Partners

You can specify up to two downstream replication partners for a single volume collection when you create multiple data protection schedules and specify a replication type of **Periodic Snapshot**.

Each protection schedule is limited to one replication partner. You can specify one partner for a schedule and the other partner for a different schedule.

A volume collection can have up to ten schedules. For example, a volume collection might have Partner_A and Partner_B as replication partners. If you set up ten schedules for the volume collection, you could have schedules one through five replicate to Partner_A and the rest replicate to Partner_B. Or you could assign Partner_B to schedules one and two and Partner_A to the rest of the schedules. There is no required order for assigning partners to schedules.

Note: If you attempt to specify a third replication partner in the set of schedules, you will receive an error message.

The replication partners can be either two on-site downstream partners or one on-site downstream partner and one HPE Cloud Volume partner.

Note: You cannot have two HPE Cloud Volume partners.

Create a Volume Collection

You can create as many volume collections as needed. An initial schedule is created automatically when you create a volume collection.

Note: If you want to specify synchronous replication as the replication type on a volume collection, you must do so when you create the volume collection. You cannot change the replication type after the volume collection is created. Also, you cannot use both protection templates and synchronous replication.

Procedure

1. Choose **Manage** > **Data Protection** > **Volume Collections**.
2. Click the plus (+) sign to add a new volume collection.
3. On the Name and Schedules page in the Create Volume Collection dialog box, add the required information.
   a) Enter a name, and, if you are using a protection template, select it.

      Note: Protection templates are not supported with synchronous replication.

   b) Select a replication type from the list and a replication partner.

      If you want to associate two downstream replication partners with the volume collection, you must specify **Periodic Snapshot** as the replication type. You can specify only one downstream partner for a protection schedule, but when you use **Periodic Snapshot** to set up the schedules, you can switch between two downstream partners as you set up the schedules. These partners can be either two on-site partners or one on-site partner and one HPE Cloud Volume partner.

   c) For the Synchronization Service, select one of the following options.

      This quiesces application I/O when snapshots are created to ensure application-consistent backups and replicas.

Option	Description
None	Create snapshots that do not need synchronization.

Option	Description
Microsoft VSS	Create application-consistent snapshots for applicable types of Microsoft applications, including Hyper-V. Synchronization quiesces volume traffic before a snapshot is taken. This ensures that your application never has a snapshot with incomplete data. Select the appropriate application and provide further information such as the application server address. For detailed information, see the *Windows Integration Guide*.
VMware vCenter	Create snapshots through a VMware vCenter Server. This ensures that snapshots are VMFS-consistent. The first time you create a volume collection with schedules that use this synchronization setting, you need to provide the vCenter host name or IP address, user name, and password. For detailed information, see the *VMware Integration Guide*.

To avoid possible performance issues for snapshot schedules that synchronize with Microsoft Exchange, do not run the snapshot verification more than once a day.

d) In the Schedules section, create a custom protection schedule.

Default values are provided for many of the fields.

- You can create multiple schedules for the volume collection.

  For example, you can create one schedule for working hours, one for peak hours, and one for weekends. Schedules can overlap, but they cannot span midnight. If you need a schedule that takes hourly snapshots from 10 PM to 4 AM, you need to create two schedules. The first schedule covers the time period from 10 PM to 11:59 PM and the second schedule covers the time period from 12 AM to 4 AM.

- If you chose replication, specify how frequently (or after how many snapshots) replication of the volumes in the volume collection should be triggered.

4. After you define all the protection schedules you need, click **Next**.
5. On the Create Volume Collection page, in the Volumes tab, select a volume that appears in the Available volumes list, click the right arrow to add it to the Selected list.

   You can filter the volumes by name and location (either in a pool or a folder). You can also select multiple volumes and add them all at once.

   Note: You cannot associate a volume from a replication destination.

   Repeat until you have added all the available volumes that you want to include in this volume collection.

6. Click **Create**.

View Volume Collection Details

Procedure

1. Choose **Manage** > **Data Protection** > **Volume Collections**.

   The list of volume collections is displayed.

2. Click the name of the volume collection for which you want to view details.

   View volume collection detail information using the Schedules, Volumes, and Snapshot Collections tabs.

3. When you are finished, click **Data Protection** to return to the list page.

Protect a Standalone Volume

Some volumes may not need to be part of a volume collection. You can associate standalone volumes with volume collections to define their snapshot and replication schedules. The volume collection associated with a standalone volume cannot contain any other volumes.

Procedure

1. Choose **Manage** > **Data Storage** > **Volumes**.
2. Choose one of the following options:

Option	Description
To create a new volume:	Click the + icon. Add all the necessary information in the dialog box. Click **More Options**. Click **Protection** on the progress bar, choose **Protect as standalone volume** and then continue with the steps in Create a Volume on page 65.
To edit an existing volume:	Click the volume name and then click **Edit**. On the Protection page, choose **Protect as standalone volume**.

3. Click **Create** to create the new volume or **Save** to save the changes to an existing volume.

Results

To remove a stand-alone volume collection or to remove protection from a volume in a stand-alone volume collection, you can edit the volume and mark it as “Unprotected.” Then the volume can be added to a volume collection that contains volumes that are not stand-alone.

Edit a Volume Collection

Procedure

You can modify a volume collection to make it more effective in a changing environment.

1. Choose **Manage** > **Data Protection** > **Volume Collections**.
2. Click the name of the volume collection to modify.
3. From the **Actions** menu, click **Edit**.
4. Modify the fields as needed.

   Make sure to click the Volumes tab to add or remove volumes from the volume collection. For information on completing the fields in the wizard, see Create a Volume Collection on page 99.

   > **Note:** If you disassociate a synchronously-replicated volume from the volume collection, it causes the associated volume on either the upstream or downstream replication partner to be disassociated also.

5. Click **Save**.

Delete a Volume Collection

You can delete any volume collection that has no volumes associated with it. You must remove all volumes prior to deleting the volume collection.

Procedure

1. Remove all volumes associated with the volume collection.
   a) Choose **Manage** > **Data Storage**.
   b) Click the **Volumes** tab, then click a volume name to open the volume details page.
   c) Click **Edit** to open the volume edit wizard.

   d) On the Protection page, select to either join a different volume collection or to remove the volume from all volume collections.
   e) Repeat as needed to assign all associated volumes to different volume collections.
2. Choose **Manage** > **Data Protection** > **Volume Collections**.
3. Click the name of the volume collection you want to delete to open its detail page.
4. In the **Actions** menu, click **Delete**.
5. Click **OK** to confirm the deletion.

Protection Templates

Protection templates are sets of defined schedules and retention limits that you use to pre-fill the protection information when creating volume collections and standalone volumes. As a result, protection templates not only minimize repetitive entry of schedules, they also minimize errors and inconsistent setups by allowing the creation and management of a finite set of protection templates to meet all business needs.

Note: You cannot define protection templates with synchronous replication settings.

After you create a volume collection, schedules and synchronization settings can be changed on the collection. This makes using the protection templates an easy, fast way to create multiple volume collections that share similar schedules: Use the same protection template to create as many volume collections as you want, then modify the volume collections with the changes specific to the needs of each collection. This means that you can create volume collections that are grouped as logical restoration groups.

You can create as many volume collections from the same protection template as desired. Later changes to the volume collection will not affect the template. Likewise, changes to the protection template do not affect previously created volume collections.

Note: You cannot edit or delete the predefined protection templates provided with the array; however, you can create new protection templates as needed.

Important: When setting up protection schedule for a protection template, be sure that you allow sufficient time for one schedule to complete before another one starts. For example, if Exchange protection schedule 1 has DB verification and replication enabled and runs every hour, and Exchange protection schedule 2 has DB verification turned off and no replication and runs every five minutes, there might not be enough time between schedule 2 snapshots for schedule 1 to start.

Create a Protection Template

You can create as many protection templates as needed. You can use the ones provided with the array, or customize your own.

Note: If you create protection templates that uses replication, configure the replication partners before you create the protection template.

Procedure

1. Choose **Manage** > **Data Protection** > **Protection Templates**.
2. Click **New Protection Template** to start the Create a protection template wizard.
3. Provide a name for the new template.

   Template names should indicate the general use that the set is designed for, are case sensitive, can contain between one and 64 alphanumeric characters, dashes (-), and dots (.), but cannot start with a dot or dash, or contain underscores, spaces, or any other punctuation.

4. For **Synchronization Service**, choose one of the following options for synchronizing volume collection snapshots with application or hypervisor (VM) components running on the volume through Microsoft Volume Shadow Service (VSS) or VMware API and supply the required information for your choice::

   - None (no synchronizing)
   - Generic
   - Microsoft VSS
   - VMware vCenter

5. (Optional) To enable the replication schedule for snapshots triggered by an external application, expand **Third-Party (Advanced)**, then check **Snapshot triggered by third-party application**.
6. Create or modify the schedule to use as the template. You can create up to ten schedules.

   To help eliminate possible performance issues for snapshot schedules that synchronize with Microsoft Exchange, do not run the snapshot verification more than once daily.

   a) **Schedule name:** Provide a name for the schedule.

      Schedule names are case sensitive, can contain between one and 64 alphanumeric characters, dashes (-), and dots (.), but cannot start with a dot or dash or contain underscores, spaces, or any other punctuation.

   b) **Take Recovery Point:** Specify how often the snapshot is taken. For example, you could specify that a snapshot be taken every 45 minutes.
   c) **Time Interval:** Enter the time range during which the system will take the snapshots. For example, you might enter 2:00 to 8:00. The system would only take snapshots from 2 a.m. until 8 a.m.
   d) **Days:** Specify which days the system takes snapshots. If you deselect a day, the system does not take snapshots on that day.
   e) **Retain:** Each schedule will store the specified number of snapshots.
   f) **Application Synchronization:** If you chose a synchronization service, select **Enabled**. If you selected Microsoft VSS as the service, you have the choice of verifying backups.
   g) **Replication Type:** Select **Periodic Snapshot** to replicate snapshots for volume collections.
   h) **Replication Partner:** Select the downstream replication partner to which the schedule will replicate the volumes in the volume collection. You must have already configured the downstream replication partner.

      Volume collections support up to two downstream replication partners; however, you can only specify one partner for one schedule. When you create another schedule, you can either specify that partner again or specify the other replication partner.

7. (Optional) Repeat these steps to create additional protection schedules for the protection template.

   > **Note:** You can create up to ten protection schedules for one protection template. The schedules can address different replication needs. For example, you might create one schedule for working hours, one for peak hours, and one for weekends. Schedules can overlap, but they cannot span midnight.

8. Click **Finish**.
   The new protection template is created and can be selected when you create volume collections.

Edit a Protection Template

You can edit user-defined protection templates, but the changes will apply only to volume collections based on the template after it has been changed. Existing volume collections are not affected.

> **Note:** The pre-defined protection templates supplied with the array cannot be edited.

Procedure

1. From the main menu, choose **Manage** > **Data Protection** > **Protection Templates**.
   The protection template summary page lists all existing templates.
2. Select the protection template to modify, then click **Edit**.

The system launches an editing wizard.

3. Make any desired changes to the protection template name, then click **Save**.
4. Click the **Synchronization** tab, and make any changes to the synchronization settings, adding or removing synchronization or changing credentials as needed.
5. Click the **Schedules** tab to create a new schedule, modify the existing schedule, or delete a schedule.
6. Click **Save** to save the protection template.

Delete a Protection Template

Over time, you may find that a protection template is no longer needed. You can delete any user-defined protection template without affecting existing volume collections.

Procedure

1. From the main menu, choose **Manage** > **Data Protection** > **Protection Templates**.
2. Select the protection template to delete, then click **Delete**.
3. Click **Yes** to confirm that you want to delete the protection template.

Snapshots

You can manage snapshots the same way that you manage volumes. In reality, snapshots are volumes. They are subject to the same controls and restrictions as volumes. You can clone, replicate, and modify snapshots. Initiators can access snapshots.

Snapshots Overview

The initial snapshot for a volume uses no space because it shares its original data with the volume from which it was taken. Each successive snapshot consumes some amount of space because it captures the changes that occurred on the volume. The changed blocks are compressed to reduce capacity consumption.

Consider the change rate of the applications using the volume, the assigned replication strategy, and the snapshot retention to determine the amount of space you need for snapshots. You can retain numerous snapshots in most environments.

Initiators access online snapshots just like they access online volumes. To access snapshot data, set the snapshot online and log the initiator into the snapshot.

When you delete a volume, the snapshots that are associated with that volume are also deleted. If the volume has online snapshots, they must be taken offline before you can delete them.

Snapshots and Daylight Savings Time

In cases where the system time changes, whether it is changed manually or automatically, if the time change is identical to a protection schedule interval, the next scheduled snapshot is skipped. Daily schedules may have two snapshots, and are skipped only if the snapshot time falls within the missed time frame. For example, if you have an hourly snapshot schedule and the system makes a Daylight Savings Time adjustment of one hour, the next scheduled snapshot is skipped because the system sees the appropriate snapshot for that hour is already taken.

Snapshot Consistency

Stagger snapshot schedules to ensure application synchronization, I/O quiescing, database verification, and so on. Consider the following points for different application types.

Microsoft application snapshots	For some Microsoft applications, such as Microsoft Exchange®, snapshots require that the application writes are flushed to the database and traffic is stopped while the snapshot is taken. This ensures that there is never partial data stored in the snapshot. The OS performs this step automatically when Microsoft VSS synchronization is enabled.
VMware snapshots	If your data center uses VMware vCenter, ensure that traffic is stopped while the snapshot is taken so that the snapshot is complete and can be cloned directly to a new virtual machine. The OS performs this step automatically when VMware vCenter synchronization is enabled.
Application-consistent snapshots with VMFS	The VMware snapshot captures the state and data of a virtual machine at a particular point in time. When creating a snapshot, VMware provides the "quiesce" option which flushes dirty buffers from the guest OS in-memory cache to disk, and offers application consistency through VSS requestor in VMware Tools. The Protection Manager takes advantage of the VMware quiesced snapshot option and combines it to achieve consistent and usable volume snapshots and replicas.

Snapshot Rate Limits

All volumes in a group are associated with a volume collection. Multiple volume collections may be created for each group, and each volume collection may have multiple protection schedules. Protection schedules may have different periods, or rates, such as hourly, daily, or weekly. An hourly schedule takes a snapshot of all volumes in the volume collection once per hour. A schedule that is configured to start at midnight begins taking snapshots of all volumes in the collection at 00:00, and at each hourly interval thereafter.

Beginning with OS 4.x, the maximum expected snapshot completion rate is 250 snapshots per minute per array group. The maximum cumulative outstanding snapshot count is the total of all snapshots for all protection schedules in the group, and cannot exceed 4,000 at any point in time. The outstanding snapshot count for a schedule is the number of snapshots started at that point in time or during the prior minute, but not completed because of the 250 snapshot per minute rate limitation. Outstanding snapshots are carried forward to the next minute, and completed at a rate of 250 per minute until all are finished.

For example, a protection schedule is configured to start and repeat every five minutes (T equals 5), and contains 270 volumes. The outstanding snapshot count at minute one is 270. All snapshots in the schedule must be completed in five divided by two (T/2), or three minutes. During minute one, 250 snapshots are taken. The remaining 20 snapshots are carried forward and completed during minute two. When the schedule repeats at the next five-minute interval, 250 snapshots are taken during minute five and the remaining 20 during minute six.

Schedules that have a lower repeat interval, which is calculated as the number of minutes in the interval, have a higher priority than schedules with a higher repeat interval. For example, daily schedules are prioritized to start before hourly schedules. When multiple schedules have the same repeat interval and are configured to start at the same time, the one that was created first has the higher priority. Higher priority schedules are considered first in determining the maximum outstanding snapshot count and the total expected snapshot completion time.

The more aggressive the schedule, the fewer volumes that can be protected. In order to prioritize all snapshots, those with daily schedules are completed before those with hourly intervals. Snapshots with hourly schedules are completed before those with intervals in minutes.

If you create ten volume collections, each with a single hourly protection schedule containing 50 volumes, a total 500 snapshots are scheduled. An hourly schedule has a time (T) period of 60 minutes. All snapshots must be completed in T divided by two, or 30 minutes. If all ten schedules are set to start at the same time, a maximum of 250 snapshots are taken during the first minute of the hour, and 250 are carried forward. The remaining 250 snapshots are taken during the second minute.

If you then create ten new volume collections, each with a daily protection schedule containing 50 volumes, the 500 new daily snapshots are added to the 500 hourly snapshots. You now have a cumulative total of 1,000 snapshots. If all ten daily schedules are scheduled to start at the same time as the ten hourly schedules, the snapshots are taken in the following order:

1. The first 250 of the daily snapshots are complete in minute 1, and the remaining 250 daily plus the 500 hourly are carried forward.
2. The remaining 250 daily snapshots are completed in minute 2, and the 500 hourly snapshots are carried forward.
3. The first 250 of the hourly snapshots are completed in minute 3, and the remaining 250 hourly snapshots are carried forward.
4. The final 250 hourly snapshots are completed in minute 4.

When you create or edit snapshot schedules, the OS makes calculations to determine whether the changes will exceed the 250 snapshots per minute or the maximum outstanding snapshot count 4,000 limits. If either one will be exceeded, the operation fails. To avoid exceeding the outstanding snapshot count when you add a new schedule or edit an existing schedule, stagger the schedule start time.

Volume and Snapshot Usage

Space used by a snapshot is never more than the space used by the volume at the time the snapshot was created. Any "live" new data introduced by snapshots is attributed to the live volume space usage and not the snapshot usage. Blocks are attributed to snapshot space usage when they are overwritten in live state. The easiest way to think about this is that snapshots consume space only when a block is modified or deleted.

For example, if you write 50 GB to a volume and take a snapshot, the initial snapshot shows zero snapshot usage, because it points to the same blocks on disk, which are "live." If you write another 50 GB to the volume, making a total of 100 GB, and then take another snapshot, the snapshots still consume no space. In fact, you can create several snapshots and they will all consume no additional space for the newly written 100 GB.

If you overwrite the 100 GB, then all snapshots start to consume space. Their cumulative space usage should be approximately 100 GB.

When some applications, such as PowerPoint, Excel, and Word modify files, the applications do not necessarily update the specific blocks in the file that changed. Instead, the applications create a new file. In this case, after you modify a file from one of these applications, a snapshot could show no usage because the original file the snapshot points to was not changed, but instead was seen as a new file.

Pending Deletions and Snapshot Usage

If there are pending deletions, the **Snapshot Usage** field generally displays a value greater than zero. This happens even if there are no user or hidden snapshots.

The array OS processes data deletion as a low priority background operation to ensure that maximum performance is available to initiators. When there are numerous large deletions or overwrite workloads, the pending deletions might increase temporarily.

Note: In the CLI, this information appears as **Uncompressed snapshot usage including pending deletes (Mib)** when you are running OS 5.1.x.x and later and as **Snapshot usage including pending deletes (MiB)** in earlier versions of the OS. In addition, the values the CLI displays for pool information and array information also include the overall pending deletions.

Automatic and Manual Snapshots

You can manually take a volume snapshot at any time. Manual snapshots are often used for testing a new application before integrating it with a production volume or for troubleshooting.

You can assign a volume to a volume collection so that snapshots and replication automatically occur based on the schedules associated with the volume collection. Automatic snapshots are typically used for backup operations. Use your existing backup software, triggered by the snapshot schedule.

Note: When the system time changes, and the time change is identical to a protection schedule interval, the next scheduled snapshot is skipped. Daily schedules may have one or more snapshots per day, and are skipped only if the snapshot time falls within the missed time frame. For example, if you have an hourly snapshot schedule and the system makes a Daylight Savings Time adjustment of one hour,the next scheduled snapshot is skipped because the system identifies that the snapshot for that hour was already taken.

Take a Manual Snapshot

You may need to take an on-demand (manual) snapshot of a volume before you update software or make hardware changes on the array.

Even if you plan to take snapshots of volumes manually or use a third-party program, you can create a volume collection without schedules on those volumes that are being manually snapshotted. You may see a message if you take a snapshot around the same time that a scheduled snapshot for the volume is going to start. Check the volume collection by clicking on its name, then click the Snapshot Collections tab to ensure that no snapshot is pending before you trigger a manual snapshot.

Note: Manual snapshots are not guaranteed to be application consistent.

Procedure

1. Choose **Manage** > **Data Storage**.
2. On the Volumes tab, click the name of the volume to select it.

3. Click the camera icon to take a snapshot.
4. In the Snapshot Volume dialog box, complete the following:
   a) Enter a name for the snapshot.
   b) Optional: Enter a meaningful description for the snapshot.
   c) Set the Status to online or offline as required for your environment.

      The default Status setting is Offline.
   d) Set the Writability status as required to make the snapshot writable or non-writable (read-only).

      The default Writability status is Non-writable.
   e) (Optional) Enable or disable Application Synchronization that may be set.

      Note: The default application synchronization setting is disabled.
5. Click **Take Snapshot**.
   A banner appears at the top of the Data Storage page that states that the snapshot was created successfully.

Results

You can verify that the snapshot has been taken by clicking the **Protection** tab. You will see that the Local Recovery Point was updated.

Modify a Snapshot

You can modify a snapshot in the following ways: edit, delete, set online, or set offline. You can clone or restore a volume from a selected snapshot.

When snapshots are created, they are set offline. Setting a snapshot offline makes it unavailable to initiators, and closes any current connections.

Note: Snapshots that are not required to be online should be kept offline until needed.

You can change the state of one or more volume snapshots at the same time if their current states are the same.

Procedure

1. Choose **Manage** > **Data Storage**.
2. On the Volumes tab, click the name of the volume to select it.
3. Click the Data Protection tab, and select the snapshot or snapshots to change.
4. You can perform the following actions: Change the state of the snapshot or snapshots.

Option	Description
Edit the snapshot	Click the pencil icon to change the snapshot name and description.
Delete the snapshot	Click the X icon.
Restore the volume from a snapshot	Click **Restore** and confirm your choice in the Restore Volume box.
Clone the volume from a snapshot	Enter a new volume name in the **New Volume Parameters** dialog box and click **OK**.
Change the status of the snapshot	Click the appropriate status, **Set Online** or **Set Offline**.

The button visible depends upon the current state of the snapshot or snapshots.

- If snapshots are online, click **Set Offline**.
- If snapshots are offline, click **Set Online**.

Delete a Snapshot

Unlike deleting a volume, deleting a snapshot has no impact on the original volume. Only the data on the snapshot is lost.

You cannot delete a snapshot while it is online or has a clone. Delete any clones and set the snapshot to offline before you delete it.

Procedure

1. Choose **Manage** > **Data Storage**.
2. Click the volume whose snapshot you want to delete.
3. Click the Data Protection tab.

   Grey icons indicate which snapshots are offline and green icons indicate which snapshots are online.
4. (Optional) If the snapshot you want to delete is online, select it, then click **Set Offline**.
5. Select one or more offline snapshots in the list, then click the X icon to delete the snapshot.
6. Click **OK** to confirm the action.

Hidden Snapshots

When you install an array, you typically set up volumes, as well as volume collections and snapshot schedules. If you do not set up any volume collections or snapshots, the array automatically generates a snapshot every hour. These snapshots are termed hidden snapshots.

While individual hidden snapshots are not listed under the Snapshot tab, hidden snapshots usage is part of the calculation of the Snapshot Usage column on the Space tab. Similarly, if you schedule snapshots that occur more than one hour apart, the array continues to generate hidden snapshots. As soon as you decrease the frequency of snapshots to something less than one hour, the array stops taking hidden snapshots.

Snapshot Framework

The Snapshot Framework allows you to write custom host- or application-aware plug-ins (also known as “agents”) to customize the pre-snapshot and post-snapshot tasks. By default, the array provides application-consistent snapshots and replication of vSphere datastores, MS-Exchange, MS-SQL, and NTFS on the following platforms:

- VMware (through vCenter synchronization)
- Microsoft SQL Server (through Microsoft VSS sync)
- Microsoft Exchange Server (through Microsoft VSS sync)

However, for applications that are not VSS-aware, a custom plug-in created with the Snapshot Framework can be used.

The Snapshot Framework dramatically expands the set of applications that can be integrated with HPE Storage Snapshots, including Linux Oracle and SAP applications, and even Windows applications that are not VSS-aware.

The Snapshot Framework does not replace VSS Integration. Any third-party backup applications that are VSS-aware can integrate with the OS normally via the Storage VSS provider; non-VSS backup applications can use REST APIs.

For information on how to develop your own agent, refer to the *Snapshot Framework Reference*.

To use the array OS CLI with your custom agent, refer to the *CLI Administration Guide*.

Managed and Unmanaged Snapshots

Snapshots and snapshot collections can be classified as either managed or unmanaged.

Managed Snapshots

Managed snapshots and snapshot collections are objects that are managed by the system and that are associated with a defined protection schedule. These snapshots are typically created in the following scenarios:

- A user performs an action on the snapshot using the array OS CLI or GUI. These snapshots are considered manual snapshots.
- Third party software performs an action on a snapshot through the REST API. These snapshots are considered manual, externally triggered snapshots.
- The array acts on the snapshot in response to a user action, such as a volume restore, resize, promote, or demote. These snapshots are considered manual snapshots.
- An agent, such as VMware or VVOL, acts on the snapshot. These snapshots are considered externally triggered snapshots.
- A snapshot is taken via the volume collection per the assigned schedule. These snapshots are considered managed snapshots and are deleted in accordance with the protection schedule associated with the volume collection.
- A snapshot is triggered by a handover action. These snapshots are considered manual snapshots though they are managed by the retention schedule and require no user action.

Unmanaged Snapshots

Unmanaged snapshots are snapshots that are no longer linked to the protection schedule that was defined when the snapshot was created. These snapshots are not automatically deleted by the array unless the Time-To-Live (TTL) feature is enabled. Refer to the *CLI Administration Guide* for information on how to use the TTL feature.

Unmanaged snapshots are created in the following scenarios:

- Dissociation of a volume from a volume collection. This can occur even after a volume is temporarily dissociated as snapshots will remain after the dissociation takes place.
- Deletion of a volume collection protection schedule from which the snapshots were created. This can occur even if a new schedule is created with same name.
- Deletion of a volume collection from which the snapshots were created. This can occur when a volume is added to a volume collection with same name.
- Renaming of the volume collection or a schedule on the upstream array group. This can create unmanaged snapshots on the downstream array group as the renamed volume collections and schedules are considered separate entities from the original ones on the downstream array group.

Risks Associated with Unmanaged Snapshots

Unmanaged snapshots can reduce the amount of reported free space available in an array group, which can limit the available space for other volumes. In worse case scenarios, unmanaged snapshots can increase array space usage beyond optimal threshold levels and can impact performance. Is is therefore recommended that you periodically review and delete any unmanaged snapshots that are no longer required in accordance with your Restore Point Objectives (RPO).

Preventing Unmanaged Snapshots

You can prevent unmanaged snapshots from being created by being aware of existing snapshots when deleting or renaming protection schedules from a volume collection or when deleting or renaming the volume collection itself. If a protection schedule or volume collection is deleted or renamed, you should review and delete unmanaged snapshots if they are no longer required. Also, be careful if you disassociate or move volumes from one volume collection to another as doing so can generate unmanaged snapshots.

NSs Snapshots

NSs snapshots are snapshots that have NSs-* prepended to the snapshot name. These snapshots are commonly created in the following scenarios:

- Volume-level restore activity
- Volume size changes

- Microsoft VSS related snapshot operations

In the case of Microsoft VSS operations, NSs snapshots are normally set to offline; however, the snapshots might appear online while an operation is in progress.

In rare cases, and more commonly in legacy code, if an unexpected failure occurs that prevents NSs snapshots from being appropriately managed, you might see an NSs snapshot left online even though there are no running back end processes that leverage the snapshot.

NSs snapshots are usually renamed upon successful operation to meet the normal snapshot-naming scheme; however, if a third-party backup requester calls our provider, this could cause the snapshot to retain the NSs-* name.

Note: NSs snapshots are created as a recovery point right before you perform certain tasks. You can delete these snapshots after you have verified that your task completed successfully, as these snapshots are not managed by the snapshot retention schedule on a volume collection or by the Time-To-Live feature.

Working with Online Snapshots

Online snapshots are useful for verifying the contents of a snapshot. They can be generated either automatically or manually.

Note: It is recommended that you use VSS verified snapshots instead of manually creating an online, writable snapshot. Depending on the type of data on the volume, having VSS enabled is necessary to maintain recoverable data.

Certain backup utilities and data scanning utilities automatically create online snapshots. Normally these snapshots remain online only for the duration of the operation. If utility does not turn off the online feature after the process finishes, you should manually turn it off.

You should **not** use online, writable snapshots as a replacement for cloning. For example, you should not use online snapshots in the following situations:

- Do not use online writable snapshots to add storage to a host by making it an extension of the existing file system.
- If you plan to use a snapshot for testing or some situation where you need to use the snapshot as a regular volume. Instead, you should create a clone and use that a new volume and migrate data as needed.

Online, writable snapshots do not maintain point-in-time (PIT) information. If you change the data on an online snapshot, those changes will persist when the snapshot is turned offline. The changes to the upstream online snapshot will not replicate and the replica snapshot will only contain the data that was used to the create the original online snapshot.

If you create an online, unwritable snapshot, the data in the snapshot cannot be changed, so you do have a PIT snapshot.

Note: If you manually create an online snapshot and you make it non-writable, you cannot change it later to make it writable.

Identify Online Snapshots Using the OS GUI

You can use the OS GUI to identify snapshots that are currently online.

Procedure

1. Select **Manage** > **Volumes**.
2. Select the volume that might have an online snapshot.
3. Click the Snapshots tab. Online snapshots show up as green.
4. Determine whether the online snapshot is connected to a host (initiator). If a host is actively using the snapshot, complete the operation that is in progress; for example migrating or moving data.
5. Determine whether there is a reason to have the online snapshot in the future:
   - Is the snapshot required by an application or script. If it is, take the following actions:
     1. Check the retention schedule to make sure the snapshot will be removed at a future date.

    2 Disconnect the snapshot from the host before the next snapshot deletion operation is scheduled to occur.

- Is this the only common snapshot between the upstream array and the downstream array. If it is, then deleting the snapshot would cause the volume to need a full re-seed.

6. If you do not need to maintain an online snapshot, perform the following steps:

    1 Disconnect the snapshot from the host.
    2 Make it offline.
    3 Delete it.

Migrate Data From an Online Snapshot to a New Volume

If you are using an online, writable snapshot as an extent to an existing file system, it is recommended that you create a new volume and migrate the data from the snapshot to it.

Procedure

1. Create a new volume.
2. Migrate the data from the online snapshot to the new volume.
3. Connect the host to new volume.
4. Verify that all data migrated successfully.
5. Gracefully disconnect the initiators from online snapshot.
6. Turn the snapshot offline and, if it is no longer needed, delete it.

Replication

You can use volume replication to copy critical data to arrays at different locations as part of your disaster recovery strategy. Replication does not take the place of snapshot backups, but it enhances the overall data recovery plan.

For data recovery tasks like recovering an accidentally deleted or corrupted file, you can take snapshots that serve as a backup. Snapshots have little performance impact, can be performed quickly, and are space efficient.

For more widespread issues like a power failure or a site disaster, replication technology can be a quick and effective way to recover data at an offsite location. In these scenarios, data can be served from the replica while the initial array is being restored.

Storage arrays use an advanced file system that provides in-line compression for data writes. Data is stored in variable-length blocks that match the logical write methodology of an application. These features minimize the amount of replication traffic to a compressed version of the logical application write and reduce bandwidth requirements.

Snapshot replication tasks are scheduled automatically through protection templates. You can implement any number of replication strategies to meet your requirements for disaster recovery. For more information on protection templates, see the chapter on *Data Protection*.

What is Replication?

Replication maintains a copy or replica of a volume or set of volumes and their snapshots on another array that is configured as one of a pair of replication partners. The replica contains the contents of a volume at the time the replica was created or last updated, as well as a configured number of prior states (snapshots). Replicas are stored at a remote array, called a replication partner, connected by a network or Internet link. A volume is always located on a different array than its replica. It is possible to retain more or fewer snapshots on the replica than on the source volume, thus providing greater flexibility in designing a recovery plan.

The HPE Peer Persistence feature is designed for applications that require zero to near zero RPO and RTO storage. The feature enables multi-site synchronous replication with automatic switchover (ASO), which allows your arrays to recover automatically and non-disruptively from a storage based failure. For the purposes of this documentation, the two components of HPE Peer Persistence are referred to by their functional descriptions, synchronous replication and ASO, rather than the feature name.

Note: The HPE Peer Persistence feature is designed to enable applications to achieve a near zero RPO only in the event of storage failures. The feature will not prevent site-to-site failures that result from host level failures.

A replica is a copy of a volume from another group (in the case of snapshot replication) or pool (in the case of synchronous replication) whose state is managed by the other group or pool. For example, all write operations to a replica originate from another group. The array that hosts the original volume and manages the state of a replica is called the upstream partner, because the data flows from it. The array where the replica resides is called the downstream partner, because the data flows to it.

The replicated volumes can be restored as complete copies of the volumes, with all schedules and administrative settings replicated, as well as the actual data. Like snapshots, replicas are created and stored based on volume collection schedules. Multiple volumes can share a volume collection schedule.

For snapshot replication only: When you promote a replica, the number of snapshots to retain is adjusted to be the maximum number of snapshots to retain on the local array, plus the number of snapshots to retain on the replica. The volume is offline until a replica is promoted. The volume and settings are visible on the replica, but they are not editable until a volume collection handover is performed.

Note: For synchronous replication, the snapshot retention limits remain with each pool after a handover.

Snapshot Replication and Synchronous Replication

There are two types of replication: snapshot replication and synchronous replication. Snapshot replication creates a backup version of your volumes so that you have a point-in-time copy to refer back to if a prior version of the data is needed. Synchronous replication provides a replica of the volumes that is created synchronously with no delay in the recovery point. It is intended for immediate recovery due to a site failure.

To assist in understanding the differences between snapshot replication and synchronous replication, the following table presents a comparison of the two.

Behavior	Snapshot Replication	Synchronous Replication	Notes
Recovery Point Objective (RPO)	Depending on the replication snapshot schedule. If the schedule is 15 minutes, then the RPO is 15 minutes	0 RPO **Note:** RTO can be < 1 minute when in a single site or when metro stretch clustering is not being used.	Failures caused by incorrect writes are not covered by synchronous replication. They can be recovered from snapshots.
Automatic recovery	No	Yes, if Automatic Switchover is configured	Only available with synchronous replication when accompanied by the Automatic Switchover (ASO) on page 125 feature.
Manual recovery	Yes	Yes	
Replication Partners	Group partners	Pool partners	Pool partners are auto-generated and deleted when the pool is deleted or merged
Maximum number of partners	2	1	
Number of protected volumes	1024 volumes	512 volumes upstream and 512 volumes downstream	
Replication configuration level	Volume collection	Volume collection	Synchronous replication is not allowed on multi-pool volume collections
Maximum number of protection schedules per volume collection	10	10	
Extent of replication	The maximum supported number of groups is four	Two arrays, two single-array pools	
Replication type	Between groups	Within group	
Replicate sub-set of Snapshots	Yes	Yes	
Hardware array models supported	All models	AFxx, HFxx, AFxxxx, CSxxxx, and HPE Alletra 6000 arrays only	For synchronous replication, the upstream array must be the same model as the downstream array

Behavior	Snapshot Replication	Synchronous Replication	Notes
Synchronous mode	N/A	Soft synchronous mode where when a volume goes out-of-sync, it continues to accept writes	
Resume automatically	Yes	Yes, through an automatic resynchronization	
Site fault tolerance	Yes	Yes	
Recovery time objective (RTO)	User initiated handover can be completed in under one minute	Switchover can be completed in under one minute	
Network connectivity for replication traffic between partners	IP	IP	
Support for multiprotocol arrays (Fibre Channel and iSCSI)	Yes	No	
Link bandwidth	N/A	10 Gpbs	
Number of links	At least one. Additional links can be added for redundancy, however traffic occurs over a single IP and port.	At least two links are recommended for redundancy and performance	
Add support non-disruptively	Yes	Yes	
Remove support non-disruptively	Yes	Yes	
Array replacement allowed	Yes	Yes, see note	**Note:** To replace an array, un-configure synchronous replication, move data to a new array, then reconfigure synchronous replication.
Changing replication type allowed	No	No	
Volume resize support	Yes	Yes, see note	**Note:** To resize a volume with synchronous replication, unconfigure synchronous replication, resize the volume, then reconfigure synchronous replication.

Behavior	Snapshot Replication	Synchronous Replication	Notes
Subnets	Arrays do not need to be in the same subnet	All arrays must be in the same subnet	
Protection templates	Yes	None provided	
Location of upstream and downstream replicated volumes	In separate groups, so in separate volume collections.	All in one volume collection	
Location of snapshots	In separate groups, so in separate snapshot collections.	Two separate snapshot collections, one for upstream and one for downstream	
Host reconfiguration required after handover	Yes	No	

Replication Partners and How Replication Works

Note:

Replication partners can be referred to differently depending on which type of replication is being used. The following describes the different types of replication partners:

- For snapshot replication: Group partners
- For synchronous replication: Pool partners
- For HPE Cloud Volumes (CV) replication: Replication store on the HPE CV portal

Note:

Replicating encrypted volumes to HPE CV requires release 5.0.6.x or later.

You can configure arrays to have up to fifty snapshot replication partners. Synchronous replication allows only one pool partner. Snapshot and synchronous replication are both automatic, based on the protection schedules assigned to the volume or volume collection.

Replication partners can be reciprocal, upstream (the source of replicas), or downstream (the receiver of replicas) partners. You can have several upstream arrays that replicate to one downstream partner. For synchronous replication, pool partners are created automatically after replication is configured.

When you enable replication of a volume for the first time, the entire data set on the volume at the time of the snapshot is replicated from the original array group (upstream) to the destination replication partner (the downstream array group). Subsequent updates replicate the differences between the last replicated snapshot on the upstream partner to the downstream partner.

It is recommended that you configure the snapshot retention count on the replica (downstream) array group to at least the number of snapshots on the upstream array group, matching the frequency of snapshots.

Note: In the majority of array operating system releases, by default, the replication partner retains only two snapshots for each replica volume in the volume collection if configuration is not adjusted.

Replication partners can use different access protocols. One of the partners can be an iSCSI array and its replication partner can be a Fibre Channel array.

Snapshot collections are replicated in the order that the collections were taken. Once replication is caught up, the upstream and downstream replication partners only retain as many snapshots as set in the retention criteria. The system deletes pending snapshot collections that exceed the retention criteria.

Create a Replication Partner

Note: This procedure does not apply to synchronous replication. The replication partners for synchronous replication are pool partners and are created automatically.

Use the management subnet for replication when any of the following conditions apply:

- Your data IPs are not routable across the network
- You want to separate replication traffic from iSCSI traffic.
- Your replication arrays are running release 1.4 or release 2.0 or later versions, and you want to separate replication traffic from iSCSI traffic

Note: For release 2.x and later, replication over a data subnet is available; however, it requires the replication control traffic to be transferred over a management subnet. If you choose to replicate over a data subnet, you must be able to do the following:

- Route the management subnet between replication partners by the default gateway for replication control traffic
- Route the data subnet between replication partners by a static route for replication data transfer traffic
- Replication partners can run different data access protocols. For example, a Fibre Channel (FC) replication partner can be created for an iSCSI array, and an iSCSI replication partner can be created for a Fibre Channel array. For replication to function on an FC array, you must also configure an Ethernet link or IP subnet.

For Fibre Channel arrays, you do not need to separate the replication traffic; replication traffic never runs over Fibre Channel.

Procedure

1. Select **Manage** > **Data Protection**, then click **You want to separateReplication Partners** in the left pane.
2. Click Add to add a new replication partner.
3. Select a replication type. If you select Cloud Replication, enter your HPE CV credentials.
4. Enter the group name (case-sensitive) of the replication partner for on-premises replication.
5. (Optional) Enter a description of the partner group.
6. Perform the following steps for on-premises replication only.
   a) Enter the hostname or IP address of the partner group.
   b) Type a shared secret. Type it again to confirm.

   Note: The shared secret must be eight or more printable alphanumeric characters with no spaces or special characters. Special characters include: ' " ` ~ ! @ # $ ^ & ( )+ [ ] {} * ; : ' " . , | < > ? / \ = % .

   c) Choose which subnet to use for the replication network. Select one of the following options:

   - Use management or controller IP addresses for replication traffic
   - Use data IP addresses for replication traffic

   Note: For release 2.x and later, replication over a data subnet is available; however, it requires the replication control traffic to transverse a management subnet.

7. Select a location for the inbound replication pool from the **Inbound Location** list.
8. (Optional for on-premises replication) Check **Use the same pool and folder as the source location**.
9. Click **Next**.
10. (Optional) Create a Quality of Service (QoS) policy, which is a bandwidth limit for replication traffic, click **Add Policy** and complete the fields in the dialog box.

    A Quality of Service (QoS) policy defines how the network resources are allocated for the replication partner.

    Note: Without a QoS policy, the replication partner can use unlimited network bandwidth.

a) (Optional) Enter a description of the policy.
b) Enter a number value and choose a bandwidth in Kbps or Mbps.
c) Indicate the time interval when the policy is in effect.

The time should be the time in the array time zone, not the client time zone.

d) Check the boxes for the days of the week when the policy is in effect.
e) Click **Create**.

11. Click **Create**.

It can take up to ten minutes for the partners to establish contact.

What to do next

Log in to the replication partner and perform the same configuration steps on the downstream array and group.

Modify a Replication Partner

> **Note:** This procedure does not apply to synchronous replication. For synchronous replication, you cannot rename a pool partner. If a pool is renamed, the pool partner will be renamed automatically.

You can modify the IP address or bandwidth requirements for a replication partner without having to recreate the replication partner.

You cannot change the name of a replication partner. You must create a new replication partner with the required name, assign the volume collection to the new replication partner, and delete the original replication partner.

For replication with HPE Cloud Volumes (HPE CV), you can only edit the description of the replication store and the QOS policy.

Procedure

1. Select **Manage** > **Data Protection** > **Replication Partners**.
2. Check the replication partner to modify.
3. On the replication details page, verify that there are no replications in progress to or from the replication partner. The bandwidth graph of the details page should show zero current bandwidth.
4. Click edit to open the editing wizard.
5. Make any necessary changes, and click **Save**.

Delete a Replication Partner

> **Note:** This procedure does not apply to synchronous replication. For synchronous replication, you cannot delete pool partners. Pool partners are deleted automatically based on the number of pools in the group.

When you delete a replication partner relationship, only the replication partner relationship is deleted, not the array.

For HPE CV replication:

- You must enter your HPE CV credentials to delete the upstream partner in HPE CV
- Only those partners that are owned by the HPE CV user can be deleted

Before you begin

- Change all volume collections so that replication is not scheduled with a partner

  For more information, see Edit a Volume Collection on page 101.

- Ensure that there are no volume collections that have the replication partner selected

  You can determine this by searching by the partner name on the volume collections page.

- Be sure to remove both the upstream and downstream replication partners unless you are using HPE CV replication.

  For HPE CV replication, you must remove the partnership from upstream then the downstream partner is automatically removed.

Procedure

1. Select **Manage** > **Data Protection** > **Replication Partners**.
2. Click the name of the the replication partner that you want to delete.
3. Click X to delete the replication partner.

   If you removed all volume collections from the source group, you can view the confirmation that the replication partner was deleted. If there are still active volume collections associated with the partner, delete those and repeat the process. You might want to promote a volume collection associated with the downstream partner before you delete it.

What to do next

Deleting the HPE CV replication partner does not delete the downstream volumes in your replication store. These volumes are still usable in the cloud. You can delete these volumes from the HPE CV portal if you want to free up space in the replication store.

Test the Connection between Replication Partners

Procedure

1. Select **Manage** > **Protection** > **Replication Partners**.
2. Check the replication partner that you want to test.
3. Click **Test** in the menu bar above the list of partners.
   If the partner is reachable, a success message indicates the replication partner was contacted. If the partner is unreachable, an error message indicates the reason. In either case, click **OK** to acknowledge the message.

Link Management and Resynchronization with Synchronous Replication

Resynchronization is a process where data is sent from the upstream pool partner to the downstream pool partner to ensure that the data at both partners is in-sync, or the same. If the two sites become out-of-sync, for example, through a pause in system connectivity, a resynchronization is performed to bring the two sites back in-sync.

Upon creation, the entire data set from the upstream volume collection is sent to the downstream volume collection. This is the initial synchronization, also known as seeding.

When a link breaks, such as a TCP link or a TCP connection and cannot be reestablished for 30 seconds, the volume transitions to an out-of-sync state.

When the volume collection is out-of-sync, new writes are not replicated to the downstream partner.

After the TCP link is restored, a resynchronization is needed to bring the arrays back into an in-sync state. The replicated volumes are scanned, and blocks that have been written since the link broke are sent to the downstream array. Volumes continue to accept I/O during the resynchronization process, and when the resynchronization is complete, the volume collection returns to an in-sync state.

In some cases a resynchronization sends more than just the missing data. For example, when you restore a volume to a snapshot or a new volume is created by cloning, the resynchronization process sends all data that has changed since the last snapshot that is common between the upstream and the downstream volume.

This type of resynchronization also happens if you remove (unconfigure) synchronous replication from a volume, and later reconfigure it, for example, by removing and later re-adding the volume to its volume collection, or by removing and recreating the synchronous replication schedule.

Snapshot Replication and Volume Collections

Volumes are replicated by associating them with volume collections that have at least one replication schedule. You can associate a new protected standalone volume with a volume collection when you create it rather than creating a volume first and then associating it with a volume collection in a separate process.

Note: If you create protection templates for volume collections that use replication, you must configure the arrays as replication partners before you begin. If you are using HPE CV, you must create a replication store on HPE CV before you create a replication partner on the on-premises array.

A volume collection can have up to ten protection schedules. One or more of these protection schedules can be replication schedules. If you have set up two replication partners, the schedules for a volume collection can be replicated to one of these two replication partners when you specify the type as **Periodic Snapshot**. Each schedule can have only one replication partner, but you can vary which of the two available partners is used with which schedule.

If a volume uses a custom performance policy for snapshot replication, you must duplicate that policy on the replication partner.

Setting up a replication for a volume collection requires that you perform the following tasks:

- Assign volumes to the volume collections
- Define the replication partners
- Indicate at what times volumes should be replicated
- Specify how many snapshots should be retained

At the scheduled time, the array from which the volume is being replicated sends the data to the downstream (receiving) replication partner.

Note: The first time that you create a replica of a volume, the entire volume is copied to the replication partner. Subsequent updates are replications of snapshots on the upstream partner.

Add Replication to a Volume Collection

Before you can set up replication, you need to configure replication partners, also known as group partners for snapshot replication, pool partners for synchronous replication, and replication stores on HPE Cloud Volumes (HPE CV). Creating replication partners automatically enables two arrays or an array and HPE CV to replicate volume collections.

If you want to specify synchronous replication as the replication type on a volume collection, you must do that when the volume collection is created. After you designate it as a synchronously-replicated volume collection, the replication type cannot be changed.

When using snapshot replication, volume collections support up to two replication partners. You specify the replication partners when you create protection schedules for a volume collection. A volume collection can have up to ten schedules. You can set up the schedules so that certain ones use one of the replication partners and others use the other replication partner.

Note: You will receive an error message if you attempt to add a third replication partner to the schedule set for a volume collection.

Before you begin

You must have a volume collection to create replicas. You cannot create replicas on demand.

Procedure

1. Go to **Manage** > **Data Protection** > **Volume Collections**.
2. On the Volume Collections page, check the checkbox for the volume collection that you want to edit.
3. In the action bar, click the pencil icon to edit the volume collection.

4. Select the **Periodic Snapshot** from the **Replication Type** list.
5. Select the replication partner from the **Replication Partner** list.
6. Click **Save**.

Results
The volumes of this volume collection will be replicated to the replication partners specified in the schedule.

Synchronous Replication

Synchronous replication provides protection from array or site failures with no data loss. It provides a zero recovery point objective, meaning that there is no data loss in the event of an array or site failure. This is not available with snapshot replication. Synchronous replication ensures that host reconfiguration is not required.

Synchronous replication allows you to protect the entire array and enable or disable protection simply by adding or removing it in the protection schedule.

You can also use the Peer Persistence feature, which combines synchronous replication with automatic switchover (ASO). Peer Persistence allows your arrays to recover automatically and non-disruptively from a storage based failure. For the purpose of this documentation, the two components of Peer Persistence are referred to by their functional descriptions, synchronous replication and ASO, rather than the feature name.

For more information on ASO, see Automatic Switchover (ASO) on page 125.

Synchronous Replication Prerequisites and Limitations

The following list includes requirements and limitations for the use of synchronous replication.

General Limitations

- Array group can consist of only two single array pools:
  - Multi-array pools are not supported.
  - Synchronous replication of multiple pool volume collections is not supported.
  - Moving synchronously replicated volumes between pools is not supported.
- The maximum number of replication volumes is 512 upstream and 512 downstream volumes.
- The hardware models must be the same for all arrays in the synchronous replication relationship.
- A 10G link between the sites (Ethernet, not FC) is required.
- Round trip latency between the sites should be less than or equal to five msec.
- You must install the latest host and client components.
- Synchronous Replication only works through storage failover and does not support host level failover.

Operations and Features not Supported with Synchronous Replication

- Unsupported arrays

  Synchronous Replication is not supported on HF20H, CS1000H, or SFAxxx arrays.
- Volume pinning
- Volume striping
- Volume resizing

  You must unconfigure synchronous replication to resize a volume.
- Volume move
- Folder space limits enforcement
- Snapshot replication

  A volume collection cannot be configured for both snapshot replication and synchronous replication.

- HPE Cloud Volume (CV) replication
- Virtual arrays
- Virtual volumes (vVols)
- SMI-S volumes
- Changing replication type
- Array replacement

  You must unconfigure synchronous replication to replace an array.

- Multiprotocol arrays (FC and iSCSI)
- Volume restore

  You must unconfigure synchronous replication to restore a volume.

Out-of-Sync Volumes

A volume collection is in-sync only if all upstream volumes in the volume collection are in-sync.

If the replication link breaks, after about 30 seconds, the volume collections transition to an out-of-sync state, and writes are accepted without being replicated. When the link is restored, the system performs a resynchronization and the volume collections transition to an in-sync state with all incoming writes written to both arrays before acknowledging the hosts.

Note: If you add a volume to a synchronously-replicated volume collection, all the volumes that are configured for synchronous replication will go out-of-sync until the newly added volume is in-sync.

Snapshots taken while the volume collection is out-of-sync are not replicated and the snapshots will only be created on the upstream volumes.

It is not possible to catch-up or replicate any snapshots that were missed while the volume was out-of-sync.

When the volume is out-of-sync, the Recovery Point Objective (RPO) is not zero. The volume might be out-of-sync due to a variety of reasons such as a resynchronization that is in progress, I/O might have been paused, the user editing the volume collection, or some other reason.

Volume Names and Replication

You can have multiple volumes with the same name. The following list states conditions to consider if you have more than one volume with the same name.

- A volume replicated within a group will have two separate instances with the same name but they must be in different pools.

  Both volumes will show up in the list of volumes with an indication of which pool the volume resides in.

- Operations that would put two volumes with the same name within the same pool, for example volume move or pool merge, will fail.

Configuring Synchronous Replication: Serial Numbers and ACLs

Serial Numbers

When synchronous replication is configured, the upstream and downstream volumes share the same serial number. On the host, there are multiple paths to a single iSCSI device with a single serial number: active paths are mapped to the upstream volume, the standby paths are mapped to the downstream volume.

From the Array System Management view, the upstream and downstream volumes are different management objects. The upstream volume has the serial number that was exported through the data path. The downstream volume has a different serial number (a secondary serial number). When synchronous replication is unconfigured, the downstream volume can be exported on the data path as an independent volume with this secondary serial number.

A handover operation switches the serial number between the upstream and the downstream volume.

ACLs

After synchronous replication has been configured, the downstream volume inherits the existing ACLs (and respective LUNs) from the upstream volume. While configured for synchronous replication, all access control changes affect both volumes. You can add or remove ACLs from either the upstream or downstream volume.

When you want to re-use an existing volume as a downstream volume for synchronous replication, you must manually move all existing ACLs to the new downstream volume.

When synchronous replication is unconfigured, the upstream volume retains all ACLs (and respective LUNs) to maintain the data service. All ACLs are removed from the downstream volume.

Configuring Synchronous Replication on a Volume Collection

You can configure synchronous replication for the volume collection. A volume collection includes a set of protection schedules for creating snapshots of each associated volume at set intervals. The protection schedule specifies the downstream partner where the volume and snapshot data is replicated.

- All upstream volumes in a synchronously replicated volume collection must belong to the same pool.
- Two different volumes with the same name in the downstream pool are not supported.
- All synchronous replication schedules must use the same downstream pool partner.

Important: If you add a volume to a synchronously replicated volume collection, all the volumes that are configured for synchronous replication will go out-of-sync until the newly added volume is in-sync.

You must create a snapshot schedule and configure the schedule with a replication partner. Creating a snapshot schedule and a replication partner allows you to perform a roll back operation, if necessary, or create clones from the snapshots.

Important: You must set up the schedule so that at least one replicated snapshot is taken every four hours. If you specify a longer time interval, you will get an alert notifying you that the schedule does not meet time recommendations for snapshots.

For a new synchronous replication configuration, downstream volumes are automatically created. If any downstream volumes exist from previous synchronous replication, they are re-used. The downstream volume inherits the state of the existing upstream volume (either online or offline).

After you configure synchronous replication for a volume collection, the following actions take place:

- A downstream volume is created in the pool partner that has the same name and is automatically added to the volume collection.
- The volumes in the downstream volume collection inherit the serial number and the existing ACLs from the upstream volumes.
- The volumes in the downstream volume collection are brought online to export the iSCSI standby paths.

For detailed instructions for creating a volume collection and configuring synchronous replication on a volume collection, see Create a Volume Collection on page 99.

Unconfigure Synchronous Replication

There are several ways to unconfigure synchronous replication.

- Disassociate all volumes from the synchronous replication volume collections.
- Delete the last synchronous replication schedule with a pool partner.
- Remove a pool partner from the last synchronous replication schedule.

When synchronous replication is unconfigured, the downstream volume is brought offline and standby SCSI paths are removed.

Reconfigure Synchronous Replication

There are several advantages to reconfiguring synchronous replication:

- Reconfiguring a volume that had been synchronously replicated previously does not require a full reseed of the data.

- You can identify a prior downstream volume in a pool partner with the same name.
- The process automatically triggers a resynchronization from a snapshot which brings the upstream and downstream sites into sync.

Before you begin

- The downstream volume must be offline.
- The downstream volume must share a common snapshot with the upstream volume.
- The downstream volume must not have any existing ACLs.

Procedure

1. Configure synchronous replication.

   See Create a Volume Collection on page 99.

2. Unconfigure synchronous replication.

   See Unconfigure Synchronous Replication on page 123.

3. Reconfigure synchronous replication.

Resize a Volume Participating in Synchronous Replication

Before you begin

1 Verify the upstream and downstream volumes both show online.

> **Important:** Note which volume/pool combination is the upstream volume.

2 Verify there is a successful common snapshot on the upstream and downstream volumes.

> **Important:** Note the volume collection that contains the volumes.

Procedure

1. Edit the volume collection and remove the upstream volume. The downstream volume will be removed automatically. See Edit a Volume on page 68 and Delete a Volume on page 72.
2. Review the volumes and make note of which pool each volume contains. The upstream volume should show online. The downstream volume should show offline.
3. Edit the upstream volume and resize. See Edit a Volume on page 68.
4. Edit the downstream volume and resize.
5. Review the volumes. Ensure they are the same size.
6. Edit the volume collection and add the upstream volume back in. The downstream volume will be added automatically.
7. View the volume collection. The remote recovery point should show **Out of sync** and the resync in progress.
8. Verify the upstream and downstream volumes. Both now show the new size and the downstream is back online.
9. Verify there is a fresh common snapshot on the upstream and downstream volumes. This ensures the new snapshot can be able to replicate downstream, for recovery.
10. On the host, rescan the disk and expand the file system.

What to do next

After the volume collection is resynchronized, verify that the volume collection works as expected.

1 Verify the expansion. Perform Volume Collection Handover (from upstream pool to downstream pool).

2 Verify the volumes have swapped upstream and downstream directions.

3 From the host, verify the volume shows the new size.

4 Perform Volume Collection Handover a second time to return to the original direction.

Automatic Switchover (ASO)

Important: Check the latest release notes before you attempt to use the Peer Persistence feature.

Automatic Switchover (ASO) is an optional, but highly recommended, feature that can be used with synchronous replication to enable automatic failure recovery. When ASO is used in conjunction with synchronous replication, the feature is known as HPE Peer Persistence.

The HPE Peer Persistence feature enables synchronous replication with ASO, which allows your arrays to recover automatically and non-disruptively from storage based failures.

Note: The HPE Peer Persistence feature is designed to enable automatic recovery failure in the event of storage failures. The feature will not prevent site-to-site failures that result from host level failures.

ASO currently works on array groups that consist of two arrays. When ASO is enabled and a switchover occurs, the partner that serves I/O for a volume collection is switched, which non-disruptively reverses the direction of the synchronous replication.

ASO facilitates automatic failure recovery through the use of a Witness daemon that can be run on an independent host (or in a separate VM) that can communicate with the group leader and the backup group leader.

Note: The Witness does not need to be on the same subnet as the array group, but its IP address must be routable from the array group's management network. The Witness can be installed in a different data center or even in a cloud environment as long as the round-trip time (RTT) between the Witness and the two arrays is 250 milliseconds or less. Multiple methods exist to deploy the Peer Persistence Witness. If the Witness is installed in a different data center or cloud environment and HPE Storage Support is needed to resolve an issue with the Witness, consider that if HPE Storage Support cannot access the data center, cloud environment, or infrastructure, troubleshooting may be limited.

When the Witness detects that an array is unavailable, the ASO process performs a handover of affected synchronous replication volume collections and seamlessly maintains the availability of group services and of synchronously replicated volumes.

To enable ASO, you must perform one of the following procedures:

- Install and configure the Witness software on a CentOS V7.9.x. client.
- Run the Witness in a separate VMware based Virtual Machine.

After the Witness is configured, you can then use the array OS GUI or CLI to set up the Witness and enable Automatic Switchover between the arrays in the group.

Note: The ASO check box is selected by default; however, ASO is not actually enabled unless the Witness is configured. For example, you might go to **Administration** > **Availability** in the array OS GUI and see that **Enable** is checked for Automatic Switchover, but the fields for the Witness are blank. In this case, ASO is not enabled. You must both configure the Witness and check the **Enable** box for ASO to be configured.

Tip: You can use the following group command to enable or disable ASO from the CLI.

```
group --edit --auto_switchover_enabled {yes|no}
```

For information about enabling, deploying, and testing the HPE Peer Persistence feature, including possible ASO failure scenarios, refer to HPE Peer Persistence Deployment Considerations in the HPE InfoSight documentation portal.

Install and Configure the Witness on a Linux server

Note: Installing the Witness on a Linux server is just one option for enabling ASO. If you prefer not to maintain a separate Linux Server, you can elect to run the Witness in a virtual machine. The Witness must be on the same management subnet as the arrays.

To install an configure the Witness on a Linux server, complete the the following steps:

Before you begin

Download the Witness software from InfoSight.

Procedure

1. Install the Witness software on a CentOS V7.7.x server.

   ```
   yum -y install /root/<hpe-alletra-witness-software>.rpm
   ```

   A service called nimble-witnessd.service is created.

2. Enable the Witness process to automatically start when the system boots.

   ```
   systemctl enable nimble-witnessd.service
   ```

3. Start the Witness process.

   ```
   systemctl start nimble-witnessd.service
   ```

4. Display the status of the Witness process.

   ```
   systemctl status nimble-witnessd.service
   ```

   A a message appears stating that the Witness is enabled. The port number that the process is running on is also displayed, which you may need to configure your firewall.

5. Create a user and password for the Witness.

   ```
   useradd <witness_user_name>
   ```

   ```
   passwd <witness_password>
   ```

   The Witness is now configured. You can now set up and enable the Witness.

Witness Library Dependecies

When installing Witness, the following libraries are required.

Library	Version
boost-filesystem	1.53.0 or later
boost-program-options	1.53.0 or later
boost-regex	1.53.0 or later
boost-system	1.53.0 or later
boost-thread	1.53.0 or later
glibc	2.17 or later
gperftools-libs	2.4 or later
keyutils-libs	1.5.8 or later
krb5-libs	1.13.2 or later
libcom_err	1.42.9 or later
libgcc	4.8.5 or later

Library	Version
libicu	50.1.2 or later
libselinux	2.2.2 or later
libstdc++	4.8.5 or later
libunwind	2:1.2 or later
pcre	8.3 or later
xz-libs	5.1.2 or later
zlib	1.2.7 or later
For PAM Authentication	
pam	1.1.8 or later
pam-devel	1.1.8 or later
For ssh-keygen	
(pre, post): openssl-libs	1:1.0.2 or later
(pre, post): openssl	1:1.0.2 or later

Run the Witness in a VMware based Virtual Machine

If you would prefer not to configure and maintain a separate Linux server on which to install the Witness, as an alternative, you can elect to deploy a separate VM that has the Witness daemon running and is pre-configured with the Witness dependencies. You can deploy this VM from an OVF template, which you can download from HPE InfoSight.

Important: HPE only supports this type of deployment via the vCenter GUI. Any other deployment method may fail.

To deploy a VM from an OVF template, complete the following steps:

1. Download the Witness OVA file from HPE InfoSight:
   - **a** 1. Log into HPE InfoSight.
   - **b** 2. Go to **Resources** > **Software Downloads**
   - **c** Locate and download the Witness OVA file.
2. Login to the vSphere Client to access the vCenter where you want to deploy the OVA witness VM.
3. Right click on the compute resource (for example, an ESX host) that you want to deploy to, and select **Deploy OVF Template**
4. From the Deploy OVF Template Wizard, complete the following steps:
   - **a** **Page 1**: Select local file, click **choose files**, and select the Witness OVA file.
   - **b** **Page 2**: Change the virtual machine name to a name that is meaningful to you.
   - **c** **Pages 3, 4, 5, 6**: Accept all default choices on each of these pages.
   - **d** **Page 7**: Provide the following information:
     - Gateway: (mandatory)
     - IP 1: (mandatory)
     - Netmask: 1 (mandatory). (See Important note below)
     - IP 2 (optional)
     - Netmask 2 (optional)
     - IP 3 (optional)
     - Netmask 3 (optional)
     - DNS: (optional, list more than one as space separated string of IP addresses)

Important:

When providing a Netmask, you must use a integer value format between 1-32 (such as **/24** for example) for the Witness service to function. Specifying a value in a format such as 255.255.255.0 might deploy the OVA, but the Witness service will fail.

If you inadvertently deploy the Witness using an incorrect format for the Netmask, you will need to redeploy the Witness VM again using the correct format.

  e. **Page 8**: Accept all default choices on this page.

5. You should see the VM with the name you chose from step 4b above. When the deployment is complete, right click on the VM and power it on.

When performing the above steps, keep the following information in mind.

- If the password for the root user is expired, you must change it when you first log on. The default witness OVA password is: **21brhGc+j6pIfApAHqEQ**. After you have changed the password, create a new user with a new user name and password by using the following commands:

  ```
  useradd <witness_user_name>
  passwd <witness_password>
  ```

  For more information about installing and configuring the Witness on a Linux server, see Install and Configure the Witness on a Linux server on page 125.

- To ensure that the basic setup is correct, you can check the status of the ovf-set service and nimble-witnessd daemon after the VM has been started by running the following commands:

  ```

  systemctl status nimble-witnessd
  systemctl status ovf-set
  ```

  If the services did not launch correctly, the errors for both services are reported in the **/var/log/NimbleStorage/** directory.

- If you need to change the network properties once the VM is deployed, you can perform the following steps:

1. Log in to the VM
2. Remove the following files:
   - /opt/NimbleStorage/ovfset/state/state_set
   - /etc/sysconfig/network-scripts/ifcfg-*
   - /tmp/ovf_env.xml
3. Shut down the VM
4. Change IP address, Netmask, DNS and Gateway values from the vCenter UI:
   a. Click the VM
   b. Go to the **Configure** tab
   c. Select **vApp Options**
   d. Select the properties you want to edit
   e. Change the values by selecting **Set Value**
5. Power on the VM

Set Up and Enable the Witness

You can set up the Witness from the CLI or the GUI. For instructions on how to set up the Witness from the CLI, refer to the *CLI Administration Guide*.

Procedure

1. From the GUI, select **Administration** > **Availability**.
2. Enter the host name or IP address of the Witness.

   The host name should be the fully qualified domain name of the host.

3. Enter the port number of the Witness.

   If you do not specify a port number, the default port number of 5395 is used.

4. Enter the user name and the password of the Witness.

   Enter the user name and password that you used when you installed and configured the witness.

5. Click **Save** to save your settings.
6. Enable the Witness using your saved settings by selecting the Automatic Switchover **Enable** check box.
7. (Optional) Click **Test** to confirm that the Witness connectivity status is Reachable for the arrays in the group.

What to do next

Important:

- Verify that the firewalld process running on the Witness allows ingress/egress communication for the slected port number.
- Verify that any firewalls between the group leader, backup group leader, and the witness allow ingress/egress communication for the the selected port number on all three.

Array Shutdown Order in Peer Persistence

When Peer Persistence is enabled, you can shut down either or both of your arrays at the same time using the shutdown option in the GUI. However, to minimize any impacts to your application environment, it is recommended that you power down and power up your arrays in the following order:

- Power Down:

  1 Power down the Backup Group Leader (BGL) first

  2 Power down the Group Leader (GL) second

  Important: Make sure you have disabled ASO (group --edit --auto_switchover_enabled no) before powering down the Backup Group Leader.

- Power Up:

  1 Power up the Group Leader first

  2 Power up the Backup Group Leader second

  Important: Make sure to enable ASO (group --edit --auto_switchover_enabled yes) after you have powered up the arrays.

Shutting Down Only the BGL or Only the GL

In certain situations, you might have the need to shut down only the Backup Group Leader or only the Group Leader. For example, in a Peer Persistence group, you will have an array in separate sites and you might need to shut down one site for planned maintenance. In that scenario, it is recommended that you perform a handover of synchronously replicated volume collections and migrate the group leader role to the surviving node before you shut down the array.

Shutting Down the GL

Procedure

1. Disable ASO and unconfigure witness.
2. Perform a handover of all volume collections from the GL to the BGL so that the BGL will have only upstream volumes serving IO.
3. Migrate GL functions to the BGL:
   a) Verify that the replicated configuration data on the backup up group leader is current with the group leader data.

   ```
   group --status
   ```

   b) Determine whether you can safely migrate the group management services from the group leader array to the backup group leader array.

   ```
   group --check_migrate
   ```

   c) Start the migration.

   ```
   group --migrate
   ```

4. Once the former BGL becomes the GL, you can shut down original GL for maintenance.
5. Once maintenance is done, turn array on.
6. Handover volume collections as needed.
7. Await synchronization to complete.
8. Enable ASO and configure the witness.

Shutting Down the BGL

Procedure

1. Disable ASO and unconfigure witness.
2. Perform a handover of all volume collections from the BGL to the GL so the GL will have only upstream volumes serving IO.
3. Verify that the GL has GL status by running CLI:

   ```
   group --status
   ```

4. Shut down the BGL.
5. Once maintenance is done, turn on array.
6. Handover volume collections to distribute volumes as needed
7. Await synchronization to complete.
8. Enable ASO and configure the witness.

Synchronous Replication and Manual Failovers

In some cases you might need to perform a manual failover of volumes that use Synchronous Replication.

Normally, if you have Automatic Switchover (ASO) and the Witness set up, this feature automatically performs a failover when either the upstream or downstream replication partner becomes unavailable. If ASO is not enabled, you must perform a manual failover.

Some of the situations that might require a manual failover include:

- ASO is not enabled because the Witness has not been installed and the backup group leader cannot be reached.
- ASO is not enabled because the Witness has not been installed and the group leader cannot be reached.
- ASO is not enabled even though the Witness is installed and the backup group leader cannot be reached.
- ASO is not enabled even though the Witness is installed and the group leader cannot be reached.

> **Note:** If you were using ASO, then before you perform a manual failover, it is a good practice to verify that ASO was correctly set up and the Witness was enabled. Make sure that the information you provided about the group leader when you set up ASO was correct.

When the group leader cannot reach the backup group leader, the group leader database transitions to out of sync. The volumes on the group leader array will remain accessible; however, any volumes on the backup group leader become unavailable.

Overview of Manual Failover Steps When Group Leader Is Unavailable

Performing a manual failover when the group leader is not available involves performing several procedures. Because the array OS GUI is not available when the group leader becomes unavailable, you must perform most of these steps from the backup group leader using CLI commands.

> **Note:** For instructions on performing the takeover, refer to the section *Perform a Manual Takeover of the Group Leader Array* in the *CLI Administration Guide*.

When the group leader cannot be reached, the following happens:

- There is no access to the array OS GUI.
- Group leader services are unavailable until a group leader takeover has been performed.
- The group leader is not able to transition out of sync. This is because the Group Data Service is unavailable until the manual takeover has been completed.
- There are only standby paths to the backup group leader until the takeover completes. At that point, the backup group leader becomes the group leader.
- The backup group leader can be accessed from the CLI using the secondary management IP address.

Before you begin the manual takeover, you must make sure there is a common snapshot between the two arrays in the group. If there is not a common snapshot, you will not be able to re-enable synchronous replication.

To perform a manual failover when the group leader that was using synchronous replication is unreachable, you must:

1. Confirm that the group leader is unavailable.

   > **Important:** If you can reach the group leader using the CLI command **group --check_takeover**, do not perform a manual takeover.

2. If you have a clustered configuration, take down the cluster.
3. From the backup group leader, use CLI commands to transition it to the role of group leader and start the group leader services.

   When the backup group leader becomes the new group leader, the previous group leader will transition to an out-of-sync state. At that time connections to it will be available.

   For instructions on performing this task, see the section *Perform a Manual Takeover of the Group Leader Array* in the *CLI Administration Guide*.

4. Use CLI commands to remove synchronous replication from the downstream partner to allow access to the volume. The following will happen:

   a. Existing ACLs from the upstream volume are cloned to the downstream volume
   b. The LUNs on the downstream volume get new numbers

   For instructions on performing this task, see the section *Remove Synchronous Replication from the Downstream Partner* in the *CLI Administration Guide*.

5 If you are using a clustered configuration, bring the cluster back up.

6 (Optional) Set up synchronous replication on the new group leader (the former backup group leader) after you have made sure that both the group leader and backup group leader are in sync.

See Add Synchronous Replication on page 132.

> **Note:** It is a good practice to set up ASO and the Witness.

7 (Optional) Perform a handover to restore the original direction.

See Perform a Volume Collection Handover on page 185.

8 (Optional) Migrate the group leader role back to the original group leader. Use CLI commands to perform this task.

Overview of Manual Failover Steps When Backup Group Leader Is Unreachable

When the group leader cannot reach the backup group leader, it transitions to out of sync. You can use either the array OS GUI or the CLI to confirm that the backup group leader is unavailable:

- The **Hardware** page in the array OS GUI displays a red asterisk next to the backup group leader.
- The CLI command **group --info |grep -i <group leader>** reports that the backup group leader is unreachable.

Before you begin the manual takeover, make sure there is a common snapshot between the two arrays in the group. The common snapshot simplifies the process of re-enabling synchronous replication.

To perform a manual failover when the backup group leader is not available, you must complete the following high-level steps:

1 Disassociate the downstream volume from the volume collection and remove synchronous replication. This will allow host connections.

You can use the array OS CLI commands to remove the downstream partner from the volume collection schedules.

> **Note:** You can re-enable synchronous replication after you complete the manual takeover and the group leader and backup group leader are in-sync again.

For information on performing this task, see the section *Remove Synchronous Replication from the Downstream Partner* in the *CLI Administration Guide*.

2 Bring the downstream volume online as a non-synchronous replication volume. When you disassociate the downstream volume and bring it online this way, the following happens:

- Existing ACLs from the upstream volume are cloned to the downstream volume.
- The LUNs on the downstream volume get new numbers.
- A new iSCSI serial number is assigned to the downstream volume.
- The downstream volume is no longer listed as a downstream volume in the GUI.

3 (Optional) When the group leader and the backup group leader are both online and in-sync again, set up synchronous replication again.

See Add Synchronous Replication on page 132.

4 Perform a handover operation.

See Perform a Volume Collection Handover on page 185.

Add Synchronous Replication

You can set up synchronous replication between the Group Leader and the Backup Group Leader after the arrays are online and in-sync.

When synchronous replication is removed, the replication partner is disassociated from the volume collection and no longer shows up with an upstream or downstream label. You can now modify the volume collection and configure synchronous replication once the arrays are back in-sync.

Procedure

1. Make sure the arrays are in-sync.

   If you go to the array OS GUI **Hardware** tab, you should see both arrays listed. If there is a red asterisk next to an array, that array is out of sync.

   You can now modify the volume collection and configure synchronous replication.

2. To reconfigure synchronous replication for the upstream partner, select the checkbox next to the volume collection and choose the ellipsis (...).
3. Select the option **Set Offline**.
4. Select **Manage** > **Data Protection** > **Volume Collections**.
5. Remove the upstream partner from the volume collection by choosing the volume collection and selecting the Edit icon (pencil).
6. Select **Next** to go to the **Volumes** page.
7. Locate the upstream volume in the **Selected** list and highlight it.
8. Select the **Remove** button to move the upstream volume to the **Available** side.
9. Select **Save**.
10. Set up synchronous replication between the two replication partners by choosing **Manage** > **Data Protection** > **Volume Collections**.
11. Select the checkbox next to the volume collection and choose the Edit icon (pencil).
12. From the Replication Partner dropdown list, choose the downstream replication partner.
13. Set the protection schedule.

    You can set it to match the previous schedule, or you can create new schedules.

14. Select **Next**.
15. Locate the replication partner in the **Available** list and select **Add** to move it to the **Selected** list.
16. Select **Save**.
17. Confirm that the replication partners are in-sync by choosing **Manage** > **Data Protection** > **Volume Collections** and checking the value listed for the Remote Recovery Point. It should be **Now**.

What to do next

You should perform a handover operation to return the original replication direction. When you perform the handover, you restore the original group leader and make the other partner the backup group leader again. For information about handovers, see Handover Overview on page 184. For information about performing a handover, see Perform a Volume Collection Handover on page 185 .

Change Partnership from Snapshot Replication to Synchronous Replication within a Group

The main advantages of synchronous replication over snapshot replication is a zero recovery point and recovery time objective. To change the partnership within a group from snapshot replication to synchrous replication, perfrom the following step:

Before you begin

Procedure

1. Remove the replica volumes from the downstream array. See Delete a Volume on page 72.
2. Remove the replication partnership. See Delete a Replication Partner on page 118.

3. Remove the partnership between the arrays and clean-up of any volume collections as needed. See Delete a Volume Collection on page 101.
4. Merge the groups. See Merge Two Groups on page 54.
5. Set up volume collections for Synchronous Replication. See Reconfigure Synchronous Replication on page 123.
6. Seed the replication partners with data.

What to do next
Enable Peer Persistence to complete the zero recovery point and recovery time objective set-up. See Automatic Switchover (ASO) on page 125.

Replication Strategy

Several options for replication strategy are available. Each has advantages and disadvantages. You need to decide on the best strategy for your environment. For example, you might use different configuration options that are based on available space, application, how critical the data is, and legal requirements. Consider your environment, applications, availability needs, storage growth patterns, and recovery windows to create a replication strategy that best serves your needs.

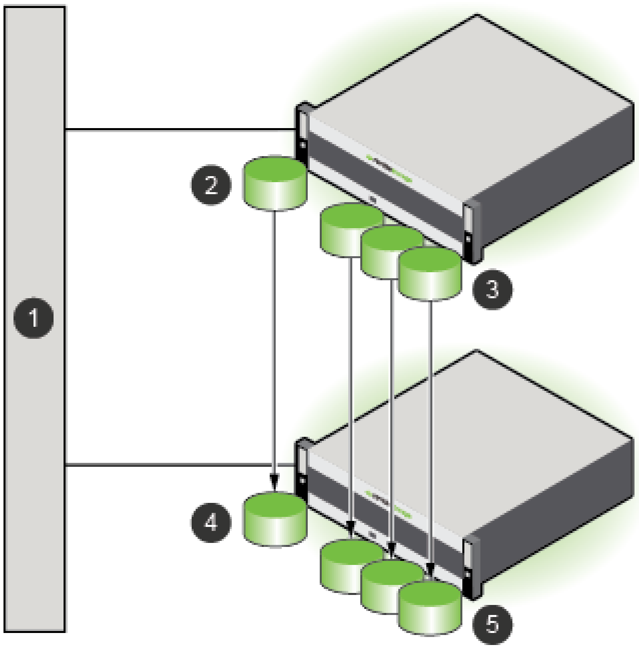
Array relationships are based on the direction of replication. The source of the volume collection that is being replicated is the *upstream* replication partner. The destination is the *downstream* replication partner. A volume source that is upstream to one partner can be downstream to another. Downstream partners can become upstream partners by sending data to other replication partners and by replicating replicas.

Note: Synchronous replication only supports a one-to-one or reciprocal replication strategy.

One-to-One Replication

Basic replication involves replicating volumes from one array to another based on the protection schedules configured for their associated volume collections. A volume collection can have up to two replication partners, but only one partner can be associated with a schedule. Volume collections can have up to 10 protection schedules.

In this scenario, the second array could be used strictly for disaster recovery. Hourly and Daily represent volume collections that are configured with protection schedules that take snapshots at the specified frequency.



1 Network

2 Single volume assigned to the Hourly volume collection

3 Multiple volumes assigned to the Daily volume collection

4 Replica of volume in the Hourly volume collection

5 Replicas of volumes in the Daily volume collection

One-to-Many Replication

You can set up a volume collection to have two replication partners. A volume collection can have up to ten protection schedules. Each schedule can have only one partner, but you can specify which partner is associated with which schedule. These schedules determine when the volumes are replicated and the array to which they are replicated.

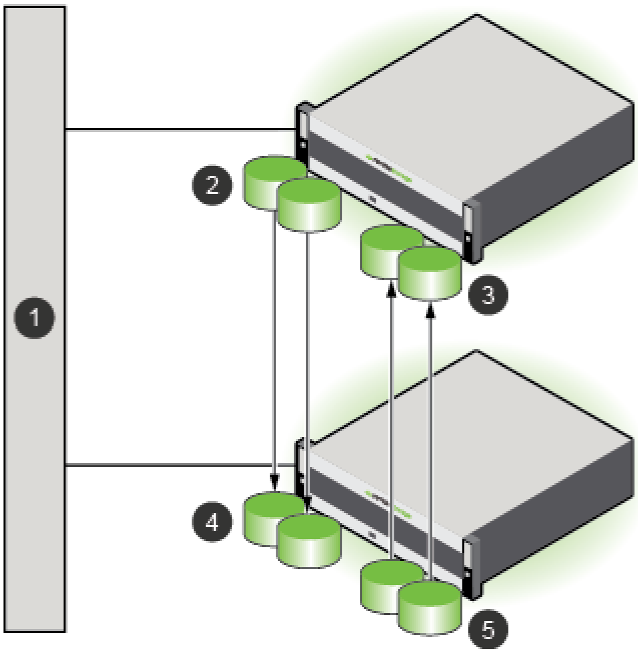
Having two partners can improve the strength of your disaster recovery plan.

For example, you can have a scenario where the volumes are replicated to one partner array on an Hourly basis and to the other partner array on an Hourly and Daily basis. Or both arrays could use the same schedule.

Reciprocal Replication

Reciprocal replication involves replicating volumes that originate on two separate arrays to each other. Volumes on one array are replicated to a second array, and volumes on the second array are replicated to the first array. Each array acts as a disaster recovery option for the other. Reciprocal replication is sometimes called *mutual replication*.

In this example, SQL and Outlook represent volume collections that are configured with protection schedules and performance policies appropriate for those application types.



1 Network

2 Multiple volumes assigned to the SQL volume collection

3 Replicas of volumes in the Outlook volume collection

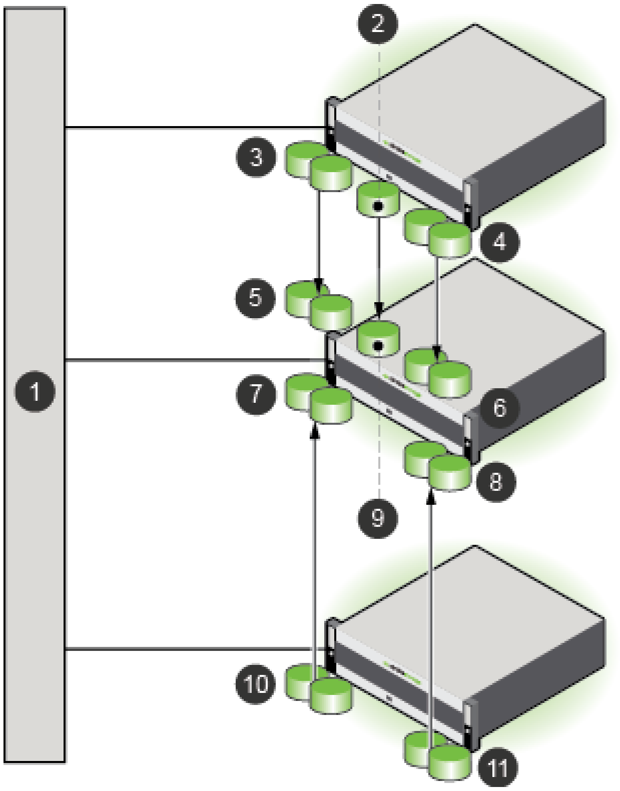
4 Replicas of volumes in the SQL volume collection

5 Multiple volumes assigned to the Outlook volume collection

Many-to-One (Centralized) Replication

You can use one array as a centralized replica for volumes that originate on several other arrays.

In this example, Hourly, Daily, SQL, Outlook, and Datastore1 represent appropriately configured volume collections.



1 Network

2 Single volume assigned to the Daily volume collection

3 Multiple volumes assigned to the SQL volume collection

4 Multiple volumes assigned to the Hourly volume collection

5 Replicas of volumes in the SQL volume collection

6 Replicas of volumes in the Hourly volume collection

7 Replicas of volumes in the Outlook volume collection

8 Replicas of volumes in the Datastore1 volume collection

9 Replica of volume in the Daily volume collection

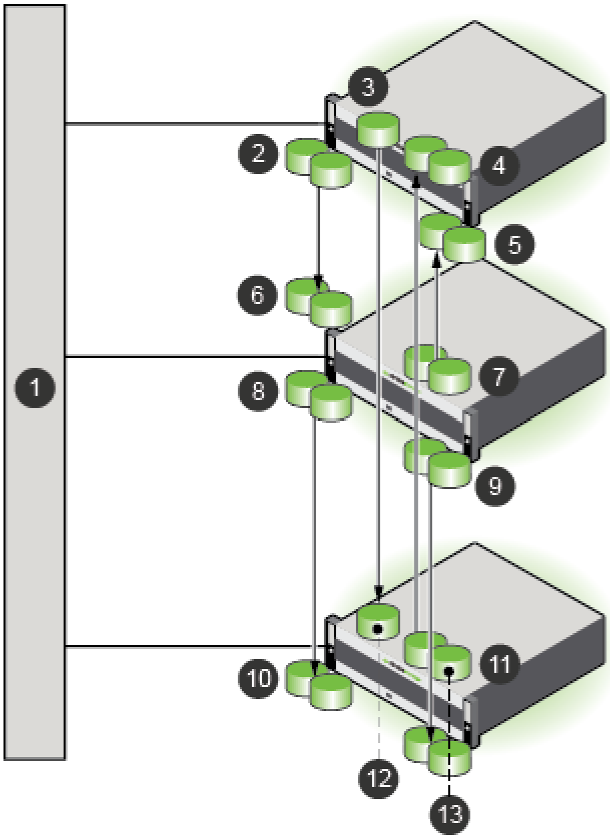
10 Multiple volumes assigned to the Outlook volume collection

11 Multiple volumes assigned to the Datastore1 volume collection

Many-to-Many Replication

One way to do many-to-many replication involves replicating volumes on the same array to multiple replication partners using multiple volume collections. The individual volume collections can have up to two replication partners.

In this example, Hourly, Daily, SQL, Outlook, Datastore1, and Temporary represent appropriately configured volume collections.



1 Network

2 Multiple volumes that are assigned to the SQL volume collection

3 Single volume that is assigned to the Daily volume collection

4 Replicas of the volumes in the Hourly volume collection

5 Replicas of the volumes in the Datastore1 volume collection

6 Replicas of the volumes in the SQL volume collection

7 Multiple volumes assigned to the Datastore1 volume collection

8 Multiple volumes assigned to the Outlook volume collection

9 Multiple volumes assigned to the Temporary volume collection

10 Replicas of volumes in the Outlook volume collection

11 Multiple volumes that are assigned to the Hourly volume collection

12 Replica of volume in the Daily volume collection

13 Replicas of the volumes in the Temporary volume collection

Replication and Folders

When you create volumes on a downstream partner, you should use a local folder. There are some differences in how folders work with synchronous replication. Folder limit enforcement and synchronous replication are independent. Therefore, you can perform the following actions:

- Associate one or more upstream synchronously-replicated volumes with a folder that has folder limit enforcement
- Associate one or more downstream synchronously-replicated volumes with another folder that has folder limit enforcement

Two folders can have a mix of synchronously-replicated and snapshot-replicated volumes, and folder limits can be set to different values, because each folder is independent of the other.

You can also choose to associate only the upstream or only the downstream volumes with a folder or volumes. It is not possible to associate both upstream and downstream volumes with the same folder, because folders are pool-scoped objects.

Either the upstream or the downstream folder (or both) can reach the folder limit. As part of folder limit enforcement, all the thin provisioned volumes in the folder are either taken offline or made read-only based on the performance policy associated with them.

When an upstream, synchronously-replicated volume is taken offline, additional I/O is not accepted.

When a downstream, synchronously-replicated volume is taken offline or is made read-only, then the upstream volume goes out of sync, but host I/O is accepted. Note that I/O resynchronization is continuously attempted by the upstream volume in this state.

Pause and Resume a Replication in Progress

Note: You cannot pause and resume a replication in progress on synchronous replication pool partners.

Procedure

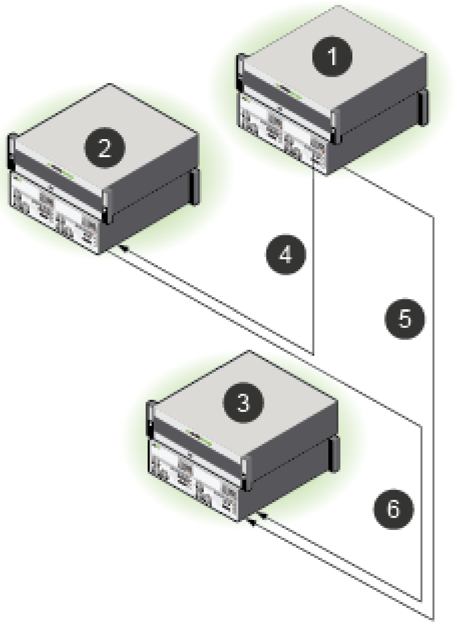
1. Select **Manage** > **Data Protection** > **Replication Partners**.
2. Click the replication partner (also known as a replication store in HPE CV) that you want to pause.
3. On the partner detail page, click **Pause**.
   The group halts all replication tasks to and from the replication partner, and all volume collections that are currently being replicated to the designated partner are paused.
4. At an appropriate time, click **Resume** to restart the replication.

Replication Seeding

If you want to replicate a snapshot collection that would take too long over a wide area network (WAN) connection, replication seeding provides an efficient method for creating a snapshot collection to use as a temporary replica. You may need to do this when you first add a replication partner, or if a replication partner needs to be re-initialized due to an accidental deletion or array replacement.

The seeding process replicates a snapshot collection to a temporary array (called the seed) over a high-speed local network (shown as *4* in the image). This third array is transported to the replication site and that same snapshot collection is then replicated from the third array to the designated replication array (shown as *6* in the image).

Once this is completed, the seed array is removed from the system and replications between the upstream replication partner and the downstream replication partner are enabled. From this point forward, the upstream and downstream arrays only need to transfer changed data (shown as *5* in the image).



1 Upstream array

2 Seed (temporary) array

3 Downstream array

4 Replication from the upstream to the seed array (one-time)

5 Replication from the upstream to the downstream array (ongoing)

6 Replication from the seed to the downstream array (one-time)

For details about replication seeding, contact support or your sales representative.

Replica Details

Note: To view details about HPE Cloud Volumes (HPE CV), you must access the HPE CV portal.

You can view the details about an on-premises replica on the volumes page for the replica. You can tell that a particular volume is a replica because it has a replica icon in the crumb trail at the top of the page. You can also verify that the **Edit** button is disabled as are the actions in the **More Actions** dropdown menu. The reason for these characteristics is because the replica is owned by the upstream group. When you access the replica from the downstream group, you can only view the replica. You cannot edit it.

The downstream group can claim a replica if the source volume is not replicating, the replication link is broken, and the source volume is no longer part of a volume collection. At this point, the claim option is enabled. After the replica has been claimed, it becomes a regular volume that belongs to the downstream group and all the actions of a regular volume are enabled.

Replication Bandwidth Limits

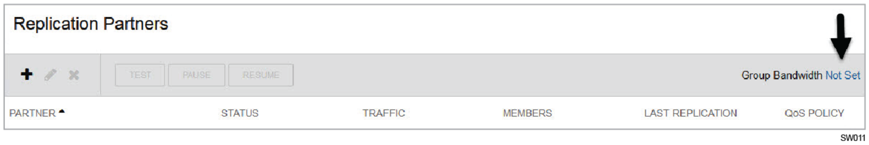
There are two kinds of replication bandwidth limits:

- The overall limit specifies the replication bandwidth for network traffic that originates from an array to all partners
- The per-partner limit specifies the replication bandwidth for network traffic that originates from an array to a specified partner

You can set only one replication bandwidth limit type at a time. If the overall limit is set, the per-partner limits are not allowed for any partner. Conversely, if any partner has per-partner limits set, you cannot set an overall bandwidth limit.

Set Overall Bandwidth Limits for Replication

If you set an overall bandwidth limit for all replications, you cannot set per-partner bandwidth throttling for each replication partner. You can limit bandwidth by using an overall policy or per-partner limits, not both.



Procedure

1. Select **Manage** > **Data Protection** > **Replication Partners**.
2. Click **Not Set** to the right of Group Bandwidth.

   By default, the link title is **Not Set** until you add a policy.
3. Click **Add Policy**.
4. In the **Group Replication Bandwidth** dialog box, create as many policies as you need.

   Policies cannot overlap. To create a pause in the schedule, set the bandwidth limit to 0 (zero).
5. Click **Set Bandwidth**.

Results

The information for the Group Bandwidth changes to indicate that at least one overall bandwidth limit is set.

Remove Overall Bandwidth Limits for Replication

If you remove overall bandwidth limits, you can create per-partner policies for each replication partner.

Procedure

1. Select **Manage** > **Data Protection** > **Replication Partners**.
2. Click **Set** to the right of Group Bandwidth.

   By default, the link title is **Not Set** until you add a policy.
3. Click **Edit**.
4. In the **Group Replication Bandwidth** dialog box, delete a single policy by clicking **Remove** next to that policy or delete all policies.
5. Click **Set Bandwidth**.

Results

The **Group Replication Bandwidth** details now indicate that the overall bandwidth limit is Not Set.

Configure Bandwidth Limitations for a Replication Partner

Bandwidth *limits* are expressed in megabits per second (Mbps) or kilobits per second (Kbps). The default unit is Mbps.

> **Note:** The following limitations apply to setting bandwidth limitations:
>
> - You cannot set bandwidth limitations on pool partners for synchronous replication.
> - If you set per-partner bandwidth throttling, you cannot set an overall bandwidth limit for all replications. You can limit bandwidth by using an overall policy or per-partner limits, not both.

Procedure

1. Select **Manage** > **Data Protection** > **Replication Partners**.

2. Check the replication partner whose bandwidth you want to define.
3. Click the pencil icon to edit the replication partner.
4. In the **Edit replication partner** dialog box, click **Next** to open the **QoS Policy** page.
   Further policies must be set to use less bandwidth than the limit that is set here.
5. To add per-partner throttling, click **Add Policy** and complete the following fields.
   a) Type a description of the per-partner limit.
   b) Set the bandwidth limit.
   c) Set the time period during which this limit should be in effect.
   d) Select the days of the week during which this limit should be in effect.
   e) Optional. Click **Add Policy** to create as many bandwidth limitation schedules as needed for different time periods, days of the week, or both.
6. Click **Save**.

Modify Per-Partner Replication Bandwidth Limits

When per-partner bandwidth throttling is configured, you can easily modify the schedules.

Procedure

1. Select **Manage** > **Data Protection** > **Replication Partners**.
2. Click the replication partner whose bandwidth limits you want to change.
3. Click **Edit**.
4. In the **Edit replication partner** dialog box, click **Next** to open the **QoS Policy** page.
   Further policies must be set to use less bandwidth than the limit that is set here.
5. Make the necessary changes:
   - Click **Remove** to delete any unneeded policies.
   - Click **Add Policy** to add any new policies.

   Policies cannot overlap.
6. Click **Save**.

Security

Arrays provide multiple features to increase security in a group of arrays.

These features include:

- Role-Based Access Control on page 143
- Microsoft Active Directory and LDAP on page 152
  - Access Control with Active Directory on page 153
  - Access Control with LDAP on page 156
- CHAP Authentication on page 163
- Secure SMTP on page 167
- Encryption of Data at Rest on page 169
- Secure Sockets Layer Certificates on page 172

For information about access to arrays and volumes and user management and supported protocols, see Access Controls on page 25.

Role-Based Access Control

Role-based Access Control (RBAC) lets you control access to groups and arrays through the use of user accounts assigned particular roles. The role determines the level of access that a user account is provided. A user account that is assigned to the Administrator role can create and manage accounts for other users.

All users can manage their own passwords and account information. Only users with an Administrator permission level (user role) can add, modify, remove, enable, or disable user accounts.

For more information about permission levels (user roles), see Permission Levels on page 143.

Permission Levels

Each feature has a minimum permission level (user role) that is required to use the feature.

The permission levels (user roles) are summarized here.

Table 10: Summary of Permission Levels (User Roles) and Access

Permission Level (User Role)	Access
Administrator	All actions
Power User	All actions except user management, inactivity timeout, array setup, and array resetup
Operator	Management actions except to delete or remove data
Guest	View information and choose VMware subnets

The following table explains the methods of user access control.

Table 11: How Nimble Interfaces Manage Access

Interface	Method of User Access Control
GUI	Disables or hides unauthorized actions.

Interface	Method of User Access Control
CLI	Ignores unauthorized actions and returns a Permission denied message.

The following table lists individual array unit-cs features, the actions associated with each feature, and the minimum permission level (user role) required to perform the action.

Table 12: Features, Actions, and Permission Levels (User Roles)

Feature	Action	Minimum Permission Level (User Role)
Alerts	List / view info	Guest
	Test	Power User
Arrays	List / view info	Guest
	Discover	Power User
	Edit array name	Power User
	Set up / Re-set up	Administrator
	Add	Power User
	Remove	Power User
	Reboot	Power User
	Shut down (halt)	Power User
	Fail over controllers	Power User
Certificates	Regenerate	Administrator
CHAP user	List / view info	Operator
	Create	Operator
	Delete	Operator
	Edit	Operator
Controllers	List / view info	Guest
	Reboot	Power User
	Fail over	Power User
Date and Time	View (local or UTC time)	Guest
	Edit	Power User
Disks	List / view info	Guest
	Add	Power User
	Remove	Power User
DNA	Enable / disable	Power User
	Set secure tunnel	Power User
	Set HTTP proxy	Power User
Domain name / DNS server for a group	List / view info	Guest
	Add	Power User

Feature	Action	Minimum Permission Level (User Role)
Expansion shelves	List / view info	Guest
	Add	Power User
	Activate	Power User
Fibre Channel interfaces	List / view info	Guest
	Edit	Power User
	Update configuration	Power User
Groups	List / view info	Guest
	List limits	Guest
	Edit inactivity timeout	Administrator
	Edit other settings	Power User
	Merge	Administrator
	Create throttle	Power User
	Edit throttle	Power User
	Delete throttle	Power User
	Initiate DNA	Power User
	Validate DNA	Power User
	Unset HTTP proxy	Power User
	Reboot	Power User
	Shut down (halt)	Power User
Help	Show the online help	Guest
Initiator groups	List / view info	Operator
	Create	Operator
	Delete	Operator
	Edit	Operator
	Add initiator	Operator
	Remove initiator	Operator
	Add subnet	Operator
	Remove subnet	Operator
IP addresses	List / view info	Guest
	Add	Power User
	Edit	Power User
	Delete	Power User

Feature	Action	Minimum Permission Level (User Role)
iSNS server for a group	Server IP address	Power User
	Port number	Power User
	Enable / disable	Power User
Migrations	List / view info	Guest
Network configurations	List / view info	Guest
	Create a draft	Power User
	Delete	Power User
	Validate	Power User
	Activate	Power User
	Edit	Power User
Network interface cards (NICs)	List / view info	Guest
	Edit	Power User
	Assign / unassign a subnet	Power User
NTP server for a group	List / view info	Guest
	Add	Power User
Performance policies	List / view info	Guest
	Create	Operator
	Delete	Power User
	Edit	Operator
Pools	List / view info	Guest
	Create	Power User
	Delete	Power User
	Edit	Power User
	Assign / unassign array	Power User
	Merge	Power User
Replication partners	List / view info	Guest
	Create	Power User
	Delete	Power User
	Edit	Power User
	Create / edit / delete QoS policy (throttle) settings	Operator
	Pause / resume replication	Operator
	Test connection	Operator

Feature	Action	Minimum Permission Level (User Role)
Routes	List / view info	Guest
	Add	Power User
	Edit	Power User
	Delete	Power User
Snapshots	List / view info	Guest
	Delete	Power User
	Edit	Operator
	Set online / offline	Operator
Snapshot collections	List / view info	Guest
	Delete	Power User
	Edit	Operator
SNMP for a group	Edit community string	Power User
	Enable / disable gets	Power User
	Edit responder port number	Power User
	Edit system contact / location	Power User
	Edit trap host IP address	Power User
	Edit trap port number	Power User
	Enable / disable traps	Power User
Software	List / view info	Guest
	Download	Power User
	Pre-check	Power User
	Update / upload	Power User
	Resume an update	Power User
Space reservations, default for a group	Volume reserve	Power User
	Volume limit	Power User
SSH keys	List / view info	Administrator
	Add	Administrator
	Edit	Administrator
	Delete	Administrator
Statistics	Display	Guest
Subnets	List / view info	Guest
	Add	Power User
	Edit	Power User
	Remove	Power User

Feature	Action	Minimum Permission Level (User Role)
Time zone	List / view info	Guest
	Change	Power User
User accounts, individual	View own profile	Guest
	Change own password / email address	Guest
User administration	List / view info	Administrator
	Add users	Administrator
	Change passwords	Administrator
	Edit user permissions	Administrator
	Edit timeout interval	Administrator
	Enable / disable users	Administrator
	Remove users	Administrator
User sessions	List / view own info	Guest
	List / view info for other users	Administrator
VMware plugins	List	Guest
	Subnet, choose	Guest
	Register / Unregister	Power User
Volumes	List / view info	Guest
	Create	Operator
	Delete	Power User
	Edit volume size	Power User
	Edit other volume settings	Operator
	Create / edit / delete ACLs	Operator
	Set online	Operator
	Set offline	Power User
	Take snapshot	Operator
	Restore from snapshot	Power User
	Clone from snapshot	Operator
	Associate with volume collection	Operator
	Disassociate from volume collection	Operator
	Claim partner volume	Power User
	Move to another pool	Power User

Feature	Action	Minimum Permission Level (User Role)
Volume collections	List / view info	Guest
	Create	Operator
	Delete	Power User
	Edit	Operator
	Validate	Operator
	Add schedule	Operator
	Edit schedule	Operator
	Delete schedule	Operator
	Take snapshot	Operator
	Restore from snapshot	Power User
	Promote	Power User
	Demote	Power User
	Hand over	Power User
	Stop replication	Power User

View User Information

All users can view their own account information. Only users with Administrator permission can view the accounts of other users.

Procedure

1. Select **Administration** > **Security** > **Users and Groups**.
2. Click the user account for which to display information.
   Details about the selected user appear to the right of the list.

Add a User Account

Each person must have a user account to access and manage an array group. The Administrator controls a user's access to the group by assigning a specific role to each user.

At a minimum, each user account must have a:

- username
- full name
- role
- inactivity timeout interval

Optional. A user account can also have a:

- description
- email address

You can include these options when you create the user account or you can add them later.

Note: In the GUI, the inactivity timeout interval set for the group is automatically applied to all user accounts. To set a shorter interval for a user, edit the user account.

You can set the timeout to a limit lower than the group timeout but not higher than the group timeout limit.

Before you begin

You must have Administrator permission to add user accounts.

Procedure

1. Select **Administration** > **Security** > **Users and Groups**.
2. Click **Add**.
3. In the Full Name field, enter the user's full name.

   The full name must be alphanumeric, 1 to 64 characters, must start with a letter, may use dashes, spaces, and apostrophes; no periods.
4. From the Role menu, choose a Role.

   Choices are: Administrator, Power User, Operator, or Guest
5. In the Username field, type the user's username.

   The username must be alphanumeric, 1 to 32 characters, must start with a letter, no spaces. The username is required for user login.
6. (Optional) In the Email Address field, enter the user's email address.
7. (Optional) In the Description field, enter a description.

   The description can have from 1 to 255 characters but no hard returns.
8. In the New Password field, enter a password.

   The password must be comprised of alphanumeric characters with a length of 8 to 512 characters. Do not use [ ] & ; ` or spaces. The password is required for user login.
9. In the Confirm Password field, enter the password again.
10. Click **Save**.
    The new user account is added to the list.

Edit a User Account

You can change the full name, role, description, and email address with this task.

You can also add or delete a description and email address with this task.

Before you begin

You must have Administrator permission to edit a user account.

Procedure

1. Select **Administration** > **Security** > **Users and Groups**.
2. In the user account list, highlight the account to edit.
3. Click **Edit**.
4. Make changes as required.
5. Click **Save**.
   The edited user account appears in the list.

Change Your Account Information

All users can add, change, or delete their own description and email address. You must log in with your own username to perform this task.

Procedure

1. Select **Administration** > **Security** > **Users and Groups**.

2. Click a name in the User list, then click **Edit**.

   You can modify the email address, description and inactivity timeout. The inactivity timeout must be less than the inactivity timeout for the group.

3. Click **Submit**.

Reset a User Account Password

When users forget their passwords, perform this task to reset the password.

Before you begin

You must have Administrator permission to reset other users' passwords.

Procedure

1. Select **Administration** > **Security** > **Users and Groups**.
2. In the user account list, click the account for which you want to reset the password.
3. From the **More Actions** drop-down menu, choose **Change Password**.
4. In the Admin Password field, type your Administrator password.
5. In the New Password field, type the user's new password.

   The password must be alphanumeric, 8 to 512 characters. The following special characters are not allowed: [ ] & ; ` and spaces.

6. In the Confirm Password field, retype the user's new password.
7. Click **Change**.
8. Send the user the new password.

Enable a User Account

You can reactivate, or enable, a previously deactivated user account.

Before you begin

You must have Administrator permission to enable user accounts.

Procedure

1. Select **Administration** > **Security** > **Users and Groups**.
2. In the user account list, highlight the account to enable.
3. From the **More Actions** drop-down menu, choose **Enable Account**.
4. Click **Enable** to confirm.
   In the user account list, the padlock icon is removed from the account.

Disable a User Account

If needed, you can temporarily suspend a user's access to the array.

Before you begin

You must have Administrator permission to disable user accounts.

Procedure

1. Select **Administration** > **Security** > **Users and Groups**.
2. In the user account list, highlight the account to disable.

3. From the **More Actions** drop-down menu, choose **Disable Account**.
4. Click **Disable** to confirm.
   In the user account list, a padlock icon is added to the account.

Remove a User Account

Before you begin

You must have Administrator permission to remove user accounts.

If needed, you can permanently remove a user account. Consider disabling the account rather than removing it.

Procedure

1. Select **Administration** > **Security** > **Users and Groups**.
2. In the user account list, highlight the account to be deleted.
3. Click the **More Actions** menu and click **Remove**.
4. Click **Remove** to confirm.
   The user account is removed from the list.

Microsoft Active Directory and LDAP

The array allows you to use either Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) to provide external authentication server support for managing and authenticating users and groups. When a user logs in to an array, the service authenticates the user based on information in a centralized domain and assigns the appropriate array role to the user. This role specifies which tasks the user can perform.

Using an external authentication server provides:

- Simplified administration. All the users and their permissions are stored in a single location. You can manage the users and set security policies, such as password strength and expiration time, from one location..
- Enhanced security. When you change user settings, you do it in one place, not on multiple arrays. For example, if you delete a user, you perform this action in one place.

Active Directory and LDAP can share a centralized domain that stores information about authorized users, groups, and hardware objects when you select the schema AD during setup.

Note: If you configure LDAP using the schema OpenLDAP, there is no connection between Active Directory and LDAP.

The array requires that you only run one service at a time. While you cannot run both Active Directory and LDAP simultaneously, you can easily switch between the services.

Important: To switch from Active Directory to LDAP, use the GUI **Leave Domain** option or the CLI **userauth --leave** command option. To switch from LDAP, use the GUI **Disconnect** option or the CLI **userauth --delete** option. These options remove the current service and its domain authentication. As a result, users who are logged in to the array using that service will no longer be able to perform tasks on the array. Any new operations will result in an error. If the users are not part of the domain you are switching to, they may not be able to log in. Local account access is permitted even if the array has stopped running an external server authentication process.

For more information about these services, see

- Access Control with Active Directory on page 153
- Access Control with LDAP on page 156

Specifying an External Authentication Directory Service

You can specify that the array use either Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) to provide external authentication server support. The first time you select either Active Directory or LDAP, you must provide domain information. After that, the array GUI displays the current service and domain information when you view the Directory information.

> **Note:** The array supports both Active Directory and LDAP; however, you cannot run both of them simultaneously. You must remove the current domain connections before you can switch between an Active Directory and LDAP configuration. See Switch Between Active Directory and LDAP Using the GUI on page 160.

Procedure

1. Select **Administration** > **Security** > **Directory**.
2. From the **Directory** dropdown list, select either **Active Directory** or **LDAP**.
3. Provide the information necessary to set up the domain and select **Connect**.

   The array displays information about the domain.
4. To confirm that the domain is connected, select **Test Connection**.

   If you need to change the configuration, select **Actions** > **Edit**. Then repeat Step 2 and Step 3.

Access Control with Active Directory

An Active Directory domain is a collection of objects within a Microsoft Active Directory network. The objects in the domain can include a single user, a group, or a hardware component, such as a computer or printer. Each domain contains a database that stores identity information about the object.

Active Directory relies on mapping Active Directory groups to array roles to determine a user's access. Users are assigned to particular Active Directory groups which are designated with specific array roles. The array roles indicate the level of access permissions that the group members have to perform particular functions.

> **Note:** Active Directory on an HPE array can support up to 100 groups per array with up to 2000 Active Directory users logged in at one time. If you exceed 2000 users, the session for the user who has been logged into the system the longest is terminated.

Guidelines for Working with Arrays and Active Directory

You can join an array to an Active Directory domain. The following list includes some guidelines to consider when working with arrays and Active Directory.

- When you add an Active Directory user to a group that is authorized to log into the array, you must use the same username and password with the array that you use with all other AD-connected systems in the environment.
- Disabling a user's Active Directory account also disables that user's access to the storage environment.
- Joining an array to a domain creates an Active Directory account for the array on Active Directory. The default Organizational Unit (OU) for the account is Computers. You can create the account under a different OU.
- The default name of the computer account is the first 15 characters of the array group name. You can specify a different computer name if you choose.

  If you use the default name, you must make sure that the first 15 characters of the array group name do not conflict with any other array group name that is in Active Directory. If you duplicate a group name, Active Directory removes the first version of the group name so that the new group name can join Active Directory. Consequently, the group with the duplicated name will not be able to log into the array even though it joined Active Directory first.

  Example:

  1 *group-array-xxxx1* was the first group to join the Active Directory domain *ZZZ*. The default AD machine account name for the array is *group-array-xxx* because the group name truncates after the first 15 characters.

2. *group-array-xxxx2* was the second group to join the Active Directory domain *ZZZ* but the default AD machine account name would also be *group-array-xxx* because the group name truncates after the first 15 characters.
3. Upon joining the AD domain, *group-array-xxxx2* replaces the AD machine account from *group-array-xxxx1* with an account for *group-array-xxxx2*. Group users are no longer able to log into *group-array-xxxx1*, although they can now log into *group-array-xxxx2*, which joined later.

- Avoid using special characters in OU and Group names. If you use special characters, they must be preceded by a single backlash, and the entire argument must be inside either single quotation marks (') or double quotation marks ("). For a list of special characters, refer to the Reserved Characters table in Distinguished Names.
- Active Directory administrators can create an account for the array in any OU and then can give storage administrators the privilege to join the domain.
- After an array has joined a domain, you can enable and disable Active Directory authentication without leaving the domain.

User Authentication and Logon

Active Directory supports the following types of user names for authentication.

- *User_name* (Authenticate with the default domain or as a local user)
- DefaultDomain\User_name (Authenticate with the default domain)
- TrustedDomain\User_name (Authenticate with the trusted domain)

Authentication uses the following guidelines:

- If you are authenticating using Active Directory, do not add a group to an array with the group type "Distribution."
- If the array is not a member of an Active Directory domain, then users are authenticated locally on the array. The account must have been created on the array in the **Administration: Users and Groups** dialog.
- If you try to authenticate to an array that is a member of an Active Directory domain, you are authenticated against the Active Directory first.

  Note: Some built-in users, such as root, admin, and nsupport, are always authenticated locally.

  If authentication to Active Directory fails for reasons other than a password failure, the array attempts to authenticate the user locally. If the local account experiences a password failure or the account does not exist locally, authentication fails.

- You can enter a username or a combination of DOMAIN\username. If you do not include DOMAIN, the authentication effort uses the default domain; that is, the domain that the array is a member of.
- The number of repeated failed login attempts allowed depends on the Password lockout setting.
- A successful login provides you with the GUI and CLI roles and capabilities as defined by the group.
- If you lose access to the array, the system response depends on whether you are logged in locally or as an Active Directory user. You might receive an error message, or you might be logged out of the array.
  - When a user is removed from an Active Directory group that has access to the array, the user is no longer able to log into the array. Existing login sessions will continue until the user logs out. This is consistent with the behavior of Windows clients and group memberships.
  - After an Active Directory group is removed from the array, users can no longer log into the group. Existing login sessions will continue until the users log out.

Preparing to Join an Array to Active Directory

There are several methods for joining the array to an Active Directory domain, including the following:

Method 1: Provide the username and password for a Domain Administrator or an Account Operator user account

An easy method to join the domain is to use an account with the proper role in an Active Directory. The array does not store the credentials. The credentials are used in a one-time operation to create the necessary Active Directory objects and trigger initial synchronization between the array and the newly created Active Directory credentials.

You can:

- Provide the credentials for an existing Domain Administrator or Account Operator account while joining the domain.

- Temporarily assign a new or existing user account to the default "Domain Admins" group or "Account Operators" group.

Method 2: AD administrator creates a machine account that lets you join the domain as a standard user

1 An Active Directory Domain Admin or Account Operator can create a machine account in Active Directory for the array.

  This account can be under either the Computers OU (Organizational Unit), which is the default, or a custom OU.

2 Record the account name and its OU.

  You only need to specify the OU if you create a custom one. You do not need to specify it when you use the default OU Computers.

3 The Active Directory Domain Administrator or Account Operator must edit the machine account and provide write/modify permissions to the standard user account that will be used to join the array to the domain.

Method 3: Set up a dedicated OU where a user or group has the necessary privileges to create or modify array machine accounts

An Active Directory Domain administrator can create an OU specifically for the storage arrays:

1 In the Active Directory Users and Computers (ADUC) right-click on the OU where the array's machine account will be created.
2 Select **Properties**.
3 From the top level, go to **View** > **Advanced Properties**.
4 Select **Permissions**.
5 Add the group with write access (or full access) to the OU.
6 Add the standard user to the group that has access to that OU.

Join an Active Directory Domain

Procedure

1. Go to **Administration** > **Security** > **Directory** > **Active Directory**.
2. Complete the fields in the Microsoft Active Directory Domain dialog box.

   For the Username and Password fields, provide credentials that have the permissions you need in the Active Directory.

   If you select **Set Manually** for the Organizational Unit, a new field appears.

   You must specify either the OU where the machine account already exists or the OU where the array machine account will be created.

   You must have the appropriate permissions that allow you to create or modify objects in this OU.

   If you manually created a machine account, it must match the name provided in the **Computer Name** field.
3. Click **Connect**.

Remove an Active Directory Domain

You can disconnect an array from an Active Directory domain. Doing this deletes the domain configuration that was connected to the array.

If you want to switch from an Active Directory configuration to an LDAP configuration, you must first remove the Active Directory domain.

> **Important:** If you disconnect an array from an Active Directory domain, all users from that domain lose access to the array.

Procedure

1. Go to **Administration** > **Security** > **Directory** > **Active Directory**.
2. From the **More Actions** menu, select **Leave Domain**.

3. Click **Confirm** in the warning box.

Access Control with LDAP

Lightweight Directory Access Protocol (LDAP) provides external authentication server support. LDAP allows you to set up user groups on a central LDAP server. You can authenticate these users and allow them to log in to storage arrays. The authorization parameters determine which role is assigned to the user.

You can have up to three LDAP servers. One is the primary server and the other two are secondary servers. The secondary servers are optional. If you have a secondary server, then, if the primary server fails, the secondary server can be used for authentication.

The secondary servers are in listen-only mode. The primary server replicates data to them. You cannot use the secondary servers for load-balancing.

Note: Secondary servers must use the same security certificate as the primary server.

Microsoft Active Directory provides an LDAP service. This service allows you to use LDAP to connect to Active Directory server.

Note: Currently the array supports either LDAP or Active Directory as the external authentication service. You can switch between LDAP and Active Directory, but you cannot run both protocols at the same time.

You can set up LDAP using the array GUI or the array CLI.

Guidelines for Working with Arrays and LDAP

Lightweight Directory Access Protocol (LDAP) requires that you join an array to an LDAP domain. You must map LDAP groups to the array. Users are assigned to specific LDAP groups, which can have specific array roles.

Login credentials

When you add an LDAP user to a group that is mapped to the array, that user is authorized to log into the array. The login credentials are based on the information you provide when you set up LDAP.

- Each username must include @<*domain_name*>. The *domain_name* is the value you supplied for domain name when you configured LDAP to work with the array.
- The password is the one you entered when you configured LDAP to work with the array.

Groups and users

LDAP supports up to 100 groups, including groups designed for LDAP internal use. It supports up to 2,000 users.

Note: When you add LDAP users, the GIDs and UIDs must be 1,000 or greater. This avoids clashes with system users. The values 0 through 999 are reserved for system use. If an LDAP server user has a GID or UID that is less than 1,000, the authentication fails with a message indicating that the user was not found.

You can have up to 10 user search bases or 10 group search bases or Directory Information Trees (DIT).

Supported schemas

The current LDAP implementation supports the following schemas:

- OpenLDAP (RFC 2307)
- Active Directory

Note: Custom schemas are not supported.

Supported domains

Currently the array supports only one LDAP domain. Once you set up the domain, it is considered to be in use even if it is disabled.

Disabling and disconnecting an LDAP domain

You can disable LDAP or even disconnect the LDAP domain from the array.

If you disable LDAP, the configuration is considered to be in use; however:

- You cannot set up any other service. If you attempt to configure a new domain, that effort will fail. You must either delete the disabled domain or re-enable it before you can configure a new domain.
- Any attempts to join a new, existing domain will fail.
- All users associated with the domain will be disconnected from the array and no longer able to log in.

If you choose to disconnect the LDAP configuration, the connection with the array is removed completely. Users who relied on LDAP authorization are no longer able to log in to the array.

Connection options

LDAP supports the following connection options:

- LDAP server host: host name or an IPv4 address

  Note: IPv6 is not supported.

- LDAP server port: 389 for LDAP or 636 for LDAP over TLS/SSL
- Encryption: StartTLS with port 389. TLS/SSL with port 636.

  Note: These are default ports. This information is in each `ldap://host:port serve` URI and each `ldap:// = StartTLS, ldaps:// = TLS/SSL` URI. You can change the port numbers in the URI.

Certificate authentication

You must import the CA certificate for the LDAP server before you attempt to connect it to the array. For example:

```
$ cert --import ldap1ca --trusted
Please enter certificate in PEM format followed by ^D:
-----BEGIN CERTIFICATE-----
MIIDZzCCAk+gAwIBAgIUXe2PtGSkULD+vdCXuJ+nGNk/ZpQwDQYJKoZIhvcNAQEL
BQAwWTELMAkGA1UEBhMCVUsxEDAOBgNVBAgMB0JyaXN0b2wxEDAOBgNVBAcMB0Jy
aXN0b2wxETAPBgNVBAoMCE5pbWJsZU9TMRMwEQYDVQQDDApSb290LWxkYXAxMB4X
DTIwMDcwODE0NTEzOFoXDTIxMDcwODE0NTEzOFowXTELMAkGA1UEBhMCVUsxEDAO
BgNVBAgMB0JyaXN0b2wxEDAOBgNVBAcMB0JyaXN0b2wxETAPBgNVBAoMCE5pbWJs
ZU9TMRcwFQYDVQQDDA5OaW1ibGVPUy1sZGFwMTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBALr+WOXB9wNBecKf3mlVTs0sQL1C7Lju3uYKPlfoWbvV2wyV
cQ7w+ksX5XyCyryBcQDGLtFUNvtvqzsgewxNNPQKbgq75v7pL2tzaxH/audddOZF
t8vlYhrGnYMocwbUzdDaTRLsMbLvtlAgsiA1dT2t37HAHRR0d76xKIQL4qQu2EZY
8+YHMCBPAM8m48nRN2ztSbIk640cCvON2fIKBQT5Rsf6iJVnChpPSxSuZDDhDJfi
buwq/EBEGRA/bg86F9tpyuPv0sE/+XMANxMUii0UWdqNdRrHLyMTL7JmoXXdYZRE
uAu5o77/jy1jdbfQB91ChwIgtVSKrJ5kt07kaGsCAwEAAaMjMCEwDwYDVR0TAQH/
BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAgQwDQYJKoZIhvcNAQELBQADggEBAAzYbxwA
lRDRdXLKtBKv+bZSodhFCZ1reet12s7lGsbpTrlMgV6gk8owXm8JfvbsPcA4CLbT
O8wPoN3RBUckn8YucvfF9n8NGL0nUGM/pOBJAnm41Es85JmNw1T8x7Ega42kgM6k
fE2Pj5t7NOyOZ245U5n8sAGph4ggZVP4iIwB/qw+Pw48SQFZvtlTYWTfTZ9xGCGt
swKzUC6G1ktjqJLqEngU4kucqMu/dRVfP9/qBKTD65yBB/fujOcSWogUapwkKnMN
b83S89dTDKnNzNmUhknV0xalLPCpl4RtlX+jRJIy9hBB309jplsp+DQeBwjCija8
F0Q91kuZRlc2fZs=
-----END CERTIFICATE----
```

For information about how the array works with certificates, see Secure Sockets Layer Certificates on page 172.

Performing searches

You can set up your LDAP implementation to perform searches for user and group information. For example, you can configure LDAP to search for a user with a specific name or all the groups that a user is a member of.

Searches are relative to the base Distinguished Name. If you do not specify a search base, LDAP searches from the base Distinguished Name. It is a good practice to limit searches to the part or parts of the directory where you know the users and groups are.

Note: A search immediately starts authenticating the search items. If you have a large domain, searching the base domain can take a long time. Restricting the search can increase the speed of the authentications.

Overview of the LDAP Workflow

The workflow for setting up Lightweight Directory Access Protocol (LDAP) requires the following high-level steps:

1 Create an LDAP server domain.
2 Map the LDAP groups to the array group roles.
3 Import the trusted certificate for the LDAP server to the array.
4 Log on to the array and go to **Administration** > **Security** > **Directory**.
5 Select **LDAP** from the drop-down list.
6 Provide the information necessary to allow LDAP to join the array.
7 After you set up the connection with the array, it is a good practice to check it. Select **Test Connection**. This action checks the array's connection to the domain.

Example of an LDAP Setup

The following example takes you through the steps to set up Lightweight Directory Access Protocol (LDAP) to work with an array. This is just an example to provide an extended workflow.

Before you can configure LDAP to connect with the array, you must import the trusted server certificate for the LDAP server to the array. This example uses an internal CA.

After the certificate has been imported, you can set up the LDAP configuration for the array.

Procedure

1. Use LDAP to connect to the Active Directory server.

   You need the host name that is used in the certificate and the domain name.

2. Using a tool such as **Adminstrative Tools** > **Certificate Authority**, locate the certificate and copy it.

   a) Select the certificate and open the certificate properties.
   b) Click **View Certificate**.
   c) Click the **Details** tab and select **View Certificate**.
   d) The Certificate Export Wizard starts. Click **Next**.
   e) Select Base-64 and click **Next**.
   f) Browse to where you want to save the copy of the certificate and enter a file name for it.

      You can enter any name you choose.

   g) Click **Finish**.

      A message is displayed telling you whether your export was successful.

3. Open the certificate in a tool such as Notepad and copy the certificate chain information.
4. Log in to the array GUI.

   Make sure you log in with administrator privileges.

5. Go to **Administration** > **Security** > **SSL Certificate**.
6. Under **Certificate Actions**, select **Import a Trusted Certificate**.

   a) Provide a name for the certificate.

      You might want to give it the same name as the domain; however, you can give it any name you choose.

   b) Paste in the certificate chain information and click **Save**.

The certificate now shows up as a trusted certificate. It will show up as a trusted connection when you connect the LDAP server to it.

7. Go to **Administration** > **Security** > **Directory** and select LDAP from the drop-down list.

Provide the Connection Details and the LDAP Search Details. Most of the fields are self-explanatory. Here are some details for some of the key fields.

> **Note:** The information you enter is divided into sections. In some cases, there is an **Add** button. These are places where you can add more information if you choose. For example, you can have up to three server URIs. The initial fields allow you to provide information for the first server URI. Selecting **Add** allows you to provide the details for a second URI. Selecting **Add** again lets you provide information for a third server URI.

- Domain. This is the local name for the domain. You can enter any name you choose. You do not need to enter a fully qualified domain name. However, when users log in to the array, they will need to enter the value you enter here as part of their username: <*username*>@<*domain*>.
- Server URL. This must be a valid URL and it must match the host name in the certificate. You can use either "ldap" or "ldaps". You can also provide a port number as part for the URL. For example, you might enter `ldaps://wintrust.net:1234`.

  You can have up to three server URIs. Use the **Add** button if you want to have more than one server URI.
- Schema. Select the schema from the drop-down list. The array currently supports two schemas:
  - AD
  - OpenLDAP
- Bind User DN. Enter the distinguished name. The user must have read and search permissions for the directory, but does not have to be an administrator. For example, if you were setting up information using the server URL above, you might enter something similar to `cn-Administrator,cn=Users,dc=wintrust,dc=NET`.
- Base DN. For the search, you can set the base domain name. You should consider where you want the search to start. If you search the entire domain, it can take a long time.
- User Search Base. You can supply a value here to focus the search area on users. You might enter something similar to `cn=USERS`. The name you enter is relative to the Base DN.

  You can have up to 10 user search base DNs. Use the **Add** button to provide information for additional user search bases.
- Group Search Base. You can supply a value here to focus the search area on groups. You might enter something similar to `ou=CompanyABC`. The name you enter is relative to the Base DN.

  You can have up to 10 group search base DNs. Use the **Add** button to provide information for additional group search bases.

8. Click the **Connect** button.

It displays the details about the LDAP directory domain you just created.

9. In the left navigation pane, go to **Users and Groups** and add a group.

You must enter the following information:

a) The Group Name.

b) The Role. Select it from the drop-down list. For more information, see Supported Array Roles on page 160.

c) The Inactivity Timeout. Enter this value as minutes.

10. Click **Submit**.

11. Test the new directory domain.

a) Log out of the array.

b) Log back in to the array.

Remember you need to enter <*username*>@<*domain_name*> where *domain_name* is the name of the LDAP domain.

Disconnect an LDAP Domain

You can disconnect an array from a Lightweight Directory Access Protocol (LDAP) domain. Doing this deletes the domain configuration that was connected to the array.

If you want to switch from an LDAP configuration to an Active Directory configuration, you must first disconnect the LDAP domain.

Important: If you disconnect an array from an LDAP domain, all users from that domain lose access to the array.

Procedure

1. Go to**Administration** > **Security** > **Directory** > **LDAP**.
2. From the **More Actions** menu, select **Disconnect**.
3. Click **Confirm** in the warning box.

Switch Between Active Directory and LDAP Using the GUI

While you can have configurations set up for both Active Directory and Lightweight Directory Access Protocol (LDAP), you cannot use them both at the same time. To switch between these two services you must remove the current domain and then use the **Edit** menu option on the **More Actions** menu to change the type of service.

When you switch from Active Directory to LDAP or vice versa, all the users who belong to the domain that was being used will no longer be able to access the array unless they are in the new domain. For users who are already logged in to the array, any new operation will result in an error.

Even if a user is part of both domains, the login requirements might be different. For example, the username for an LDAP authorized user takes the format <*username*>@*domain_name*> where *domain_name* is the value you entered when you created the LDAP configuration.

Regardless of which service you are using, local account access is still permitted.

Procedure

1. Go to **Administration** > **Security** > **Directory**.
2. Select the currently in use directory service from the drop-down list.
3. When the configuration appears, select **More Actions**.
4. Select the correct action for your service and follow the prompts:
   - Active Directory: Select **Leave Domain**
   - LDAP: Select **Disconnect**
5. From the **More Actions** drop-down menu, select **Edit**.
6. In the **Type** field, select the directory service you want to use. You can now edit the configuration information.

   Follow the prompts to save your changes.

Common Active Directory and LDAP Tasks

There are several tasks you can perform that apply to both Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP).

Both services support the same array roles and rules for working with array groups.

Supported Array Roles

The array roles indicate the level of access permissions that group members have to perform particular tasks. Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP) support the following roles:

- Administrator: This role allows users to perform all actions.

- PowerUsers: A user can perform most actions. A user cannot perform user management tasks, set inactivity timeouts, or perform array setup.
- Operator. The user can perform most management operations. The user cannot delete or remove data.
- Guest. The user can view information and choose VMware subnets.

If the user belongs to a group that is not associated with any role or if the group is disabled, the user will not be able to log in to the array.

If a user belongs to multiple groups that have different roles, the group-role mapping that is used depends on whether Active Directory or LDAP is being used:

- Active Directory: The role with the fewest privileges is used.
- LDAP: The role with the highest privileges is used.

Note: You can check a user's role by running the **userauth --test_user** command from the array CLI.

When an array administrator makes a change to the group-based RBAC rules, users who are logging in will use the updated roles. Any users who are already logged in will receive the new privileges for subsequent operations.

Disable a Domain for Active Directory or LDAP

You can disable an Active Directory or Lightweight Directory Access Path (LDAP) domain at any point. When you disable it, the domain continues to exist, but it cannot be used.

Important: When domain authentication is disabled, users who belong to the domain can no longer access the array. For users who are already logged in to the array, any new operation results in an error. Local account access is still permitted.

Procedure

1. Go to **Administration** > **Security** > **Directory** > ***<your_service>***.
2. From the **More Actions** menu, select **Disable**.
3. Click **Confirm** in the warning box.

Enable a Domain for Active Directory or LDAP

By default, authentication is enabled after you join the domain. However, if you disable the domain for the service you are using, you must enable it in order to use it. This is true for both Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP).

If you make any changes on the Active Directory or LDAP server that are related to the domain configuration on the array, you might need to disable the service and re-enable it to clean up the cache.

Procedure

1. Go to **Administration** > **Security** > **Directory** > ***<your_service>***.
2. From the **More Actions** menu, select **Enable**.
3. Select **Test Connection** to ensure that the array is connected to the domain.

Test the Domain Connection

After you set up your configuration on the array, it is a good practice to confirm that the domain can connect to the server for that service (either Active Directory or LDAP).

Procedure

1. Go to **Administration** > **Security** > **Directory**.
2. Select your service from the drop-down list.
3. When the domain configuration appears, select **Test Connection**.

A pop-up box appears telling you that the array is successfully connected to the domain. If you do not get this message, there is a problem with the setup.

How Group Roles Apply to Active Directory, LDAP

To use either Active Directory or Lightweight Directory Access Protocol (LDAP), you must associate group names with array user roles. You can only assign one role to each group. The role can be:

- Administrator
- PowerUser
- Operator
- Guest

If a user belongs to a group that is not associated with a role or if the group is disabled, the user will not be able to log in to the array.

When a user belongs to multiple groups, the role mapping differs depending based on the service being used:

- Active Directory: The most restrictive role is used. This is the role with the fewest privileges.
- LDAP: The most permissive role is used. This role has the most permissions. Having the most permissions helps ensure backward compatibility.

When an administrator changes the role-based access control (RBAC) rules for a group, those revised roles apply the next time a user logs in. If a user is currently logged in, the revised roles apply the next the user performs an opersation.

Array Group Names

Active Directory and Lightweight Directory Access Protocol (LDAP) both allow you to set up a group with a name and then change that group name later.

If the group name is in a group mapping, you must create a group mapping that uses the new name and delete the old group mapping.

Note: If you are using Active Directory with a Windows server prior to Windows 2000, you cannot use special characters in group names. The system changes the special characters to underscores (_), which changes the group name. Also, you must log in to the array using the pre-Windows 2000 login name, which is shown on the Account tab of the Active Directory server user property page.

Add a Group to a Domain

Before you begin

You must already be a member of a domain to add a group.

Procedure

1. Go to **Administration** > **Security** > **Users and Groups**.
2. Click **+Group**.
3. Enter a group name.

   Note: The group name cannot be changed after the group is created.

4. Complete the remaining fields and click **Submit**.

Results

The page displaying the new group opens and shows all recent activity.

Remove an Active Directory or LDAP Group

When an Active Directory or Lightweight Directory Access Protocol (LDAP) group is removed from a domain, only the users from that group lose access to the array. Users from other groups in the domain continue to have access.

> **Note:** After a group is removed from the array, users can continue to log in to the group and perform actions for approximately five minutes. After five minutes, the user can no longer access the group.

Procedure

1. Go to **Administration** > **Security** > **Users and Groups**.
2. Select a group from the Users and Groups list.
3. Choose **More Actions** > **Remove**.
4. Click **Remove** in the Remove Group warning box.

Disable an Active Directory or LDAP Group

You can disable a group that is part of a Active Directory or Lightweight Directory Access Protocol (LDAP) domain.

> **Note:** If a group is disabled, users will not be able to log in to the Active Directory or LDAP domain.

Procedure

1. Go to **Administration** > **Security** > **Users and Groups**.
2. Select a group from the Users and Groups list.
3. In the Disable Group Access warning box, click **Disable**.

   A red icon appears next to the group name to indicate that it has been disabled.

Enable an Active Directory or LDAP Group

If a group in an Active Directory or Lightweight Directory Access Protocol (LDAP) configuration has been disabled, you can enable and make it available to users.

Procedure

1. Go to **Administration** > **Security** > **Users and Groups**.
2. Select a group from the Users and Groups list.
3. Choose **More Actions** > **Enable Access**.

Edit Active Directory Group or LDAP Information

You can edit a group in an Active Directory or Lightweight Directory Access Protocol (LDAP) configuration and change information such as the group role, the description, the inactivity timeout, and other elements of the configuration.

Procedure

1. Go to **Administration** > **Security** > **Users and Groups**.
2. Select a group from the Users and Groups list and click **Edit**.

CHAP Authentication

As the name implies, Challenge-Handshake Authentication Protocol (CHAP) uses a challenge-response mechanism to authenticate iSCSI initiators. A shared "secret," or password, let the system verify that the iSCSI initiator is who it claims to be and is authorized to access the volume.

Before you can use CHAP authentication, set up the CHAP secret on the volume and on the iSCSI initiator. CHAP secrets must be between 12 and 16 characters long. For the best security, the secret should be random letters and numbers, not a word that could be guessed. If your iSCSI initiator imposes further restrictions on the CHAP secret, you must adhere to these stricter regulations.

When creating a CHAP secret, adhere to the strictest regulations: 12-16 characters containing no spaces or the special characters (' " ` ). The CHAP user name should not contain characters such as : ~ ! @ # $ ^ & ( ) + [ ] {} * ; : ' " ., % | < > ? / \ = `.

Create a CHAP Account for Volume Scoped Target Volumes

CHAP (Challenge Handshake Authentication Protocol) users share a "secret." This CHAP secret is a word, phrase, or series of characters that both the array and the initiator know. The array will only allow access to those iSCSI initiators who respond with the correct secret.

Procedure

1. Go to **Manage** > **Data Access** > **CHAP Accounts**.
2. Click **+** to open the New CHAP Account dialog box.
3. Enter a name for the CHAP user.

   This is a convenient way to remember CHAP associations.
4. Enter the CHAP secret.

   CHAP secrets must be between 12 and 16 characters, can not contain [ ] & ; or `, and are case sensitive. This must also be made available to the iSCSI initiator. The GUI runs over a secure connection, so the password is protected.
5. Click **OK**.
6. Use your iSCSI initiator software to add the CHAP secret to the iSCSI initiator configuration. The method used to add the CHAP secret to the iSCSI initiator is based on your OS and iSCSI management tool.

Create a CHAP Account for Group Scoped Target Volumes

For Group Scoped Target (GST) Volumes, CHAP is configured at the initiator access level. Added initiators in the CHAP account will be used for GST volumes only. For more information about Group Scoped Target, see Group Scoped iSCSI Target on page 79.

Procedure

1. Go to **Manage** > **Data Access** > **CHAP Accounts**.
2. Click **+** to open the New CHAP Account dialog box.
3. Enter a name for the CHAP user.

   This is a convenient way to remember CHAP associations.
4. Enter the CHAP secret.

   CHAP secrets must be between 12 and 16 characters, can not contain [ ] & ; or `, and are case sensitive. This must also be made available to the iSCSI initiator. The GUI runs over a secure connection, so the password is protected.
5. Add Initiators from the IQN selection list.
6. Click **OK**.
7. Use your iSCSI initiator software to add the CHAP secret to the iSCSI initiator configuration. The method used to add the CHAP secret to the iSCSI initiator is based on your OS and iSCSI management tool.

Assign a CHAP User to a Volume

The CHAP user must be created before it can be assigned to a volume. Multiple volumes can be assigned to the same CHAP user.

Procedure

1. Assign a volume CHAP user access in one of two ways.
   - During the volume creation access is set in the initial wizard page's **Access Control** section.
   - After creation, edit the volume's Access selection. Modify the volume and select **Access** > **Add...**
2. Click **Limit access**.
3. Enable Authenticate using CHAP user name, then select the CHAP user to assign.
4. Click **Next** if you are creating a volume, or **OK** if you are editing a volume.

What to do next

After assigning a CHAP user to a volume, ensure that you provide the iSCSI initiator with the CHAP secret and CHAP user name.

Modify a CHAP User Account

For increased security, you may want to change the CHAP secret at regular intervals, or if you suspect that an unauthorized computer has accidentally gained access to the array.

> **Note:** If you change a CHAP secret, all volumes protected with this CHAP account will be inaccessible until the corresponding iSCSI connections are changed and synchronize with the new CHAP secret. Consider this when you determine what time to make these changes.

Procedure

1. Go to **Manage** > **Data Access** > **CHAP Accounts**.
2. Select the CHAP user whose CHAP secret you want to modify.
3. Click the pencil icon to edit the CHAP account. Enter the new CHAP secret.

   CHAP secrets must be between 12 and 16 characters, can not contain [ ] & ; or `, and are case sensitive.
4. Click **OK**.
5. Use your iSCSI initiator software to change the CHAP secret to the iSCSI initiator configuration. The method used to add the CHAP secret to the iSCSI initiator is based on your OS and iSCSI management tool.

Remove CHAP User Access Control From a Volume

Before you can delete a CHAP user, you must remove the CHAP user access control from any volumes that are using it.

To find the list of volumes protected by a particular CHAP account, click the number in the Associated Volumes column on the CHAP Accounts page. The Group page opens displaying the volume details.

Procedure

1. Go to **Manage** > **Data Storage** and select the volume that you want to edit.
2. Click **Edit** and click **Next** until you get to the **Access** section.
3. Edit the volume to either use a different access control or none.
4. Repeat this for each volume assigned to the CHAP user.

Delete a CHAP User

Delete CHAP users that are no longer needed.

Before you begin

Before you can delete a CHAP user, you must remove the CHAP user access control from any volumes that are using it.

Procedure

1. Go to **Manage** > **Data Access** > **CHAP Accounts**.
2. Select the CHAP user to delete.
3. Click **Delete**.
4. Click **Yes** to confirm that you want to delete the CHAP user.
5. Use your iSCSI initiator software to change the CHAP secret to the iSCSI initiator configuration. The method used to delete the CHAP secret to the iSCSI initiator is based on your OS and iSCSI management tool.

Login Banner

By default, a login banner displays in the GUI interface for all controllers in an array group. However, the banner can be configured to not be displayed (deleted). It can also be configured to be displayed either before prompting for user's credentials, or after user authentication. By default, the login banner is displayed after user authentication.

Important: You must have Administrator privileges to configure the login banner.

The login banner has a factory default login banner message, but the message can be edited to suit your specific requirements. The message is restricted to 2,048 ASCII printable characters with support for newline. International characters are not supported. (The official Department of Defense [DoD] banner character count is about 1,200 characters.) An edited banner message can be reset to the factory default message.

Edit the Login Banner

Before you begin
Ensure that you have Administrator priviledges.

Procedure

1. Choose **Administration** > **Customization** > **Login Banner**.
2. Check the **Enable Banner** check box to make the banner display during login.

   If the check box is unchecked, the login banner will not be displayed.
3. Do one of the following:
   - Edit the banner message to suit your requirements.
   - Click **Restore Factory Default** to overwrite the current banner message with the factory default message.
4. Check the **User Agreement** check box to make the login banner display before user authentication.

   If the check box is unchecked, the login banner is displayed after user authentication.
5. (Optional) Click **Preview** to see how the login banner will look when enabled.

   Click **Ok** to return to the login banner edit page.
6. Click **Save**.

Multihost Access

The array supports multihost access. When an initiator connects to a target, the access control records do not automatically prevent multiple initiators to connect. As long as the access control record limitations are met, the initiator can connect.

In some environments, you may need multiple initiators to access a target. These conditions include the following:

- A virtual server that manages multiple connections
- An environment in which initiators on the same computer do not use the same IQN

- An environment that uses a Distributed Lock Manager

Using MPIO

Note: Ensure that you have an active iSCSI connection before installing MPIO. Not having an active connection before installing MPIO causes the Add support for iSCSI devices feature to be unavailable.

Install an MPIO product on the system that is accessing the array. MPIO requires multiple network adapters dedicated to the iSCSI task. When connecting your iSCSI initiators, select Properties and click MPIO.

MPIO determines which paths to a device are in an active state and can be used for load balancing. The load balancing policy (Least Queue Depth is recommended by HPE) is set in the DSM. This policy determines how the I/O requests are actually routed.

MPIO for Windows

For information on installing and configuring MPIO on Windows, refer to the *Windows Integration Guide*. It was based on installing MPIO onto a Windows 2008 Server. MPIO is an optional component with Windows 2008 Server. The process is similar on a Windows 2003 server after obtaining the MPIO component.

MPIO for Linux

For information on installing and configuring MPIO on a Linux-based system, refer to the *Deployment Consideration for Linux on Fibre Channel* and *Deployment Considerations for Linux on iSCSI*.

Multitenancy

For Container Storage Providers (CSP) running on Kubernetes, the array supports multitenancy, where a single installation can serve multiple distinct tenants confined to folders.

Note: Multitenancy is only supported using the CSP via the REST API. To access this feature, you must use the HPE Container Storage Interface (CSI) Driver for Kubernetes. For more information, refer to the *HPE Storage Container Orchestrator Documentation*.

Array administrators can add or remove a tenant, edit a tenant's folders and password, and get information on all or a specific tenant.

Note: Group merge is not supported with the multitenancy feature.

This command is only available for the Administrator role. For more information, see tenantadmin in the *Command Reference*.

Secure SMTP

You can configure simple or secure Simple Mail Transfer Protocol (SMTP) to send alerts from groups to external servers. Alerts are identifiers about specific actions that occur on a group of arrays.

Prior to version 2.3, you could configure only a simple (or regular) SMTP relay of email alerts.

In version 2.3 and later, you can configure either a regular or a secure SMTP relay.

Configure Email Alerts

You can configure email alerts to use regular or secure Simple Mail Transfer Protocol (SMTP) processing, depending on which mode is appropriate for your environment.

You might choose to use regular SMTP for email alerts if you have an SMTP server installed on your network that accepts email messages from external parties. You might choose to use secure SMTP if you have an SMTP server installed on your network, but prefer to disallow anonymous relays, or if you do not have an internal email server because you implemented cloud-based email, such as Office 365.

You can configure email alerts differently for each group of arrays. You must have at least Power User permission to configure SMTP-based email alerts.

Procedure

1. Go to **Administration** > **Alerts and Monitoring** > **Email**.
2. For both regular and secure SMTP, specify values for the fields that are enabled by default.

Option	Description
'Send From' Address	Specify the email address used by the group to send email alerts. It does not have to be a valid email address, but it must have a valid email address format. Include the group name for easy identification and filtering.
'Send To' Addresses	Specify the email address of one or more administrators who should receive email alerts from the group of arrays. These addresses do have to be real email addresses. You do not need to specify an email address for the support team when you enable sending event data to support.
Send event data to Support	Retain or disable automatically sending event data to the support team. Event data includes the alerts sent to the specified 'Send To' email addresses. **Note:** SMTP is used as a backup for the default HTTP transport mode for event data.
Hostname or IP Address	Specify the hostname or IP address of an SMTP server that the group uses to send email alerts and event data.
SMTP Port	Specify the SMTP port number to use. Default: 25.

3. For **Authentication**, select the default value of No for regular SMTP or select Yes for secure SMTP.
4. For secure SMTP only, specify values for the fields that are enabled after you select Yes for the **Authentication** option.

Option	Description
Username	Specify the username for the SMTP account. The *Username* value must start with an alphabetic character and can be up to 64 alphanumeric characters. The following special characters are also valid, as long as a dot (period) is not the last character: + (plus sign) - (hyphen or dash) _ (underscore) . (period)
Password	Specify the password for the SMTP account. The *Password* value can be up to 255 printable characters. The password is not hashed.
Encryption	Retain the default of None or select the encryption type. Selecting any type other than None requires using username and password authentication. • None means that email alerts are unencrypted. • STARTTLS means that secure SMTP over transport layer security (TLS) is used. The STARTTLS encryption option can be an appropriate choice if you implemented cloud-based email. • SSL/TLS means that secure sockets layer (SSL) with transport layer security (TLS) is used. The SSL version is not subject to CVE-2014-3566, the POODLE vulnerability in SSLv3. The SSL/TLS encryption option can be an appropriate choice if you have a secure SMTP server installed on your network.

5. Click **Save** to save the configuration.

6. (Optional) Click **Test** to send a test message to verify the configuration and then click **OK** to acknowledge the successful message.

Encryption of Data at Rest

You can enable encryption at the group level or at the volume level as required for each group of arrays in your environment. Before you can create encrypted volumes, you must perform an initialization step that creates the master key. The master key protects the keys that are used to encrypt volume data. The master key is protected by a passphrase that is specified when creating the master key. At times, it will be necessary to enter the passphrase to enable access to encrypted volumes.

The encryption state of a volume is established when the volume is created, and cannot be changed afterward. Cloned volumes inherit the encryption state of their parent. The group configuration contains a default encryption default setting, where you can either enable or disable AES-256-XTS encryption. (The AES-256-XTS encryption algorithm is specifically designed for use in encrypting block storage.) The group configuration also contains an encryption scope setting, which specifies where and how to apply the encryption default setting. You can force the encryption default setting to be applied to all new volumes in the group, or allow overriding the encryption default setting on a per-volume basis.

The group configuration contains an encryption mode setting that defines behavior on system restarts. The value can be set to "secure" or "available." In secure mode, the encryption passphrase must be entered every time the group leader array is restarted to unlock the master key. In most cases, available mode stores enough information in non-volatile memory to recover the master key without entering the passphrase. The information is not stored on disk. Available mode is provided for convenience in situations where the physical security of the array is unlikely to be compromised.

Important: Even though available mode significantly reduces the number of times you must enter a passphrase when a group leader array restarts, it does not guarantee that you will never have to enter a passphrase after a restart. There are certain scenarios where you would still have to specify a passphrase while in available mode to access encrypted data, including:

- Controller upgrade: If array controllers are being upgraded to a newer model, you must enter a passphrase. While data is recovered from the non-volatile memory, access to encrypted volumes is not.
- NVRAM loss: In the rare case where non-volatile memory (NVRAM) is lost, you must enter a passphrase to access encrypted volumes. Older arrays (CS2xx and CS4xx series) that remain powered off for a long time could lose NVRAM as a result of battery discharge.

CAUTION:

- If you lose the passphrase for the master key or access to the external key manager, data in encrypted volumes cannot be retrieved. Store the passphrase in a secure, accessible place.
- If your encryption requirement changes after creating a volume, you cannot change its encryption status. You can create a new volume with the encryption status that you need, and migrate the data to the new volume.
- Performance might be slow when accessing encrypted volumes from the CS210 or CS215; however the performance impact due to encryption will be less severe on the CS235 arrays.

Enable Encryption

Beginning with version 6.0, you have the option of using a passphrase for local key management or using external key management for your encryption keys. The use of encryption involves using keys to encrypt volume data. Two important points to remember are the following:

- If you lose the passphrase for the master encryption key or access to the external key manager, data in the encrypted volumes cannot be retrieved.
- The encryption status of a volume cannot be changed.

To ensure that you are aware of the requirements for encrypting volumes, read the information in Encryption of Data at Rest on page 169.

Before you begin

You must have Administrator privileges to change the encryption configuration.

Procedure

1. Go to **Administration** > **Security** > **Encryption**.
2. Complete the fields as needed for your environment.

   Option **Description**

   Passphrase

   Here you have the option of entering a passphrase to enable encryption with local key management or setting up an external key manager. When initially enabling encryption, enter a passphrase value of any printable characters with a length between 8 and 64 characters, inclusive, and then confirm your entry. Printable characters are English-language alphanumeric characters, spaces, and special characters. Foreign-language characters are not supported. You can optionally select the option to show the characters as you type so that you can verify entering the same value in both fields.

   > **Note:** After you save the initial configuration, you can change the passphrase value by clicking the Modify Passphrase button. You must know the current value to modify the value.

   System Startup Mode

   Select whether administrators or operators must enter the passphrase for encrypted volumes when the array restarts.

   - Enabling Available mode does not require passphrase entry every time the group leader array restarts. (However, some rare scenarios may still require passphrase entry.) Available mode is useful in physically secured and lights-out data centers. Available mode is the default system startup mode.
   - Enabling Secure mode requires passphrase entry every time the group leader array restarts. Secure mode is useful if you move the array from one location to another or if the array is stolen. Because only authorized personnel know the passphrase, data is inaccessible without knowing the passphrase.

   Default Setting

   Select "Enable encryption on newly created volumes (Cipher: AES-256-XTS)" to enable encryption by default when authorized users create volumes. Deselect this option to create unencrypted volumes by default.

   Scope

   Select where and how to apply the encryption Default Setting.

   - Force the default setting to be applied to all new volumes in the group means that when authorized users create volumes, encryption is enabled or disabled based on whether encryption is enabled or disabled for the Default Setting. Users cannot override the Default Setting when creating volumes.
   - Allow overriding the default setting on a per-volume basis means that when authorized users create volumes, the Default Setting is applied, but it can be changed. For example, if you choose to enable encryption by default, then an authorized user can choose not to encrypt a new volume when creating it.

3. When prompted to save your passphrase in a secure place, read the message and click **I accept** to acknowledge that you understand the ramifications of a lost passphrase and to save the encryption settings.

   Do not forget your passphrase. Lost passphrases cannot be retrieved and will result in permanent loss of data.

What to do next

Based on your selections for Default Setting and Scope, volumes that authorized users create after enabling encryption are either automatically encrypted or can be encrypted on a case-by-case basis.

> **Note:** Volumes that were created in versions earlier than version 2.3.x are not encrypted and cannot be edited to be encrypted. The encryption state specified when creating a volume cannot be changed for the life of that volume.

External Key Manager Support

An External Key Manager is a third-party server on which encryption keys are stored. With External Key Manager support, the array can store the master key in an external server. Volume, clone, replication, backup or copy keys remain local to that array. They are unlocked with the Master Key, which is obtained from the External Key Manager.

The Key Management Interoperability Protocol (KMIP) is a communication protocol that defines message formats used to manipulate cryptographic keys on a key management server. This facilitates data encryption by simplifying encryption key management. KMIP uses the Cryptsoft library, which provides interoperability with all major key management servers. More information is available at Cryptsoft (https://www.cryptsoft.com/).

Certificate-based mutual authentication is used between arrays and the KMIP Server. When an external Key Manager is configured on the array, encryption is enabled. If a Key Manager is deleted from the array, encryption remains active on it.

Setting Up An External Key Manager

Before you begin

This is the procedure for setting up the external key manager on the array group. To add the array group as a client, see the external key manager documentation.

Procedure

1. Go to **Administration** > **Security** > **Encryption**.
2. Click **External Key Manager**, and then click **Add Key Manager**.
3. Complete the fields as needed for your environment.

Option	Description
Name	The human-friendly name of the External Key Manager.
Description	Additional context.
Hostname or IP Address	The Hostname or IP of the External Key Manager.
Port	The number of the port over which the External Key Manager and the Array communicate. **Note:** Ensure that the array can access the External Key Manager with the provided Hostname or IP on the specified port. The default TCP port for KMIP is 5696.
Protocol	The KMIP protocol used by the External Key Manager. This allows you to select the version, such as 1.0, 1.1, 1.2, or 1.3, of the KMIP protocol used by the External Key Manager.
Username / Password	The credentials necessary to access the External Key Manager.

Results

After you have added the new External Key Manager, on startup, the array by way of GMD requests the Master Encryption Key from the External Key Manager. If mutual authentication is successful, the array receives the Master Encryption Key and the remaining keys that are used to unlock the volumes, clones, and replications.

Secure Sockets Layer Certificates

To establish a secure connection with a website or other server, the server presents a certificate to authenticate its identity. Certificates are an important component of Secure Sockets Layer (SSL) because they prevent others from impersonating a secure website or server.

The following types of certificates are supported:.

- **Array certificate chain:** Generated when the array is first started.
- **Group certificate chain:** Generated when the array is configured as a group leader.
- **Custom certificate chain:** (SSL Certificate) Either a self-signed certificate or a certificate generated by exporting the Certificate Signing Request (CSR) and then signing and importing the root certificate authority (CA) and signed certificates. This is the most secure type of certificate.

An SSL certificate is an electronic document that verifies ownership of a public key and ensures the identity of your server, which provides greater security of online interactions. The certificate includes the following information:

- Information about the key
- The identity of its owner

The digital signature verifies that a trusted third party (the CA) has authenticated the identity of the organization that owns the key and has verified that the contents of the certificate are correct.

If the signature is valid, and the person examining the certificate trusts the signer, then they know that it is safe to use that key to communicate with its owner.

To get an SSL certificate, you must create a Certificate Signing Request (CSR). Then, you send the CSR data file to the CA and the response that you receive from the CA is your SSL certificate. This SSL certificate is the intermediate chain public key and you import the key through the GUI or CLI.

After you receive the certificate and install it on your server, the identity of your server can be authenticated.

You can also import a trusted certificate.

Create and Import a Custom Certificate or Certificate Signing Request

You can use the GUI to generate a self-signed certificate or a certificate signing request (CSR). You can then import a certificate authority (CA) signed custom certificate.

> **Note:** If you already have a custom certificate and you add another one, the add operation becomes a replace operation and replaces your current custom certificate.

Procedure

1. From the GUI, select **Administration** > **Security** > **SSL Certificate**.
2. From the SSL Certificates and Signing Request page, click the plus (+) icon to add a certificate.
3. Under Certificate Actions, use the drop-down list to select the operation you want to perform.

   The list provides you with the following options:

   1 Generate a self-signed custom certificate
   2 Generate a certificate signing request (CSR)
   3 Install a CA (certificate authority) signed certificate
   4 Import a trusted certificate
   5 Install a custom PKCS12 bundle.

   > **Note:** The array supports only RSA certificates. If your PKCS12 bundle does not contain an RSA private key, generate a new PKCS#12 file using an RSA private key.

4. Enter the required information.

   For the first two options in the Step 3 list, you can provide the following:

   - The certificate information including the number of days the certificate will be valid
   - The FQDN list
   - The IP address

   Note: If you do not specify values for these fields, then the default values are used to generate the CSR or self-signed custom certificate.

   For the third option, You must paste in the CA Certificate chain and the signed certificate. Use PEM format for this information.

   For the fourth option, enter the name of the certificate and check the button that specifies the method you want to use to provide the certificate chain.

   For the last option, use the Choose File browse option to locate the PKCS12 bundle. You can enter a password; however, you can create a bundle without a password and import it. For security purposes, it is a good practice to always create the bundle with a password.

   Note: The file that you upload must contain the entire certificate chain. If it does not, an error occurs.

5. Select Save.

Delete Certificates

You can delete custom certificates and trusted certificates. When you delete one of these certificates, the system also removes any custom-ca or custom-csr. However, deleting the custom-ca does not remove the custom certificate. If there is a valid custom certificate signed by the CA, then the custom-ca cannot be deleted.

Note: The array and group certificates are generated by the system and cannot be deleted.

Procedure

1. From the GUI, select **Administration** > **Security** > **SSL Certificate**.
2. Select the custom certificate or the custom-ca or custom-csr that you want to delete.
3. Select the delete (x) icon. The system asks you to confirm that you want to delete the certificate.

   You can only delete one certificate at a time. If you select multiple certificates, the delete (x) icon is grayed out.

   If you are attempting to delete a custom-ca that is being used by a custom certificate, the operation will fail.

4. Select Remove.

Monitoring Your Arrays

An array runs well after it is installed and configured. It normally requires only minimum maintenance. It is a good idea, though, to monitor the system regularly to make sure that everything is working as expected.

You can choose options from the GUI **Monitor** menu to monitor the array in real time. You can track system trends and proactively ensure that no bottlenecks occur. The intuitive monitoring system lets you see space usage and performance at a glance.

In addition to monitoring your array, you can monitor certain host features. The GUI **Monitor** menu also includes a **Hosts** section, where you can find information about Cross-Stack Analytics for Hyper-V and Host Diagnostics.

Several array monitoring options use common controls. When you monitor capacity, performance, interfaces, connections, the audit log, or replication, you can specify the time interval of interest to you:

- **Real-time**, which is useful for monitoring real-time activity
- Last 3 minutes (**3M**), which is useful for monitoring very recent activity
- Last 60 minutes (**1H**), which is useful to determine whether an activity is a temporary or recurring condition
- Last 24 hours (**1D**), which is useful for tracking activity patterns for the day
- Last 7 days (**1W**), which is useful for tracking activity patterns for the week
- Last 30 days (**1M**), which is useful for tracking activity patterns for the month
- Custom, which lets you specify a time interval of interest

The selected interval determines how much data is shown. The longer the time interval, the more compressed the data appears in the graph. Use longer time intervals for tracking trends that you can use for purchasing estimates and capital expense projections.

When you monitor **Capacity** or **Performance**, you can also select one or all volumes to include in the data collection. By default, all volumes are included. However, you can limit the display to a specific volume.

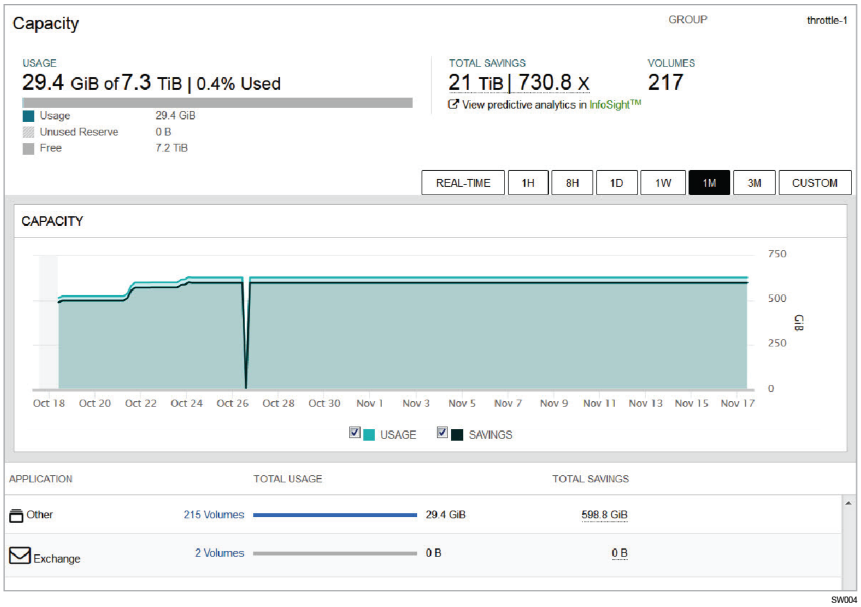
The other monitoring options do not have the **Real-Time** and **Volume** common controls. Those pages provide other ways to track activity patterns.

Monitor Capacity

When you monitor capacity for a group or a pool, you can see the number of volumes, the data usage (for both volumes and snapshots), the unused reserve, the free space and the size. If you can hover over the total savings, you can see a breakdown of the savings achieved through thin provisioning and data reduction techniques like compression, cloning and deduplication.

When you monitor space for a folder, you can see the total usage of the folder and its distribution into volume usage, snapshot usage and unused reserve. If the folder has a limit, you will see the limit as well as the volume count.

When you monitor space for a volume, you can see the volume usage, unused reserve, free space, and size. It also shows you the space used by snapshots of this volume and the total usage of the volume.



Capacity

GROUP throttle-1

USAGE
29.4 GiB of 7.3 TiB | 0.4% Used

Usage	29.4 GiB
Unused Reserve	0 B
Free	7.2 TiB

TOTAL SAVINGS
21 TiB | 730.8 X
View predictive analytics in InfoSight™

VOLUMES
217

APPLICATION		TOTAL USAGE		TOTAL SAVINGS
Other	215 Volumes		29.4 GiB	598.8 GiB
Exchange	2 Volumes		0 B	0 B

SW004

Procedure

1. Go to **Monitor** > **Capacity**.

   > **Note:** In the GUI, information is refreshed automatically every minute. Therefore, the space usage that is reported can be up to one minute out of date.

2. Select one of the following time intervals:
   - Real time
   - One of the predefined time intervals
   - Custom interval

   a) If you selected **Real Time**, you can click **Pause** to stop real-time updates and freeze the data on screen.
   b) Click **Resume** to continue tracking space usage.

3. Enter the name of the volume that you want to monitor in the **Filter by Volume** field.
4. Select the name of the volume you want to monitor from the popup list.

   When you monitor specific volumes, you can track whether one application uses more or less space than expected. This information can help you decide whether to make schedule modifications for a volume collection to improve efficiency in how the space is used. For example, you may find that you need to take fewer snapshots for a volume, freeing up the space for other applications.

Monitor Performance

You can monitor the performance levels of all volumes on an array or a specific volume.

Procedure

1. Go to **Monitor** > **Performance**.
2. Select one of the following time intervals:
   - Real time
   - One of the predefined time intervals
   - Custom interval

a) If you selected **Real Time**, you can click **Pause** to stop real-time updates and freeze the data on screen.
b) Click **Resume** to continue tracking space usage.

3. Enter the name of the volume that you want to monitor in the **Filter by Volume** field.
4. Select the name of the volume you want to monitor from the popup list.
   The following data appears:

   - Latency, which displays the average time that the array takes to internally complete read and write requests
   - IOPS (input/output requests per second), which are a measure of performance and display how many requests per second the array handles
   - MiB/s, which displays the number of mebibytes per second that is being successfully delivered by the array
   - Cache hit rate for random reads, which displays the percentage of read requests that have been received and served by the flash cache

     When the application tries to access data, it first checks the cache. If the data is already in the cache, the data is then displayed. Otherwise the array attempts to access the data from the disk drive. This process is known as a *cache hit*.

Monitor Interfaces

You can monitor throughput for interfaces to determine whether traffic is balanced appropriately. As you move over the graphs, informational boxes pop up indicating the I/Os for each interface.

Procedure

Monitor interface traffic.

1. Go to **Monitor** > **Interfaces**.
2. Select one of the following time intervals:

   - Real time
   - One of the predefined time intervals
   - Custom interval

   a) If you selected **Real Time**, you can click **Pause** to stop real-time updates and freeze the data on screen.
   b) Click **Resume** to continue tracking space usage.

Monitor Replication

You can monitor the lag time of replications when sending data to a partner or receiving data from a partner.

Procedure

1. Go to **Monitor** > **Replication**.
2. Select a specific replication partner or all replication partners from the **Replication Partner** dropdown list.
3. Select one of the following time intervals:

   - Real time
   - One of the predefined time intervals
   - Custom interval

   a) If you selected **Real Time**, you can click **Pause** to stop real-time updates and freeze the data on screen.
   b) Click **Resume** to continue tracking space usage.

Results

The upper part of the page provides information about the replication throughput while sending or receiving data. If you are monitoring data the selected array is sending, the lower part of the page provides the following information for lagging replications:

- Volume Collection, which identifies the volume collections
- Time Lag, which displays an estimated amount of time that the replication is lagging
- Data Remaining, which specifies the amount of data that still needs to be sent
- Last Recovery Point, which identifies the time of the last completed replication

Monitor Data Migration

The Data Migration page only shows data migration between arrays, when you add or remove an array to or from a pool.

Before you begin

You must have more than one array in your system.

Procedure

Go to **Monitor** > **Data Migration**.

The Data Migration page is not visible if there is no data migration in progress.

Global Search

You can look for global-search objects by name from anywhere in the GUI. The header in the GUI has a **Search by Name** field so that you can search for objects of interest from anywhere in the GUI. The global-search object types include volumes, volume collections, pools, arrays, initiator groups, CHAP accounts, users, protection templates,performance policies, and replication partners.

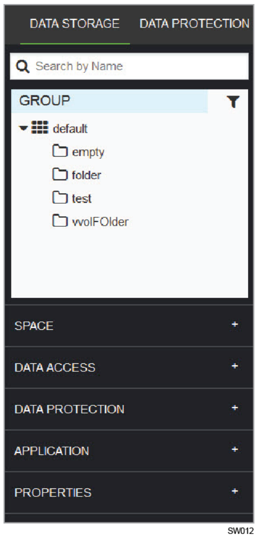
> **Note:** Initiators, snapshots, snapshot collections, and protection schedules are not global-search object types. Initiators are listed for an initiator group. Snapshots, snapshot collections, and protection schedules are listed either for a volume or for a volume collection.

Results from a global search include only the object types that your role lets you access. For example, if you log in as a user with Guest permission, your search results do not include CHAP accounts. However, if you log in as a user with Operator, Power User, or Administrator permission, your search results do include CHAP Accounts. Only users with Administrator permission see users in their search results.

Search for Objects

You can use global search from anywhere in the GUI to find objects of interest. The global-search object types include volumes, volume collections, pools, arrays, initiator groups, CHAP accounts, users, protection templates, performance policies, and replication partners. Object types are sometimes called object sets.

Search for users by entering some or all of their user name or their full name. The *user name* is sometimes called the account name or the login name. Search for other global-search object types by entering some or all of their name.



Procedure

1. Start typing characters in the **Search by Name** field in the top right corner of the dashboard.
   The system filters objects that have the specified characters in their name and that are appropriate for your permission level. The search results are grouped by object type and displayed in alphabetic order within each object type. The query string is highlighted in the object name.

   > **Note:** As you type more characters in the **Search by Name** field, the search results typically decrease because fewer objects match the search query. If you make a typing error, you might see a message that there are No items to show. Press the backspace key on your keyboard to remove the last characters you typed, or click the x to the right of the text entry field to remove all characters so that you can start over.

2. Select an object name in the list of search results, or click **View Details**, **View All**, or **View All Arrays** at the bottom of a category of search results.

   - Select an object name to open the detail page for that object so that you can view details about the object or edit the object in some way.
   - Click **View Details** to open the object-type summary page with only objects that match the search query visible. This link appears when two, three, or four objects of the object type match the search query.
   - Click **View All** to open the object-type summary page with only objects that match the search query visible. This link appears when five or more objects of that object type match the search query.

     When you click either of the View links, you can select whichever object name is of interest on the filtered list page to open the detail page for that object.

   - Click **View All Arrays** in a multi-array group to open the array management page with all arrays in the group visible. The list on the array management page is not filtered to match the search query.

Filter Objects

Several summary pages in the GUI provide filter fields and search capability so that you can find specific objects you need quickly. Over time, arrays can accumulate a large number of volumes, snapshots, events, and audit log entries. To make it easier to find specific objects of interest, you can filter the objects that appear.

> **Note:** The filtering capability described here is sometimes called *faceted browsing*, faceted searching, or faceted navigation.

Procedure

1. Open the summary page of interest.
   For example, choose **Manage** > **Data Protection** to open the Volumes Collections summary page. Or click **Events** to open the Events summary page.
2. In the bottom left corner of the summary page, check to see how many objects exist.
   The legend identifies that the page is Displaying 1 - N of X, where N is the number of objects on the current page and X is the total number of objects of the selected type. If all objects fit on a single page, then N and X are the same value. If you resize the window, then the value of N changes, but X stays the same.
3. (Optional) If the filter fields do not appear, you can expand them with the plus and minus signs (+, -).
4. In the filter fields to the left of the summary list, select filter criteria in appropriate fields for the object type.
   Or, if you know any part of the object name or activity type, start typing characters in the **Search by Description** field. A Search field is not available for all object types. For example, the Events summary page has filter fields, but no search capability.
5. If the filtered results are not what you expect to see, clear the previously selected filter criteria and specify new criteria.
6. (Optional) From the filtered list of objects on the summary page, click an object name to open the corresponding detail page.

Syslog

Syslog is a standard for computer message logging. It is supported on a variety of devices and platforms, and is used to store management, security, informational, debugging, and other types of messages about these devices.

The syslog stores important information such as records of administrator manipulation of the storage array, and a history of alerts or issues with the array. Using syslog, system log files can be shipped from an array group to a centralized, remote server. The benefits of this include:

- Cost savings - system log files can be archived on inexpensive media rather than on the array.
- Ease of use - a central repository consolidates data from multiple arrays into one area, so it is not necessary to log into every array to get the data.
- Data analytics - it's easier to examine logs for troubleshooting, security, and health-related issues if they are on a central device.

With syslog enabled, arrays can communicate with third party monitoring tools without the need of custom code because it uses the standard syslog protocol.

Arrays support the Red Hat Enterprise Server and Splunk implementations of syslog. UDP is used to communicate between the array group and the syslog server (SSL is not supported at this time). One syslog message is generated for each alert and audit log message. Alert severity types include INFO, WARN and ERROR.

Enable Syslog

Note: To enable syslog you must have Power User privileges or higher.

Procedure

1. Log into the array.
2. Go to **Administration** > **Alerts and Monitoring** > **Syslog**.
3. Check the **Enable Syslog Server** checkbox to enable the **Syslog Server** and **Port** fields.
4. In the **Syslog Server** field, enter a valid host name or IP address of the syslog server you will use.
   No check is performed to determine whether the host name exists or the IP address exists or is valid.
5. In the **Port** field, enter the number of the UDP port used to communicate with the server.
   The port must be a valid integer [0-65535]. Unsupported and invalid ports within this range will not be validated.
6. Click **Save**.

The value for the port is validated.

- If there is an error in validation, a tooltip message is displayed showing the error.
- If there is no error, the settings are saved. Syslog is now enabled for this array, using the server and port you specified.

Disable Syslog

Note: To disable syslog you must have Power User privileges or higher.

Procedure

1. Log into the array.
2. Go to **Administration** > **Alerts & Monitoring** > **Syslog**.
3. Uncheck the **Enable Syslog Server** checkbox.
   The **Syslog Server** and **Port** fields are disabled.
4. Click **Save**.
   Syslog is now disabled for this array.

   Note: When the **Enable Syslog Server** checkbox is disabled, the fields are not cleared. Any values in the **Syslog Server** or **Port** fields will remain visible.

Audit Log Management

The audit log keeps records of all user-initiated non-read operations performed on the array, and which user performed the operation. You can search the audit log by activity and object type, name or both. You can also filter the audit log by time range, username, activity category, and access type. Administrators can view the audit log in a summary table with faceted browsing by time, activity category, and across access type.

Audit logging has changed from version 2.2.3.0, including which operations are audited, and syslog message format. Operations are not audited on non-group leader arrays, or on the standby controller of the group leader array, to which only the root user has access. In addition, console logout is not audited. Operations cannot be logged before the group is set up, which is when audit logging begins.

Audit logs, along with alerts, are posted to a syslog server if one is configured, using the following format:

Jan 22 17:51:01 sjc-b11-va-B NMBL: Group:group-sjc-b11-va Type:2001 Time:Thu Jan 22 17:51:01 2015#012 Id:275 Object Id:- Object:vol-10 Access Type:pam Client IP:10.20.20.248 Status:Succeeded

Audit log messages are not sent through emails, SNMP traps, or to InfoSight in real time. However, error messages for failed operations are converted to HTTP-like errors.

Audit logs are merged during a group merge, beginning with the users. Users from the source group are remapped to new users in the destination group. After the users are merged, the audit logs are merged.

The audit log is automatically purged. When the count reaches 21,000, an alert is sent warning that a purge will occur when the count reaches 24,000. At 24,000 messages, the oldest 5000 messages are purged (the most recent 19,000 log entries are kept).

Audit Log Panel

Users with the Administrator role can access the audit log page by selecting **Monitor** > **Audit Log**.

The main audit log page has two panels - a summary table panel on the right that provides a list of audit log records, and a collapsible facets panel on the left used to narrow down audit log records in the table. When the panel is collapsed, any facet settings remain in effect.

Facets Panel

The facets panel provides four ways to filter content:

- Search by activity or object - Enter words (case insensitive) to search by activity or object. The log table list changes depending on the words you enter. You will not be able to search on deleted users, root users, or system users.
- Date Range - Select from a dropdown list of common time intervals (All, Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, and Custom...). The default value is *All*. *Last* means last from the current time. Selecting the Start Time and End Time fields under Custom Displays allows you to specify a date and time range. Any values you enter remain in effect when *All* or *Last* is selected. Audit log records are filtered whenever you make a selection from the dropdown list or enter a valid start and end date after selecting Custom.
- Activity Category - Check up to six checkboxes (Data Provisioning, Data Protection, Data Access, User Access, System Configuration, Software Update) to filter the log table list by type of activity audited. Audit log records are filtered when a checkbox is checked or unchecked.
- Access Type - Check up to three checkboxes (API, CLI, GUI) to filter the log table list by type of access audited. Audit log records are filtered when a checkbox is checked or unchecked.

Summary Table

The summary table has six columns which can be used to sort or filter the data:

- Time - Provides sorting and filtering of when activities take place. The Time filter is the same as the one provided in the facets panel.
- Activity - Provides filtering of user actions. You can use the Activity filter to further refine what you have selected in the facets panel.
- Status - Provides sorting of operation status icons (successful, in process, or failed). Hovering the mouse over a failed status icon displays a tooltip describing the cause of the failure.
- User - Provides sorting of full names of registered users. Clicking the hyperlinked username brings up the user details page.
- Client IP Address - Provides sorting of the IP addresses where the activity was invoked.
- Access Type - Provides sorting and filtering of access methods (API, CLI, GUI). The Access Type filter is the same as the on provided in the facets panel.

The summary table is refreshed whenever you change the facet panel settings. You can also refresh the table by clicking the refresh icon in the upper right corner of the panel. The table does not refresh automatically.

Note: System users (such as VSS agent) are shown as *<system>* in the username column and *System* in the User Full Name column. User information can be empty if the authentication failed (for example, from an expired session).

User Management

Users with the Administrator role can access the Manage Users page by selecting **Administration** > **Security** > **Manage Users**. This page shows an audit log summary table for the selected user. All user's activities are displayed. To show new user activity, reload the table or reselect the user.

For other tasks you can perform from this page, see Role-Based Access Control on page 143.

Hosts

The GUI **Hosts** section, which is included in the **Monitor** menu, allows you to collect information about hosts. The section provides you with the following options:

- Hyper-V Analytics. From this tab you can display configuration and statistical data about Hyper-V hosts on which you have installed Cross-Stack Analytics for Hyper-V (previously referred to as Stackvision). This is an HPE feature that enables you to collect telemetry data from Hyper-V based virtualized infrastructures and analyze the data in the HPE InfoSight portal.

- Host Diagnostics. From this tab you can gather diagnostic information about the Windows hosts associated with the array and send it to support if you encounter a problem with the array. The Host Diagnostics feature is included as an option with HPE Storage Toolkit for Windows, starting with NWT 7.1.0.

Monitor Host Administrative Data Using Cross-Stack Analytics for Hyper-V

The GUI lets you view the data provided by Cross-Stack Analytics for Hyper-V (previously referred to as Stackvision) as well as perform an on-demand collection of the data.

Cross-Stack Analytics for Hyper-V collects telemetry data from Hyper-V based virtualized infrastructures and analyzes the data in the HPE InfoSight portal. InfoSight includes a powerful data analytics platform that enables you to:

- Analyze your Hyper-V virtual environment along with your environment
- Collect configuration information, performance metrics, and logged data from hosts, hypervisors and applications
- View and analyze telemetry data as part of the data collection packages that are sent from the arrays

The virtualized infrastructure performance data that is sent to InfoSight is correlated and displayed in an easy-to-understand visualization that enables you to quickly analyze potential issues.

Before you can enable Hyper-V analytics, you must download and install the HPE InfoSight Hyper-V Collector Toolkit. Then you must register your Hyper-V hosts and your array with the Collector Toolkit agent. For instructions on how to perform these steps, refer to *Getting Started with Cross-Stack Analytics for Hyper-V*, which is available on the InfoSight documentation portal.

After you have installed the HPE InfoSight Hyper-V Collector Toolkit and registered your Hyper-V hosts and your array, you can display the following collected configuration and statistical data on your array:

- The name of the Hyper-V host machine being monitored

  Note: This is the Hyper-V host on which the Hyper-V Collector is installed.

- The IP address of the host machine
- Whether the data collector is enabled
- The date when the host machine was last polled for configuration information
- The date when the host machine was last polled for statistics

Data collection is performed automatically; however, you can elect to collect data on demand. With automatic data collection, data is collected at the following frequency:

- Statistical data is collected every 20 seconds at the host and sent to the array every 10 minutes.
- Configuration data is collected every 30 minutes at the host and sent to the array every 24 hours.

To collect data on demand, perform the following steps:

1. Go to **Monitor** > **Hosts** > **Hyper-V Analytics**.
2. Click the name of a Hyper-V host machine in the Hyper-V Analytics window. The Agent Details window appears, in which you can view information about a specific host machine.

From the Agent Details window, you can poll for configuration and statistical data on demand by clicking on a collection button.

- Click the **COLLECT CONFIG** button to collect configuration information.
- Click the **COLLECT STATS** button to collect statistical information.

The Agent Details window provides polling status data about specific Hyper-V machines, which includes the following information:

- NAME
- HOSTNAME
- LAST STATUS POLL (by date)
- LAST STATUS POLL STATUS (including whether or not a connection was successful)
- LAST STATISTICS POLL (by date)
- LAST STATISTICS POLL STATUS (including whether or not a connection was successful)

Gather Host Diagnostics Information

When you select **Monitor** > **Hosts** > **Host Diagnostics** from the GUI, you can gather log information from the Windows hosts that have been registered with a group on the array and send that information to support. Support can use this information in connection with the information provided by DNA about the array to resolve possible issues. You must have Power User or above privileges to run Host Diagnostics.

Note: For information about DNA, see HPE Storage Diagnostics for Analytics on page 189.

The **Host Diagnostics** tab displays all the Windows hosts that have been registered with a group. You must use Host Diagnostics or Host Diagnostics Registration Tool to register the hosts.

Note: Host Diagnostics is a feature provided by the HPE Storage Toolkit for Windows 7.1.0 and later. At this time, Host Diagnostics supports only Windows hosts. Details about installing and using Host Diagnostics are provided in the *Windows Integration Guide*, which is available on the Documentation Portal on HPE InfoSight

To use the GUI to collect logs, you must be logged on with Power User or higher credentials. In addition, you must have enabled DNA for the array.

From the Host Diagnostics tab, you can select up to ten hosts and click the **Collect Logs** button to gather their log files. You get an error if you select more than ten hosts. Host Diagnostics can run log collections for four hosts concurrently and have six hosts in the queue.

The display refreshes every 15 seconds so you can monitor the operations.

When the log collection completes successfully, you can select the host and view its details page. Host Diagnostics provides the following Collection Details:

- **Collection Time** provides the start time for the collection operation.
- **Collection Status** provides information about whether the collection operation has finished.
- **DNA Time** is the timestamp on the log bundle. You must provide this information to Support. The DNA Time uses the format year-month-day hour-minutes-seconds array-timezone. For example, if the array is located in the Eastern Daylight Timezone, you might see the following value for DNA Time:

```
2020-9-25 21:53:15 0000 EDT
```

Host Diagnostics automatically places the log bundle ono the InfoSight share drive where Support can get it. You must send Support the DNA timestamp. Support uses that to locate the log bundle.

Disaster Recovery

For disaster recovery, you must have at least one additional array that is configured as a replication partner. Replication partners can serve data to the original initiators while the original array is inaccessible. By including multiple arrays in your network, you can quickly restore access to data even in case of a catastrophic failure.

In the unusual event of a complete failure of the array, set the replication partner online and point your initiators to the volumes on the replication partner. Your volume data is available to applications during the recovery of the data to the failed array.

There are two methods to move operations from one volume collection to its replication partner; the handover method and the promotion and demotion method. If the original array is accessible, handover is always preferred.

Note: You cannot use the promotion and demotion method with synchronous replication.

In case of a complete failure, within the Site Recovery Manager (SRM) the "failback" procedure is to delete the failed VM from vCenter, then replicate the backed-up LUNs to a new VM.

Important: Follow the procedures in this section to perform disaster recovery using the array only. For information on disaster recovery in HPE Cloud Volumes, refer to the HPE CV portal documentation.

Handover Overview

A *handover* is a controlled way to migrate all volumes associated with a particular volume collection to a replication partner without any loss of data. The new owner must be a downstream replication partner for replicas based on this volume collection.

Note: To use handover, the replication partners must be active and functional.

A handover instructs a downstream replication partner to become the upstream replication partner and provide the initiators access to volumes. It allows that replication partner to take ownership of a volume collection. Handovers to HPE Cloud volume partners are not supported.

Note: If the schedules for the volume collection use multiple partners, performing a handover will halt the schedules for the other downstream replication partner. These schedules will resume if you perform a handover back to the original upstream array.

When you perform a handover, the system displays a confirmation prompt. You can set up a CLI command to prevent the prompt from appearing. See the **volcoll** command in the *Command Reference* for more information.

The results of handing over a volume collection are:

- The volumes associated with the volume collection on this array are set offline.
- For snapshot replication only: Snapshots of the associated volumes are taken.
- For snapshot replication only: The snapshots are replicated to the downstream replication partner.
- Volume collection ownership is transferred to the replication partner.
- The volumes associated with the volume collection on the replication partner are set online.
- Schedules that apply to the other downstream partner halt.

By default, the direction of replication is automatically reversed. That is, when the downstream group becomes the owner of the volume collection, the upstream group becomes its replication partner.

Note: A handover with synchronously replicated volume collections is transparent to the hosts and does not involve any downtime or host reconfiguration.

Perform a Volume Collection Handover

As part of your disaster recovery strategy, you can perform a handover operation with volume collections that use snapshot replication and synchronous replication.

With synchronous replication, you can hand over an in-sync volume collection. For out-of-sync volume collections, you must unconfigure synchronous replication to gain access to the downstream volumes or wait for the volume collections to complete synchronization and move in-sync.

Before you begin

You must have a remote schedule configured for the volume collection that you want to hand over.

Procedure

1. Shut down any application that uses any of the volumes associated with the volume collection you are going to hand over.
2. Go to **Manage** > **Data Protection** > **Volume Collections**.
3. Click the name of the volume collection to hand over.
4. In the detail page for the selected volume collection, click **Actions** > **Handover**.
5. If the volume collection uses multiple downstream partners, the system displays a warning message listing the partners and telling you that the operation will break replication to the other partner. Enter **Yes** to continue the handover operation..
6. Choose the replication partner group as the New Volume Collection Owner from the drop-down menu.

   Note: The amount of time it takes for a handover to complete can vary depending on the load and the data volume.

7. If you do not want to reverse the direction of replication, uncheck **Automatically reverse the direction of replication**.
8. Click **OK** to begin the handover process.
9. Refresh the browser page and verify that the direction for the volume collection is now labeled Replica.
10. Under Schedule, verify that the **Owned by** and **Replicate to** fields have reversed partner names.

    - The volume collection ownership is transferred to the specified downstream partner.
    - The volumes associated with the volume collection on the upstream array are now in a standby state.
    - The volumes associated with the volume collection on the downstream array are now in an active state and are serving I/O.
    - The direction of replication is reversed if you selected that option.
    - If the schedule set for that volume collection includes multiple downstream replication partners, the schedules for the other downstream partner are halted.
    - With synchronous replication, the snapshot retention limits remain with each pool during a handover.

What to do next

After you perform a handover, you have the option of restoring the group leader and backup group leader to their original states by performing a group leader migration. See the *CLI Administration Guide* for information about performing a group migration.

Make a Replica Available to Applications

Before you begin

The original volume must be offline, whether due to disaster or as part of a planned outage. If this is a planned outage, perform a replication immediately prior to failing over the original array.

Procedure

1. Disconnect any iSCSI initiators from the offline volume.
2. Log into the replication partner and bring the volume online.
3. Connect the iSCSI initiators to the volumes on the replication partner as described in *Connecting iSCSI initiators to volumes*.

Promote a Volume Collection

If you are using snapshot replication, you can use the promote procedure to have a downstream replication partner take ownership of the volume collection. The volumes that are associated with the volume collection are set to online, so they are available for reading and writing. All the ACLs from the upstream partner are moved to the downstream partner that you are promoting.

It is best to only use this procedure when the upstream array is not available.

If the volume collection uses multiple downstream replication partners, performing a promote halts all replication to the group that is being promoted. It does not affect replication to the other partner.

Note: The promote procedure only works with snapshot replicated volume collections. You cannot promote a synchronously replicated volume collection.

Procedure

1. Go to **Manage** > **Data Protection**.
2. Select the volume collection that you want to promote.
3. Click the ellipsis icon (...) and then **Promote**.
4. Click **OK**.

What to do next

- Point your iSCSI initiators to the newly promoted volumes (members of the volume collection).
- (Optional) Replicate the volume collection back to the original primary array from the newly promoted array.
- Log into the original array (replication partner) and demote the original volume collection. See Demote a Volume Collection on page 186 for more information.

Demote a Volume Collection

If you are using snapshot replication, you can use the demote procedure to make a different group the upstream partner. When you perform this operation, the volumes associated with the volume collection are set to offline and a snapshot is created. Control over the volume collection is then transferred to replication partner you specify. You can use this option following a promote operation to revert the volume collection to the previous replication partner.

Note: The demote procedure only works with snapshot replicated volume collections. You cannot demote a synchronously replicated volume collection.

Procedure

1. Go to **Manage** > **Data Protection**.
2. Select the volume collection to be demoted.
3. Click **Actions** > **Demote**.
4. Choose a partner name from the **Partner Name** menu.
5. If the volume collection uses multiple downstream partners, the system displays a warning message listing the partners and telling you that the operation will break all replication. Enter **Yes** to continue the demote operation..

6. Click **OK**.

What to do next

Ensure that you do not have any iSCSI initiators that point to the demoted volumes (members of the demoted volume collection).

Claim a Volume

Claiming a volume lets you take ownership of a formerly replicated volume that is no longer part of a volume collection on the downstream replication partner. Without claiming the volume, you cannot make any changes to the volume attributes.

Claiming a volume should be used if a primary upstream partner is no longer present and access to the replicated volume is required at the downstream site, or if you want to migrate this volume replica to a new volume collection belonging to the downstream partner system.

Note: This function is not supported with synchronously replicated volumes.

Procedure

1. Go to **Manage** > **Data Storage**.
2. Check the checkbox next to the name of the volume to claim.
3. On the volume details page, click **More Actions** > **Claim**.

Array Administration

Array administration involves performing many array-based administrative tasks. Examples include email alert configuration, password management, timeout activity, SNMP, and HTTP proxy settings.

Configure Email Alerts

You can configure email alerts to use regular or secure Simple Mail Transfer Protocol (SMTP) processing, depending on which mode is appropriate for your environment.

You might choose to use regular SMTP for email alerts if you have an SMTP server installed on your network that accepts email messages from external parties. You might choose to use secure SMTP if you have an SMTP server installed on your network, but prefer to disallow anonymous relays, or if you do not have an internal email server because you implemented cloud-based email, such as Office 365.

You can configure email alerts differently for each group of arrays. You must have at least Power User permission to configure SMTP-based email alerts.

Procedure

1. Go to **Administration** > **Alerts and Monitoring** > **Email**.
2. For both regular and secure SMTP, specify values for the fields that are enabled by default.

Option	Description
'Send From' Address	Specify the email address used by the group to send email alerts. It does not have to be a valid email address, but it must have a valid email address format. Include the group name for easy identification and filtering.
'Send To' Addresses	Specify the email address of one or more administrators who should receive email alerts from the group of arrays. These addresses do have to be real email addresses. You do not need to specify an email address for the support team when you enable sending event data to support.
Send event data to Support	Retain or disable automatically sending event data to the support team. Event data includes the alerts sent to the specified 'Send To' email addresses. **Note:** SMTP is used as a backup for the default HTTP transport mode for event data.
Hostname or IP Address	Specify the hostname or IP address of an SMTP server that the group uses to send email alerts and event data.
SMTP Port	Specify the SMTP port number to use. Default: 25.

3. For **Authentication**, select the default value of No for regular SMTP or select Yes for secure SMTP.
4. For secure SMTP only, specify values for the fields that are enabled after you select Yes for the **Authentication** option.

Option	Description
Username	Specify the username for the SMTP account. The *Username* value must start with an alphabetic character and can be up to 64 alphanumeric characters. The following special characters are also valid, as long as a dot (period) is not the last character: + (plus sign) - (hyphen or dash) _ (underscore) . (period)

Option	Description
Password	Specify the password for the SMTP account. The *Password* value can be up to 255 printable characters. The password is not hashed.
Encryption	Retain the default of None or select the encryption type. Selecting any type other than None requires using username and password authentication. • None means that email alerts are unencrypted. • STARTTLS means that secure SMTP over transport layer security (TLS) is used. The STARTTLS encryption option can be an appropriate choice if you implemented cloud-based email. • SSL/TLS means that secure sockets layer (SSL) with transport layer security (TLS) is used. The SSL version is not subject to CVE-2014-3566, the POODLE vulnerability in SSLv3. The SSL/TLS encryption option can be an appropriate choice if you have a secure SMTP server installed on your network.

5. Click **Save** to save the configuration.
6. (Optional) Click **Test** to send a test message to verify the configuration and then click **OK** to acknowledge the successful message.

HPE Storage Diagnostics for Analytics

DNA collects product operational data including the performance, reliability, and configuration characteristics of the array and sends this information to HPE support once per day. The information is used for proactive monitoring, analysis, and problem resolution. No user data is ever accessed or collected by DNA.

By default, DNA is enabled. Leaving DNA enabled is strongly recommended because this allows support personnel to continually monitor the health of the array and recommend corrective actions in case of any issues.

Note: If you encounter a problem, it can also be helpful to gather host information and send that to the support also. You can use the Host Diagnostics tool to do this. See Gather Host Diagnostics Information on page 183.

Enable DNA

Procedure

1. Go to **Administration** > **Alerts and Monitoring** > **Diagnostics**.
2. **Allow HPE to collect analytics data automatically from this product** is enabled by default.
3. (Optional) Check **Enable Secure Tunnel**.
4. Click **Save**.
   DNA is enabled on your array.

Disable DNA

If you disable DNA, no statistics or diagnostics are sent to support. Leaving DNA enabled is strongly recommended.

Procedure

1. Go to **Administration** > **Alerts and Monitoring** > **Diagnostics**.
2. Clear the **Allow HPE to collect analytics data automatically from this product** checkbox to disable DNA. Support can no longer proactively monitor your system health.
3. Click **Save**.

4. To re-enable DNA, return to this page and re-select **Allow HPE to collect analytics data automatically from this product**, then click **Save**. A checkmark appears when DNA is enabled.

Manually Send DNA

If you are asked to do so, you can send DNA at any time for analysis and problem resolution. No user data is ever accessed or collected by DNA.

Procedure

1. Go to **Administration** > **Alerts and Monitoring** > **Diagnostics**.
2. Click **Send**.

Enable a Secure Tunnel

Support may request a tunnel into the array to help troubleshoot an issue. You will be able to enable a secure tunnel that will allow support to open a tunnel. By default, secure tunnels are disabled.

Procedure

1. Go to **Administration** > **Alerts and Monitoring** > **Diagnostics**.
2. Check **Enable Secure Tunnel**.
3. Click **Save**.

   If you click **Test**, the array tests that all the connections are active and that DNA is enabled. If you click **Send**, the diagnostics are sent manually.

Configure a Proxy Server

Some features require a secure Internet connection. If your network requires the use of a general proxy server or an HTTP proxy server for secure connections, configure the array to use the correct server.

Procedure

1. Go to **Administration** > **Network** > **Proxy**.
2. Click **Use proxy server**.
   The page expands to allow you to provide information about your proxy server setup.
3. Enter the IP address or host name of your proxy server.
4. Enter the HTTP proxy server port. By default, the TCP/UDP port 8888 is used.
5. If your proxy server requires a username and password combination, enter it in the appropriate field. Not all proxy servers require this type of login. If yours does not require it, leave the fields blank.
6. Click **Save**.
   The HTTP proxy server (and a secure connection) is now used when connecting to the Internet.

Usage Analytics

The motivation for gathering analytics from user interaction with the product is to help HPE Storage understand usage behavior and improve the user experience. With that goal in mind, if you enable usage analytics when you configure your array, the collected data will be analyzed to identify areas for potential improvement.

In particular, we want to know which pages you visit most, how you perform particular actions, how long you spend on particular pages, how you use different aspects of the application and so on.

Through the usage analytics, we will be able to do the following:

- Learn how users interact with the GUI
- Collect data to help analyze user behavior

- Determine how many users interact with the GUI each day

> **Note:** The collection of usage analytics does not actually begin until the array setup is complete. We do not collect any personally identifiable information and the usage analytics are not customer visible.

Enable and Disable Usage Analytics

Use this procedure to enable or disable usage analytics.

You can also enable usage analytics during the array setup process.

Procedure

1. Go to **Administration** > **Alerts and Monitoring** > **Diagnostics**.
2. Check or uncheck **Enable analytics on user actions**.
3. Click Save.

Usage Analytics and Software Updates

We do not provide an option to enable or disable usage analytics during software updates. You can change the setting after the update.

To change the setting, run the command to enable or disable usage analytics or click **Administration** > **Alerts and Monitoring** > **Diagnostics**.

If you updated from an array version that did not support the usage analytics feature (versions earlier than 5.1.4.0), then usage analytics is disabled by default.

If you updated from an array version that supports this feature (versions 5.1.4.0 and later), the setting on the source version is carried forward and applied to the new version.

Change the Array Name

Changing the array name does not change the array serial number or any other information.

Procedure

1. Go to **Hardware**.
2. From the **Actions** dropdown menu, select **Edit Array Name**.
3. A warning box opens. Click **Rename** and **OK** to continue.
4. Enter the new name for the array. Array names are case sensitive, can contain between one and 64 alphanumeric characters, dashes (-), and dots (.), but cannot start with a dot or dash or contain underscores, spaces, or any other punctuation.
5. Click **OK**.

Set Up SNMP

The array uses SNMP to communicate with network management systems. It supports SNMP versions 1, 2, and 2c. However, the device sends traps but does not receive them. You can download the SNMP MIB from the support site.

> **Note:** The array uses the alert level settings for email alerts to determine the events that are sent as SNMP traps.

SNMP sends information to the network in one of two ways. Using the first method, the network management system sends a request to retrieve information and then subsequently receives a response. Using the second method, the traps are sent automatically, based on trap level settings.

Procedure

1. Go to **Administration** > **Alerts and Monitoring** > **SNMP**.
2. In the SNMP Get panel:
   a) Check **Enable SNMP Get**.
   b) Type a new password in the **community string** field if you want to use a password other than the default password, which is public.

      The community string represents a password that is shared between the client and server (network management system). It can be represented with up to 64 alphanumeric characters, and can contain a hyphen, colon, or period. However, only alphanumerics are allowed to begin the string.
   c) Type the port number in the **SNMP Port** field if you want to use a port number other than the default port number, which is 161.
   d) Type the administrative contact email address for the array in the **System Contact** field.
   e) Type the physical location of the array in the **System Location** field.
3. In the SNMP TRAP panel:
   a) Click **Enable SNMP Trap**.
   b) Type a host name or fully qualified domain name in the **Trap Destination** field.

      The trap destination represents the hostname of the network management system to which SNMP traps are sent.
   c) Type the port number in the **Trap Destination Port** field if you want to use a port number other than the default port number, which is 162.
4. Click **Save**.

Fail Over a Controller

A failover switches management of the array from the active controller to the standby controller.

While you can manually perform a failover, a failover can also be system driven. For example, in an iSCSI array, a failover can occur when the standby controller has better connectivity. In a Fibre Channel array, a failover will occur when the active controller loses all connectivity.

Note: A failover will not start automatically until connectivity to the array is lost for ~6 seconds.

You must perform a failover during a controller upgrade or when directed by support.

Before you begin

Failover requires one controller to be in Active mode and the other controller to be in Standby mode.

Procedure

1. In the GUI, choose **Hardware**.
2. From the list of arrays, click the array you want to fail over.
3. In the Array view, note which controller is Active and which is Standby.
4. Click **Make Active** on the Standby controller.
5. In the confirmation dialog box, click **Yes**.
   During the failover operation, the standby controller first goes into Solo mode, and then into Active mode. The active controller goes into Unknown mode, then into Stale mode, and finally into Standby mode.

Shut Down an Array

If you shutdown an array used in peer persistence, manually hand over each volume before shutting down the array. If you do not, all volumes become unavailable.

Procedure

1. Go to **Administration** > **Shut down**.

   Note: When shutting down an array, make sure you manually power off any expansion shelves.

2. Click **Shut Down Array**. You will be asked for the administrator password.
3. Enter the password and click **Shut down**.

Alarm Management

Alarms help users to better monitor and manage their storage by alerting them to a variety of different events. Compared to events, which are presented in a log based on the sequence of the occurrence of the event, alarms are active issues on the array presented in real time.

The alarms have multiple states including open, acknowledged, and closed. You can perform the following actions with the alarms:

- Set and modify reminders for the alarms
- Mute reminders for a period of time
- Set or modify the frequency of the reminders
- Disable the reminders

The alarms have numerous properties, including the following:

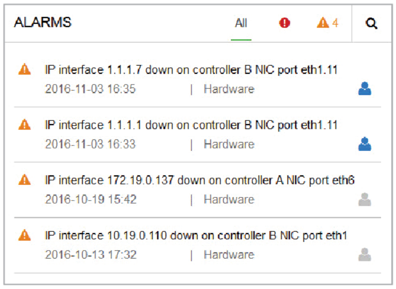
- Event time
- Severity
- Category
- Description
- Object type
- Object name
- Status
- Username of the acknowledging user
- Array name
- Group name
- Time of acknowledgment
- Recovery time
- Object ID

  Object IDs might not exist for events that are raised by platform.

Where to Find Alarm Information on the GUI

There are several places in the GUI to find information about alarms and notifications.

- If there is an active unacknowledged alarm, a banner will appear across the top of the UI dashboard. There is a link you can click to acknowledge the alarm.
- On the dashboard of the UI, the alarms are listed on the right side panel. You can view the alarms by severity or view the entire list.



IP interface 1.1.1.7 down on controller B NIC port eth1.11
2016-11-03 16:35 | Hardware

IP interface 1.1.1.1 down on controller B NIC port eth1.11
2016-11-03 16:33 | Hardware

IP interface 172.19.0.137 down on controller A NIC port eth6
2016-10-19 15:42 | Hardware

IP interface 10.19.0.110 down on controller B NIC port eth1
2016-10-13 17:32 | Hardware

SW003

- If there are any active alarms and notifications, a bell would appear next to the Events menu heading on the dashboard.
- The alarms are also listed on the Alarms page. You can access the page by going to the **Events** page and clicking the **Alarms** tab.

Acknowledge and Unacknowledge Alarms

Acknowledging alarms indicates who is responsible for handling the issue that was indicated by the alarm. Acknowledgements are also helpful because it makes those alarms that are not acknowledged more visible allowing you to know about any array conditions that are not being addressed.

Procedure

1. Go to **Events** and click the **Alarms** tab.

   A list of all the alarms on the array displays.
2. Check the alarm or alarms that you want to acknowledge.
3. Click **Acknowledge**.

   If you want to unacknowledge the alarm or alarms, just click **Unacknowledge**.

Change an Alarm Reminder

Before you begin
An alarm must be acknowledged before the reminder can be modified.

Procedure

1. Go to **Events** > **Alarms**.
2. Select the alarm for which you want to change the reminder.
3. Click **Change Reminder**.
4. Enter an interval and select a unit of time.
5. Click **Save**.

Enable Alarms

Note: Although you can enable alarms through the GUI, you can only disable alarms through the CLI.

Procedure

1. Go to the **Events** page and select the **Alarms** tab.
2. If alarms are disabled, an alert message appears and states that you must enable alarms. Click **OK**.
3. In the Alarms pane, a message appears that states that alarms have been disabled. Click the **Enable alarms now** link
   A banner appears stating that the alarms have been successfully enabled.

Delete Alarms

Be careful using this procedure because alarms indicate severe conditions on the system.

Procedure

1. Go to the **Events** page and select the **Alarms** tab.
2. Select the alarm then click **DELETE**.

Events

The array monitors events and displays them on the Events page. Events can let you know when something needs your attention, or when an event may be about to occur. They are an excellent diagnostic aid when you attempt to locate the source of a problem or potential problem on the array.

The array provides two locations from which you can view events: the events summary and recent events, as shown on the Home page, and a list of all events that you can filter as shown on the *Events* details page. Each event has a priority that you can use to filter information in the list, as well as determine whether or not the event requires manual intervention.

Event Severity Levels

The array uses the standard alert system that supports three basic levels of severity. Depending on the level of the event that has been logged, immediate action could be required.

Table 13: Event Severity Levels

Severity Level	Description	Examples
All	All events are shown, regardless of severity. Manual intervention may or may not be needed.	
Critical	An event has occurred that requires immediate attention. Data loss or hardware damage may occur if action is not taken quickly. Critical alerts also trigger email notification, defined on the Administration tab.	The system has reached space capacity. A drive has failed.
Warning	An event has occurred that might impact system performance. Action will likely be necessary, but no damage will occur if the action is not taken immediately.	A scheduled snapshot was not completed successfully. A drive is experiencing write errors.
Info	An event has occurred that does not require action to be taken and does not affect system performance. This level of event is useful for troubleshooting or for determining system trends.	The administrator password was changed. A controller was restarted.

View Events

The Events page shows events that occurred on the array. You can filter events to narrow the focus of the list. The filter is not persistent: it reverts to the default each time you open the GUI. By default, all events are displayed.

Procedure

1. From the menu banner in the array OS dashboard, select **Events**.
   The Events Log opens.
2. In the Severity field, select the severity filter limits.

Limit the list of events to only those of a specific severity level and category (type). For example, you can choose filter limits to see only critical volume events and verify that a specific event occurred, or to view all informational events to track general activity levels.

3. Filter further by selecting an event category.
4. Select the date range for which you want to view events.

   The date range that you select depends on what you are looking for. For example, if a large number of events occurred around the same time, you might want to look at the last 7 days or 30 days to see if the events were part of a larger pattern or were an anomaly that was caused by a one-time occurrence.

   Often one event triggers others. For example, a disk failure can cause a scheduled replication or snapshot to fail. Using the recent events list can help you determine if this is the case. You can then take any necessary action.

5. Select the array or arrays that you want to include.

   Note: The Array field only appears if multiple arrays are supported in the network environment.

Audit Logs

The array OS audit log keeps records of all user-initiated, non-read operations performed on the array. Administrators can view the audit log in a summary table with faceted browsing by time, activity category, and across access type.

System Limits and Timeout Values

This section summarizes the system limits for both iSCSI and Fibre Channel arrays, and provides references to information for host timeout values.

Host Timeout Values

For information about host timeout values, please see the following Knowledge Base articles:

KB-000052 Windows: Host Timeout Values

KB-000087 VMware: Host Timeout Values

KB-000304 Linux: Host Timeout Values

These documents are available on the HPE InfoSight Documentation web page. Refine your search by clicking the Knowledge Base Article link in the left navigation pane. Alternatively, enter the article identification, for example, KB-000052, in the Search window at the top of the page, then click **Search**.

System Limits

This section summarizes the system limits. Alerts or log messages are generated when the system reaches the warning count, so this is a *threshold*. No more objects of the specified type can be created when the system reaches the maximum count, so this is a *limit*.

Important:

Volume scalability to 10,000 volumes per group is supported when the group leader is an array model that supports 10,000 volumes, and it belongs to a pool that can also support this limit. Pool limits are the same as the limits of the smallest capacity array in the pool.

See the notes at the end of the table for information about array models that support specific limits.

See *Relationship of Groups, Pools, Arrays, Folders, and Volumes* in the *Array Overview* section for information about the scope of objects in single-array and multi-array groups.

Table 14: System Limits

Object Type	Scope	iSCSI Maximum	FC Maximum	Warning	Notes
Array	Group	4	4	4	
	Pool	4	4	4	
Branch	Group	10,000	10,000	9,500	
CHAP user	Group	1024	N/A	960	
Data connection	Controller	80000 15000	80000 15000	72000 13500	An iSCSI or a Fibre Channel path to a volume 1 (80000) 2 (15000)
Session	Array	12000	12000	None	An iSCSI session or FC login

Object Type	Scope	iSCSI Maximum	FC Maximum	Warning	Notes
FC initiator	FC port	N/A	256	None	Prior to OS 4.x, this value was 128.
Folder	Pool	128	128	None	
	Group	128	128	None	
Initiator	Initiator group	256	256	240	
	Group	10,000	10,000	9,500	
Initiator group	Subnet	60	N/A	54	
	Group	1,024	1,024	960	
Network configuration	Array	4	4	4	
Performance policy	Group	100	100	90	
Pool	Group	4	4	4	
Protection schedule	Group	5,000	5,000	4,500	
	Protection template	10	10	8	
	Volume collection	10	10	8	
Protection template	Group	50	50	45	
Replication bandwidth policy (throttle)	Group	50	50	45	
	Replication partner	25	25	20	
Replication partner	Group	50	50	45	
	Pool	50	50	45	
Route	Network configuration	10	10	8	
SSH key	User	10	10	8	
Snapshot	Group	300,000 190,000	300,000 190,000	275,000 175,000	1 2 3
	Pool	300,000 190,000	300,000 190,000	275,000 175,000	1 2 3
	Volume	1,000	1,000	900	

Object Type	Scope	iSCSI Maximum	FC Maximum	Warning	Notes
Writable Snapshot	Array	40000 10000	40000 10000	None	1 2 4
Snapshot Collection	Volume Collection	1,000	1,000	900	
Subnet	Network configuration	60	60	54	
User account	Group	100	100	90	
Volume	Group	10,000 1,024	10,000 1,024	9,200 960	1 2
	Pool	10,000 1,024	10,000 1,024	9,200 960	1 2
	Performance policy	10,000 1,024	10,000 1,024	9,200 960	1 2
	Volume collection	50	50	45	Volumes in a collection can exist in different pools.
	Synchronous replication	512	512	N/A	These values also apply to Peer Persistence.
	Volume limit	127 TiB	127 TiB	N/A	
Volume access control list (ACL)	Group	65,536	65,536	60,000	
	Pool	65,536	65,536	60,000	
	Volume	64	64	60	
Volume collection	Group	2,000 512	2,000 512	1,800 480	1 2

Note:

1 Limits apply to AF5000, AF7000, AF9000, AF40, AF60, AF80, and HPE Alletra 6000 model arrays.

2 Limits apply to all model arrays not listed in Note 1.

3 A frequent schedule is a schedule in a volume collection that triggers snapshots more often than every five minutes. There is a limitation of five frequent schedules per array group. There is no restriction on schedules with a period of five minutes or more.

4 Writable snapshots also count against the total Snapshot limit.

Firewall Ports

Configure local ports for HTTP, HTTPS, iSCSI, SNMP, SSH (incoming and outgoing), and other data and management protocols.

Configure Firewall Ports

Use this information to configure local ports for incoming and outgoing HTTP, HTTPS, iSCSI, SCP, SNMP, SRM, SSH, TCP, and other data and management protocols.

Table 15: Group Egress Ports – External Port

Port Number	Service	Protocol	Destination DNS/IP
443 TCP	DNA, heartbeat	HTTPS	nsdiag.nimblestorage.com
443 TCP	Storage array alerts *	HTTPS	nsalerts.nimblestorage.com
443 TCP	Storage array statistics	HTTPS	nsstats.nimblestorage.com
443 TCP	Software downloads	HTTPS	update.nimblestorage.com
443 TCP	Storage array initialization	HTTPS	device.cloud.hpe.com
443 TCP	Storage array initialization	HTTPS	common.cloud.hpe.com
443 TCP	Data Services Cloud Console	HTTPS	console-*instance*.data.cloud.hpe.com tunnel-*instance*.data.cloud.hpe.com *instance*.data.cloud.hpe.com Where *instance* can be **eu1** for Europe, **jp1** for Japan, or **us1** for America. For example: console-eu1.data.cloud.hpe.com tunnel-eu1.data.cloud.hpe.com
2222 TCP	Secure tunnel	SSH	hogan.nimblestorage.com
4311 TCP	HPE Storage Protection Manager	SOAP/HTTP	application server IP **
8443 TCP	vCenter VASA/vVol integration	HTTPS	Management IP address and both diagnostic IP addresses

Port Number	Service	Protocol	Destination DNS/IP

* An array sends DNA messages using HTTPS POST back to support, if it is enabled. If three HTTPS POST attempts are made and they all fail, these notifications will revert to email relay.

** If the application server connecting with these ports on an array is on the same side of the firewall as the array, you do not need to open these ports in the firewall.

Note: The array may initiate connections to these external addresses from the Management and Data IP addresses or any controller support IP address.

Note: When configuring firewall rules for the destinations listed above, it is recommended that you specify the destination by host name rather than by IP address, and allow DNS to resolve the IP address. In the event that there is a change in the publicly available IP address for one of these destinations, the change will be communicated by a notification on the InfoSight portal. Other methods of sending notifications of such changes may be chosen as needed.

Table 16: Intra-group Ports – TCP Ports Needed Between Arrays in a Group

Port Number	Service	Protocol	IP Address
4211 TCP	Array setup (incoming) and management (intra-group)	SOAP/HTTP	Data IP(s)
4212 TCP	Group controller management	HTTP	Data IP(s)
4241 TCP	Group controller management	DTS	Data IP(s)
5394 TCP	Group leader failover communication	HTTPS	Management IP(s)
5395 TCP	Witness daemon communication	HTTPS	Management IP(s)
5432 TCP	Group configuration synchronization	DTS	Data IP(s)
5521 TCP	Group data services	DTS	Data IP(s)
5525 TCP	Synchronous Replication (ASD)	DTS	Management/Data IP(s)
5526 TCP	Synchronous Replication (ASD)	DTS	Management/Data IP(s)
5527 TCP	Synchronous Replication (ASD)	DTS	Management/Data IP(s)
5706 TCP	Group event reporting	SOAP/HTTP	Data IP(s)
6716 TCP	DSD miscellaneous management	SOAP/HTTP	Data IP(s)
6717 TCP	GMD array management (GAI)	SOAP/HTTP	Data IP(s)
6718 TCP	Group controller management	DTS	Data IP(s)
6719 TCP	Data forwarding	DTS	Data IP(s)
6720 TCP	Bin migration	DTS	Data IP(s)
6721 TCP	Bin map management – DSD	DTS	Data IP(s)

Port Number	Service	Protocol	IP Address
6722 TCP	iSCSI	DTS	Data IP(s)
6723 TCP	Bin map management - GDD	DTS	Data IP(s)
6724 TCP	iSCSI	DTS	Data IP(s)
6725 TCP	DSD volume management	SOAP/HTTP	Data IP(s)
6726 TCP	SCSI	DTS	Data IP(s)
6727 TCP	SCSI	DTS	Data IP(s)
6728 TCP	Key Protocol	DTS	Data IP(s)
6729 TCP	LU cache (DSD-GDD)	DTS	Data IP(s)
6730 TCP	Key Protocol	DTS	Data IP(s)
6731 TCP	LU cache (DSD-DSD)	DTS	Data IP(s)
6732 TCP	Synchronous Replication (DSD-GDD)	DTS	Data IP(s)
6733 TCP	Synchronous Replication (DSD-GDD)	DTS	Data IP(s)
6740 TCP	Synchronous Replication	DTS	Data IP(s)
6741 TCP	Synchronous Replication Resynchronization	DTS	Data IP(s)

Note: If the arrays within the group are on the same side of the firewall, you do not need to open these ports in the firewall.

Table 17: Inter-group Ports – TCP Ports Needed Between Replication Partners

Port Number	Service	Protocol	IP Address
4213 TCP **	Replication control (exchange of replication configuration information between groups)	SOAP/HTTP	Management IP address and both diagnostic IP addresses of all replication partners and group members
4214 TCP **	Replication data (transfer of replicated data)	NS-REPL	Use either: 1 — All IP addresses in the management subnet of all replication partners and group members or 2 — All data IP addresses in the chosen data subnet of all replication partners and group members *
5391 TCP **	Secure web-service communications Exchange of SSL keys for encrypted volumes	SOAP/HTTPS	Management IP address and both diagnostic IP addresses

Port Number	Service	Protocol	IP Address

* Assumes that all replication partners were chosen to perform replication transfer over the data subnet.

Important:

There are two options for replication:

1. Replication transfer and replication over the Management subnet.
2. Replication transfer over data subnet specified during replication partner configuration. Replication control is still transferred over the management subnet per table.

Note: If the arrays in the two groups are on the same side of the firewall, you do not need to open these ports in the firewall.

** This port must be open between the SRM server and the Nimble array.

Table 18: Group Ingress Ports – External Ports

Port Number	Service	Protocol	IP Address
22 TCP	Group management (CLI)	SSH	Management IP address and both diagnostic IP addresses
161 UDP	SNMP get	SNMP	Management IP address and both diagnostic IP addresses
redirect 80 TCP to 443 TCP ***	Group management (GUI), redirects to 443 TCP	HTTP	Management IP address and both diagnostic IP addresses
443 TCP / 5392 TCP	Group management (GUI)	HTTPS	Management IP address and both diagnostic IP addresses
3260 TCP	SNMP statistics	iSCSI	Data IP(s) and discovery IP(s)
4210 TCP ***	Group management (GUI charts and NPM)	SOAP/HTTP	Management IP address and both diagnostic IP addresses
4211 TCP	Array setup (incoming) and management (intra-group)	SOAP/HTTP	Data IP(s)
5988 TCP	CIM server **	HTTP	Management IP address and both diagnostic IP addresses
5989 TCP	CIM server	HTTPS/CIM-XML	Management IP address and both diagnostic IP addresses
5390 TCP	Secure web-service communications	SOAP/HTTPS	Data IP(s)
5391 TCP ***	Third-party agents and utilities	SOAP/HTTPS	Management IP address and both diagnostic IP addresses *
5392 TCP ***	Group management, third-party agents and utilities	REST API	Management IP address and both diagnostic IP addresses *
5393 TCP	Array Management, third party utilities and agents	HTTPS	Management IP address and both diagnostic IP addresses *
8443 TCP	vCenter VASA/vVol integration	HTTPS	Management IP address and both diagnostic IP addresses

Port Number	Service	Protocol	IP Address

* Some third-party utilities may use both TCP port 5391 and TCP port 5392. Refer to the relevant integration guides available on InfoSight, or from the third-party software vendor for more information.

** Fibre Channel arrays do not use the CIM server (cimserver) service, so port 5989 does not need to be open on them.

> **Note:** If the client and the arrays within the group are on the same side of the firewall, you do not need to open these ports in the firewall.

*** This port must be open between the SRM server and the Nimble array.

Table 19: Group Egress Ports – Other External Ports

Port Number	Service	Protocol	Destination DNS/IP
25 * UDP & 25 * TCP	SMTP	SMTP	SMTP server IP
53 / UDP & 53 TCP	DNS	DNS	DNS server IP
123 / UDP	NTP	NTP	NTP server IP
162 * / UDP	SNMP trap	SNMP	SNMP trap listener
443 TCP	HTTPS	HTTPS	vCenter IP
514 UDP	Syslogd	UDP	Syslog server IP
4311 TCP	Microsoft VSS	VSS	Application server IP
Configurable TCP	HTTP	HTTP	HTTP proxy server IP
53 TCP/UDP ** 88 TCP/UDP ** 123 UDP *** 137 TCP/UDP 139 TCP/UDP 389 TCP/UDP 445 TCP	Active Directory Authentication	DNS, Kerberos, SMB	All Active Directory domain controllers

* Default, but can be changed.

** DNS services should be provided by the domain controller, or by an alternative with the appropriate zones and AD records.

*** Array should be configured to use the Active Directory server as the NTP server, or the array and domain controllers should be configured to use the same NTP server. Array clock must remain within 5 minutes of the domain controller clock, or domain authentication will fail.

> **Note:** If the service is on the same side of the firewall as the array, you do not need to open these ports in the firewall.