Hitachi Virtual Storage Platform One File

File management software release 1.2.0

NAS File OS release 15.3 or later

File Administrator User Guide

This document describes the administration procedures for File Administrator.

MK-24VSP1F003-03
October 2024

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

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Contents

Preface

This document describes the administration procedures for File Administrator.

Getting help

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

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

Comments

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

Thank you!

Accessing product documentation

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

Chapter 1: Overview

Hitachi Virtual Storage Platform One File is a highly secure file storage platform that supports on-premises and hybrid cloud settings to ensure data mobility and governance for managed NAS servers. The intuitive File Administrator GUI lets you configure, manage, and monitor managed servers and associated file systems and data.

File Administrator also includes analytic, reporting, and alerting features that help you to achieve optimal performance in a NAS environment and to prevent possible problems.

This document describes features that are specific to File Administrator. Other applications that make up the VSP One File management software are described in other publications.

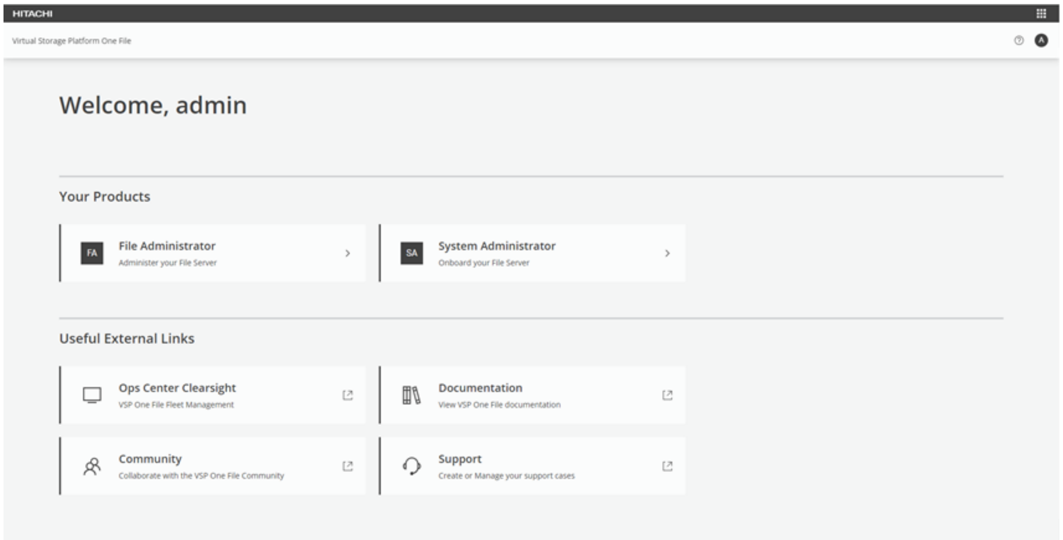
Chapter 2: Introduction to the File Administrator GUI

The File Administrator GUI is accessible from the VSP One File **Welcome** page.

Navigating the Welcome page

The **Welcome** page opens when you log in to the VSP One File management software. Use this page to access File Administrator.

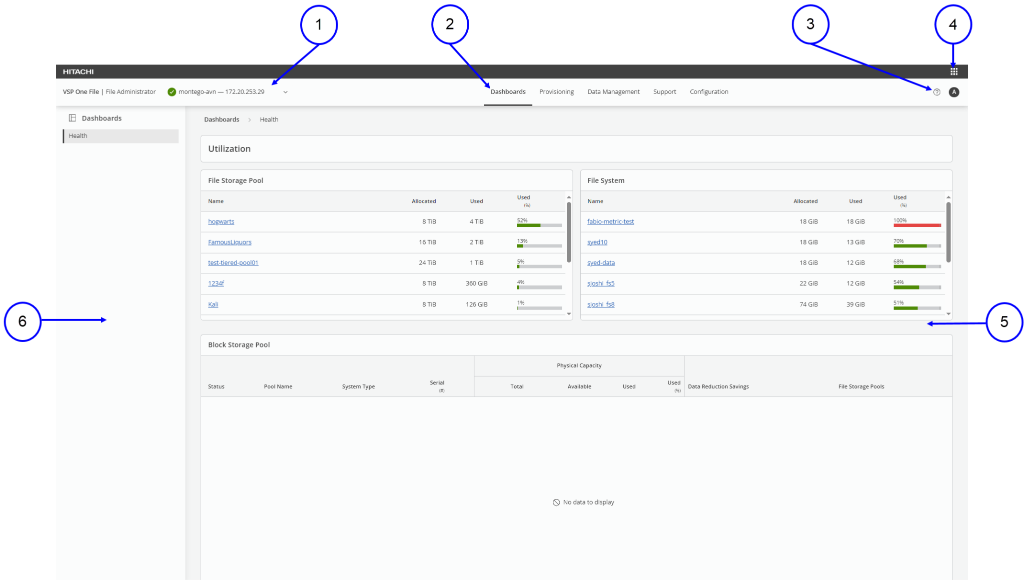
You can also access Hitachi Ops Center Clear Sight (log on credentials are required), the VSP One File documentation and community forum, and product support from the **Welcome** page.


HITACHI
Virtual Storage Platform One File
Welcome, admin
Your Products
FA
File Administrator
Administer your File Server
SA
System Administrator
Onboard your File Server
Useful External Links
Ops Center Clearsight
VSP One File Fleet Management
Documentation
View VSP One File documentation
Community
Collaborate with the VSP One File Community
Support
Create or Manage your support cases

The applications that appear on the **Welcome** page depend on the assigned user role. For information about using the System Administrator and Keycloak application GUIs, see the *Hitachi Virtual Storage Platform One File Installation and Configuration Guide*.

Navigating the GUI

The File Administrator GUI contains menus and other navigation and support tools to help you to easily set up, configure, and use the application to manage a file server.



Utilization

File Storage Pool

Name	Allocated	Used	Used (%)
hogwarts	8 TiB	4 TiB	52%
FamousLiquors	16 TiB	2 TiB	13%
test-tiered-pool01	24 TiB	1 TiB	5%
1234f	8 TiB	360 GiB	4%
Kali	8 TiB	126 GiB	1%

File System

Name	Allocated	Used	Used (%)
fabio-metric-test	18 GiB	18 GiB	100%
syed10	18 GiB	13 GiB	70%
syed-data	18 GiB	12 GiB	68%
sjoshi_fs5	22 GiB	12 GiB	54%
sjoshi_fs8	74 GiB	39 GiB	51%

Block Storage Pool

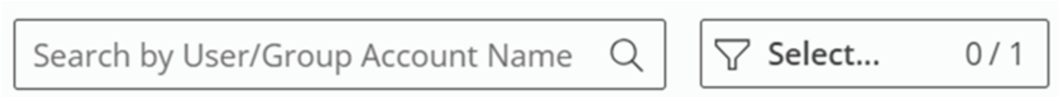
				Physical Capacity					
Status	Pool Name	System Type	Serial (#)	Total	Available	Used	Used (%)	Data Reduction Savings	File Storage Pools

No data to display

Items	Description	Definition
1	Managed servers list	The managed servers list opens the list of managed servers added in the File Administrator.
2	Applications menus	An application menu opens the application pane that contains links to features and tasks associated with that menu.
3	Support menu	The support menu contains icons to access online help and user actions (Log out and About).
4	App switcher	The app switcher menu (⠿), which you use to switch to another VSP One File application.
5	Application pane	The contents of the application pane depend on the active application menu. This pane contains links to associated features and tasks.
6	Navigation pane	The navigation pane contains the same links as in the application pane in an expandable and collapsible menu.

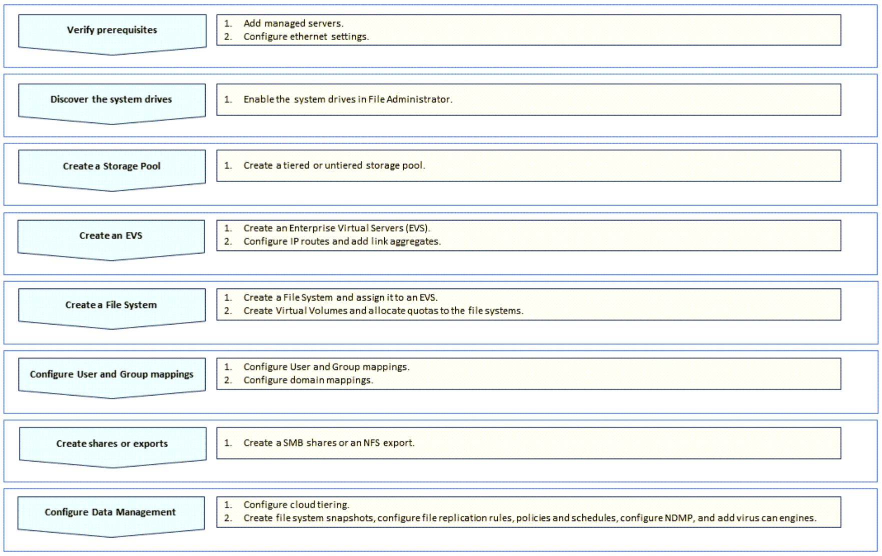
Search and filter options

The application panels in the GUI contain search and filter options as shown in the following example. You can narrow the list of items shown in the panel by using these options.



Chapter 3: Workflow for setting up the File Administrator

The following figure shows the workflow followed by an administrator to set up the File Administrator.



Verify prerequisites	1. Add managed servers. 2. Configure ethernet settings.
Discover the system drives	1. Enable the system drives in File Administrator.
Create a Storage Pool	1. Create a tiered or untiered storage pool.
Create an EVS	1. Create an Enterprise Virtual Servers (EVS). 2. Configure IP routes and add link aggregates.
Create a File System	1. Create a File System and assign it to an EVS. 2. Create Virtual Volumes and allocate quotas to the file systems.
Configure User and Group mappings	1. Configure User and Group mappings. 2. Configure domain mappings.
Create shares or exports	1. Create a SMB shares or an NFS export.
Configure Data Management	1. Configure cloud tiering. 2. Create file system snapshots, configure file replication rules, policies and schedules, configure NDMP, and add virus can engines.

1. Make sure that you have configured the Ethernet settings during the installation of the VSP One File Management Software and added managed servers during the first time set up of the software. For more information, see the *Virtual Storage Platform One File Management Software Installation and Configuration Guide*.
2. Enable system drives (on page 24) in File Administrator as logical units (LUNS) to create storage pool.
3. Create an untiered storage pool (on page 26) or create a tiered storage pool (on page 27) to host the virtual servers.
4. Create an EVS (on page 32) to host the file systems and configure IP routes (on page 200) and add link aggregates (on page 196) to connect to the EVS.
5. Create a file system (on page 37) in an EVS to store files and directories. Create virtual volumes (on page 44) from a file system to allocate and control directories for projects, users, or groups. Create quotas (on page 47) for users or groups accessing the file system or control the capacity and number of files within a virtual volume.
6. Configure user mapping or group mapping (on page 168) and domain mapping (on page 170) for the file system to provide access to UNIX, Windows, NFSv4, and Kerberos users and groups.
7. Create an SMB share (on page 53) or an NFS export (on page 50) to provide access to Windows or UNIX users with access to the file systems.

8. Configure data migration (on page 109) to move data between two on-premises file systems or between an on-premises file system and S3-compatible object storage. For data protection, configure file system snapshots (on page 65), configure file system replication policies (on page 77), configure NDMP (on page 100), and add virus scan engines (on page 107).

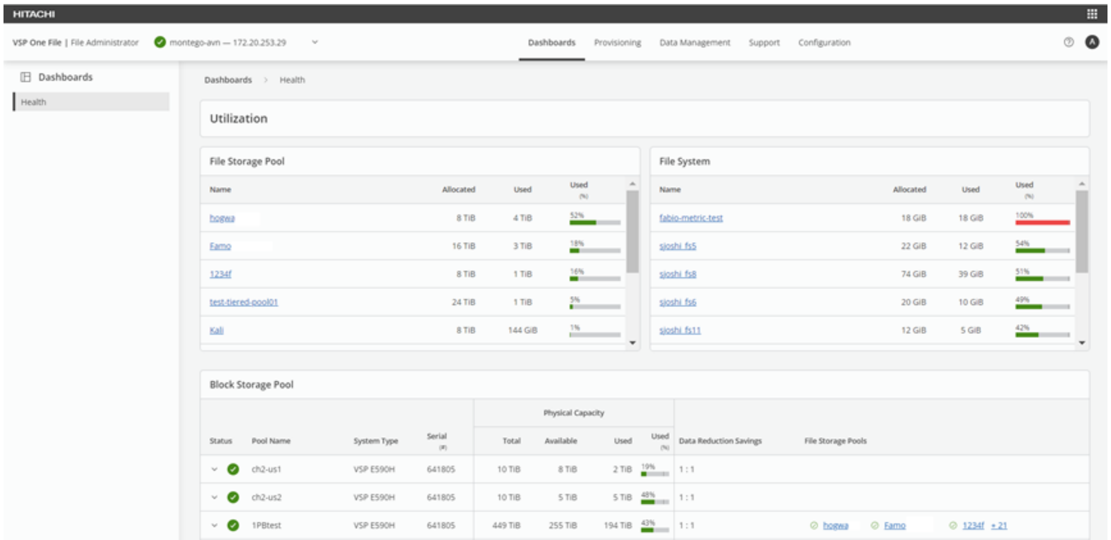
Chapter 4: Monitoring system performance

Monitoring performance is crucial to effective system management. The Health dashboard displays key resource information that you can use to quickly monitor system health and performance.

This dashboard displays capacity usage for file systems and storage pools to help you to avoid performance issues such as the system slowing down as usage nears thresholds or halting if the system unexpectedly runs out of storage space. By monitoring capacity usage through the dashboard, you can take actions to reduce usage or determine if additional storage is required before severe issues arise.

If system drives in a storage system are shared by file and block storage pools, you can monitor the capacity for both pool types from the dashboard. To monitor block storage pools, you must first register the storage systems that are associated with the pools as described in the Registering a block storage system (on page 139). The block storage systems must be VSP One Block 20 or later systems.

To open the dashboard, click the Dashboards application menu.



File Storage Pool

Name	Allocated	Used	Used (%)
hogwa	8 TiB	4 TiB	52%
Famo	16 TiB	3 TiB	18%
1234f	8 TiB	1 TiB	16%
test-tiered-pool01	24 TiB	1 TiB	5%
Kali	8 TiB	144 GiB	1%

File System

Name	Allocated	Used	Used (%)
fabio-metric-test	18 GiB	18 GiB	100%
sjoshi_fs5	22 GiB	12 GiB	54%
sjoshi_fs8	74 GiB	39 GiB	51%
sjoshi_fs6	20 GiB	10 GiB	49%
sjoshi_fs11	12 GiB	5 GiB	42%

Block Storage Pool

				Physical Capacity					
Status	Pool Name	System Type	Serial (#)	Total	Available	Used	Used (%)	Data Reduction Savings	File Storage Pools
✓	ch2-us1	VSP E590H	641805	10 TiB	8 TiB	2 TiB	19%	1 : 1	
✓	ch2-us2	VSP E590H	641805	10 TiB	5 TiB	5 TiB	48%	1 : 1	
✓	1PBtest	VSP E590H	641805	449 TiB	255 TiB	194 TiB	43%	1 : 1	hogwa Famo 1234f + 21

The dashboard contains the following panels to report data by resource type:

- File Storage Pool panel (on page 17)
- File System panel (on page 17)
- Block Storage Pool panel (on page 18)

File Storage Pool panel

The **File Storage Pool** panel displays the top ten managed file storage pools by the percentage of storage used in descending order. The panel includes the following information:

Name

The name of the storage pool. Click the link to view and manage the storage pool configuration information. For information about managing storage pools, see Storage Pools (on page 25).

Allocated

The amount of storage allocated to the storage pool.

Used

The amount of storage that is used by the pool.

Used Percentage

The percentage of storage that is used by the pool. A color-coded bar is included to quickly alert you to the status of the storage usage:

- Green: The percentage of storage used is normal.
- Red: The percentage of storage used meets or exceeds the threshold set for the storage pool.

File System panel

The **File System** panel displays the top ten managed file systems by the percentage of storage used in descending order. The panel includes the following information:

Name

The name of the file system. Click the link to view and manage the file system configuration information. For information about managing file systems, see File systems (on page 37).

Allocated

The amount of storage allocated to the file system.

Used

The amount of storage that is used by the file system.

Used Percentage

The percentage of storage that is used by the file system. A color-coded bar is shown to quickly alert you to the status of the storage usage:

- Green: The percentage of storage used is normal.
- Red: The percentage of storage used meets or exceeds the threshold set for the file system.

Block Storage Pool panel

If block storage systems are registered in the VSP One File System Administrator, the **Block Storage Pool** panel displays the status and performance data for the storage pools that are associated with the storage system. For information about how to register block storage systems, see Registering a block storage system (on page 139).

Important: The block storage systems must be VSP One Block 20 or later systems.

This panel includes the following information:

Status

The status of the storage pool that indicates the pool is OK or there is a warning.

Pool Name

The storage pool name.

System Type

The storage system that contains the system drives that are in the storage pool.

Serial Number

The storage system serial number.

Physical Capacity

Total

The amount of storage allocated to the storage pool.

Available

The amount of storage available to the storage pool.

Used

The amount of storage used by the storage pool.

Used (%)

The percentage of storage that is used by the storage pool. A color-coded bar is shown to quickly alert you to the status of the storage usage:

- Green: The percentage of storage used is normal.
- Red: The percentage of storage used meets or exceeds the threshold set for the storage pool.

Data Reduction Savings

The ratio of data reduction (deduplication and compression) savings for the storage pool. For example, a ratio of 2:1 indicates a 50% reduction in storage usage.

File Storage Pools

The associated file storage pools. Click a link to view and manage the storage pool configuration information. For information about managing storage pools, see Storage Pools (on page 25).

Capacity Utilization

The capacity usage for the storage pool displayed as a graph to show usage peaks and trends. To view the graph, expand the storage pool row. By default, the graph shows usage, the warning threshold, and the depletion threshold. Click a metric label to add or remove the metric from the graph.

Chapter 5: Storage provisioning

Provisioning includes managing secure access to user data and creating and managing Enterprise Virtual Server (EVS) instances, file systems, virtual volumes, system drives, and storage pools.

System drives

System drives (SDs) are the basic logical storage element used by the NAS server. Storage systems use RAID controllers to aggregate multiple physical disks into SDs (also known as Logical Units or LUs). An SD is a logical unit made up of a group of physical disks or flash drives. The size of the SD depends on factors such as the RAID level, the number of drives, and their capacity.

When you create SDs:

- Use the Hitachi storage management application appropriate for your storage system. You cannot create SDs using File Administrator or the NAS server command line.
- When creating SDs, you may need to specify array-specific settings in the storage management application. Also, depending on the firmware version of the array, there may be device-specific configuration settings.

For more information about the settings required and the firmware that is installed for each type of storage system, contact customer support.

The System Drives pane displays all the SDs in the storage system.The following table describes the fields in this pane:

Field	Description
Licensing Capacity Used	This shows the amount of storage present in the storage subsystem is listed as the Licensing Capacity Used. The current capacity cannot exceed the licensed limit.
Licensing Limit	This shows the current amount of storage supported by the installed license is listed as the Licensing Limit.
Filters	By default, all system drives are shown. With shared storage systems, it might be necessary to filter the system drives list. You can narrow the list by using the search or filters option.
ID	This shows the numeric identifier of the system drive. A numeric identifier of the system drive, which is assigned by the server. It is sometimes useful to know the ID when examining the server event log.
Capacity	This shows the size of the system drive.
LUN	The LUN of each system drive is assigned by the storage array when the LUN is created.
Block Pool ID	This shows information about the system drive's virtualization layer. The options are: ▪ HDP pool number ▪ DDM UVM pool number ▪ UVM ▪ None - if none of the options apply to the system drive
Comment/Array Name	This allows additional descriptive information to be assigned to a system drive to help make it more identifiable when viewed elsewhere in the UI.
Storage Pool	This shows the name of the storage pool of which the system drive is a part.
Stripesets	When a storage pool is initially created, it has one stripeset, and all the data is striped across the system drives in that stripeset. Each time a storage pool is expanded, a stripeset is added. For example, Stripeset 0, Stripeset 1.
Access	This shows whether the server has access to the system drive. To perform actions on the system drive, such as creating a file system, Access must be set to Allowed. Set Access to Allowed for all configurations other than shared storage system configurations.
Status	This is an indicator of the health of the system drive. The following describe the possible status of the system drive: ▪ OK

Field	Description
	▪ Offline ▪ Not Present ▪ Initializing ▪ First Invalid ▪ Failed ▪ Disconnected ▪ Write Protected ▪ Secondary ▪ Formatting You can get more information about the state of the system drives from the server event log.
View	This shows details about the selected system drive, such as the manufacturer, the rack name, storage capacity, FC path, and configuration.
More actions menu	This allows you to perform operations like Forget, Allow access, and Deny access on the selected drive.
Allow access	This makes the selected system drive available for use.
Deny access	In shared storage systems, some system drives may need to be set with Deny access to ensure they are not accessed unintentionally.
Forget	This removes the selected system drive from the list. If the system drive has been removed from the RAID rack or if the RAID rack has been removed from the storage system, click Forget to remove it from the list of configured system drives.

To view additional details about the individual system drives, click View next to each drive. For more information, see System Drive details (on page 22)

System Drive details

You can view additional details which are specific to the selected system drives.

The following table describes the fields on this pane:

Field	Description
Overview	
Comment	This shows additional information about the system drive. Additional descriptive information can be assigned to a system drive to help make it more identifiable when viewed elsewhere in the GUI. This field is visible when you click on the edit icon.
System Drive ID	This shows the system drive identifier.
Hitachi Storage Array Serial Number	This shows the name of the RAID rack hosting the system drive.
Capacity	This shows the size of the system drive.
Access	This shows whether the server has access to the system drive. To perform actions on the system drive, such as creating a file system, Access must be set to Allowed. Set Access to Allowed for all configurations other than shared storage system configurations.
Logical Unit ID (LUID)	This shows an unique internal identifier of the system drive. The LUID is created by the RAID controller.
GAD	This shows whether the system drive is a Global Access Device (GAD). ▪ **Yes** indicates that the system drive is a GAD. ▪ **No** indicates that the system drive is not a GAD. ▪ **Unknown** indicates that the system drive's GAD status is not available.
Virtualization	This shows information about the system drive virtualization layer. The options are: ▪ HDP pool number ▪ DDM UVM pool number ▪ UVM ▪ None - if none of the options apply to the system drive
Drive Status	This shows the status of the system drive. The status is an indicator of the health of the system drive. The following describes the possible states of the status indicator: ▪ Green and OK - The system drive is operating normally. ▪ Amber: The system drive is operational, but it is initializing or performing a consistency check.

Field	Description
	- Red: There is a fault in the system drive and it is not operational. - Grey: The system drive is not present. For more information about the state of the system drive, refer to the server event log.
Storage Pool Configuration	
Storage Pool Configuration	This section shows the Storage Pool Name and the Storage Pool Status information.
Actions	
Allow Access	Select a system drive and click Allow Access to make the drive available for use.
Deny Access	In shared storage systems, some system drives may need to be set with Deny Access to ensure they are not accessed unintentionally.
Forget	This removes the selected system drive from the list. If the system drive has been removed from the RAID rack, or if the RAID rack has been removed from the storage system, click Forget to remove it from the list of configured system drives.

Enabling a system drive

Before you begin

Make sure that the system drive is discovered by File Administrator and the status is OK.

By default, a new system drive is disabled.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **System Drives**.
2. In the **System Drives** pane, identify the system drive you want to enable.
3. Select the system drive, and then click **Allow access**.

Filter for system drives

You can select filter criteria for the system drives displayed in the System Drives pane.

Field	Description
Access	Allows you to display system drives that have access allowed or access not allowed.
Status	Allows you to display system drives that are healthy, unhealthy, or not present. An unhealthy system drive is one that currently has one or more of the following situations: ▪ Multiple disk failures (dependent on the RAID configuration) that caused the SD to go offline. ▪ Loss of connection to the storage device.
Storage Pool	Allows you to display system drives that are part of one or more storage pools. You can display system drives that match a specified status (in a storage pool, not in a storage pool, or in an unloadable storage pool), or you can display all system drives in a specified storage pool.
Storage Pool Status	Filters the storage pool status based on health of the storage pool.
Reset	Resets all values on this page to the system defaults.

Storage Pools

A storage pool is the logical container for a collection of four or more system drives (SDs). There are two types of storage pools: untiered and tiered.

An untiered storage pool contains SDs created on one or more storage systems in the same storage tier. These storage systems must have comparable performance characteristics. To create an untiered storage pool, you must have at least four unused system drives on the storage system. These system drives will be used to create the pool.

A tiered storage pool is a combination of SDs from high-performance storage, such as flash memory, with lower-performance devices, such as Serial Attached SCSI (SAS) or Near Line SAS (NL SAS). It must include two tiers.

- Tier 0 is used for metadata, and the best-performing storage should be designated as Tier 0.
- Tier 1 is used for user data.

When creating a tiered storage pool, you must have at least four unused SDs available for each tier. First, create the user data tier (Tier 1), and then create the metadata tier (Tier 0).

Storage pool chunks

Storage pools are made up of multiple small allocations of storage called chunks.

Chunk size is an important consideration when creating storage pools. Chunks are established during the creation of the storage pool, with a recommended size range referred to as the guideline chunk size. The guideline chunk size is between 500 MiB and 18 GiB. Each storage pool can contain up to 60,000 chunks.

Larger chunks maximize scalability, while smaller chunks allow more granular file system expansion because a file system always expands by a whole number of chunks.

When creating storage pool using File Administrator, the guideline chunk size is set to 18 GiB (the maximum allowable size).

Creating a storage pool

You can create a storage pool using available SDs. The storage pool can be expanded up to 256 SDs.

To achieve the best performance when creating a tiered storage pool, store the metadata tier (Tier 0) on the storage system with the highest performance.If all system drives have the same performance characteristics, then create an untiered storage pool.

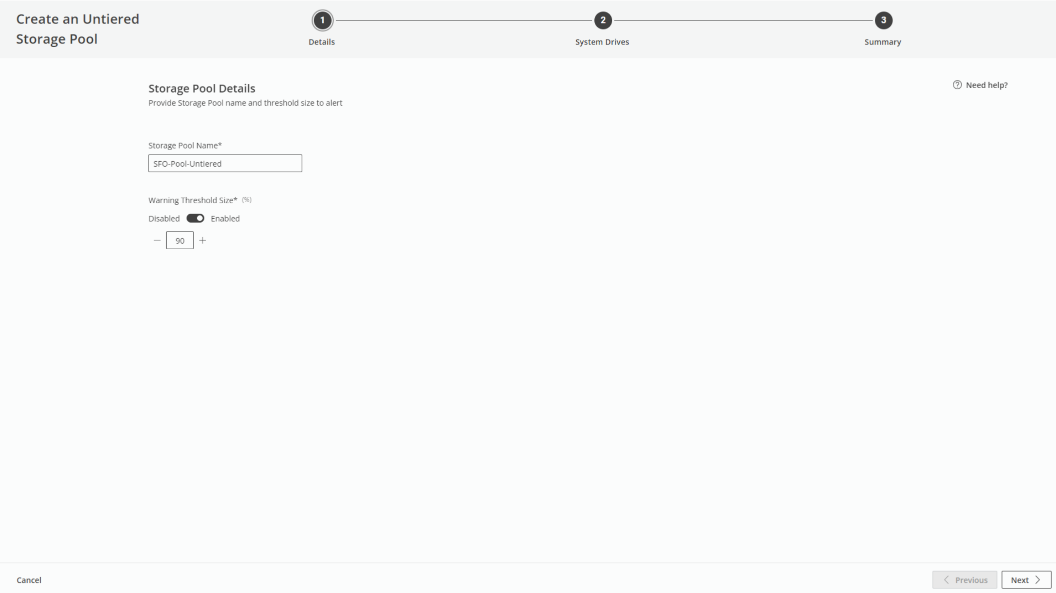
Before creating a storage pool, make sure system drives are enabled and ready to use.

Creating an untiered storage pool

Create an untiered storage pool containing system drives created on one or more storage systems in the same storage tier.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Storage Pools**, and then click **Create Storage Pool**.
2. On the **Choose Storage Pool Type** page, in the **An Untiered Storage Pool** tile, click **Create**.
3. In the **Details** page, complete the following information, and then click **Next**.
   a. Enter the storage pool name.
   b. Enable or disable the warning threshold. If you enable the threshold, set the threshold size. The default is 90.



Storage Pool Details

Provide Storage Pool name and threshold size to alert

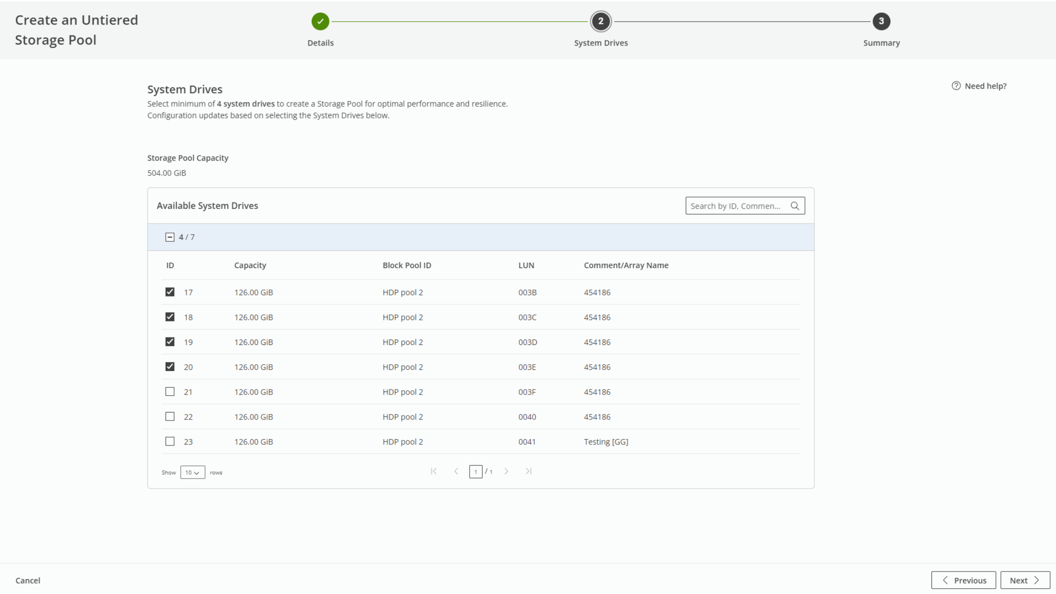
Storage Pool Name*: SFO-Pool-Untiered

Warning Threshold Size* (%): Disabled / Enabled (Enabled)

− 90 +

4. In the **System Drives** page, select four or more system drives to create a storage pool, and then click **Next**.

   An untiered storage pool cannot contain system drives with different disk types or RAID levels on the RAID system.



System Drives

Select minimum of **4 system drives** to create a Storage Pool for optimal performance and resilience.
Configuration updates based on selecting the System Drives below.

Storage Pool Capacity

504.00 GiB

Available System Drives

⊟ 4 / 7

	ID	Capacity	Block Pool ID	LUN	Comment/Array Name
☑	17	126.00 GiB	HDP pool 2	003B	454186
☑	18	126.00 GiB	HDP pool 2	003C	454186
☑	19	126.00 GiB	HDP pool 2	003D	454186
☑	20	126.00 GiB	HDP pool 2	003E	454186
□	21	126.00 GiB	HDP pool 2	003F	454186
□	22	126.00 GiB	HDP pool 2	0040	454186
□	23	126.00 GiB	HDP pool 2	0041	Testing [GG]

Show 10 rows   1 / 1

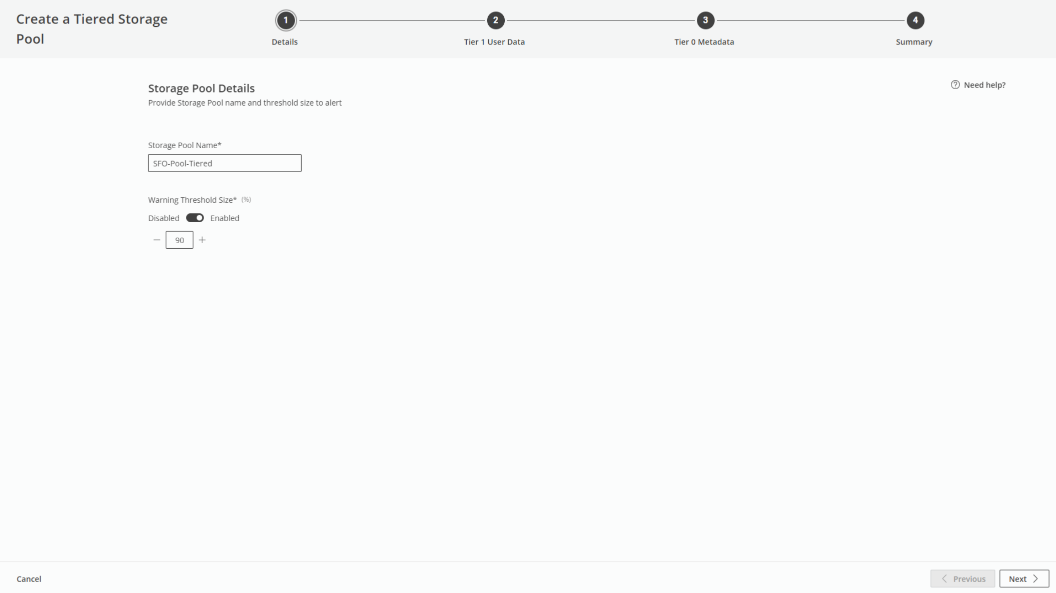
5. In the **Summary** page, review the storage pool configuration, and then click **Create**.

Creating a tiered storage pool

Create a tiered storage pool, which is a combination of system drives from high-performance storage, such as flash memory, and system drives from lower-performance storage, such as Serial Attached SCSI (SAS) or Near Line SAS (NL SAS).

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Storage Pools**, and then click **Create Storage Pool**.
2. On the **Choose Storage Pool Type** page, in the **A Tiered Storage Pool** tile, click **Create**.
3. In the **Details** page, complete the following information, and then click **Next**.
   a. Enter the storage pool name.
   b. Enable or disable the warning threshold. If you enable the threshold, set the threshold size. The default is 90.



Storage Pool Details
Provide Storage Pool name and threshold size to alert

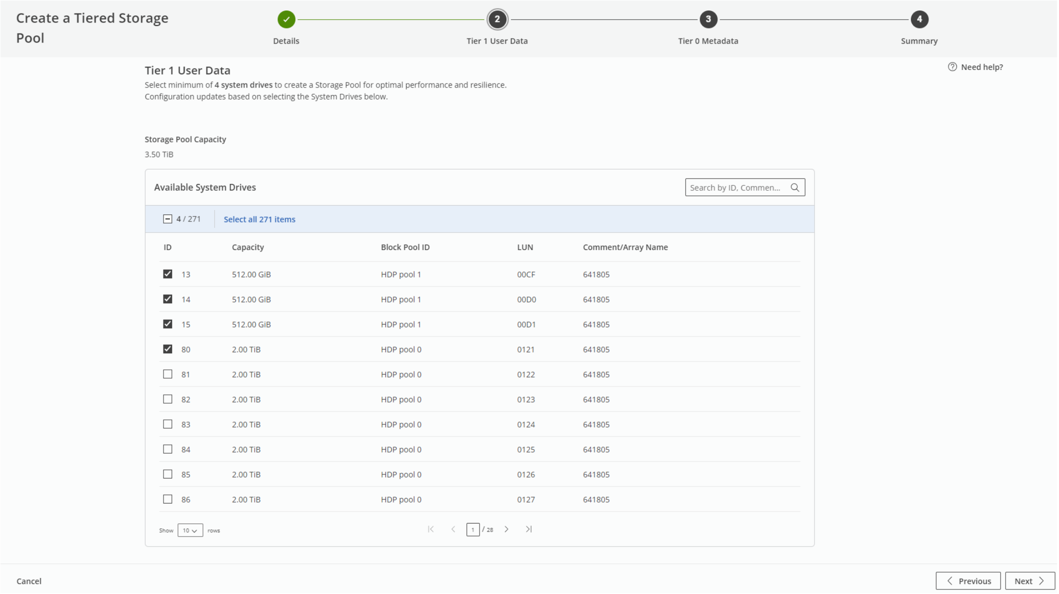
Storage Pool Name*: SFO-Pool-Tiered

Warning Threshold Size* (%): Disabled / Enabled (Enabled)

90

4. In the **Tier 1 User Data** page, select four or more system drives to create a storage pool, and then click **Next**.

   A tiered storage pool can contain system drives with different disk types if they are in different tiers on the RAID system. A tiered storage pool cannot contain system drives with different RAID levels on the RAID system.



Tier 1 User Data

Select minimum of **4 system drives** to create a Storage Pool for optimal performance and resilience.
Configuration updates based on selecting the System Drives below.

Storage Pool Capacity

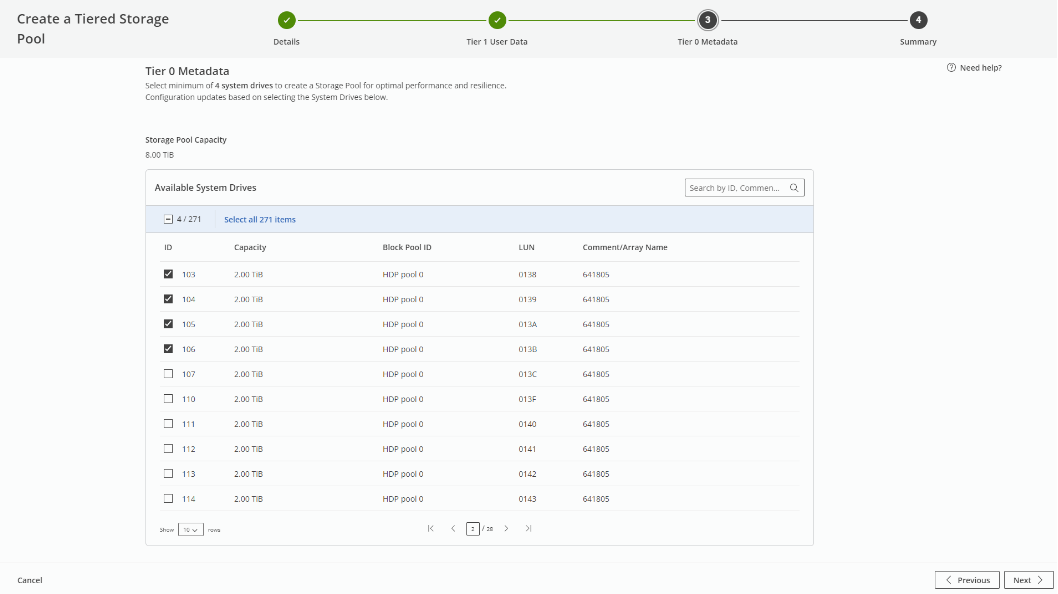
3.50 TiB

Available System Drives

4 / 271 Select all 271 items

ID	Capacity	Block Pool ID	LUN	Comment/Array Name
☑ 13	512.00 GiB	HDP pool 1	00CF	641805
☑ 14	512.00 GiB	HDP pool 1	00D0	641805
☑ 15	512.00 GiB	HDP pool 1	00D1	641805
☑ 80	2.00 TiB	HDP pool 0	0121	641805
□ 81	2.00 TiB	HDP pool 0	0122	641805
□ 82	2.00 TiB	HDP pool 0	0123	641805
□ 83	2.00 TiB	HDP pool 0	0124	641805
□ 84	2.00 TiB	HDP pool 0	0125	641805
□ 85	2.00 TiB	HDP pool 0	0126	641805
□ 86	2.00 TiB	HDP pool 0	0127	641805

5. In the **Tier 0 Metadata** page, select four or more system drives, and then click **Next**.



Tier 0 Metadata

Select minimum of **4 system drives** to create a Storage Pool for optimal performance and resilience.
Configuration updates based on selecting the System Drives below.

Storage Pool Capacity

8.00 TiB

Available System Drives

4 / 271 Select all 271 items

ID	Capacity	Block Pool ID	LUN	Comment/Array Name
☑ 103	2.00 TiB	HDP pool 0	0138	641805
☑ 104	2.00 TiB	HDP pool 0	0139	641805
☑ 105	2.00 TiB	HDP pool 0	013A	641805
☑ 106	2.00 TiB	HDP pool 0	013B	641805
□ 107	2.00 TiB	HDP pool 0	013C	641805
□ 110	2.00 TiB	HDP pool 0	013F	641805
□ 111	2.00 TiB	HDP pool 0	0140	641805
□ 112	2.00 TiB	HDP pool 0	0141	641805
□ 113	2.00 TiB	HDP pool 0	0142	641805
□ 114	2.00 TiB	HDP pool 0	0143	641805

6. In the **Summary** page, review the storage pool configuration, and then click **Create**.

Denying access to a storage pool

You can deny access to a storage pool if you no longer want to use it with the local VSP One File server or cluster.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Storage Pools**.

2. In the **Storage Pools** pane, select the storage pools for which you want to deny access, and then click **Deny access**.

   The storage pool is removed from the list. The access status of the system drives that are associated with the storage pool changes to **Not allowed**.
3. To restore the storage pool, navigate to **Provisioning** > **Capacity** > **System Drives**, select the system drives associated with the storage pool, and then click **Allow access**.

   The storage pool reappears in the storage pools list.

Expanding a storage pool

You can expand the storage pool by adding additional SDs to it. Before expanding a storage pool review the following information:

- Expand the storage pool by increasing the storage capacity by adding additional SDs to the storage system. The storage pool can grow up to a maximum capacity of 1 PiB (Pebibyte) or 256 SDs. When you expand the storage pool by adding SDs, this process does not interrupt client access to the storage resources.
- When you initially create a storage pool, it contains a single stripeset. Each time you expand the storage pool, you add another stripeset. You can add up to a maximum of 64 stripesets.
- The storage pool contains the file systems and allows users to manage settings that apply to all file systems within it. For example, File System Auto-expansion, the settings you apply to a storage pool can either enable or disable the expansion of all file systems in that pool. By default, a storage pool supports up to 32 file systems. File systems that you recently deleted and that remain in the recycle bin do not count toward this limit.
- If one tier of a tiered storage pool fills up before the other tier, you can expand only the filled tier without expanding the other. When expanding a tier, make sure the SDs you add have the same performance characteristics as those already in the tier. For example, don't add NL SAS (nearline SAS) SDs to a tier that already consists of flash drives.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Storage Pools**.
2. In the **Storage Pools** pane, select the storage pool that you want to expand, and then click **View**.
3. On the storage pool details page, click **Expand**.
4. Select the system drive that you want to add, and then click **Expand**.

Editing storage pool information

You can edit the storage pool name, warning threshold size, and set the file system auto-expansion.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Storage Pools**.
2. In the **Storage Pools** pane, select the storage pool that you want to edit, and then click **View**.

3. In the storage pool name pane, click the edit icon.
4. Edit the storage pool information, and then click **Save**.

Deleting a storage pool

You can delete the storage pool if it is no longer required.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Storage Pools**.
2. Select one or more storage pools that you want to delete, and then click **Delete**.
3. Click **Delete** to confirm.

Enterprise Virtual Servers

An Enterprise Virtual Server (EVS) enables client connections to file systems on physical nodes and manages virtualized file and administrative services. Each EVS is assigned unique network settings and storage resources, which provides the flexibility to logically partition access to shared storage resources.

Each physical node can host a maximum of 64 EVS instances. However, a clustered managed server can host a maximum of 64 EVS instances from all nodes in the cluster.

Using security contexts

An EVS is configured to use an individual or global security configuration. These security configurations are referred to as contexts. If an EVS is assigned an individual security context, the settings override the default global security context settings.

To use the individual security context, the VSP One File EVS Security license key is required.

Using an individual security context

An EVS that uses the individual security context is always treated as an individual unit even if it uses the same security context settings as another EVS.

The individual security context enables multiple groups, such as departments, customers, or organizations, to share storage resources, while ensuring that groups do not have access to the data for other groups.

For example, if a server or cluster has six EVS instances, you can define individual security contexts for two of the instances so that the virtual servers are assigned to Windows domains that are different than the server or cluster domain. For network clients, access to the file systems in the two virtual servers can then be restricted or allowed by using standard network security policies such as username or user group membership.

When an EVS that uses an individual security context migrates to a different server or cluster, the EVS retains all specified security settings.

When using an individual security context for an EVS, consider the following points:

- A system administrator with sufficient privileges can move a file system from one EVS to another, but a warning is issued if the security contexts of the source and destination EVS instances are different.
- Each EVS can be configured to connect to several external name servers, and each EVS can connect to different name services.
- You must configure each EVS separately even if the virtual server uses the same individual context settings as other virtual servers.

Using the global security context

If an EVS does not have an assigned individual security context, the EVS security context defaults to the global security context.

If an EVS is assigned the global security context and the EVS migrates to a different server or cluster, the EVS uses the global settings of the server or cluster to which it migrates.

⚠ **WARNING:** If an EVS is assigned to an individual security context and is then reconfigured to use the global security context, and the EVS was using a different Windows domain than the server or cluster, SMB names and SMB share names are no longer valid. This occurs because SMB names and share names are associated with a specific Windows domain, and the Windows domain name changed. In this scenario, you must remove all SMB names for the EVS and all SMB shares for the file systems in the EVS. Then, you must recreate the EVS SMB names and the SMB shares for the file systems in the EVS. For information about configuring SMB shares, see SMB shares (on page 53).

Creating an EVS

An EVS must be created and assigned an IP address before it is used. After you create an EVS, assign one or more file systems to provide file services.

Procedure

1. Navigate to **Provisioning** > **Virtual File Server** > **Enterprise Virtual Server** and then click **Create EVS**.
2. In the **Create EVS** dialog box, complete the following information, and then click **Create**.
   a. Enter the name of the EVS.

      The name can contain only alphanumeric characters and "-". The maximum number of characters is 15.

   b. Select the node where you want to create the EVS.
   c. Add an IP address with a prefix to assign to the EVS.

      For example, 172.12.12.12/20.

   d. Select one of the available ports for the EVS.
   e. (Optional) Enter an ID for a VLAN to associate with the EVS IP address.

      The valid values are 1-4095.

f. Click **Add**.

Changing the EVS security context to individual

Before you begin

Make sure that the EVS Security license key is installed.

To assign an individual security context to an EVS, you must first disable the EVS. Disabling the EVS unmounts all file systems and disconnects all users. After you enable the EVS again, you have to recreate the file access protocols, specify user and group access, and configure name services for the EVS.

Procedure

1. Navigate to **Provisioning** > **Virtual File Server** > **Enterprise Virtual Server**.
2. In the **Enterprise Virtual Server - EVS** pane, select the EVS, and then click **View**.
3. In the EVS name pane, click **Disable** and confirm the action, and then click the edit icon.
4. In the **EVS Security** list, change the EVS security context to **Individual**.
5. Click **Save**, and then click **Enable**.

Next steps

After changing the security context, complete the following information:

1. Recreate the SMB names, and reconfigure the SMB shares and NFS exports for the file systems in the EVS.
2. Specify the user and group access for the EVS.
3. Configure name services for the EVS.
4. If necessary, configure the EVS name space.

Adding a file system to an EVS

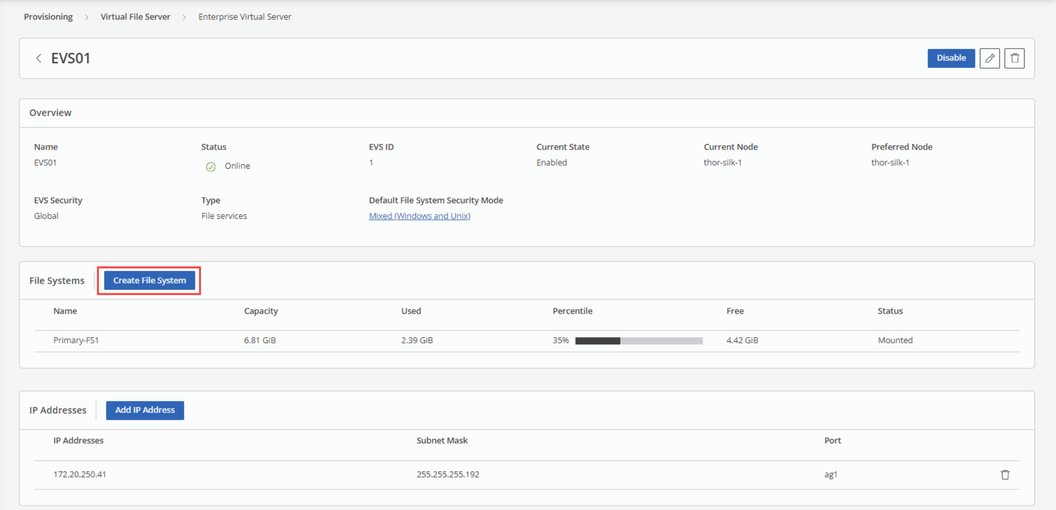
Before you begin

Make sure that there is an existing storage pool. For information about creating and managing storage pools, see Storage Pools (on page 25).

After an EVS is created, you can create a new file system on the EVS or relocate a file system currently assigned to another EVS to an EVS of your choice. Each EVS has a limit of 128 file systems.

Procedure

1. Navigate to **Provisioning** > **Virtual File Server** > **Enterprise Virtual Server**.
2. In the **Enterprise Virtual Server - EVS** pane, identify the EVS on which you want to create the file system, and then click **View**.
3. In the **File Systems** pane, click **Create File System**.



Provisioning > Virtual File Server > Enterprise Virtual Server
EVS01
Disable

Overview

Name	Status	EVS ID	Current State	Current Node	Preferred Node
EVS01	Online	1	Enabled	thor-silk-1	thor-silk-1

EVS Security	Type	Default File System Security Mode
Global	File services	Mixed (Windows and Unix)

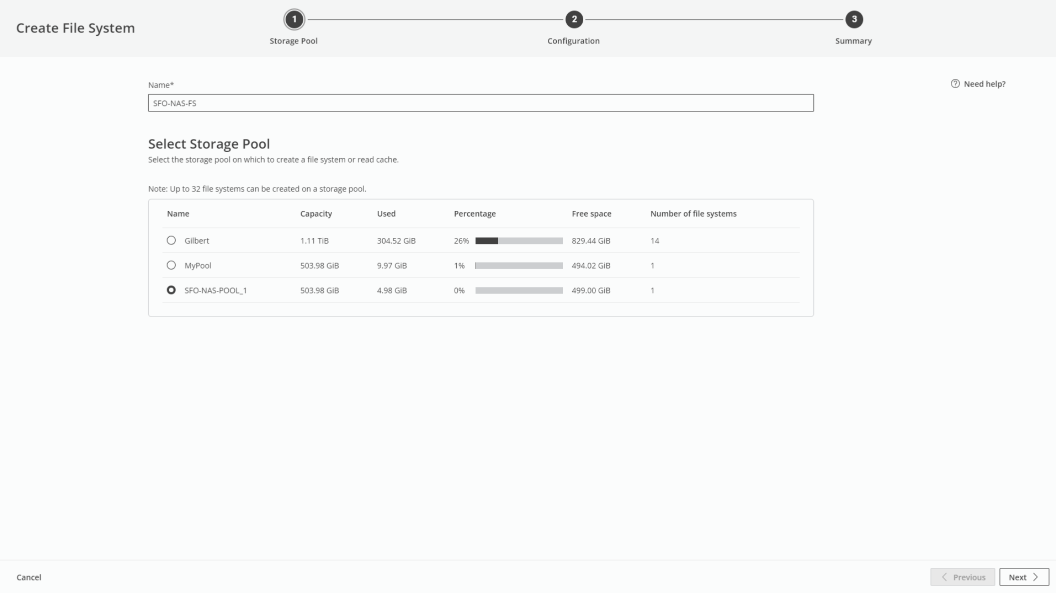
File Systems

Name	Capacity	Used	Percentile	Free	Status
Primary-FS1	6.81 GiB	2.39 GiB	35%	4.42 GiB	Mounted

IP Addresses

IP Addresses	Subnet Mask	Port
172.20.250.41	255.255.255.192	ag1

4. In the **Storage Pool** page of the **Create File System** wizard, enter the name for the file system, select the required storage pool, and then click **Next**.



Name*: SFO-NAS-FS

Select Storage Pool

Select the storage pool on which to create a file system or read cache.

Note: Up to 32 file systems can be created on a storage pool.

Name	Capacity	Used	Percentage	Free space	Number of file systems
○ Gilbert	1.11 TiB	304.52 GiB	26%	829.44 GiB	14
○ MyPool	503.98 GiB	9.97 GiB	1%	494.02 GiB	1
● SFO-NAS-POOL_1	503.98 GiB	4.98 GiB	0%	499.00 GiB	1

5. In the **Configuration** page, complete the following information, and then click **Next**.

   a. Select one of the following options to specify the file system size allocation:

      - Select **On Demand** to create a small file system, allowing it to expand to the size limit automatically.

        In the **Initial Size** and **Size Limit** boxes, enter the initial size for the file system and the size limit in GiB, TiB, or PiB.

      - Select **Now** to create the file system to the full size specified by the size limit. You can expand the file system a maximum of 1 TiB at a time.

        In the **Size Limit** box, enter the initial size for the file system in GiB, TiB, or PiB.

b. (Optional) Set the **Default Snapshot Retention** toggle to **Enable** to set a default retention period for file system snapshots. This toggle is disabled by default.

   Snapshots create near instantaneous, read-only images of an entire file system at a specific point in time. You can use snapshots to restore lost files without having to retrieve the data from backup media. For more information about creating and managing snapshots, see Snapshots (on page 65).

c. From the **Assign to EVS** list, select the EVS to assign to the file system.

d. (Optional) Set the **Object replication target** toggle to **Yes** to configure the file system as the intended target of an object replication.

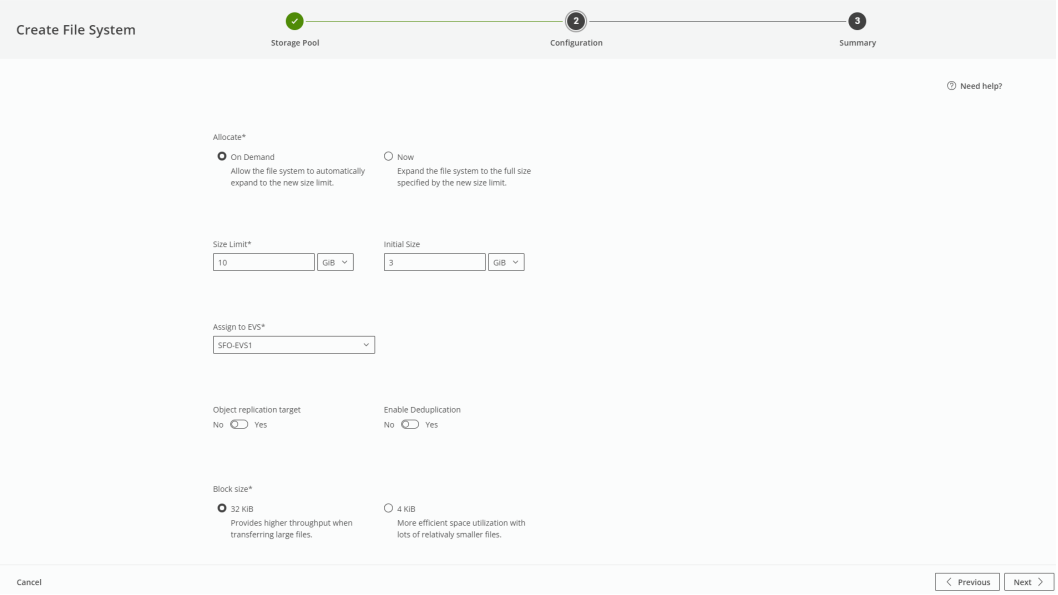
   Object replication uses policies and schedules to determine which file systems are replicated, where they are replicated, and when replication jobs are run. For more information about creating and managing object replication, see Replication (on page 76).

e. (Optional) Set the **Enable Deduplication** toggle to **Enable** to enable deduplication on the file system.

   Deduplication is a file system feature that incorporates enhancements to the file system and the application layer. Deduplication features the ability to reduce redundancy in stored data blocks. All data in the specified file system is scanned at intervals and duplicate blocks are removed, resulting in reclaimed disk space. All deduplication activity and the elimination of redundant blocks is transparent to the user.

   This option is available only if you are creating the file system on a Hitachi Virtual Storage Platform 5000 series managed server.

f. Select **32 KiB** or **4 KiB** as the block size for the file system.



Allocate*

● On Demand
Allow the file system to automatically expand to the new size limit.

○ Now
Expand the file system to the full size specified by the new size limit.

Size Limit* 10 GiB

Initial Size 3 GiB

Assign to EVS* SFO-EVS1

Object replication target No ○ Yes

Enable Deduplication No ○ Yes

Block size*

● 32 KiB
Provides higher throughput when transferring large files.

○ 4 KiB
More efficient space utilization with lots of relativaly smaller files.

6. In the **Summary** page, review the information about the file system, and then click **Create**. Alternatively, you can add another file system by clicking **Create & add another**.

Modifying an EVS

You can change the name, preferred node, and the security settings of an EVS. You can also add a new IP address to the EVS.

Procedure

1. Navigate to **Provisioning** > **Virtual File Server** > **Enterprise Virtual Server**.
2. In the **Enterprise Virtual Server - EVS** pane, identify the EVS that you want to edit, and then click **View**.
3. In the EVS name pane, click the edit icon.
4. Edit the name of the EVS and change the node where the EVS is located.

   The name can contain only alphanumeric characters and "-". The maximum number of characters is 15.
5. To add an IP address to the EVS, click **Add IP Address**, and then complete the following information:
   a. In the **Add IP address** dialog box, add the IP address, select a port, add an optional VLAN, and then click **Add**.

      Add the IP address with a prefix to assign to the EVS. For example, 172.12.12.12/20.

      Enter an ID for a VLAN to associate with the EVS IP address. The valid values are 1-4095.

   b. Click **Add**.
6. Click **Save**.

Deleting an EVS

You must disable an EVS before you can remove it. When you disable an EVS, all file systems are unmounted and all users are disconnected.

Before you begin

Make sure that all file systems in the EVS are unmounted.

Procedure

1. Navigate to **Provisioning** > **Virtual File Server** > **Enterprise Virtual Server**.
2. In the **Enterprise Virtual Server - EVS** pane, locate the EVS that you want to remove.
3. Review the status of the EVS. If the EVS status is online, select the EVS, and then click **Disable**.
4. Click **OK, Continue** to confirm.
5. Select the EVS, and then click **Delete**.
6. Click **Delete** to confirm.

Enabling an EVS

Enabling an EVS reconnects the users to the file systems configured within an EVS.

Procedure

1. Navigate to **Provisioning** > **Virtual File Server** > **Enterprise Virtual Server**.
2. In the **Enterprise Virtual Server - EVS** pane, locate the EVS that you want to enable.
3. Select the EVS, and then click **Enable**.

Disabling an EVS

Disabling an EVS unmounts all file systems within an EVS and disconnects the users from the file systems.

Before you begin

Make sure that the users are not connected to the file systems within the EVS.

Procedure

1. Navigate to **Provisioning** > **Virtual File Server** > **Enterprise Virtual Server**.
2. In the **Enterprise Virtual Server - EVS** pane, locate the EVS that you want to disable.
3. Select the EVS, and then click **Disable**.
4. Click **OK, Continue** to confirm.

File systems

A file system typically consists of files and directories. Data about the files and directories, along with other attributes, is the metadata. The data within the file system, both user data and metadata, is stored on the storage media of a storage system.

File system access protocols

The NAS server supports the SMB, NFS, and FTP protocols for client file access, and iSCSI for block-level access to storage. All supported protocols can be enabled or disabled.

The NAS server provides access to the same file space via multiple protocols, including NFS, SMB, and FTP. However, with iSCSI, Logical Units (LUs) are located on file systems, and thus, it is not possible to access folders and files through the NFS and SMB protocols.

These protocols, except FTP, require a license key for activation.

Creating a file system

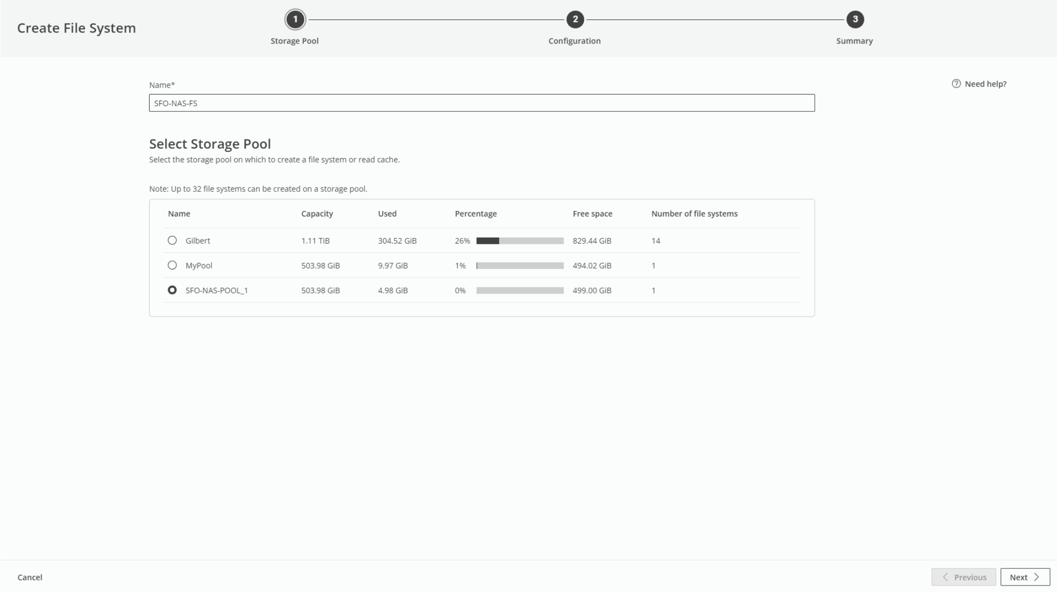
You can create one or more file systems.

Before you begin

A storage pool must be created before a file system can be created. To create a storage pool, see Creating a storage pool (on page 26).

Procedure

1. Navigate to **Provisioning** > **Capacity** > **File Systems**.
2. In the **File Systems** pane, click **Create File System**.
3. In the **Storage Pool** page of the **Create File System** wizard, enter the name for the file system, select the required storage pool, and then click **Next**.



Name*: SFO-NAS-FS

Select Storage Pool

Select the storage pool on which to create a file system or read cache.

Note: Up to 32 file systems can be created on a storage pool.

	Name	Capacity	Used	Percentage	Free space	Number of file systems
○	Gilbert	1.11 TiB	304.52 GiB	26%	829.44 GiB	14
○	MyPool	503.98 GiB	9.97 GiB	1%	494.02 GiB	1
●	SFO-NAS-POOL_1	503.98 GiB	4.98 GiB	0%	499.00 GiB	1

4. In the **Configuration** page, complete the following information, and then click **Next**.

   a. Select one of the following options to specify the file system size allocation:

      - Select **On Demand** to create a small file system, allowing it to expand to the size limit automatically.

        In the **Initial Size** and **Size Limit** boxes, enter the initial size for the file system and the size limit in GiB, TiB, or PiB.

      - Select **Now** to create the file system to the full size specified by the size limit. You can expand the file system a maximum of 1 TiB at a time.

        In the **Size Limit** box, enter the initial size for the file system in GiB, TiB, or PiB.

   b. (Optional) Set the **Default Snapshot Retention** toggle to **Enable** to set a default retention period for file system snapshots. This toggle is disabled by default.

      Snapshots create near instantaneous, read-only images of an entire file system at a specific point in time. You can use snapshots to restore lost files without having to retrieve the data from backup media. For more information about creating and managing snapshots, see Snapshots (on page 65).

   c. From the **Assign to EVS** list, select the EVS to assign to the file system.

   d. (Optional) Set the **Object replication target** toggle to **Yes** to configure the file system as the intended target of an object replication.

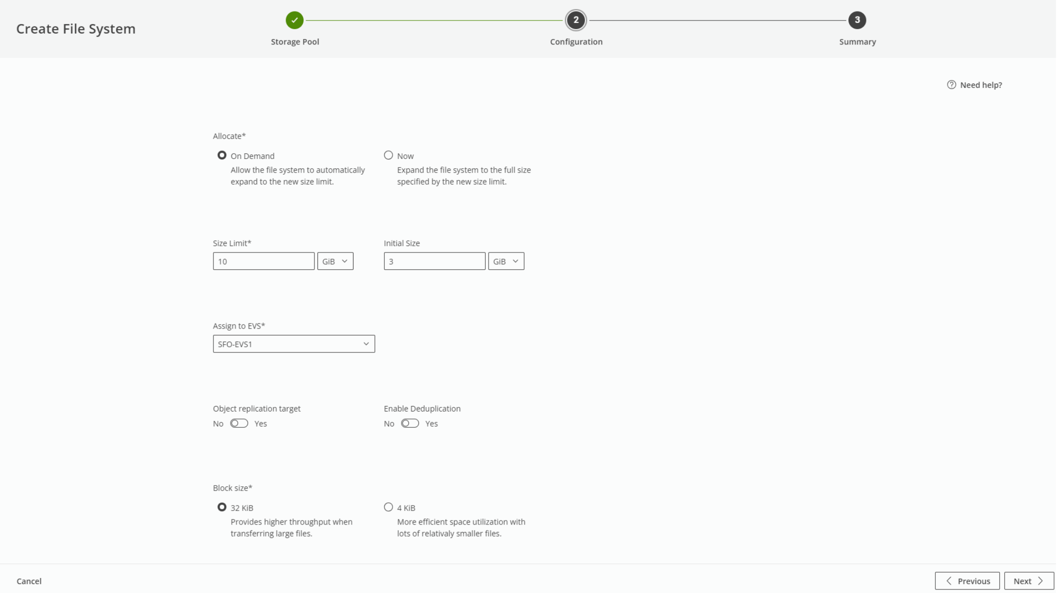
      Object replication uses policies and schedules to determine which file systems are replicated, where they are replicated, and when replication jobs are run. For more information about creating and managing object replication, see Replication (on page 76).

e. (Optional) Set the **Enable Deduplication** toggle to **Enable** to enable deduplication on the file system.

   Deduplication is a file system feature that incorporates enhancements to the file system and the application layer. Deduplication features the ability to reduce redundancy in stored data blocks. All data in the specified file system is scanned at intervals and duplicate blocks are removed, resulting in reclaimed disk space. All deduplication activity and the elimination of redundant blocks is transparent to the user.

   This option is available only if you are creating the file system on a Hitachi Virtual Storage Platform 5000 series managed server.

f. Select **32 KiB** or **4 KiB** as the block size for the file system.



Allocate*
● On Demand
Allow the file system to automatically expand to the new size limit.
○ Now
Expand the file system to the full size specified by the new size limit.

Size Limit* 10 GiB
Initial Size 3 GiB

Assign to EVS* SFO-EVS1

Object replication target: No ○ Yes
Enable Deduplication: No ○ Yes

Block size*
● 32 KiB
Provides higher throughput when transferring large files.
○ 4 KiB
More efficient space utilization with lots of relativaly smaller files.

5. In the **Summary** page, review the information about the file system, and then click **Create**. Alternatively, you can add another file system by clicking **Create & add another**.

Next steps

After the file system is created, you can configure additional settings such as enabling thin provisioning or setting usage thresholds. To configure additional settings, see Configuring a file system (on page 39).

Configuring a file system

Multiple configuration options are set when a file system is created. After the file system is created, you can configure additional settings such as enabling thin provisioning or setting usage thresholds. You can also modify existing settings such as the file system name or the default snapshot retention period.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **File Systems**.

2. Locate the file system that you want to configure, and then click **View**.
3. In the file system name pane, click the edit icon.
4. Configure or modify the following information, and then click **Save**.

   > **Tip:** The information that you can modify depends on the managed server associated with the file system and the file system status.

   - **Name**: Change the file system name.
   - **Deduplication**: Enable or disable deduplication for the file system. This setting defaults to the setting selected when the file system was created.
   - **Thin Provisioning**: Enable or disable thin provisioning for the file system. This setting is enabled by default.
   - **Security Mode**: Select a security mode. By default, the file system inherits the security mode from the parent file system. For information about security modes, see Security modes (on page 177).
     - **Inherited (Unix - supports Windows)**
     - **Mixed (Windows and Unix)**
     - **Unix (supports Windows)**
   - **Object Replication Target**: Enable or disable the file system as an object replication target.

     This setting defaults to the setting selected when the file system was created.
   - **Syslock**: Enable or disable syslocked mode for the file system. When syslocked mode is enabled for a file system, NDMP has full access to the file system and can write to it during a backup or replication, but the file system remains in read-only mode to clients using the file service protocols (NFS, FTP, and iSCSI).

     This setting is disabled by default.
   - **Transfer Access Points During Object Replication**: Enable or disable the transfer of shares and exports (access points) during an object replication. If enabled, the file system can transfer access points during an object replication. If disabled, the file system cannot transfer access points.

     This setting is disabled by default.
   - **Transfer XVLs as Links During Object Replication**: Enable or disable the transfer of migrated files as links during an object replication rather than transferring the file contents.

     This setting is disabled by default.

- **Default Snapshot Retention**: Enable or disable the default snapshot retention and set the retention interval period.

  This setting defaults to the setting selected when the file system was created.

  > **Caution:** You cannot disable this option or modify the retention interval after the option is enabled without the assistance of Hitachi Vantara Support.

- **Usage Thresholds**: Set warning and severe usage thresholds for the file system. Usage thresholds are expressed as a percentage of the space that has been allocated to the file system. When a threshold is reached, an event is logged and, depending on quota settings, an email might be sent.

  Set the **Warning** threshold to a high, but not critical, level of usage.

  Set the **Severe** threshold to a critical level of usage. This threshold represents a situation in which an out-of-space condition might be imminent.

  You can define both warning and severe thresholds for any of the following:

  - **Live file system**: The percentage threshold for space used by data.
  - **Snapshots**: The percentage threshold for file system snapshots.
  - **Entire file system**: The percentage threshold for the total of the live file system data and snapshots.

  To ensure that the live file system does not expand beyond the severe threshold, select **Do not allow the live file system to expand above its Severe limit**.

Formatting a file system

Formatting a file system prepares it for use by clients for data storage. File systems created through the File Administrator are formatted and mounted automatically. So, you do not need to perform this process frequently. Manually formatting a file system will delete data from the selected file system.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **File Systems**.
2. Locate the file system that you want to format, and then click **View**.
3. Review the status of the file system. If it is mounted, from the more actions menu, select **Unmount**, and then select **Format**.
4. In the **Format File System** dialog box, do the following:
   a. Acknowledge to proceed with formatting that will delete data from the selected file system.
   b. Select **32 KiB** or **4 KiB** as the block size for the file system.

      32 KiB: Provides higher throughput when transferring large files.

      4 KiB: Efficient space utilization management of numerous relatively smaller files.

   c. Select **Object replication target**, to configure the file system as the intended target of an object replication. Selecting this option formats the file system to allow shares and exports.

   d. Select **Support and enable dedupe**, to support and enable deduplication on the file system.

5. Click **Format**.

Mounting a file system

When a file system is formatted, it can be made available for sharing or exporting and can be accessed by network clients. Typically, file systems are auto-mounted. However, if auto-mounting fails, it is possible to mount the file system manually. The auto-mounting of a file system can fail in the following scenarios:

- The file system was not mounted when the server was shut down.
- Auto-mounting was disabled using the command line interface.
- A storage system failure caused the server to restart.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **File Systems**.
2. Select the file system that you want to mount, and then click **Mount**.

Expanding a file system

If auto-expansion was disabled when the file system was created, you can add storage capacity to a file system manually.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **File Systems**.
2. Locate the file system for which you want to expand the size.
3. From the more actions menu, click **Expand**.
   The Expand File System side panel displays the current size limit and capacity, with an option to expand the file system.
4. Expand the file system using one of the following options:
   - **On Demand**, to create a small file system, allowing it to expand to the size limit automatically.
   - **Now**, to create the file system to the full size specified by the size limit.
5. Enter the size limit in bytes using units like: GiB, TiB, or PiB.
6. Click **Expand**.

Unmounting a file system

Unmount a file system when it needs to be removed from service. For a client, the file system disappears. This action does not harm the file system or affect its data.

Note: You do not need to unmount a file system before shutting down or restarting a server or cluster. Suppose a mounted file system was unmounted when the server or cluster was shut down or restarted. In that case, the file system will not automatically be mounted when the server or cluster is restarted.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **File Systems**.
2. Select the file system that you want to unmount, and then click **Unmount**.

Deleting a file system

You can delete a file system only after unmounting the file system. Unmounting a file system disconnects all users from the file system.

Before you begin

Make sure that no users are connected to the file system.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **File Systems**.
2. Locate the file system that you want to delete.
3. Review the status of the file system. If it is mounted, select the file system, then click **Unmount**.
4. Click **Unmount** to confirm.
5. Select the file system, and then click **Delete**.
6. Click **Delete** to confirm.

Virtual volumes

Virtual volumes are discrete areas of storage that are divided from a file system. A virtual volume provides a simple method for allocating and controlling directories for projects, users, or groups. Capacity and number of files within a virtual volume can be controlled using quotas.

The terms *user* and *group* are used to indicate NFS or SMB users and groups.

Virtual volumes have the following characteristics:

- EVS / File System or Cluster Namespace: Shows the EVS and the file system in which the virtual volume is created.
- Name: A name or label by which the virtual volume is identified. This is same as a SMB share or NFS export rooted at the virtual volume root directory.
- Path: The directory at the root of the virtual volume.
- Email Contacts: A list of email addresses to which information and alerts about virtual volume activity are sent. The list can also be used to send emails to individual users.

Creating a virtual volume

Create a virtual volume from a file system to allocate and control directories for users or groups.

Before you begin

- Make sure that an Enterprise Virtual Server (EVS) is created.
- Make sure that a File System is created and mounted.
- Make sure that the user and group quotas are created.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Virtual Volumes**, and then click **Create Virtual Volume**.
2. In the **Configurations** page, complete the following information, and then click **Next**.
   - a. Select the EVS and file system where you want to create a virtual volume.
   - b. Enter the name for the virtual volume.
     - The name can be up 128 characters.
     - Do not use the characters ?*=+[];:/,<>\| in the name.
     - Do not use the name A$ as it is reserved for the Windows Event Viewer.
   - c. If you require a SMB share of the same name as this virtual volume, select the **Create a SMB Share with the same name as the Virtual Volume** checkbox.
   - d. If you require a NFS export with the same name as the virtual volume, select the **Create a NFS Export with the same name as the Virtual Volume** checkbox.
   - e. If there is a possibility that this new NFS export will overlap an existing export, select the **Allow exports to overlap** checkbox.
   - f. Enter the path to the directory at the root of the virtual volume or click **Browse** and navigate to the file system path. If the directory is new and does not exist, select **Create path if it does not exist**.
   - g. (Optional) Enter email addresses in **Email Contacts**.

     > **Note:** Email lists are limited to a maximum of 512 characters. When virtual volume reaches to quota limits the email contacts added here are notified. If no email contacts are specified for the virtual volume, the server generates events for quota warnings.
3. In the **Set Defaults** page, set the **User Quota Defaults** and **Group Quota Defaults**, and then click **Next**.
   - a. In **Usage**, enter the usage limit of the virtual volume for a user or a group. Additionally, select the usage in KiB, MiB, GiB, TiB or PiB from the list.
   - b. In **File Count**, set the file count limit of the virtual volume for a user or a group.
   - c. Select **Hard Limit** to ensure that the usage limit or the file count does not exceed.
   - d. Set the **Alert Warning** value to trigger a warning alert when the usage or file count limit reaches this value.

   e. Set the **Alert Severe** value to trigger a severe alert when the usage or file count limit reaches this value.
   f. Select the **Log Quota Events in the managed server's Event Log** checkbox to log all users or groups quota events in the VSP One File server event log.

   If you do not want to set the default user and group quota, click **Skip**.

4. In the **Summary** page, review the virtual volume configurations, and the click **Finish**. Alternatively, you can add another virtual volume by clicking **Create and add another**.

Modifying a virtual volume

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Virtual Volumes**.
2. In the **Virtual Volumes** pane, select the EVS and file system associated with the virtual volume from the list of EVS instances.
3. Locate the virtual volume that you want to modify, and then click **View**.
4. In the virtual volume name pane, click the edit icon, and modify the information that you want to change.
5. Click **Save**.

Deleting a virtual volume

Before you begin

You cannot delete a virtual volume that contains files.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Virtual Volumes**.
2. In the **Virtual Volumes** pane, select the EVS and file system associated with the virtual volume from the list of EVS instances.
3. Select one or more virtual volumes that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Quotas

Using a quota, you can allocate the maximum amount of disk space a user or group may use. It can be flexible in its adherence to the rules assigned and is applied per file system.

Quotas can be configured for users and groups on a file system or a virtual volume. Default quotas can be set for users and groups, and these defaults apply when specific quotas are not defined for users or groups in a file system or a virtual volume.

Quotas are also configured to limit the total size of a virtual volume. User or group quotas configured at the file system level can be different from the quotas configured at the virtual volume level.

Quotas on virtual volumes

Three types of quotas are maintained for each virtual volume:

- **Explicit User or Group Quotas**: A quota explicitly created to impose restrictions on an individual user or group, defining a unique set of thresholds.
- **Default User or Group Quotas**: A quota set automatically for all users and groups that do not have explicit quotas, set by defining a set of Quota Defaults (thresholds) for creating a quota automatically when a file is created or modified in the virtual volume.

  Default quotas for virtual volumes operate in the same way as those defined for file systems. User or Group quota defaults define a set of thresholds for creating a quota for a user or group the first time that user or group saves a file in the virtual volume.

  Initially, quota defaults are not set. When activity occurs in the virtual volume, it is tracked, but quotas are not automatically created. When at least one threshold is set to a non-zero value, a User or Group quota (as appropriate) is created for the owner of the directory at the root of the virtual volume.
- **Virtual Volume Quotas**. A virtual volume quota tracks the space used within a specific directory on the virtual volume. A quota can be explicitly created to define a set of thresholds restricting all operations in the virtual volume, unrelated to which user or group initiated them.

> **Note:** Quotas track the number and total size of all files. At specified thresholds, emails alert the list of contacts associated with the virtual volume and, optionally, *Quota Threshold Exceeded* events are logged. Operations that would take the user or group beyond the configured limit can be disallowed by setting hard limits.

When *Usage* and *File Count* limits are combined, the server will enforce the first quota to be reached.

Important information about virtual volumes and quotas

The server treats the virtual volume 'root' directory, together with all its sub-directories, as a self-contained file system. The virtual volume tracks its usage of space and number of files, to provide a way of monitoring file system usage. This tracking allows quotas to be imposed on disk space usage, as well as the total number of files.

Quotas can be set for the entire virtual volume, and on individual users, and on groups of users. Default user and group quotas can be defined, and in the absence of explicit user or group quotas, the default quotas apply.

The following caveats apply in measuring the virtual volume status against quota thresholds:

- **Metadata and snapshot files**. Neither file system metadata nor snapshot files count towards the quota limits.
- **Symbolic link calculation**. Files with multiple hard links pointing to them are included only once in the quota calculation. A symbolic link adds the size of the symbolic link file to a virtual volume and not the size of the file to which it links.

Adding a quota

You can create explicit user and group quotas, user and group quotas for virtual volumes, and quota for a virtual volume irrespective of user or groups.

Before you begin

- Make sure that an Enterprise Virtual Server (EVS) is created.
- Make sure that a file system is created and mounted.
- If you want to apply the quota to a virtual volume, make sure that you have created a virtual volume in the selected EVS / File System as described in Creating a virtual volume (on page 44).

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Quotas**, and then click **Create Quota**.
2. In the **Create Quota** pane, select the EVS and file system where you want to create the quota from the list of EVS instances.
3. In the **Virtual Volume** option, select one of the following:
   - To create a quota for only a virtual volume or for a user or a group accessing a virtual volume, select **Yes**, and then select a virtual volume from the list.
   - To create a quota for an explicit user or group, accept the default **No**.
4. Select one of the following quota types. The quota types available and the quotas that are created depend on the **Virtual Volume** option selection.

Choice	Description
User	Select this option and enter the user account name to create a user quota for the selected virtual volume or to create an explicit user quota. The valid input here is the `domain\user` for SMB or `user` for NFS.
Group	Select this option and enter the group account name to create a group quota for the selected virtual volume or to create an explicit group quota. The valid input here is the `domain\group` for SMB or `group` for NFS.
Virtual Volume	Creates virtual volume quota irrespective of a user or a group.

5. In **Usage**, enter the usage limit of the user or group or virtual volume. Additionally, select the usage in KiB, MiB, GiB, TiB or PiB from the list.
6. In **File Count**, set the file count limit of the user or group or virtual volume.

7. Select **Hard Limit** to make sure that the usage limit or file count limit is not exceeded.
8. Set the **Alert Warning** value to trigger a warning alert when the usage or file count limit reaches this value.
9. Set the **Alert Severe** value to trigger a severe alert when the usage or file count limit reaches this value.
10. Select the **Log Quota Events in the managed server's Event Log** checkbox to log all users or groups quota events in the NAS server event log.
11. Click **Create**.

Modifying a quota

You can modify only the usage and file count limits of an existing quota in the File Administrator.

Procedure

1. Navigate to **Provisioning** > **Capacity** > **Quotas**.
2. In the **Quotas** pane, select the EVS and file system associated with the quota from the list of EVS instances.
3. Locate the quota that you want to modify, and then click **Edit**.
4. In the **Quota Details** dialog box, modify the information that you want to change.
5. Click **Save**.

Deleting a quota

Procedure

1. Navigate to **Provisioning** > **File Services** > **Quotas**.
2. In the **Quotas** pane, select the EVS and file system associated with the quota from the list of EVS instances.
3. Select one or more quotas that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

NFS exports

The Network File System (NFS) protocol is a fundamental component of most UNIX networks, and it enables PC and UNIX workstations access files on the other system. This section describes how to set up NFS exports, the prerequisites, and supported client protocols.

The VSP One File server implements the file-serving functions of an NFS server, providing normal file-serving functions such as:

- Managing exports.
- Handling files, including reading, writing, creating, and linking files.
- Manipulating directories, including creating, reading, and searching directories.

- Enabling byte-range locking for files.
- Managing file access control (permissions).
- Managing file and directory attributes, including size and access time.
- Supporting hardlinks and symbolic (soft) links.

Supported clients and protocols

The VSP One File server supports all clients compliant with NFS v2, v3, v4, and v4.1 standards. NFS v2, v3, v4, and v4.1 are supported over TCP. The following table summarizes the supported versions of NFS and other UNIX protocols:

Protocol	Supported versions
NFS	v2, v3, v4, and v4.1
Port Mapper	v2
Mount	v1 and v3
Network Lock Manager (NLM)	v1, v3, and v4
Network Status Monitor (NSM)	v1

⚠ **Caution:** While it is possible to use UDP with NFS on versions 2 and 3, it is not recommended due to inherent risks. On the VSP One File server, UDP is not automatically presented as a transport option for the NFS service by the Port Mapper service.

Sharing resources with NFS clients

Set the NFS version and create exports for sharing resources with the NFS client.

Set the NFS version

The VSP One File server supports NFS versions 2, 3, 4, and 4.1.

Procedure

1. Navigate to **Provisioning** > **File Services** > **NFS Exports**.
2. In the **NFS Exports** pane, from the more actions menu, select **NFS Setup**.
3. In the **Max Supported NFS Version** list, select the NFS version.

   Note: If you change the NFS version, the change applies to all NFS exports across all EVS instances.

4. Click **Save**.

Creating an NFS export

Create an NFS export to provide clients with access to files on the server. You can create one or more NFS exports.

Procedure

1. Navigate to **Provisioning** > **File Services** > **NFS Exports**.
2. In the **NFS Exports** pane, click **Create Export**, and complete the following configuration information. For more information about the configuration fields, see Additional information about adding an NFS export (on page 50).
   - Select the EVS and associated file system to which the NFS export will provide access.
   - Enter the NFS export name.
   - Enter the path to the source directory that you want to export. To locate an existing directory, click **Browse**.

     If the file system is mounted read-only, you cannot create a new directory. Select an existing directory path.
   - Select the optional path settings:
     - **Create path if it does not exist**: Creates the path automatically.
     - **Allow this export path to overlap other exports**: Allows the export path to overlap other exports.
   - Select an option from **Show Snapshots** list to show or hide snapshots.
   - Select a value from the **Local Read Cache** to enable or disable read caching.
   - Select an option from the **Transfer to Object Replication Target** list to enable or disable transferring NFS exports to recovered file systems.
   - Enter the IP addresses, host names, or NIS netgroups of authorized NFS clients in the **Access Configuration** box.

     To secure and control access to exports, follow these guidelines when specifying the IP addresses, Guidelines for entering values in the Access Configuration field (on page 211)
3. Click **Create**.

Additional information about adding an NFS export

The following table describes additional information required to create an NFS export:

Item	Description
Path Options	Determines the path options: ▪ Create path if it does not exist: Select to create the path automatically when it does not exist (filesystems only). Automatically created directories are owned by the root user and group (UID:0 / GID:0) and have full permissions (read, write, and execute). You can create these directories using the SMB or NFS protocols, or explicitly grant the appropriate permissions after creation using this option. ▪ Allow this export path to overlap other exports: Select to allow the export path to overlap other exports. This option is useful if you plan to create nested exports in the future. By choosing this option, you can subsequently export subdirectories of the root directory and make each of them accessible to different groups of users. For example, you can export the root directory of a volume and share it only with managerial staff. **Note:** If the file system is mounted read-only, for example it is an object replication target, it is not possible to create a new directory. Select a path to an existing directory.
Show snapshots	Determines how to show snapshots. ▪ Show and Allow Access, to display and allow access to snapshots. ▪ Hide and Allow Access, to hide snapshots, but still allow access to the hidden snapshots. ▪ Hide and Disable Access, to hide and not allow access to snapshots.

Item	Description
	Note: For this change to become effective on NFS clients, all NFS clients must unmount and then remount the export, or the administrator must run the `'touch.'` command in the root directory of the export.
Local Read Cache (file systems only)	Allows caching of files or cross file system links from the file system to which this export points: ▪ Do not cache files (not licensed), does not allow read caching of files and cross file system links. The read caching feature requires a license. ▪ Cache all files, allows caching of files and cross file system links in the file system of the export. Cross file system links are local links that point to a data file in a remote file system. The remote file system can be on a remote server or storage device. ▪ Cache cross-file system links, allows only cross file system links to be cached Local read caching is not supported for NFS v4 and v4.1 clients.
Transfer to Object Replication Target (file systems only)	Determines whether the export should be activated when the replication target of the file system associated with this export is switched to read-write mode. Only those NFS exports marked as transferable will be imported. ▪ Use FS default, defaults to the setting for the file system Transfer Access Points During Object Replication setting (enabled or disabled). ▪ Enable, transfers NFS exports to recovered file systems. ▪ Disable, deactivates NFS export transfers to recovered file systems.
Access Configuration	To secure and control access to shared resources, follow these guidelines when

Item	Description
	specifying the IP addresses of the clients that can access them. Guidelines for entering values in the Access Configuration field (on page 211)

Modifying NFS export information

Procedure

1. Navigate to **Provisioning** > **File Services** > **NFS Exports**.
2. In the **NFS Exports** pane, select the EVS associated with the export from the list of EVS instances.
3. Locate the export that you want to modify, and then click **View**.
4. In the export name pane, click the edit icon, and modify the information that you want to change.
5. Click **Save**.

Deleting an NFS export

Procedure

1. Navigate to **Provisioning** > **File Services** > **NFS Exports**.
2. In the **NFS Exports** pane, select the EVS associated with the export from the list of EVS instances.
3. Select one or more exports that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

SMB shares

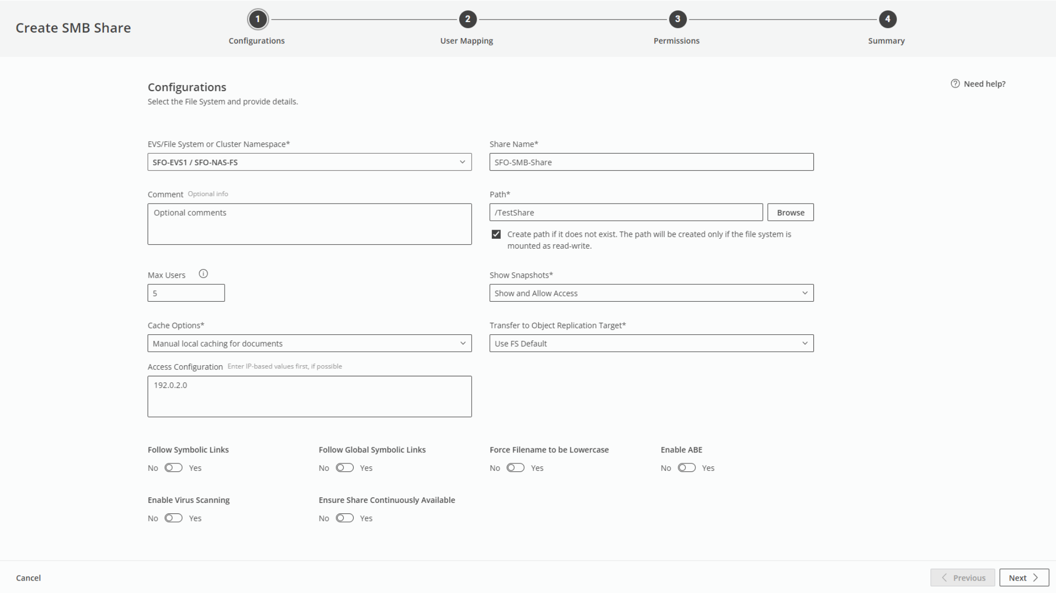
SMB shares allow file system access from Windows and other clients that support the SMB protocol.

Creating an SMB share

Create an SMB share to provide clients with access to files on the server. You can create one or more SMB shares.

Procedure

1. Navigate to **Provisioning** > **File Services** > **SMB Shares**.
2. In the **SMB Shares** pane, click **Create Share**.
3. In the **Create SMB Share** wizard, complete the following configuration information, and then click **Next**. For more information about the configuration fields, see Additional information about creating an SMB share (on page 56).



Configurations

Select the File System and provide details.

EVS/File System or Cluster Namespace*: SFO-EVS1 / SFO-NAS-FS

Share Name*: SFO-SMB-Share

Comment (Optional info): Optional comments

Path*: /TestShare

☑ Create path if it does not exist. The path will be created only if the file system is mounted as read-write.

Max Users: 5

Show Snapshots*: Show and Allow Access

Cache Options*: Manual local caching for documents

Transfer to Object Replication Target*: Use FS Default

Access Configuration (Enter IP-based values first, if possible): 192.0.2.0

Follow Symbolic Links: No ○ Yes

Follow Global Symbolic Links: No ○ Yes

Force Filename to be Lowercase: No ○ Yes

Enable ABE: No ○ Yes

Enable Virus Scanning: No ○ Yes

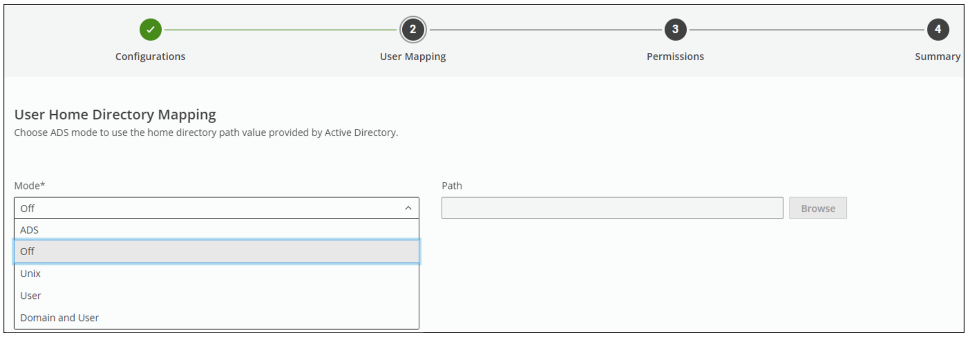
Ensure Share Continuously Available: No ○ Yes

- Select the EVS and associated file system or cluster namespace to which the SMB share will provide access.
- Enter the SMB share name.

  Enter optional additional information for the SMB share in the **Comment** box. The comment should be meaningful to you and other users.
- Enter the directory path on the file system that you want to share. To locate an existing directory, click **Browse**.
  - To automatically create the path select the **Create path if it does not exist**.
- Enter the maximum number of users who can access the share simultaneously. By default, a share has unlimited access.

  > **Note:** This setting limits the number of users that can access a share. It does not provide security restrictions.
- Select an option from **Show Snapshots** list to show or hide snapshots.
- Select a value from the **Cache Options** list to alter the caching option (Offline Files Access).
- Select an option from the **Transfer to Object Replication Target** list to make the SMB share transferable.
- Enter the IP addresses of the clients who can access the share in the **Access Configuration** box. To secure and control access to the share, follow these guidelines when specifying the IP addresses, Guidelines for entering values in the Access Configuration field (on page 211).
- Enable the following configuration options based on your requirements: **Follow Symbolic Links**, **Follow Global Symbolic Links**, **Force File name to be Lowercase**, **Enable ABE**, **Enable Virus Scanning**, and **Ensure Share Continuously Available**.

4. In the **User Mapping** page, complete the following information, and then click **Next**.



User Home Directory Mapping

Choose ADS mode to use the home directory path value provided by Active Directory.

Mode*: Off

Path:

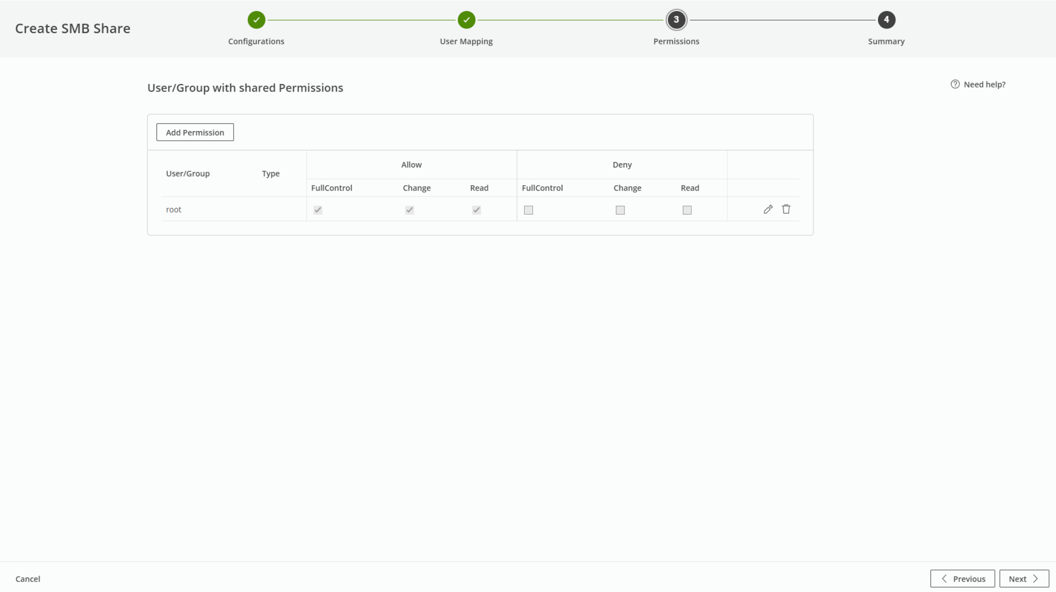
- Select one of the following modes for creating individual user home directories:
  - **ADS:** Creates user home directories using the information provided by the Active Directory server. If selecting this option, do not specify a **Path**.
  - **Off:** Disables automatic creation of home directories for users on the share. This is the default option.
  - **Unix:** Create the home directory by converting the user's UNIX user name to lowercase.
  - **User:** Creates the home directory by converting the user's Windows username to lowercase. The Windows domain name associated with the user is ignored in this process. For example, if a user is `DOMAIN\John Smith`, the home directory is created as `john_smith`.
  - **Domain and User:** Creates the home directory by generating a directory named according to the user's Windows domain name. Following this, the Windows username of the user is converted to lowercase, creating a sub-directory under that name. For example, if a user is `DOMAIN\John Smith`, the home directory is created as `domain\john_smith`.
- Enter the path for creating home directories.

  Home directories for each user are created in the specified **Path** relative to the share root. The share root must be specified without a leading backslash(`\`). If this field is left blank, the user home directories are created directly in the share root.

  By default, only one share per file system can be configured for home directories. The **`smb-home-directory`** command can be used to relax this restriction. However, it's important to avoid configuring conflicting home directories.

  For example, there will be no conflict between a share using the path `\home1` and another share using the path `\home2` regardless of the configured home directory paths. If a share is set with the path `\` along with a default home directory path, it can clash with a share using the path `\dir` and a default home directory path.

5. In the **Permissions** page, assign the access permissions to individual users and groups within the SMB share, and then click **Next**. If you select **FullControl for Allow**, the user or group can perform all actions. By default, a share has full access.



User/Group with shared Permissions

User/Group	Type	Allow			Deny			
		FullControl	Change	Read	FullControl	Change	Read	
root		☑	☑	☑	□	□	□	

6. Review the information about the SMB share, and then click **Create**. Alternatively, you can add another SMB share by clicking **Create & add another**.

Additional information about creating an SMB share

The following table describes the additional information required to create an SMB share:

Field	Description
Show Snapshots	▪ Show and Allow Access: Shows and allows access to snapshots. ▪ Hide and Allow Access: Hides snapshots, but allows access to the hidden snapshots. ▪ Hide and Disable Access: Hides and does not allow access to snapshots.
Cache Options	To alter the caching option (Offline Files Access), select the new value from the Cache Options list. ▪ Manual Local Caching for Documents. The manual mode permits the user to specify individual files required for offline access. This operation guarantees a user can obtain access to the specified files whether online or offline. ▪ Automatic Local Caching for Documents. This automatic mode is applied for all non-executable files on the entire share. When a user accesses any non-executable file in this share, it is made available to the user for offline access. This operation does not guarantee that a user can access all the non-executable files because only those files that have been used at least once are cached. Automatic can also be defined for programs.

Field	Description
	▪ Automatic Local Caching for Programs. The Automatic mode is applied for all executable files on the entire share. When a user accesses any executable file in this share, it is made available to the user for offline access. This operation does not guarantee that a user can access all the executable files because only those executable files that have been used at least once are cached. ▪ Local Caching Disabled. No caching of files or folders occurs.
Transfer to Object Replication Target	When a file system is recovered from a snapshot, one of the final steps is to import the SMB shares found in the snapshot representing the selected version of the file system. Only those SMB shares marked as transferable are imported. Specify one of the following: ▪ Use FS default: Defaults to the setting for the file system Transfer Access Points During Object Replication setting (enabled or disabled). ▪ Transfer: SMB shares are transferred to recovered file systems. ▪ Do not transfer: SMB shares are not be transferred to recovered file systems.
Access Configuration	IP addresses of the clients who can access the share. Up to 5,957 characters allowed in this field. To secure and control access to shared resources, follow these guidelines when specifying the IP addresses of the clients that can access them. Guidelines for entering values in the Access Configuration field (on page 211).
Follow Symbolic Links	Enables the following of symlinks on the share.
Follow Global Symbolic Links	Enables to follow global (absolute) symlinks using the Microsoft® DFS mechanism for this share.
Force Filename to be Lowercase	Forces all filenames generated on this share to be lowercase. This is useful for interoperability of UNIX applications.
Enable ABE	Access-based Enumeration (ABE) is a Microsoft® feature that displays only the files and folders that a user has permissions to access. When a user does not have access permissions for a file or a folder, Windows® hides the folder from the user. This feature is active only in an SMB share. **Note:** Enabling ABE can impact SMB performance.
Enable Virus Scanning	Enabling virus scanning for an SMB share scans the files within the share for viruses when a user accesses the file.

Field	Description
	Virus scanning can be enabled for each EVS. If virus scanning is enable for the EVS that hosts the file system pointed to by the share, it will be automatically enabled when the share is created. If you have not enabled virus scanning, you can enable it later for each EVS.
Ensure Share Continuously Available	Enables persistent file handles and transparent failover on the SMB share. Windows-based clients can continuously access the SMB share if a network or cluster node fails. For example, if one cluster node fails, the client transparently migrates to another cluster node without any interruption to the client applications. This SMB3 option is available only in a clustered environment of more than one cluster node, and is disabled by default. **Note:** Share Continuous Availability should be enabled only where required, like with Microsoft Hyper-V or Microsoft SQL Server, as it affects SMB performance. It is recommended to disable DDNS on the server when using this feature. If the file system is designated as an object replication target, continuous availability is only achieved after promoting the file system.

Use the following guidelines to enter the IP addresses of users who can access the share.

Guidelines for entering values in the Access Configuration field

Use the following guidelines to enter the IP addresses of users who can access the share.

Value	Description
Blank or `*` Partial addresses using wildcards. Example: `10.168.*.*` Clients with matching addresses can access the share.	All users can access the share.
Specific addresses Example: `10.168.20.2`	Users with the specified IP address can access the share.
Specific address range Example: `10.168.20.0/16`	Users with an IP address within the specified IP address range (10.168.20.0 to 10.168.20.255) can access the share.
Partial addresses using wildcards Example: `10.168.*.*`	Users with matching addresses can access the share.

Modifying SMB share information

Procedure

1. Navigate to **Provisioning** > **File Services** > **SMB Shares**.
2. In the **SMB Shares** pane, select the EVS associated with the share from the list of EVS instances.
3. Locate the share that you want to modify, and then click **View**.
4. In the share name pane, click the edit icon, and modify the information that you want to change.
5. Click **Save**.

Deleting an SMB share

Procedure

1. Navigate to **Provisioning** > **File Services** > **SMB Shares**.
2. In the **SMB Shares** pane, select the EVS associated with the share from the list of EVS instances.
3. Select one or more shares that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Controlling access to shares using permissions

Access to shares is restricted through a combination of share-level and file-level permissions. These permissions determine the extent to which users can view and modify the contents of the shared directory. When users request access to a share, their share-level permissions are checked. If authorized to access the share, their file-level permissions are checked. If the share-level permissions differ from the file-level permissions, then more restrictive permissions are applied, as described in the following table, where [a] = “allowed” and [d] = “denied”:

Activity	Read	Change	Full
View the names of files and subdirectories	a	a	a
Change to subdirectories of the shared directory	a	a	a
View data in files	a	a	a
Run applications	a	a	a
Add files and subdirectories	d	a	a
Change data in files	d	a	a
Delete files and subdirectories	d	a	a

Activity	Read	Change	Full
Change permissions on files or subdirectories	d	d	a
Take ownership of files or subdirectories	d	d	a

One of the features of SMB is the ability to assign rights to computer accounts. A computer account is generated automatically by the operating system and registered in Active Directory. It can be used for authentication within a domain. Computer account authentication can be done only by an application which has built-in support. For example, Hyper-V server allows storing virtual machines on remote shares. Such shares should allow full access for the computer account of a computer running Hyper-V server.

When configuring access to a share, it is only possible to add users or groups that are:

- Known to domain controllers.
- Seen by the server on the network.

  When a user is granted access to a shared file, the user's access level is determined by the most permissive access level they have. For example, if a user has read access to a file, but also belongs to a group with change access to the same file, the user will have change access to the file.

Adding or changing SMB share access permissions

Procedure

1. Navigate to **Provisioning** > **File Services** > **SMB Shares**.
2. In the **SMB Shares** pane, select the EVS associated with the share from the list of EVS instances.
3. Locate the share for which you want to add or change the access permission, and then click **View**.
4. In the **SMB Share** pane, in the **Share Permissions** section, you can add permissions for a new user or group or change the permissions for an existing user or group.
   - To add permission for a new user or group:
     a. Click **Add Permissions** and enter the name of the new user or group.
     b. Select the **Allow** or **Deny** check boxes to set the appropriate permissions. If you select **FullControl** for Allow, the user or group can perform all actions.
     c. Click the checkmark icon to save the changes.
   - To change the permissions for an existing user or group:
     a. Select the user or group for which you want to change permissions.
     b. Click the edit icon, and select the **Allow** or **Deny** check boxes to set the appropriate permissions. If you select **FullControl** for **Allow**, the user or group can perform all actions.
     c. Click the checkmark icon to save the changes.

iSCSI Logical Units

An iSCSI Logical Unit (LU) is a type of block storage that can be accessed by iSCSI initiators as a locally attached hard disk. An LU is stored as a file on the server file system. iSCSI LUs are bound in size using the server size management tools, including virtual volumes and quotas. LUs are created with a specific initial size but can be expanded over time, as demand requires.

A file must have an `.iscsi` extension to identify it as an iSCSI LU. However, apart from this extension there is no other way to determine that a file represents an LU.

Note: Hitachi Vantara recommends that all iSCSI LUs are placed within a directory, for example `/.iscsi/`. This provides a single repository for the LUs in a known location.

After an LU is created and the iSCSI domain name is set, an iSCSI Target is created to allow access to the LU. A maximum of 32 LUs can be configured for each iSCSI Target. For more information on iSCSI Target, see iSCSI targets (on page 157).

Logical unit security

As LUs are files, they can be accessed over other protocols, such as SMB and NFS. This renders LUs vulnerable to malicious users who can modify, rename, delete or otherwise affect them.

Caution: Hitachi Vantara recommends setting sufficient security on either the LU file, the directory in which it resides, or both, to prevent unwanted accesses.

Concurrent access to logical units

The iSCSI implementation of the server allows multiple initiators to connect to a single LU, which is necessary for applications and operating systems that support, or rely upon, concurrent file system access. However, concurrent access can be detrimental to a client machine when the client is unaware of other clients accessing the file system. For example:

- Simultaneous independent updates to the same files.

  Scenario: Two independent Microsoft Windows clients can connect to the same LU, containing an NTFS file system.

  Result: If allowed to simultaneously and independently modify data, metadata, and system files, conflicting disk updates will quickly corrupt the file system.

- Simultaneous access to separate partitions.

  Scenario: An LU contains two distinct NTFS partitions, with one Microsoft Windows client connected only to the first partition, and another connected only to the second partition.

  Result: As a Microsoft iSCSI client attempts to mount each partition it encounters on the LU, a Microsoft Windows client mounting an NTFS partition update system files on all partitions; therefore, even though the two clients are accessing separate partitions within the LU, both clients updates system files on both partitions, causing conflicting system file updates, causing one or both of the clients to fail.

Taking snapshots of logical units

The contents of an iSCSI LU are controlled entirely by the client accessing the contents. The server cannot interpret the file systems or other data contained within an LU in any way. Therefore, the server has no knowledge of whether the data held within an iSCSI LU is in a consistent state. This introduces a potential problem when taking a snapshot of an LU.

For example, when a client creates a file, the client must also insert the file name to the host directory. This means that more than one write is required to complete the operation. If the server takes a snapshot after the file object has been created, but before its name has been inserted into the directory, the file system contained within the snapshot will be inconsistent. If another client were to view the snapshot copy of the file system, the client would see a file object without a name in a directory. This example provides only one possible scenario for snapshot inconsistency.

⚠ **Caution:** Hitachi Vantara recommends that prior to taking a snapshot of an iSCSI LU, all applications should be brought into a known state. A database, for example, should be quiesced. Disconnecting the iSCSI initiators from the LUs undergoing snapshot is also recommended. This guarantees that all pending writes are sent to the LU before the snapshot is taken.

VSP One File server supports creation of snapshots of the attached storage systems with Microsoft® Volume Shadow Copy Service (VSS). Snapshots created by VSS are exported as iSCSI logical units.

Volume full conditions

Unexpected volume full conditions can occur with iSCSI LUs, as shown by the following two examples:

- Directly Attached Disks: When a client uses a directly attached disk, it can monitor the amount of available free space. If a partition contains no free space, the client can return a Volume Full condition. In this way, the client can ensure against file system corruption due to running out of disk space part way through an operation.
- iSCSI LU: On iSCSI LUs with snapshots enabled, old data is preserved, not overwritten. Therefore, overwriting an area of an LU causes the server to allocate extra disk space, while using no extra disk space within the client's partition, causing a Volume Full condition to occur, even when partitions within the LU contain free space. In this scenario, a client may receive a Volume Full condition part-way through an operation, causing file system corruption. Although this corruption is fixable, this situation should be avoided.

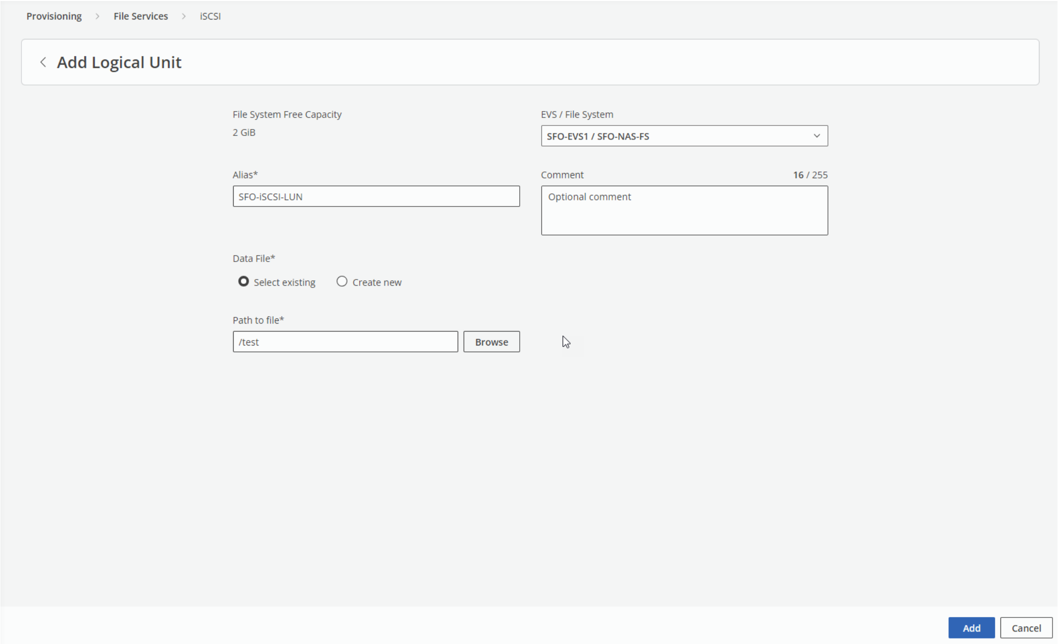
  Note: Hitachi Vantara recommends allocating sufficient disk space on the server to contain all iSCSI LUs and snapshots, as well as careful monitoring of free disk space.

Adding an iSCSI logical unit

Procedure

1. Navigate to **Provisioning** > **File Services** > **iSCSI**, and then click **Add Logical Unit**.

2. In the **Add Logical Unit** pane, select the EVS and the file system where you want to create the logical unit.



Provisioning > File Services > iSCSI

Add Logical Unit

File System Free Capacity
2 GiB

EVS / File System
SFO-EVS1 / SFO-NAS-FS

Alias*
SFO-iSCSI-LUN

Comment 16 / 255
Optional comment

Data File*
● Select existing ○ Create new

Path to file*
/test

3. Enter a name (alias) for the logical unit.
4. (Optional) In **Comments**, enter additional information about the logical unit.

   The comments box supports a maximum of 255 characters.
5. Select one of the following options to add a data file, and then click **Add**.
   - To use an existing logical unit, provide the location of the logical unit data file.
   - To create a new logical unit data file, enter a path to the logical unit data file to be created, the new file name, and the file size.

Modifying an iSCSI logical unit

Procedure

1. Navigate to **Provisioning** > **File Services** > **iSCSI**.
2. In the **iSCSI Logical Units** pane, select the EVS associated with the logical unit from the list of EVS instances.
3. Locate the logical unit that you want to modify, and then click **View**.
4. In the logical unit name pane, click the edit icon, and modify the information that you want to change.
5. Click **Save**.

Deleting an iSCSI logical unit

Procedure

1. Navigate to **Provisioning** > **File Services** > **iSCSI**.
2. Select one or more logical units that you want to delete, and then click **Delete**.

3. Click **Delete** to confirm.

In the confirmation dialog box, click **Delete the Logical Unit from server's configuration** or **Delete the Logical Unit from server's configuration with the logical unit data file from the file system**. If you choose to delete the logical unit from server configuration with the data file, you have to force delete the logical unit as the data file cannot be deleted if the underlying file system is not available.

Chapter 6: Data management

Data management includes configuring cloud tiering and data protection features.

Protection

Data protection tasks include configuring snapshots, replication policies, and Network Data Management Protocol (NDMP) settings, and enabling virus scanning.

Snapshots

Snapshots are useful in situations where data availability cannot be disrupted by management functions like system backup and data recovery. They create near-instantaneous, read-only images of an entire file system at a specific point in time. This allows for easy restoration of lost files without having to retrieve the data from backup media.

File system snapshots

You can take a single snapshot of the file system at any time by initiating it manually. This allows you to capture the current state of the file system whenever required.

Creating a snapshot

You can create a snapshot to generate near-instantaneous, read-only images of an entire file system at a specific point in time.

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **File System Snapshots**.
2. In the **Snapshots** pane, select the EVS and file system from the list of EVS instances.
3. Click **Take a Snapshot**.
4. In the **Take a Snapshot** dialog box, enter the name for the snapshot.

   The name must not contain more than 255 characters, spaces, or special characters.
5. Set the **Retention Status** toggle to **Enabled** to set a retention period for file system snapshots. This toggle is disabled by default.

   If you set a retention period while creating a file system, the **Retention Status** toggle is enabled by default and shows the set retention period. You can change the retention period by using the **Customize** option.
6. Click **Save**.
   A snapshot is created. You can view the snapshot information on the **Snapshots** pane.

Managing a snapshot

You can view snapshot information, rename a snapshot, or delete a snapshot.

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **File System Snapshots**.
2. In the **Snapshots** pane, select the EVS and file system associated with the snapshot from the list of EVS instances.

   The following table describes the fields on the **Snapshots** pane:

Field	Description
Overview	
Name	The name of the snapshot.
File System	The source EVS and file system for the snapshot.
Replicated from Snapshot	Indicates that the snapshot is created through object replication.
Creation Time	The time and date the snapshot was created.
Retention	The retention period of the snapshot. If the snapshot is not retained it will show Not Retained.
Created By	Displays how the snapshot is created. For example, Manually, Rule, Object Replication, and so on.
Preserved Space	The space that is allocated for the snapshot.
Freeable Space	Click **View Size** to view the disk space that will become available when you delete the snapshot.
Actions	
Rollback	Rolling back a file system from a snapshot recovers the file system to the state that it was when the snapshot was created. For instructions, see Rolling back a file system from a snapshot (on page 67).
Rename	You can rename manually created snapshot names, but not those created by snapshot rules.

Field	Description
Extend Retention	You can extend the snapshot retention period to any date later than the current period, but you cannot set it to a date earlier than the current period.
Delete	You can delete the selected snapshot.

Deleting a snapshot

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **File System Snapshots**.
2. In the **Snapshots** pane, select the EVS and file system associated with the snapshot from the list of EVS instances.
3. Select one or more snapshots that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Rolling back a file system from a snapshot

Rolling back a file system from a snapshot recovers the file system to the state that it was when the snapshot was created. For example, if a file system is corrupted due to an event such as a RAID controller crash, storage system component failure, or power loss, you can roll back to a previous snapshot of the file system.

A file system rollback from a snapshot requires the FS_RECOVER_FROM_SNAP licensed service on the managed server. For information about viewing licensed services, see Viewing license information (on page 143).

> **Note:** You can roll back a file system from a snapshot only when the configured number of preserved file system checkpoints were created since the snapshot was created. For example, if a file system is configured to preserve 128 checkpoints (the default), you can roll back the file system from a snapshot only after a minimum of 128 checkpoints are created. If less than the configured number of checkpoints are created, you can roll back from an earlier snapshot or from a checkpoint. To roll back from a checkpoint, use the `fs-checkpoint-select` command as described in the command reference for the storage platform.

The following file system rollback considerations apply:

- All snapshots are discarded after the rollback completes.
- No new snapshots occur until all previous snapshots are discarded.
- After you roll back a file system and mount it in read/write mode, you cannot undo the rollback or roll back again to a different snapshot or checkpoint.

The following types of rollbacks are available:

- Regular Rollback: The file system is rolled back to a selected snapshot. This option is also available for file systems that are object replication targets.
- Promote: The file system is rolled back to a selected snapshot and then is promoted to a live file system. This option is available only for file systems that are object replication targets.
- Demote: The file system is rolled back to a selected snapshot and is then demoted to an object replication target. This option is available only for file systems that are not object replication targets.

Rolling back a file system

A rollback restores a file system, or a file system that is used as an object replication target, to a selected snapshot.

Before you begin

Review the considerations for a rollback in Rolling back a file system from a snapshot (on page 67).

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **File System Snapshots**.
2. In the **Snapshots** pane, select the EVS and file system associated with the snapshot from the list of EVS instances.
3. Locate the snapshot that you want to roll back to, click the more actions menu, and then click **Rollback**.
4. In the **Roll Back File System** pane, select **Regular Rollback**
5. Review the details for the file system that is associated with the snapshot: EVS name, file system name, and file system mount status.
6. Review and configure the rollback steps. The steps include automatically unmounting the file system.
   a. In the **Recover file system to snapshot created at** list, select the snapshot that you want to roll back to.

      The snapshots are listed by date and time. The name is also shown for the selected snapshot.

b. In the **Remount file system as** list, select one of the following options:

   - **Mount read write**: This option mounts the file system in read/write mode and is the default. If you roll back a file system and mount it in read/write mode, you cannot undo the rollback or roll back again to a different snapshot.
   - **Mount read only**: This option mounts the file system in read-only mode. If a file system is an object replication target, it must be mounted in read-only mode. You can also mount the file system in read-only mode for other reasons such as to verify the file system status and decide whether to remount the file system in read/write mode or to restore to a different snapshot.
   - **Do not mount**: This option prevents the file system from mounting. Some features, such as formatting a file system, require that the file system is unmounted. You must also unmount a file system to remove it.

7. Click **Rollback**, and then click **Continue** to confirm.

Rolling back and promoting a file system

A promoting rollback restores a file system that is an object replication target to a live file system.

Before you begin

Review the considerations for a rollback in Rolling back a file system from a snapshot (on page 67).

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **File System Snapshots**.
2. In the **Snapshots** pane, select the EVS and file system associated with the snapshot from the list of EVS instances.
3. Locate the snapshot that you want to roll back to, click the more actions menu, and then click **Rollback**.
4. In the **Roll Back File System** window, select **Promote**.
5. Review the file system details: EVS name, file system name, and file system mount status.
6. Review the details for the latest object replication version: status, source file system, source server, and source file system status.
7. Review and configure the rollback steps. The steps include automatically unmounting the file system.

   a. In the **Recover file system to snapshot created at** list, select the snapshot that you want to roll back to.

      The listed snapshots are shown by date and time. The version snapshot name and source file system are shown for the selected snapshot.

b. In the **Remount file system as** list, select one of the following options:

   - **Mount read write**: This option mounts the file system in read/write mode and is the default. If you roll back a file system and mount it in read/write mode, you cannot undo the rollback or roll back again to a different snapshot.
   - **Mount read only**: This option mounts the file system in read-only mode. If a file system is an object replication target, it must be mounted in read-only mode. You can also mount the file system in read-only mode for other reasons such as to verify the file system status and decide whether to remount the file system in read-write mode or to restore to a different snapshot.
   - **Do not mount**: This option prevents the file system from mounting. Some features, such as formatting a file system, require that the file system is unmounted. You must also unmount a file system to remove it.

c. Under **Remove access points**, select **Shares** and **Exports** (the defaults) to exclude SMB shares and NFS exports from the rollback. To include shares or exports, clear the applicable checkbox.

   For information about SMB share access points, see the description of **Transfer to Object Replication Target** in Additional information about creating an SMB share (on page 56).

   For information about NFS export access points, see the description of **Transfer to Object Replication Target** in Additional information about adding an NFS export (on page 50).

8. If the object replication target and the promoted file system are on the same EVS, you must select the export that the NFS clients will access. You can choose exports on the source file system (the default) or on the promoted file system.
9. Click **Rollback**, and then click **Continue** to confirm.

Rolling back and demoting a file system

A demoting rollback restores a file system to a selected snapshot, and then demotes the file system to an object replication target.

Before you begin

Review the considerations for a rollback in Rolling back a file system from a snapshot (on page 67).

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **File System Snapshots**.
2. In the **Snapshots** pane, select the EVS and file system associated with the file system snapshot from the list of EVS instances.
3. Locate the snapshot that you want to roll back to, click the more actions menu, and then click **Rollback**.
4. In the **Roll Back File System** window, select **Demote**.
5. Review the file system details: EVS name, file system name, and file system mount status.

6. Review and configure the rollback steps. The steps include automatically unmounting the file system.
   a. In the **Recover file system to snapshot created at** list, select the snapshot that you want to roll back to.

      The listed snapshots are shown by date and time. The snapshot name is shown for the selected snapshot. If available, the object replication policy is also shown.
   b. Under **Remove access points**, select **Shares** and **Exports** (the defaults) to exclude SMB shares and NFS exports from the rollback. To include shares or exports, clear the applicable checkbox.

      For information about SMB share access points, see the description of **Transfer to Object Replication Target** in Additional information about creating an SMB share (on page 56).

      For information about NFS export access points, see the description of **Transfer to Object Replication Target** in Additional information about adding an NFS export (on page 50).
7. Click **Rollback**, and then click **Continue** to confirm.

Managing file system rollback reports

When you roll back a file system to a snapshot, information for that rollback is presented in a report. The report includes detailed information such as the snapshot that was used for the rollback, status of the rollback, the rollback start and end time, and whether shares or exports were recovered in the rollback. The report also includes a log of the rollback events.

Viewing a file system rollback report

You can view the status of file system rollback jobs and other detailed information in reports.

Procedure

1. Navigate to **Data Management** > **Snapshots** > **File System Rollback Reports**.
2. In the **File System Rollback Reports** pane, select the EVS and file system associated with the snapshot rollback from the list of EVS instances.
3. Locate the rollback report, and then click **View**.
4. Click the **Recovery Details** tab to view the report details.

   The following information is shown:

Field/Item	Description
File System Details	
EVS / File System	The EVS and associated file system that was rolled back.
File System Status	The mount status of the file system: **Mounted** or **Unmounted**.
Recovery Details - Progress	

Field/Item	Description
Active	Specifies whether the rollback job is in progress or complete.
Last Status	The status of the last completed rollback.
Start Time	The start time for the rollback job.
End Time	The end time for the rollback job.
Recovery Details - Request Summary	
Recovery Option	Specifies whether a demote or promote rollback type is enabled. If the demote or promote rollback type is not enabled, this value is **No**.
Recover Shares	Specifies whether SMB shares are included in the rollback.
Recover Exports	Specifies whether NFS exports are included in the rollback.
Log Level	Specifies the level of information that is in the report log. The following values ▪ **Error**: Logs only error level events. ▪ **Warning**: Logs only warning level events. ▪ **Info**: Logs all events. ▪ **None**: No events are logged.
Rollback to Snapshot	The snapshot the file system was rolled back to.
Fix Name Clash	Specifies whether a new name is generated for the recovered mount point if there is a name clash with an existing mount point within the same EVS.
Skip Identical Shares / Exports	Specifies whether mount points are skipped from recovery if there is an existing mount point that targets the same file system and the same path.
NFS Client Access	If the object replication target and the promoted file system are on the same EVS, specifies how the NFS client accesses the export.
Recovery Details - Source File System (Transfer Access Point) Setting	
For this Promotion	Specifies whether mount points are recovered with the `Use file system default` transfer setting for exports and shares.
Recovery Statistics - Shares	

Field/Item	Description
Total Successfully Recovered	If SMB shares were included in the rollback, the number of shares recovered.
Total Failed to Recover	If SMB shares were included in the rollback, the number of shares that failed to recover.
Total Skipped	If SMB shares were included in the rollback, the number of shares that were skipped.
Recovery Statistics - Export	
Total Successfully Recovered	If NFS exports were included in the rollback, the number of exports recovered.
Total Failed to Recover	If NFS exports were included in the rollback, the number of exports that failed to recover.
Total Skipped	If NFS exports were included in the rollback, the number of exports that were skipped.

5. Click the **Log Details** tab to view log information for the file system rollback. Log information is not shown if the **Log Level** is **None**.

Downloading a file system rollback report

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **File System Rollback Reports**.
2. In the **File System Rollback Reports** pane, select the EVS and file system associated with the snapshot rollback from the list of EVS instances.
3. Select one or more reports that you want to download, and then click **Download**.
4. Click **Continue** to confirm.

Deleting a file system rollback report

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **File System Rollback Reports**.
2. In the **File System Rollback Reports** pane, select the EVS and file system associated with the snapshot rollback from the list of EVS instances.
3. Select one or more reports that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Managing snapshot rules

Snapshot rules define the scope for taking snapshots. You can target a specific file system and manage its snapshots separately.

Creating a snapshot rule

You can create a snapshot rule to specify which file systems to include in the snapshot.

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **Snapshot Rules**.
2. Select the EVS and click **Add Rule**.
3. In the **Add Snapshot Rule** dialog box, select the EVS and associated file system.
4. Enter the rule name.

   The rule name can contain alphanumeric characters, and the special characters underscore (_) and hyphen (-).
5. Specify the number of snapshots to keep before deleting the oldest.
6. Set the **Retention Status** toggle to **Enabled** to set a retention period for file system snapshots. This toggle is disabled by default.

   If you set a retention period while creating a file system, the **Retention Status** toggle is enabled by default and shows the set retention period. You can change the retention period by using the **Customize** option
7. Select one of the following policies to apply when the snapshot rule queue is full and a new snapshot request is made by the rule:
   - **Move out of queue and delete:** The oldest snapshots are removed from the queue and are scheduled for deletion if if retention is enabled, or deleted immediately if not.

     When you use this policy, avoid creating snapshots faster than they are deleted. Doing so can cause the file system to exceed its snapshot limit (1024) or run out of space. The retention interval should be less than the queue size multiplied by the snapshot interval. For example, if you schedule snapshots hourly and the queue size is 24, set the retention to less than 24 hours. In this case, when you schedule a new snapshot, and the queue is full, the system will immediately delete the oldest snapshot as its retention period expires.
   - **Ignore retention and delete:** The oldest snapshots are moved out of the queue and deleted immediately, even if retention is enabled.
   - **Stop creating new snapshots:** Stops taking new snapshots if retention is enabled for the oldest snapshot in the queue and the retention period has not expired.
8. Click **Save**.

Next steps

After creating the snapshot rule, it must be scheduled to run. For more information, see Create the snapshot rule schedule (on page 75).

Editing a snapshot rule

You can edit the snapshot rule name and queue size by performing the following steps.

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **Snapshot Rules**.
2. In the **Snapshot Rules** pane, select the EVS associated with the rule from the list of EVS instances.
3. Locate the rule that you want to modify, and then click **Edit**.
4. In the **Edit Snapshot Rule** dialog box, modify the information that you want to change.
5. Click **Save**.

Deleting a snapshot rule

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **Snapshot Rules**.
2. In the **Snapshot Rules** pane, select the EVS associated with the rule from the list of EVS instances.
3. Select one or more snapshot rules that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Snapshot schedules

Snapshot schedules allow you to configure when and how often a snapshot is taken so you do not have to trigger the snapshot process manually.

Creating the snapshot rule schedule

You can create a schedule for snapshot rules to specify how often a rule should run.

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **Snapshot Schedules**, and then click **Add schedule**.
2. In the **Add Snapshot Schedule** dialog box, complete the following information, and then click **Save**.
   a. Select the EVS and associated snapshot rule that you want to schedule.
   b. Select one of the following schedules:
      - **Periodic:** Select a frequency to run the scheduled rule. For example, if you set it to run every `4` hours and enter a time range in 24 hours format, the snapshot rule automatically runs and takes a snapshot every four hours within the specified time.
      - **Once Daily:** Select the days of the week and specify the time. For example, if you select `Wednesday` and `Sunday` and specify `15:30`, the snapshot rule will automatically run and take a snapshot every Wednesday and Sunday at the specified time.

   c. Add one or more email addresses to receive snapshot notifications.

   The snapshot schedule is created.

Editing the snapshot rule schedule

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **Snapshot Schedules**.
2. In the **Snapshot Schedules** pane, select the EVS associated with the schedule from the list of EVS instances.
3. Locate the schedule that you want to modify, and then click **Edit**.
4. In the **Edit Snapshot Schedule** dialog box, modify the information that you want to change.
5. Click **Save**.

Deleting the snapshot rule schedule

Procedure

1. Navigate to **Data Management** > **Protection** > **Snapshots** > **Snapshot Schedules**.
2. In the **Snapshot Schedules** pane, select the EVS associated with the schedule from the list of EVS instances.
3. Select one or more snapshot schedules that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Replication

Replication allows you to copy or relocate both file data and file system metadata. Using replication, you can relocate file system data and CNS links, SMB shares, permissions and all other file-level metadata. Administrators can use File Administrator to configure policy-based replication jobs independently from other backup strategies.

Replication is a licensed feature, and the license must be installed before replications can be performed.

Replication policies and schedules

File replication and object based file system replication provides a manual or automatic mechanism for copying or relocating file system, file system data and file system metadata such as access points, security descriptors, and other file system related data.

File replication can be used to selectively copy file system data based on the directory location and file attributes such as name and size

Object replication can mirror file systems at different physical locations, which can be used as a disaster recovery configuration. Unlike file replication, object-based replication operates on the entire file system, not at the individual file or directory level. Object replication also allows CNS links, SMB shares and NFS exports to be re-located.

Object replication, like file replication, uses policies and schedules to determine which file systems get replicated, where they are replicated, and when replication operations are run. Policies specify the replication source and the target, and schedules specify the timing and the interval of repetition.

Adding a file replication policy

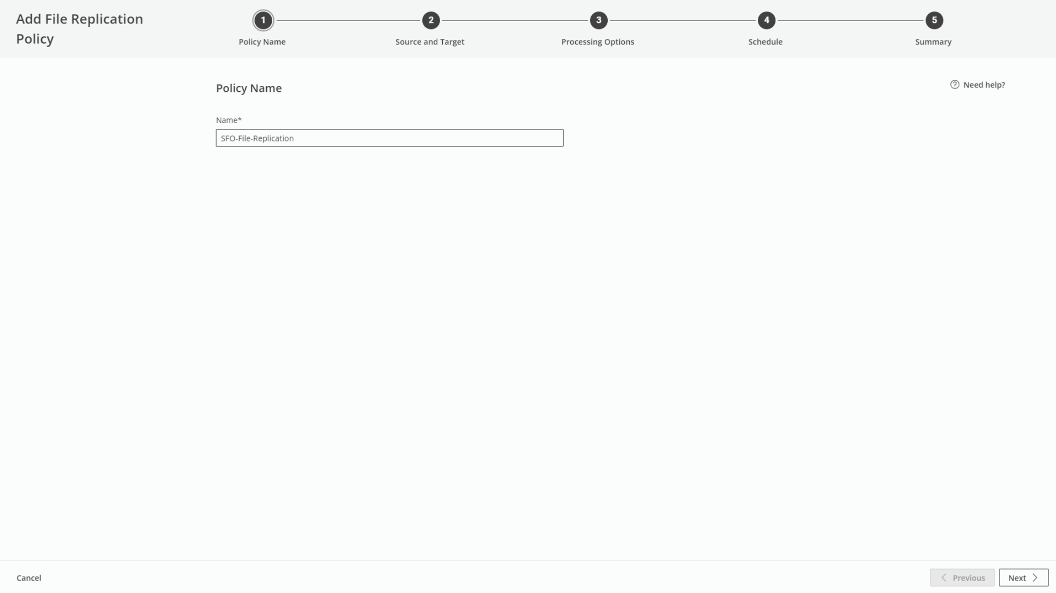
Before you begin

Make sure that you create a snapshot rule for the EVS where you are creating the file replication policy.

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **Policies and Schedules**, click **Add Policy**, and then select **File Replication**.
2. In the **Policy Name** page, enter a name of the file replication policy, and then click **Next**.

   The **Name** box supports alphanumeric characters (A-z, a-z and 0-9), hyphen, and underscore.

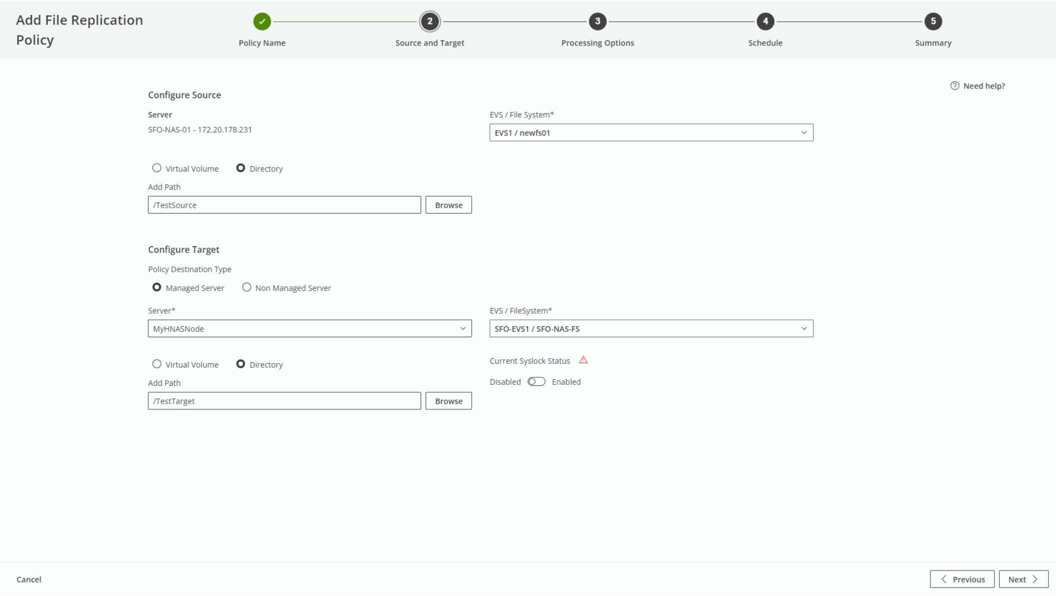
   Add File Replication Policy

   Policy Name

   Name*: SFO-File-Replication

3. In the **Source and Target** page, configure the following settings, and then click **Next**.
   a. Select the EVS and the file system where you want to add the file replication policy.
   b. Select a virtual volume or select a directory and enter the path of the file system.
   c. For the replication policy destination, select managed server or non managed server and then enter the details of the server.

      For more information on setting source and target, see Additional information about creating file replication policy (on page 80).



Configure Source

Server: SFO-NAS-01 - 172.20.178.231

EVS / File System*: EVS1 / newfs01

○ Virtual Volume ● Directory

Add Path: /TestSource

Configure Target

Policy Destination Type: ● Managed Server ○ Non Managed Server

Server*: MyHNASNode

EVS / FileSystem*: SFO-EVS1 / SFO-NAS-FS

○ Virtual Volume ● Directory

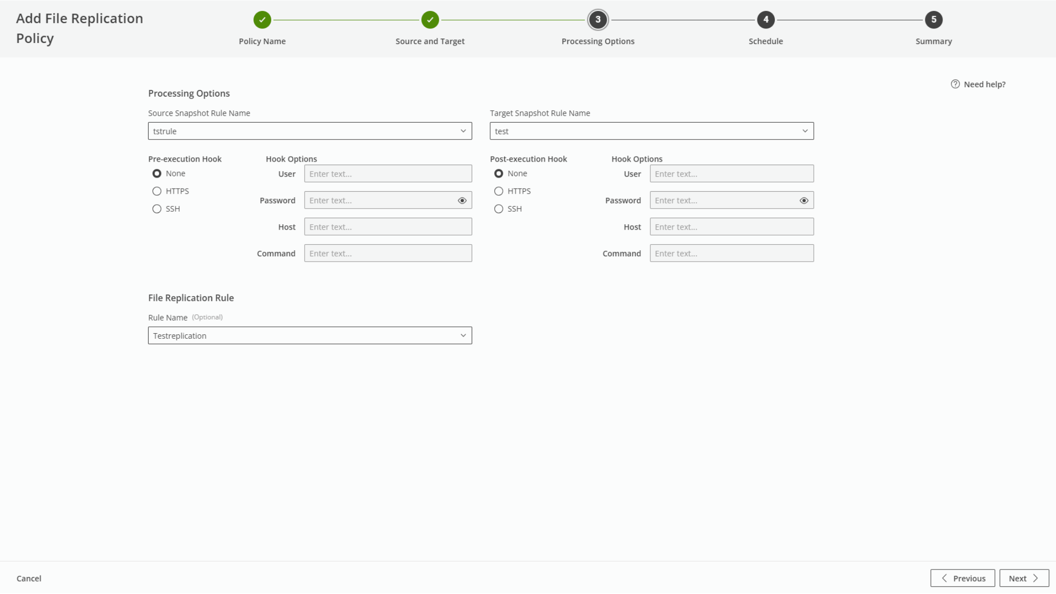
Add Path: /TestTarget

Current Syslock Status ⚠

Disabled ○ Enabled

4. In the **Processing Options** page, set the source snapshot replication rule, target snapshot rule. If required, set the pre and post execution hook and the optional file replication rule and then click **Next**.

   For more information on setting processing options, see Additional information about creating file replication policy (on page 80).



Processing Options

Source Snapshot Rule Name: tstrule

Target Snapshot Rule Name: test

Pre-execution Hook: ● None ○ HTTPS ○ SSH

Hook Options: User: Enter text... Password: Enter text... Host: Enter text... Command: Enter text...

Post-execution Hook: ● None ○ HTTPS ○ SSH

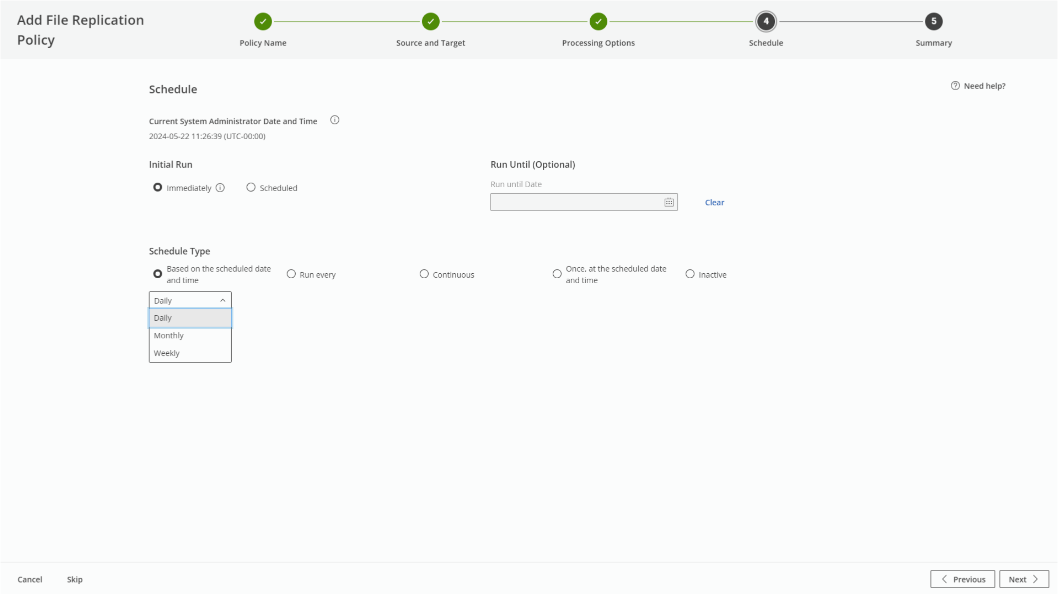
Hook Options: User: Enter text... Password: Enter text... Host: Enter text... Command: Enter text...

File Replication Rule

Rule Name (Optional): Testreplication

5. In the **Schedule** page, set the file replication schedule and then click **Next**.

   For more information on setting file replication schedule, see Additional information about creating file replication policy (on page 80).



Schedule

Current System Administrator Date and Time
2024-05-22 11:26:39 (UTC-00:00)

Initial Run
● Immediately ○ Scheduled

Run Until (Optional)
Run until Date

Schedule Type
● Based on the scheduled date and time ○ Run every ○ Continuous ○ Once, at the scheduled date and time ○ Inactive

Daily
Daily
Monthly
Weekly

6. In the **Summary** page, review the file replication policy configurations, and then click **Add**. Alternatively, you can add another file replication policy by clicking **Create & add another**.

Additional information about creating file replication policy

The following tables describes the additional information about the fields that are required while creating a file replication policy:

Field	Description
Policy Name	
Name	Name of the replication policy. The name should not contain spaces or any of the following characters: \/<>"'!@#$%^ %&*(){}[] +=?:;,~`|.'
Configure Source	
Server	Name of the server or cluster that has the source file system for the replication policy. This field cannot be changed.
EVS / File System	Name of the replication source EVS and file system.
Virtual Volume	The virtual volume which is used as the source of the file replication.
Directory	The directory path which is used as the source of file replication.
Configure Target (managed server)	
Server	Name of the server or cluster that hosts the destination file system for the replication policy.
EVS / File System	Name of the target EVS and file system.
Virtual Volume	The virtual volume which is used as the target of the file replication.
Directory	The directory path which is used as the target of file replication.
Current Syslock status	Indicates if the file system is in Syslocked mode. Set the syslock toggle to Enabled to make the file system read-only for the clients. By default, syslock is disabled. When system lock is enabled for the destination file system, a warning icon is displayed. NDMP has full access to the file system and can write to the syslocked file system during a backup or replication, but the file system remains in read-only mode to clients using the file service protocols (NFS, SMB, FTP, and iSCSI). If the destination file system is not in syslock mode during a replication operation, clients may write to the file system, creating inconsistencies between the source and target of the replication.

Field	Description
	During transfer of primary access operations, both the source file system and the destination file system are put into System Lock mode.
Configure Target (non-managed server)	
NDMP User Name	Name of the NDMP user configured on the replication target server.
NDMP User Password	Password for the selected NDMP user.
File Serving IP Address / Host Name	Name of the server containing the target EVS and file system.
File System	Name of the target file system.
Path	The directory path of the file system.
Processing Options	
Source Snapshot Rule Name	The snapshot rule for replication of the source file system.
Destination Snapshot Rule Name	The snapshot rule to use for the snapshot of the destination file system following a successful replication.
Pre-/Post-execution hook	Connects to another client for running a user-defined script before or after each replication. You have an option to use HTTPS or SSH to connect to the client.
File Replication Rule Name	(Optional) Choose the file replication rule for the file replication policy.
Schedule	
Current Server Date and Time	Shows the current date and time of the server.
Immediately	Runs the associated policy as soon as the schedule is successfully created.
Scheduled	▪ Time of Initial Run: Specify the time, using the 24-hour format (such that 11:59 PM will be entered as 23:59).

Field	Description
	▪ Date of Initial Run: Specify the date for the first run of the policy. Use the format `YYYY/MM/DD` (year/month/day), or select the date by clicking the calendar icon to display the calendar. When using the calendar control, select the desired day by clicking the link on the day in the calendar. You can change the month and year displayed by clicking the next button or the previous button to move forward or back in one month increments.
Run until Date	(Optional) If you do not specify a date for a final run, the policy runs at the interval specified in the Schedule section.
Schedule Type	Select one of the options to select a replication schedule type: ▪ Based on the scheduled date and time: Select daily, monthly, or weekly based on the scheduled date and time. ▪ Runs every: Enter the number of days, hours, or minutes based on the scheduled date and time. ▪ Continuous: Enter the number of hours after which a a new replication job starts. The new replication job can start immediately (0 hours), or after pausing a specified number of hours. ▪ Once, at the scheduled date and time.: Schedules the policy to run only once, at the scheduled Time and Date of Initial Run ▪ Inactive: Pauses the replication schedule. **Note:** If an excess amount of time elapses between replication runs, snapshots may take up a larger amount of space. By default, replication-defined snapshots are purged after 7 days (configurable to 40 days). Waiting 8 or more days between replication runs could result in a full replication.

Adding an object replication policy

Before you begin

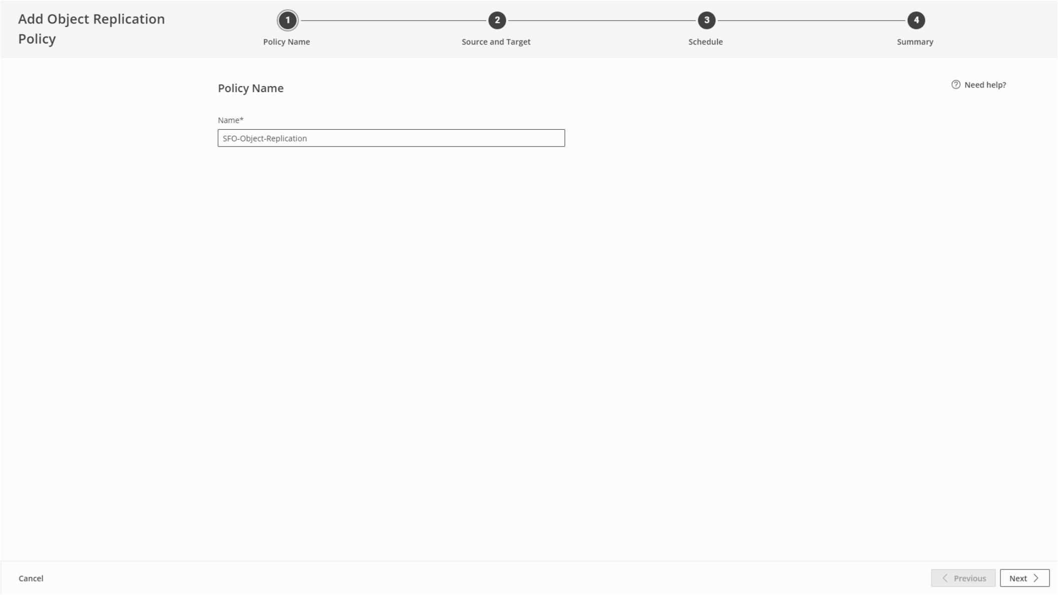
Make sure that you create a snapshot rule for the EVS where you are creating the object replication policy.

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **Policies and Schedules**, click **Add Policy**, and then select **Object Replication**.

2. In the **Policy Name** page, enter a name of the object replication policy, and then click **Next**.

   The **Name** box supports alphanumeric characters (A-z, a-z and 0-9), hyphen, and underscore.

   Add Object Replication Policy

   Policy Name

   Name*: SFO-Object-Replication

3. In the **Source and Target** page, configure the replication policy source and target settings, and then click **Next**.

   a. Select the EVS and the file system where you want to add the object replication policy.

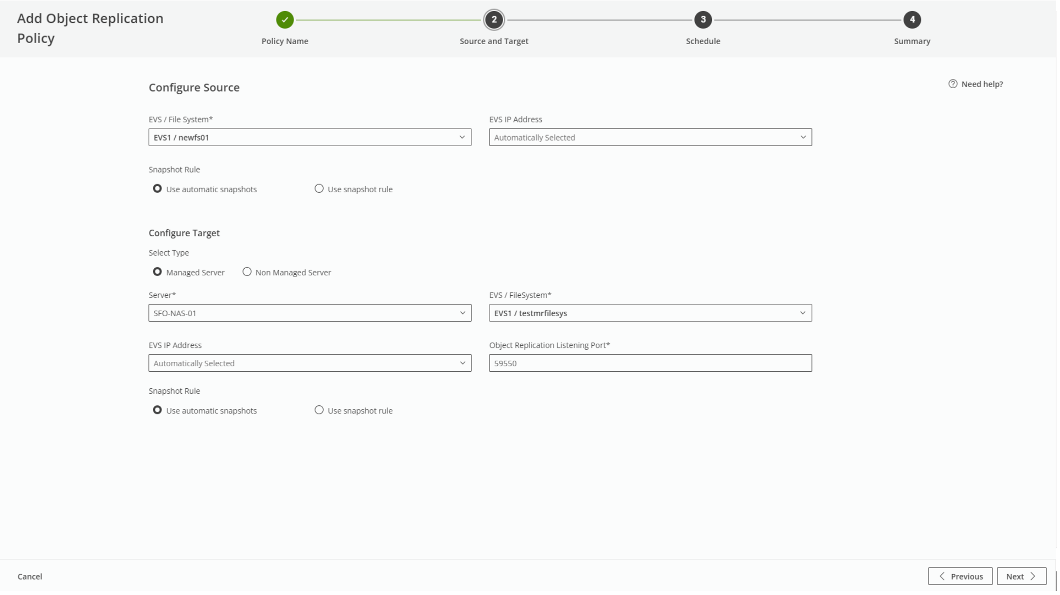
   b. Select the IP Address associated with the EVS.

   c. Select an existing snapshot rule or use automatic snapshots for the source replication policy.

   d. For the replication policy target, select managed server or non managed server and then enter the details of the server.

   e. Select an existing snapshot rule or use automatic snapshots for the target replication policy.

      For more information on configuring source and target, see Additional information about creating object replication policy (on page 85).



Configure Source

EVS / File System*: EVS1 / newfs01

EVS IP Address: Automatically Selected

Snapshot Rule: ● Use automatic snapshots ○ Use snapshot rule

Configure Target

Select Type: ● Managed Server ○ Non Managed Server

Server*: SFO-NAS-01

EVS / FileSystem*: EVS1 / testmrfilesys

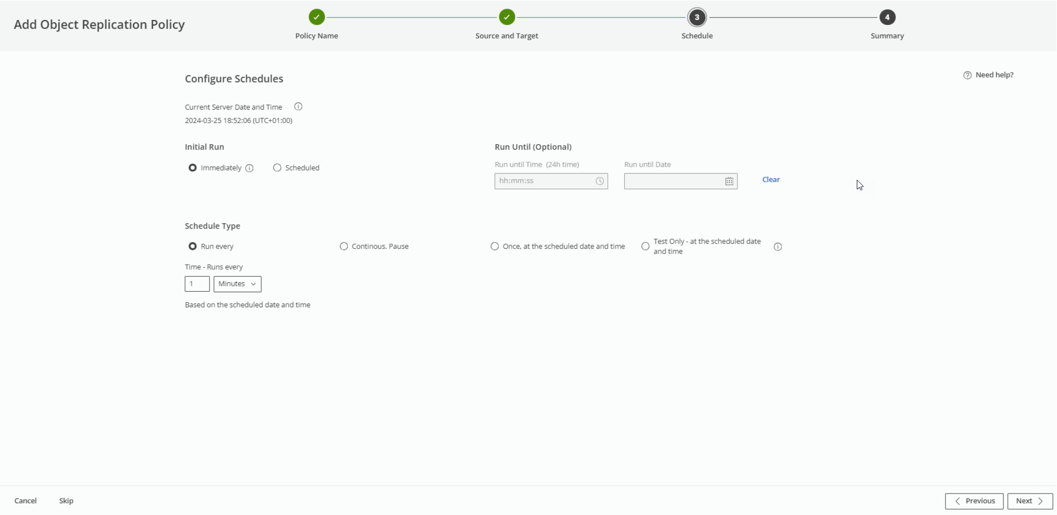
EVS IP Address: Automatically Selected

Object Replication Listening Port*: 59550

Snapshot Rule: ● Use automatic snapshots ○ Use snapshot rule

4. In the **Schedule** page, set the object replication schedule and then click **Next**.

   For more information on configuring object replication schedule, see Additional information about creating object replication policy (on page 85).



Configure Schedules

Current Server Date and Time
2024-03-25 18:52:06 (UTC+01:00)

Initial Run: ● Immediately ○ Scheduled

Run Until (Optional)

Run until Time (24h time): hh:mm:ss

Run until Date:

Schedule Type: ● Run every ○ Continous. Pause ○ Once, at the scheduled date and time ○ Test Only - at the scheduled date and time

Time - Runs every: 1 Minutes

Based on the scheduled date and time

5. In the **Summary** page, review the object replication policy configurations, and then click **Add**. Alternatively, you can add another object replication policy by clicking **Create & add another**.

Additional information about creating object replication policy

The following tables describes the additional information about the fields that are required while creating a object replication policy:

Field	Description
Policy Name	
Name	Name of the replication policy. The name should not contain spaces or any of the following characters: \/<>"'!@#$%^ %&*(){}[] +=?:;,~`|.'
Configure Source	
EVS / File System	Name of the replication source EVS and file system.
EVS IP Address	IP address for the source EVS. The default value for this field is 'Automatically selected'.
Use automatic snapshots	Allows the replication to use its default snapshot rule to take and manage snapshots. **Note:** If you choose this option, each incremental snapshot is deleted when the next replication runs. Therefore, because the snapshot queue only contains one snapshot, it is recommended that replications are not scheduled too closely together in order to prevent an existing snapshot from being removed before the next replication starts.
Use snapshot rule	The source snapshot retention policy can be customized to retain a different number of snapshots on the source file system. **Note:** If you choose this option, set the schedule for the snapshot rule so a snapshot is created before the replication runs, to ensure that a new snapshot is available for the replication. A snapshot of the source file system is only taken if the replication policy is configured to use an automatic snapshot rule. If it is using a named rule, the replication will use the latest snapshot created by that rule; it does not take one automatically.
Configure Target (managed server)	
Server	Name of the server or cluster that hosts the destination file system for the replication policy.
EVS / File System	Name of the target EVS and file system.
EVS IP Address	IP address for the target EVS. The default value for this field is 'Automatically selected'.

Field	Description
Object Replication Listening Port	The port on which the destination server is listening. The default is 59550.
Configure Target (non-managed server)	
File Serving IP Address / Host Name	Name of the server containing the target EVS and file system.
File System	Name of the target file system.
Object Replication Listening Port	The port on which the destination server is listening. The default is 59550.
Use automatic snapshots	Allows the replication to use its default snapshot rule to take and manage snapshots on the object replication target.
Use snapshot rule	Allows the snapshot retention policy to be customized to retain a different number of snapshots on the source and destination.
Schedule	
Current Server Date and Time	Shows the current date and time of the server.
Immediately	Runs the associated policy as soon as the schedule is successfully created.
Scheduled	▪ Time of Initial Run: Specify the time, using the 24-hour format (such that 11:59 PM will be entered as 23:59). ▪ Date of Initial Run: Specify the date for the first run of the policy. Use the format `YYYY/MM/DD` (year/month/day), or select the date by clicking the calendar icon to display the calendar. When using the calendar control, select the desired day by clicking the link on the day in the calendar. You can change the month and year displayed by clicking the next button or the previous button to move forward or back in one month increments.
Run until Date	(Optional) If you do not specify a date for a final run, the policy runs at the interval specified in the Schedule section.
Schedule Type	Select one of the options to select a replication schedule type: ▪ Based on the scheduled date and time: Select daily, monthly, or weekly based on the scheduled date and time. ▪ Runs every: Enter the number of hours or days based on the scheduled date and time.

Field	Description
	▪ Continuous: Enter the number of hours after which a new replication job starts. The new replication job can start immediately (0 hours), or after pausing a specified number of hours. ▪ Once, at the scheduled date and time: Schedules the policy to run only once, at the scheduled Time and Date of Initial Run ▪ Inactive: Pauses the replication schedule. **Note:** If an excess amount of time elapses between replication runs, snapshots may take up a larger amount of space. By default, replication-defined snapshots are purged after 7 days (configurable to 40 days). Waiting 8 or more days between replication runs could result in a full replication.

Modifying an object replication policy

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **Policies and Schedules**.
2. In the **Replication Policies and Schedules** pane, identify an object replication policy you want to modify and then click **View**.
3. In the replication policy name pane, click the edit icon and modify the policy name, change the source snapshot rule, the target object replication port, and then click **Save**.

   For more information on configurations of object replication policy, see Additional information about creating object replication policy (on page 85).

Modifying a file replication policy

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **Policies and Schedules**.
2. In the **Replication Policies and Schedules** pane, identify a file replication policy you want to modify, and then click **View**.
3. In the replication policy name pane, click the edit icon and change the current syslock status of the file system, modify the policy name, change the source snapshot rule name and the destination snapshot rule name, pre-execution hook, post-execution hook, add the optional file replication rule, and then click **Save**.

   For more information on the configurations of file replication policy, see Additional information about creating file replication policy (on page 80).

Modifying a replication schedule

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **Policies and Schedules**.
2. In the **Replication Policies and Schedules** pane, identify a file or an object replication policy schedule you want to modify, and then click **View**.
3. In the replication policy page, click **Schedules** tab, identify the schedule you want to modify, and then click **Edit**.
4. Modify the schedule running time and frequency, and then click **Save**.

   For more information on configurations of a file or an object replication policy schedule, see Additional information about creating file replication policy (on page 80) and Additional information about creating object replication policy (on page 85).

Deleting a replication policy

Policies with an active replication cannot be deleted unless the you abort the active replication. Deleting a replication policy also deletes all related schedules. If you want to bulk delete replication policies, ensure that the type of the policies are the same, as file replication policies and object replication policies must be deleted separately.

⚠ **Caution:** Aborting an active replication job during policy deletion may leave the policy target in an inconsistent state.

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **Policies and Schedules**.
2. Select one or more replication policy that you want to delete, and then click **Delete**.

   Note: Make sure that the policy type is same while you are selecting the policy for deletion.

3. Select to abort all active replication jobs, if necessary, and then click **Delete** to confirm.

File replication rules

Replication rules comprise optional configuration parameters that allow replications to be tuned to enable or disable specific functions or to optimize performance.

Replication Rules control values like the number of read-ahead processes, minimum file size used in block replication, when snapshots are deleted and whether replications will include migrated files. The server default values should be optimal in most cases; however, these values can be changed to customize replication performance characteristics based on the data set.

Adding a file replication rule

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **File Replication Rules**, and then click **Create Rule**.

2. Enter a rule name and a description of the rule.

   Names in alphanumeric characters, hyphens, and underscores are only supported.
3. Enter the type of files to exclude from the rule, select block-based replication minimum file size, number of additional server connections, and number of read ahead processes. For more information, see Additional information about creating a file replication rule (on page 89).
4. Set the following settings to **System Default**, and then click **Create**.

   - Pause While Replications Finish Writing
   - Use Changed Directory List
   - External Migration Links
   - Delete the Snapshot
   - Take a Snapshot
   - Migrated File Re-migration
   - Migrated File Exclusion
   - Ignore File Attribute Changes

   For more information, see Additional information about creating a file replication rule (on page 89)

   Hitachi Vantara recommends to set the settings to **System Default**. If you want to change the system defaults, contact your Hitachi representative.

Additional information about creating a file replication rule

The following table describes the additional information about the fields that are required while creating a file replication rule.

Field	Description	Default
Files to Exclude	Specifies files or directories to exclude from a replication. When specifying a file or directory, enter either: ▪ A full path name, relative to the top-level directory specified in the replication path. The path name must begin with a forward slash (/); at the end, an asterisk (*) can be entered as a wildcard character. ▪ A terminal file or directory name, which is simply the last element in the path. The wildcard character, *, may be included but only at the start or the end of the name. ▪ A list of files or directories to exclude from a replication. When listing files or directories to exclude from a replication, all items in the list must be separated by a comma.	None are excluded.
Block-based Replication Minimum File Size	Block replication minimum file size controls the minimum file size that is used for block replication. The list options available are: 256 or 512 K, and 1, 2, 4, 8, 16, 32, 64 or 128 MB. For instance, if this option is set to 64 MB: ▪ For a source data file of 63 MB, for which the system determines that only 1 MB has changed, the entire source file (63 MB) will be replicated. ▪ For a source data file of 65 MB, for which the system determines that only 1 MB has changed, only the delta will be replicated. **Note:** Requires a replication license to function.	Minimum file size used for block replication is 32 MB.
Use Changed Directory List	Indicates if incremental replications will search for changed files in directories that only contain changed files. Processes not using the changed directory list must search the entire directory tree looking for changed files. When using the changed directory list, however, the search is limited to those directories that contain changed files.	Disabled.

Field	Description	Default
	Options: ▪ System Default: uses the currently specified system default. ▪ Enabled: uses the changed directory list. ▪ Disabled: always searches the entire directory tree for changed files (a full hierarchical search). **Note:** Using the change object list is likely to improve performance in some cases; for example, where there are sparse changes. However, it can degrade performance where there are many changes throughout the directory structure. The calculation of the change list might take a long time as there can be a long delay between replications. Use Changed Directory List should only be selected if a large part of the directory tree will be unchanged between replication copies. Also, the list can include up to one million directories that contain changed files. If this limit is exceeded the replication reverts to a full hierarchical scan.	
Number of Additional Server Connections	Controls the number of additional server connections that are established during a replication operation. Ranges from 0 to 30. Increasing the number of additional server connections might improve performance by allowing multiple transfers in parallel. **Note:** Each additional server connection consumes system resources, and best practices indicate limiting the number of additional server connections to situations in which they improve performance. Also, as the number of additional server connections is	Number of additional server connections that are established during a replication operation is four.

Field	Description	Default
	increased, more read-ahead processes are required.	
Number of Read Ahead Processes	Controls the number of read-ahead processes used when reading directory entries during a replication. Each additional read-ahead process uses system resources, so it is best to limit the number of additional processes unless it makes a significant difference in performance. While the default number of read-ahead processes is suitable for most replications, file systems made up of many small files increase the amount of time spent reading directory entries proportionately. In such cases, adding additional read-ahead processes may speed up the replication operation.	If a value is not set, the default value is set by the application (depending on the number of read-ahead processes set in Number of Additional Server Connections).
Pause While Replication(s) Finish Writing	By default, the data management engine imposes an interlock to stop NDMP backups and accelerated data copies (ADCs) from the destination of a replication during active replication writes. This function supports installations that replicate to a particular volume, then back up from that volume. However, as the lock is held at the volume level, it may be useful to override this action in the case of directory-level replication. To make use of this replication interlock, specify this rule option on both the replication that waits and the replication that is waited upon. As a best practice: ▪ Create one rule with this option enabled and have each participating replication policy enable the same rule. ▪ Then, schedule the replication policy that waits to run after the replication policy that is waited upon.	No
Take a Snapshot	Overrides the Backup configuration option `Automatic Snapshot Creation`. The setting for this option should be left as the system default in almost all cases. The only case in which it might be useful is when taking a single, non-incremental copy of a file system or a directory. If there is insufficient space on	Yes. Snapshots are taken and backed up automatically.

Field	Description	Default
	the file system to take a snapshot, the copy may be taken from the live file system by selecting Disable. However, it should be noted that copying the live file system while it is changing may give an inconsistent copy. Disabling snapshot usage will affect the ability to run incremental replications. This option should only be set to No if the rule is going to be used for a one-off full replication. ▪ Enable this option to support incremental replication copies. ▪ Disable only for full replication copies or when making a complete copy of a directory. Different files will be copied at different times, so if the source file system is changing and there are dependencies between different files on the system, then inconsistencies may be introduced. **Note:** Snapshots are an integral part of the algorithm for incremental replication, and disabling snapshot usage will affect the ability to run incremental replications. This option must be enabled in order to make incremental replication copies.	
Delete the Snapshot	Determines when snapshots are deleted. The setting for this option should be left as the system default in almost all cases. The only case in which it might be useful is when taking a single, non-incremental copy of a file system or directory. If the file system is short on space, it may be useful to request the immediate	If the replication is an incremental replication, the application automatically selects the correct setting.

Field	Description	Default
	deletion of the snapshot taken for the replication. The deletion options are: ▪ **Immediately** deletes snapshot after replication is done. ▪ **Last** preserves snapshot for use with incremental replications. ▪ **Obsolete** deletes an automatically created snapshot when the next backup of the same level is taken. ⚠ **Caution:** As changing these settings can adversely affect the replication process, Hitachi Vantara recommends that this option be changed only at the direction of your Hitachi Vantara representative.	
Migrated File Exclusion	Indicates if the replications will include files whose data has been migrated to secondary storage. ▪ Enabled: the replication will not include files whose data has been migrated to another volume using the Data Migrator facility. ▪ Disabled: migrated files and their data are replicated as normal files.	Disabled
Migrated File Remigration	Controls the action at the destination when the source file had been migrated. ▪ Enabled: the file will be remigrated on recovery provided the volume or virtual volume has a Data Migrator path to indicate the target volume. ▪ Disabled: all the files and their data will be written directly to the recovery or replication destination volume.	Enabled. Re-migration of the files is attempted.
Ignore File Attribute Changes	Specifies that files in which the only change is an attribute change, are not included in a replication. Only enable this option if you are certain that you do not want to replicate files with only attribute changes.	Disabled

Field	Description	Default
External Migration Links	Controls when a replication operation encounters a cross volume link (a link to a file that has been migrated to an external server). ▪ If set to system default, the replication operation uses the default setting, which is Re-migrate. ▪ If set to Re-migrate, the replication operation copies the file contents but marks the file as having been externally migrated. The destination remigrates to secondary storage if there is an existing data migration path. This is the default behavior. Use this setting when the replication is between a main site and a disaster recovery site, in which the disaster recovery site includes a similar data migration configuration. ▪ If set to Ignore, the replication operation copies only the files on the primary (migrated files are not copied). Use this setting when files have been migrated because they are less useful, so they are not replicated in order to save time. ▪ If set to Re-create link, the replication operation copies only the details of the cross volume link. The cross volume link is recreated on the destination if the relevant external migration data path is in place and the migrated file is accessible. Use this setting when the replication is between storage servers or clusters on the same site, and there is a single external migration target server.	Re-migrate

Field	Description	Default
	Note: For externally migrated files, to make sure that the file or link is replicated properly, you should either: ▪ Specify that the replication operation should remigrate files and the destination should test before recreating links (using the **migration-recreate-links-mode** command). ▪ Specify that the replication operation should re-create links and the destination should always recreate links (using the **migration-recreate-links-mode** command).	

Modifying a file replication rule

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **File Replication Rules**.
2. In the **File Replication Rules** pane, identify the rule you want to modify and then click **View**.
3. In the file replication rule name pane, click the edit icon.
4. Edit the file replication rule description, change the file replication rule settings, and then click **Save**.

   For more information on file replication rule settings, see Additional information about creating a file replication rule (on page 89).

Deleting a file replication rule

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **File Replication Rules**.
2. Select one or more file replication rules that you want to delete, and then click **Delete**.
3. Click **Delete** to confirm.

Replication reports

Replication reports provide a detailed information on the amount of data that has been replicated and the job's success or failure status. You can use this information to analyze the impact of a specific incremental replication policy and to help you make performance adjustments to the replication policy and schedule.

Viewing the object replication report

You can view detailed information about object replications jobs that are in progress or complete.

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **Status**.
2. In the **Replication Reports** pane, select the EVS and file system associated with the object replication from the list of EVS instances.
3. Click the **Object Replication** tab.
   The following table describes the information in **Object Replication** tab.

Column	Description
Policy	The replication policy name.
Source File System	The file system selected for replication.
Source Snapshot	The source snapshot selected for replication.
Target EVS / File System	EVS and the associated file system where the replicated data is stored.
Target Snapshot	The snapshot created on the target file system to replicate the state of the data captured in the source snapshot.
Start Time	The date and time that the replication job started.
Status	The status of the replication job. The values are: complete or failed.

4. To view a detailed report for an individual replication, identify the replication that you want to view, and then click **View**.
   The report page opens with the Report Details and Log Details tab.
5. Click **Report Details** tab to view the detailed information about the replication job.

   The following table describes the information in the **Report Details** tab.

Field	Description
Overview	
Policy Name	The replication policy name.
Source EVS / File System	The file system selected for replication.
Target EVS / File System	EVS and the associated file system where the replicated data is stored.

Field	Description
Report Summary	
Source Snapshot	Source snapshot selected for replication.
Target Snapshot	The snapshot created on the target file system to replicate the state of the data captured in the source snapshot.
Start Time	The date and time that the replication job started.
End Time	The date and time that the replication job ended.
Duration	The duration required for a replication job schedule to complete.
File System Data Transferred	The amount of data that is replicated.
File System Transfer Rate	The speed at which data is replicated.
Objects Complete	The number of objects that have successfully completed replication.
Object Transfer Rate	The rate at which objects are transferred.
Object Replication Type	The status of the replication. The status is one of the following values: **Full Copy**: A complete initial replication of the entire source to the target. **Incomplete Copy**: The replication did not complete.
Status	The status of the replication job. The values are: green for success and red for failure.

6. Click **Log Details** tab to view detailed logs for the replication policy that is completed or running.

Viewing a file replication report

You can view detailed information about the file replication jobs that are in progress or complete.

Procedure

1. Navigate to **Data Management** > **Protection** > **Replication** > **Status**.
2. In the **Replication Reports** pane, select the EVS and file system associated with the file replication from the list of EVS instances.

3. Click the **File Replication** tab.
   The following table describes the information in **File Replication** tab.

Column	Description
Schedule ID	The ID number for the completed replication job.
Policy	The replication policy name.
Completed	The month, date, year, and time that the replication was completed.
Duration	The duration required for a replication schedule to complete.
Bytes Transferred	The amount of data that is replicated.
Status	The status of the replication job. The values are: complete or failed.

4. To view a detailed report for an individual replication, identify the replication that you want to view, and then click **View**.
   The report page opens with the Report Details and Log Details tab.
5. Click **Report Details** tab to view the detailed report about the replication.

   The following table describes the information in the **Report Details** tab.

Field	Description
Policy Name	The replication policy name.
Schedule ID	The completed replication schedule ID.
Status	The status of the replication job. The values are: green for success and red for failure.
Frequency	The frequency at which the replication job is scheduled to run.
Destination Server / EVS	The NAS server and the associated EVS where the replicated data from the source is stored.
Rule	The name of the rule used by the replication policy.
Start Time	The date and time that the replication job started.
End Time	The date and time that the replication job ended.

Field	Description
Duration	The duration required for a replication schedule job to complete.
Bytes Transferred	The quantity of data has undergone replication.
Copy Type	The type of the replication performed. The replication type is one of the following values: **Full Copy**: A complete initial replication of the entire source to the target. **Incomplete Copy**: The replication did not complete. **Incremental Copy**: A replication of the changes on the source file system to the target. **Restart Copy**: The replication started from the point of failure of the previous replication. **Rollback Copy**: After a failed replication run, the target file system is rolled back to the state following the last successful replication.

6. Click the **Log Details** tab to view detailed logs of a replication policy that is completed or running.

NDMP configuration

The VSP One File server supports Network Data Management Protocol (NDMP), an open standard protocol for network-based backups, with two significant advantages:

- It allows the VSP One File management software to control backup and recovery on another device without transferring the backup data across the network.
- It can preserve security settings in a mixed protocol environment, including virtual volume and quota information.

Configuring NDMP information

You can specify NDMP configuration information for a cluster or for the managed server, including NDMP username, password, version, and port.

Procedure

1. Navigate to **Data Management** > **Protection** > **NDMP** > **Configuration**.

2. In the **NDMP Configuration** pane, click the edit icon.
3. In the **NDMP Settings**, complete the following information:
   - Enter the username and password required to access and configure the NDMP settings for the VSP One File servers.

     The username can be up to 20 characters long and cannot contain the following characters: \ / < > " '
   - Enter the NDMP version. By default, the VSP One Fileserver uses NDMP version 4 for backup and recovery functions.

     You can configure the VSP One File server to use NDMP version 2 or 3 if required. Set NDMP to version 2 only if your backup software specifically requires it.

     The incremental data replication and Accelerated Data Copy (ADC) require NDMP version 3 or 4.
   - Configure the NDMP port number. By default, port 10000 is used.
4. In the **Automated Snapshot Use**, select one of the following options:
   - **Do not automatically create snapshots, but backup from the live file system** performs a backup directly from the live file system without taking a snapshot.
   - **Automatically create snapshots** takes a snapshot before performing the backup. This option does not affect file replication snapshots.
5. In **Automated Snapshot Deletion**, select one of the following options:
   - **Delete snapshot after use** deletes an automatic snapshot after completion of the backup for which it was taken. To prevent accumulation of snapshots, select this option for full backups or if the file system is changing rapidly.
   - **Delete snapshot after next backup** deletes an automatic snapshot after it has been used as the basis of a new incremental backup. With the exception of full backups, this option supports incremental backup schedules based on the preceding backup.
   - **Delete snapshot when obsolete** deletes an automatic snapshot upon next backup at the same level. For example, a snapshot taken for a full backup is deleted when the next full backup completes. This option supports differential backup schedules based on a common base backup.

     > **Note:** Snapshots initiated by the Microsoft Volume Shadow Copy Service (VSS) might not be deleted by rule. These snapshots should be managed through the application that requested the snapshot. You can delete these snapshots through the **Snapshots** page.
6. In the **Automated Snapshot Retention** box, set the number of days to retain snapshots before they are automatically deleted. The valid range for this setting is 1 to 80 days. Make sure the retention time is longer than the total duration required for two replication cycles, including the interval and copy time, to avoid premature deletion of snapshots before the next successful copy.
7. Click **Save**.

Next steps

Start the NDMP server. For more information, see Enabling and disabling NDMP services (on page 102).

Enabling and disabling NDMP services

You can start and stop the NDMP service manually, and you can set it to be enabled so that it starts automatically at boot.

Enabling the NDMP server at boot initiates NDMP functionality as part of the setup sequence and initializes services and components for NDMP activites. The NDMP server accepts commands for tasks such as backup and recovery operations.

Procedure

1. Navigate to **Data Management** > **Protection** > **NDMP** > **Configuration**.
2. In the **NDMP Configuration** pane, click **Start Server** to start the NDMP server. You can stop the NDMP server at any time by clicking **Stop Server**. This will terminate NDMP tasks that are currently in progress.
3. Click **Enable Server** to configure the NDMP server to start when the VSP One File server starts. Click **Disable Server** if you do not want the NDMP server to start automatically when the VSP One File server starts.

Configuring NDMP devices

NDMP devices present on the Storage Area Network (SAN) and visible to the VSP One File server appear in the device list. You must manually allow or deny access to these devices.

Note: To configure the VSP One File to work with an NDMP device, you must specify the device name for each autochanger and tape drive you want to use, and then assign these device names to an EVS. You can set these device names using CLI commands. For more information on how to specify the device name, see the VSP One File Command Reference.

The following table describes the fields in the Device List page. To view this information navigate to Data Management > Protection > NDMP > Device List.

Field	Description
ID	The device identifier.
Access	Indicates if device access is allowed (Allow) or denied (Deny).
EVS	Indicates the specific EVS to which the device is assigned. To change the device assignment, select the EVS to which you want to assign the device. For more information, see Changing NDMP device assignment (on page 104)

Field	Description
Hardware Details	Displays hardware details about the device: ▪ Device Type: Tape drive or autochanger. ▪ Manufacturer (Model):The manufacturer and model of the device identified during the device discovery process. ▪ Version:The firmware version currently on the device at the time of device discovery.
Device Identification	Identification information about the device: ▪ NDMP Device Name: The name used by the VSP One File server to identify the device. ▪ Location: The name of the autochanger that holds the drive and the position of the drive in the autochanger. For example, the location of the first drive in autochanger `/dev/mc_d010 is /dev/mc_d010 : 1`. ▪ Serial Number: The device serial number, if detected during device discovery. ▪ Fibre Channel Address: The device Fibre Channel node name. ▪ LUN: LUN identifier for the device. When the VSP One File server cannot determine the location of a tape drive, it displays *unknown*. In such cases, check for the following conditions: • The tape library is offline. • The autochanger might not support the method for querying the tape drive location or might not be configured to accept the query. If this is the case, compare the serial numbers of the tape drives with those displayed in the tape library to confirm their locations. • When the autochanger and the tape drive are connected to different servers, use the tape drive serial numbers to match the device name displayed by one server with the location shown on the other.

Allowing access to NDMP devices

An NDMP device must be assigned to an EVS before it can be used by the VSP One File server.

Procedure

1. Navigate to **Data Management** > **Protection** > **NDMP** > **Device List**.

2. In the **NDMP Device List** pane, select one or more devices, and then click **Allow Access**.

Changing NDMP device assignment

An NDMP device can be shared among EVS instances if the following conditions are met:

- EVS instances must be within the same cluster.
- The NDMP device is not shared with another VSP One File server.
- The NDMP device is not shared with another storage device.

Procedure

1. Navigate to **Data Management** > **Protection** > **NDMP** > **Device List**.
2. In the **NDMP Device List** pane, locate the device you want to reassign, and then click **View**.
3. Click the edit icon, and select the EVS to which you want to assign the device.

Removing or denying access to NDMP devices

If the NDMP server is using a device, any requests to deny access or make changes to the device are not addressed until the NDMP server completes the current task.

Procedure

1. Navigate to **Data Management** > **Protection** > **NDMP** > **Device List**.
2. You can either deny access to a device or you can remove it.
   - To deny access, select one or more devices, and then click **Deny Access**. This option is available only for devices that have Allowed access.
   - To remove, select one or more devices, and then click **Forget.** This option cannot be used for NDMP devices that are functional and performing their intended tasks.

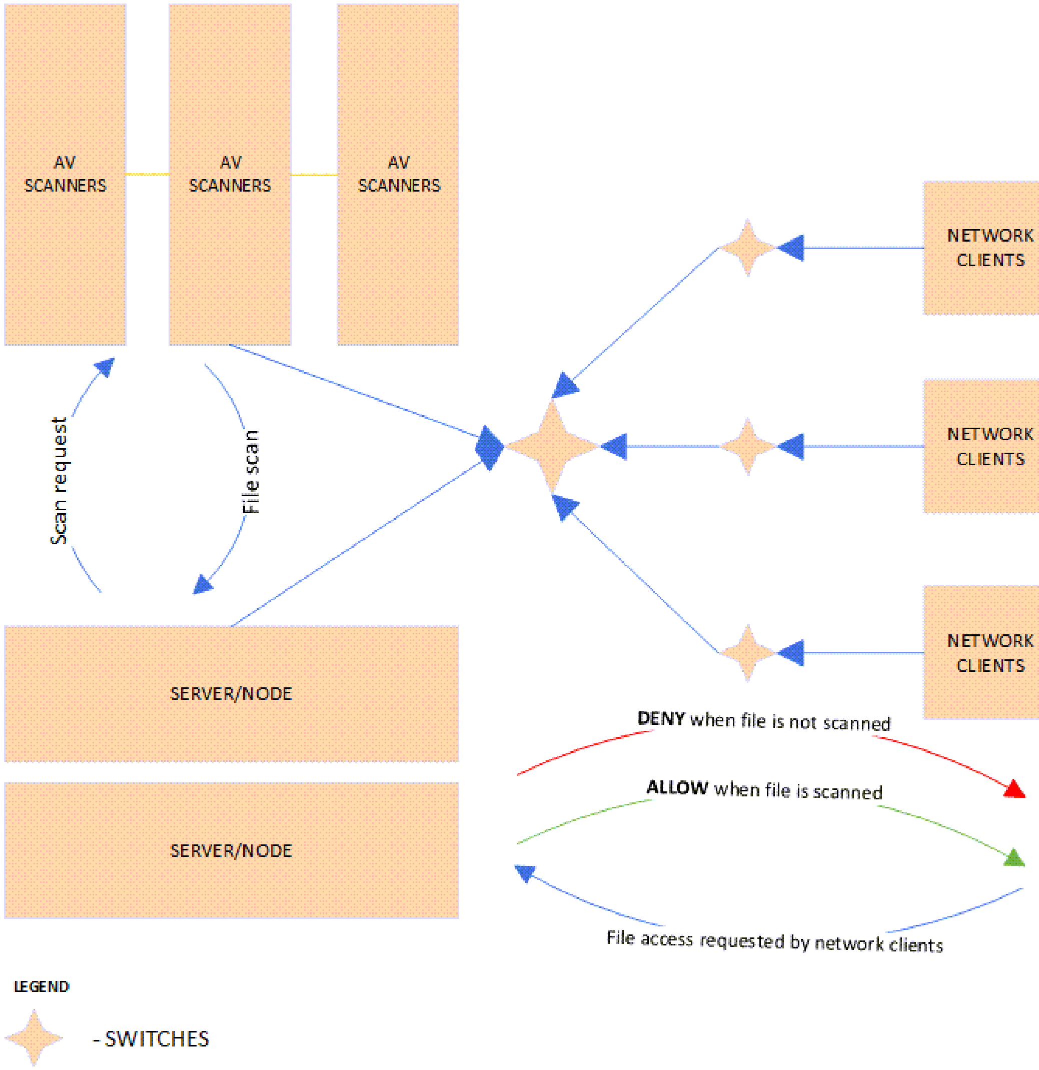
Virus scanning

Overview

The VSP One File servers proactively submit files for scanning to the scan engine on both open (writable) and closed (read-only) file systems. If a file has not been verified by a virus scan engine as clean, a notification is sent to the server and scanning must be done before it can be accessed. However, scanning for viruses when a client on the network is trying to access the file can take time on read-only files (SMB clients may experience a temporary loss of data access). To reduce this latency and ensure maximum accessibility of data, multiple virus scan engines can be configured to support each EVS on which virus scanning is enabled. Files are automatically queued for scanning when they are created or modified. Queued files are scanned promptly, expediting the detection of viruses in new or modified files, and making it unlikely that an infected file remains dormant on the system.

When a virus is detected, a severe event is placed in the event log, identifying the path of the infected file and the IP address of the infected machine.

Virus scanning statistics for a server (in 10-second time slices) are available for viewing in File Administrator since the previous reboot or since the point when statistics were last reset.



You can configure multiple virus scan engines using the RPC protocol or the ICAP protocol to enhance the performance and to maintain high availability of the VSP One File server. The server does not scan files but provides a connection with configured virus scan engines on the network. If a virus scan engine fails during a virus scan, the server automatically redirects the scan to another virus scan engine.

The Internet Content Adaption Protocol (ICAP) is an open standard used to connect devices to enterprise-level virus scan engines. RPC is a remote procedure call interface that some scan engines support.

The server maintains a file type inclusion list that allows you to control the files that are scanned (for example, .exe, .dll, .doc). The default inclusion list includes most file types commonly affected by viruses. You can also create a file type exclusion list to exclude files from virus scanning. Using an exclusion list helps reduce the load on the virus scanning engines and the network. The inclusion and exclusion lists support wildcards.

If virus scanning is temporarily disabled, files are marked as required scanning. If virus scanning is re-enabled, the marked files are scanned the next time the SMB client accesses the files.

Enabling virus scanning on the VSP One File server

Before you begin

Make sure that at least one virus scan engine is registered in File Administrator.

If virus scanning is enabled and configured for the global context or for the EVS hosting the file system pointed to by the share, virus scanning is enabled by default when the share is created. If virus scanning is not enabled for the global context or for the EVS hosting the file system pointed to by the share, virus scanning is not enabled by default when a share is created. You can enable it on each EVS.

Procedure

1. Navigate to **Data Management** > **Protection** > **Antivirus** > **Virus Scanning**.
2. In the **Virus Scanning** pane, select the EVS on which you want to enable virus scanning from the list of EVS instances.
3. Click the edit icon, and then set the **Status** toggle to **Enabled**.
4. Select one of the following protocols to connect to the virus scan engine:
   - RPC
   - ICAP
5. Select one of the following options for the files to be scanned:
   - To scan all file types, select **All files**.
   - To scan a file type from the list of extensions, select **User defined**.

     To add a file extension to the list of extensions, click **Add**. The file extension must be in uppercase letters, numbers or in combination of uppercase letters and numbers. The file extension list also supports wildcards. For example, `XL?` matches to `.XLS` and `.XLX` files.

     To remove a file extension from the list, click **Delete**. To revert to the default file extension list, click **Restore**.

> **Note:**
>
> The default list of file extensions contains the following most commonly used file types. Contact the antivirus software vendor for an up-to-date list of file types that should be included for scanning and modify the file extension list accordingly. Select the file types that you want to scan based on your requirements, the antivirus software used, and the recommendations of the antivirus software manufacturer.
>
> `386, ACE, ACM, ACV, ACX, ADT, APP, ASD, ASP, ASX, AVB, AX, BAT, BO, BIN, BTM, CDR, CFM, CHM, CLA, CLASS, CMD, CNV, COM, CPL, CPT, CPY, CSC, CSH, CSS, DAT, DEV, DL, DLL, DOC, DOT, DVB, DRV, DWG, EML, EXE, FON, GMS, GVB, HLP, HTA, HTM, HTML, HTT, HTW, HTX, IM, INF, INI, JS, JSE, JTD, LIB, LGP, LNK, MB, MDB, MHT, MHTM, MHTML, MOD, MPD, MPP, MPT, MRC, MS, MSG, MSO, MP, NWS, OBD, OBT, OBJ, OBZ, OCX, OFT, OLB, OLE, OTM, OV, PCI, PDB, PDF, PDR, PHP, PIF, PL, PLG, PM, PNF, PNP, POT, PP, PPA, PPS, PPT, PRC, PWZ, QLB, QPW, REG, RTF, SBF, SCR, SCT, SH, SHB, SHS, SHT, SHTML, SHW, SIS, SMM, SWF, SYS, TD0, TLB, TSK, TSP, TT6, VBA, VBE, VBS, VBX, VOM, VS?, VSD, VSS, VST, VWP, VXD, VXE, WBT, WBK, WIZ, WK?, WML, WPC, WPD, WS?, WSC, WSF, WSH, XL?, XML, XTP`

6. Click **Save**.

Adding a virus scan engine

You can add a virus scan engine only if the virus scanning protocol is set to ICAP.

> **Note:** If RPC protocol is used to configure a virus scanning engine, the virus scanner should be configured to make a connection to the EVS. When a successful connection is made, the virus scan engine appears in the Registered Virus Scan Engines list.

Procedure

1. Navigate to **Data Management** > **Protection** > **Antivirus** > **Virus Scanning**.
2. In the **Virus Scanning** pane, select the EVS on which you want to add the virus scan engine from the list of EVS instances.
3. In the **Registered Virus Scan Engines** pane, click **Add Scan Engine**.
4. In the **Add Scan Engine** dialog box, complete the following information:
   a. Verify the EVS where you want to add the virus scan engine.
   b. Enter the IP address or the fully qualified domain name (FQDN) of the virus scan engine host.

      The IP address and FQDN should be in the format `255.255.255.255` and `hostname.domain.com`.
   c. Enter the port of the scan engine host.

      The default port is 1344.

d. Enter the name of the scan engine service provided by the ICAP virus scan engine vendor.

   The default name is AVSCANRESP.

   The name of the scan engine may include letters, numbers, special characters and spaces. Examples of scan engine names are Virusscanengine@1 and virus_scan 1.

5. Click **Add**. The newly added virus scan engine appears in the **Registered Virus Scan Engines** list for the selected EVS.

Enabling a virus scan engine

Procedure

1. Navigate to **Data Management** > **Protection** > **Antivirus** > **Virus Scanning**.
2. In the **Virus Scanning** pane, select the EVS associated with the virus scan engine from the list of EVS instances.
3. In the **Registered Virus Scan Engines** pane, select one or more virus scan engines, and then click **Enable**.

Disabling a virus scan engine

You can disable a virus scan engine that you do not want to use. Disabling a virus scan engine results in faster file access but no virus detection.

Procedure

1. Navigate to **Data Management** > **Protection** > **Antivirus** > **Virus Scanning**.
2. In the **Virus Scanning** pane, select the EVS associated with the virus scan engine from the list of EVS instances.
3. In the **Registered Virus Scan Engines** pane, select one or more virus scan engines, and then click **Disable**.

Forcing files to be rescanned

To avoid virus threats and loss of data, it is important to rescan all files, including those that have not changed since the last time they were scanned. Rescanning migrated files increases file recall times for users (including scan time) the first time each file is accessed.

Procedure

1. Navigate to **Data Management** > **Protection** > **Antivirus** > **Virus Scanning**.
2. Click **Request Full Scan** to start scanning all files.

Modifying a virus scan engine

You can modify only the port and the name of the virus scan engine.

Procedure

1. Navigate to **Data Management** > **Protection** > **Antivirus** > **Virus Scanning**.

2. In the **Virus Scanning** pane, select the EVS associated with the virus scan engine from the list of EVS instances.
3. In the **Registered Virus Scan Engines** section, locate the the virus scan engine that you want to modify, and then click **View**.
4. In the **Scan Engine Details** dialog box, modify the information that you want to change.
5. Click **Save**.

Deleting a virus scan engine

Deleting a virus scan engine may reduce the latency of accessing the data on file systems but increases the threat of virus attacks and may result in loss of data.

Procedure

1. Navigate to **Data Management** > **Protection** > **Antivirus** > **Virus Scanning**.
2. In the **Virus Scanning** pane, select the EVS associated with the virus scan engine from the list of EVS instances.
3. Select one or more virus scan engines, and then click **Delete**.

Mobility

Mobility tasks include migrating data and metadata from an on-premises file system to an S3-compatible object storage or another on-premises file system.

Data migration to cloud

Data migration is the process of moving data and its metadata from an on-premises file system to an S3-compatible object storage or another on-premises file system. This option allows you to move older data to free up capacity on the primary on-premises file system.

Workflow for migrating the data

Complete the following workflow to move data:

1. Add a cloud account (on page 112).
2. Add a cloud destination (on page 113).
3. Add a path (on page 114), to establish the relationship between the primary on-premises file system (source) and S3-compatible object storage or another on-premises file system (destination) to migrate data.
4. Add a data migration rule (on page 115), to specify the type of files and the conditions under which they will be migrated.
5. Add a data migration policy (on page 119), to define rules to apply to specific data migration path based on the available free space on the primary file system.
6. Add a data migration schedule (on page 119), to determine the appropriate time for data migration policies to run.

Requirements for migrating the data

Before initiating the data migration process, make sure that you have the following:

- A cloud account with one of the following S3-compatible object storage: Amazon S3, Microsoft Azure, Hitachi Content Platform (HCP), HCP S3, and S3 Cloud Object Storage (HCP for cloud scale and IBM® cloud object storage).
- To migrate data to HCP S3 and HCP for cloud scale you must install an SLL certificate.
- The credentials of a user with read and write permissions to the cloud account.
- A destination location to store the migrated files, in the cloud or on-premises file system.

The following table lists the required information for adding a cloud account and destination for a supported S3-compatible object storage.

Before initiating the data migration, you have an option to test the migration flow by creating an account using Test as the provider. This option allows you to preview the outcome of the migration process without actually moving any data.

S3-compatible object storage	Account type	Server name	Destination location	User credentials	Secret credentials
HCP and HCP S3	Data Access Account with read, write, delete, purge, and search permission.	Fully qualified domain name of the HCP namespace for the account credentials and must have an assigned owner.	The folder path.	Username of the Data Access Account.	The password of the Data Access Account
Amazon S3	Access Management (IAM) account.	Auto-populates with aws.amazon.com.	The bucket with or without a subfolder.	Access key	Secret Access Key
Microsoft Azure	Azure storage account.	Auto-populates with azure.microsoft.com.	The bucket with or without a subfolder.	Name of storage account	Primary or Secondary Access Key
S3 Cloud Object Storage (HCP for cloud scale and IBM® cloud object storage)	Cloud Object Storage account.	User must provide an endpoint name.	The bucket with or without a subfolder.	Access key	Secret Access Key
Test	test	For the test account you can leave the Server Name field blank.	test	test	test

Cloud accounts

Add a cloud account to the File Administrator to move files to the object storage.

Adding a cloud account

Add a cloud account to establish seamless connectivity with the object storage.

Before you begin

Review the requirements for migrating the data.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Cloud Accounts**.
2. Click **Add Account**, and complete the following information:
   - Enter the cloud account name. The name cannot contain spaces or the following special characters: `"'*/;:<>?\|`
   - Select the supported object storage from the list.
   - If you select Microsoft Azure or Amazon S3, the server name is displayed in the **Server** field. You cannot modify this default server name.
   - Enter the user credentials and secret credentials.
3. Click **Add**.

Modifying cloud account information

You can modify the server name, user credentials, and secret credentials.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Cloud Accounts**.
2. Locate the cloud account that you want to modify.
3. Select the cloud account, and then click **Edit**.
4. Modify the information that you want to change, and then click **Save**.

   For HCP and HCP S3, you can switch between HCP and HCP S3 providers if an SSL certificate is installed on the VSP One File server.

   You cannot change the server name for Microsoft Azure and Amazon S3 cloud accounts.

Deleting a cloud account

You cannot delete the cloud account if it is being used by the cloud destination.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Cloud Accounts**.
2. Select the cloud account that you want to delete, and then click **Delete**.
3. Click **Delete** to confirm.

Cloud destinations

A cloud destination is a location where all the migrated files are stored.

Adding a cloud destination

Add a cloud destination for data migration.

Before you begin

- Review the requirements for migrating the data.
- To move the data, make sure that you have set up a destination location.

  For example:

  - Amazon S3, it is a `bucket/subfolder`. The subfolder is optional.
  - HCP, HCP S3, and Test, it is a `subfolder`.
  - Microsoft Azure, it is a `container`.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Cloud Accounts**, and then select the **Destination** tab.
2. Click **Add Destination**, and complete the following information:
   - Enter the cloud destination name. The name cannot contain spaces or the following special characters: `"'*/;:<>?\|`
   - Select the cloud account.
   - Enter the destination location.
   - Set **Encrypt in Transit** to `Yes`, to encrypt the data in transit.

     Data in transit is encrypted by default for all cloud providers except HCP and HCP S3. If the HCP destination is outside your company's firewall, make sure to manually encrypt it by setting the **Encrypted In Transit** to `yes`.
3. Click **Add**.

Modifying cloud destination information

You can change the name of the cloud destination, link it to a different cloud account, and modify its location.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Cloud Accounts**, and then select the **Destination** tab.
2. Locate the cloud destination that you want to modify.
3. Select the cloud destination, and then click **Edit**.
4. Modify the information that you want to change, and then click **Save**.

Deleting the cloud destination

You cannot delete the cloud destination if it is being used by the data migration path.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Cloud Accounts**, and then select the **Destination** tab.
2. Select the cloud destination that you want to delete, and then click **Delete**.
3. Click **Delete** to confirm.

Data migration paths

Create a data migration path that defines the migration destination. A data migration path is a long-term association between a source and destination.

You can add an on-premises or a cloud path.

To add an on-premises file system path, see Adding an on-premises data migration path (on page 114).

To add a cloud path, see Adding a cloud path (on page 114).

Adding an on-premises data migration path

Add an on-premises file system path to move data between on-premises file systems.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Paths**, and then select the **HNAS Path** from the **Add Path** list.
2. In the **Add HNAS Path** dialog box, complete the following information:
   - Select the source EVS and file system from which you want to migrate the data.
   - Select the virtual volume that you want to migrate.

     By default, the data migration includes the entire file system. To configure migration at the individual virtual volume level, select the virtual volume to be used as the primary source for the data migration path.
   - Select the destination EVS and the file system to migrate the data.
3. Click **Add**.

Adding a cloud path

Add a cloud path to move the data from the on-premises file system to object storage.

Before you begin

Make sure that the cloud destination is added.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Paths**, and then select the **Cloud Path** from the **Add Path** list.
2. In the **Add Cloud Path** dialog box, complete the following information:
   - Select the source EVS and file system from which you want to migrate the data.
   - Select the cloud destination to migrate the data.
3. Click **Add**.

Deleting data migration paths

You cannot delete a data migration path if it is being used by the data migration policy.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Paths**.
2. Select the data migration path that you want to delete, and then click **Delete**.
3. Click **Delete** to confirm.

Data migration rules

Add a data migration rule to define the set of conditions that trigger the data migration.

Adding a data migration rule by definition

You can add data migration rules using rule syntax. The rules syntax combines `INCLUDE` and `EXCLUDE` statements, where you can add various expressions to specify file types and migration conditions within these statements. For example, `INCLUDE (<FILENAME *.mp3> AND <FILE_SIZE_OVER 2GB>)`. In this example, rule syntax defines to include files with an `mp3` extension and a size exceeding `2GB` to move.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Rules**, and then select the **By Definition** from the **Add Rule** list.
2. In the **Add Data Migration Rule By Definition** dialog box, complete the following information:
   - Enter the name for the data migration rule.
   - Select the rule type. WFS/HNAS for an on-premises file system and Cloud for object storage.
   - Enter the description of the rule, explaining its purpose for your reference.
   - Set the **Case-sensitive pattern checks** to `Yes`, to enable case-sensitive rule checking.
   - Enter the rule syntax.
3. Click **Add**.

Adding data migration rule by template

You can create a data migration rule using the supported templates and completing the necessary information and criteria to create the rule.

- By File Name: Migrates all files with the same name and extension. For example,
  - `dbfile.db` migrates all files with the name `dbfile` and the extension `.db`.
  - `*.db` migrates any file with an extension of `.db` regardless of the file name.
  - `dbfile.*` migrates all files with the name `dbfile` and any extension.
  - `*dbfile.db` migrates all files ending with the name `dbfile` and the extension `.db`.
  - `dbfile*` migrates all files with a name beginning with `dbfile` and having any extension.
- By Last Access Time: Migrates files based on their last access time, either accessed or not within a specific period.
- By Last Access Time and File Name: Migrates files with a specific name and extension that have not been accessed within a specific period.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Rules**, and then select **By Template** from the **Add Rule** list.
2. In the **Add Data Migration Rule By Template** dialog box, select one of the following rule templates and specify the rule details and criteria:

- **By File Name:** Migrates all files with the same name and extension:

Field	Description
Type	Select the rule type. WFS/HNAS for an on-premises file system and Cloud for object storage.
Name	Enter the name for the data migration rule.
Description	Enter the description of the rule, explaining its purpose for the reference.
Case-sensitive pattern checks	Set the **Case-sensitive pattern checks** to `Yes`, to enable case-sensitive rule checking.
Include Criteria	In **All files named**, enter the file name and extension to be migrated to the destination. More than one file name or extension can be named in this field separated by commas. For example, *.jpg, *.bmp, *.zip. Select condition **Include** or **Exclude**, to include the files of the specified type or exclude files not of the specified type.

- **By Last Access :** Migrates files based on their last access time, either accessed or not within a specific period.

Field	Description
Type	Select the rule type. WFS/HNAS for an on-premises file system and Cloud for object storage.
Name	Enter the name for the data migration rule.
Description	Enter the description of the rule, explaining its purpose for the reference.
Include Criteria	Specify the criteria for the file to me migrated. Select Inactive less or Inactive over and specify number of days, hours, and minutes.

Field	Description
	For example: If you select **Active within** and specified three days, it considers files active if they have been accessed or modified within the specified duration that means any file accessed or modified within the last three days is considered active, while files not meeting this criterion are inactive. If you select **Inactive over** and specified three days, it considers files inactive if they have not been accessed or modified for a period exceeding the specified duration, that means any file not accessed or modified for more than three days is considered inactive, while files accessed or modified within the last three days are active.

- **By File Name and Last Access :** Migrates files with a specific name and extension that have not been accessed within a specific period.

Field	Description
Type	Select the rule type. WFS/HNAS for an on-premises file system and Cloud for object storage.
Name	Enter the name for the data migration rule.
Description	Enter the description of the rule, explaining its purpose for the reference.
Case-sensitive pattern checks	Set the **Case-sensitive pattern checks** to `Yes`, to enable case-sensitive rule checking.
Include Criteria	In **All files named**, enter the file name and extension to be migrated to the destination. More than one file name or extension can be named in this field separated by commas. For example, *.jpg, *.bmp, *.zip. In **All files not accessed within** enter the number and select days, hours, and minutes.

Field	Description
	For example, If you want to migrate all JPEG images and ZIP archives to the destination. In the **All files named** field, enter `*.jpg, *.zip`. You want to migrate files that haven't been accessed within the last six days. In the **All files not accessed within** field, enter `6` and select `days`. With the criteria set, any JPEG image or ZIP archive file that has not been accessed within the last six days will be migrated to the destination.

3. Click **Add**.

Modifying data migration rule information

You can change the rule description and definition. You can also set the Case-sensitive pattern checks.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Rules**.
2. Locate the rule that you want to modify, and then click **Edit**.
3. Modify the information that you want to change, and then click **Save**.

Data migration policies and schedules

Add data migration policy and schedule to plan, execute, and manage data migration activities.

Adding a data migration policy

Before you begin

- Add data migration path.
- Add data migration rules.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Policies and Schedules**, and then click **Add Policy**.

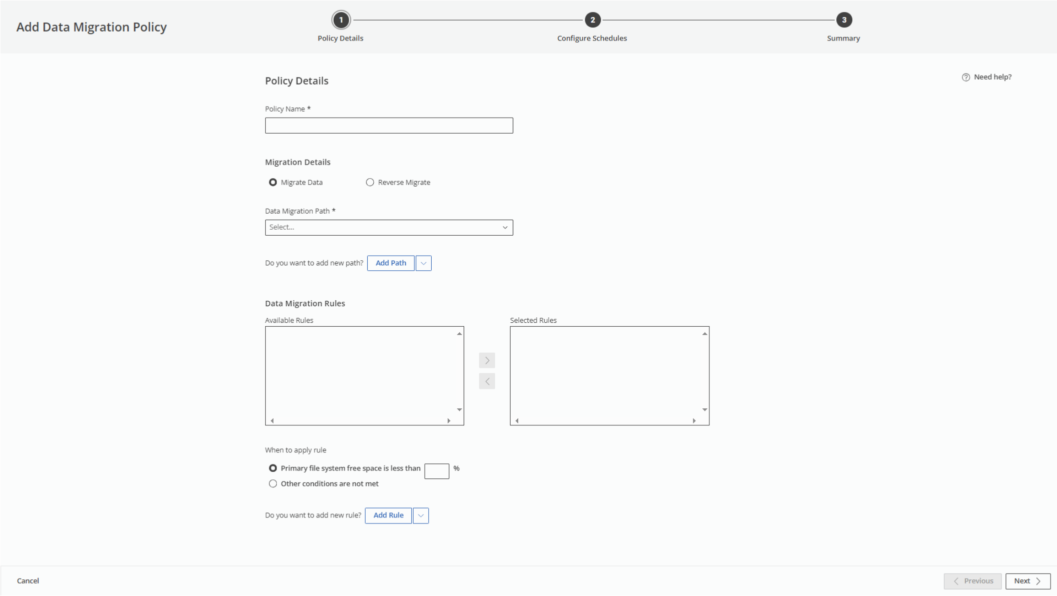
2. In the **Policy Details** page, complete the following information, and then click **Next**.

   - Enter the name for the data migration policy. The name can consist of alphanumeric characters, underscores (_), or hyphens (-), with a maximum length of 50 characters. Special characters and spaces are not allowed.
   - Select the migration type whether Migrate data or Reverse migrate.

     Migrate Data: Migrates data from the source to the destination.

     Reverse Migrate: Reverts the data from the destination to the source.

     You can only reverse migrate from the WFS/HNAS destination. Files migrated from the source to the destination will be returned to the EVS and File System when the reverse migration policy criteria are met.
   - Select the data migration path. The following data migration source and destinations information is displayed:
     - **Primary EVS/File System:** Displays the name of the EVS and file system as primary storage (the migration source).
     - **Virtual Volume:** Virtual volumes are not relevant when migrating data to object storage.
     - **Secondary Target Type:** Displays an on-premises file system or cloud destination type.
     - **Secondary File System:** Displays the name of the file system on the secondary system (the migration destination).
   - Select the rule. The rule defines the set of conditions that trigger the data migration or reverse data migration.
   - You can specify one of the following conditions to the selected rules:
     - When the primary file system free space falls below X% . Set the percentage level for this condition.
     - When other conditions are not met. These conditions are defined in the selected rules.



Add Data Migration Policy

1 Policy Details — 2 Configure Schedules — 3 Summary

Policy Details

ⓘ Need help?

Policy Name *

Migration Details

● Migrate Data ○ Reverse Migrate

Data Migration Path *

Select...

Do you want to add new path? Add Path

Data Migration Rules

Available Rules

Selected Rules

When to apply rule

● Primary file system free space is less than □ %

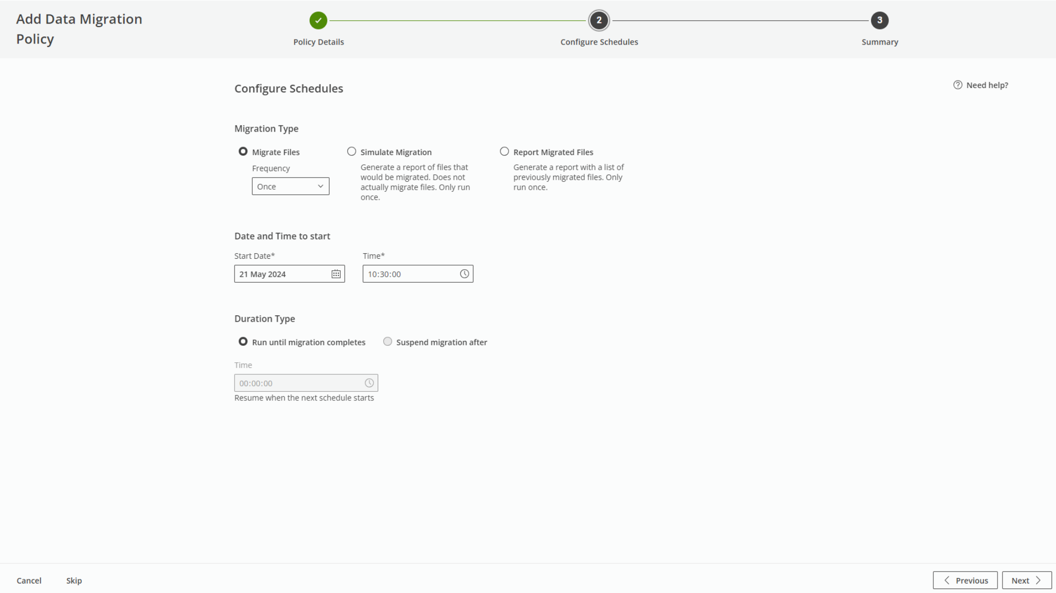
○ Other conditions are not met

Do you want to add new rule? Add Rule

Cancel

Previous Next

3. In the **Configure Schedules** page, complete the following information, and then click **Next**.
   - Select one of the following migration types:
     - **Migrate Files:** Select how often you want the policy to run: once, daily, or weekly. For example, if you select the `Once` option, the policy runs only once at the specified date and time.
     - **Simulate Migration:** Select this option to generate a report of the files that will be migrated in the next schedule. This action initiate file migration and only runs once.
     - **Report Migrated Files:** Select this option to generate a report of already migrated files. This option only applies to the WFS/HNAS migration type and only runs once.
   - Specify the date and time for scheduling the execution of the policy.
     - Select the start date from the calendar for the initial run.
     - Enter the scheduled run time using a 24-hour clock. For example, enter 11:59 PM as 23:59:00.
   - Select one of the following duration types:
     - **Run until migration completes:** The policy will continue to run until the migration process is complete.
     - **Suspend migration after:** The policy stops at a specified time in the time field and will resume at the next schedule. This option applies only to the Cloud migration type.



Configure Schedules

Migration Type

● Migrate Files

Frequency: Once

○ Simulate Migration

Generate a report of files that would be migrated. Does not actually migrate files. Only run once.

○ Report Migrated Files

Generate a report with a list of previously migrated files. Only run once.

Date and Time to start

Start Date*: 21 May 2024

Time*: 10:30:00

Duration Type

● Run until migration completes ○ Suspend migration after

Time: 00:00:00

Resume when the next schedule starts

4. In the **Summary** page, review the data migration policy, and the click **Add**. Alternatively, you can add another data migration policy by clicking **Create & add another**.

Viewing and modifying data migration policy

You can view the data migration policy details, add new rules, remove existing rules linked with the policy, and add new schedule.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Policies and Schedules**.
2. Select the data migration policy that you want to view or edit, and then click **View**.
   The **Overview** tab lists the policy details, and the **Schedules** tab lists the schedule information.
3. To modify the policy details, click the edit icon. You can add new rules, remove existing rules linked with the policy, and add new schedule.
4. Click **Save**.

Modifying data migration schedule

You can modify migration types, date and time to start, and duration type of the schedule.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Policies and Schedules**.
2. Select the migration policy for which you want to change the schedule, and then click **View**.
   The **Overview** tab lists the policy details and the **Schedule** tab lists the schedule information.
3. Click the **Schedule** tab, select the schedule that you want to change, and then click **Edit**.
4. Modify the information you want to change, and then click **Save**.

Viewing and downloading the data migration status report

After completing a data migration policy cycle, a data migration report is generated that includes details about migrated files and available free space before and after the migration. The reports of the last five scheduled migrations are saved, and the older ones are purged.

Procedure

1. Navigate to **Data Management** > **Mobility** > **Cloud Tiering** > **Status**.
2. Locate the report that you want to view.
3. Click **View**.
   The **Report Details** and **Log Details** tabs are displayed.
   - **Report Details** tab shows the migration summary and source and destination statistics.
   - Click the **Log Details** tab to view detailed logs for the data migration.
4. To download the report, click the download icon. The report is downloaded in compressed file format.

Chapter 7: System configuration

System configuration includes configuring managed servers and nodes, managing access and settings for the VSP One File server, configuring protocols for file access and transfer, and managing file services.

System

System tasks include configuring and monitoring managed servers, nodes, and firmware, and registering license keys.

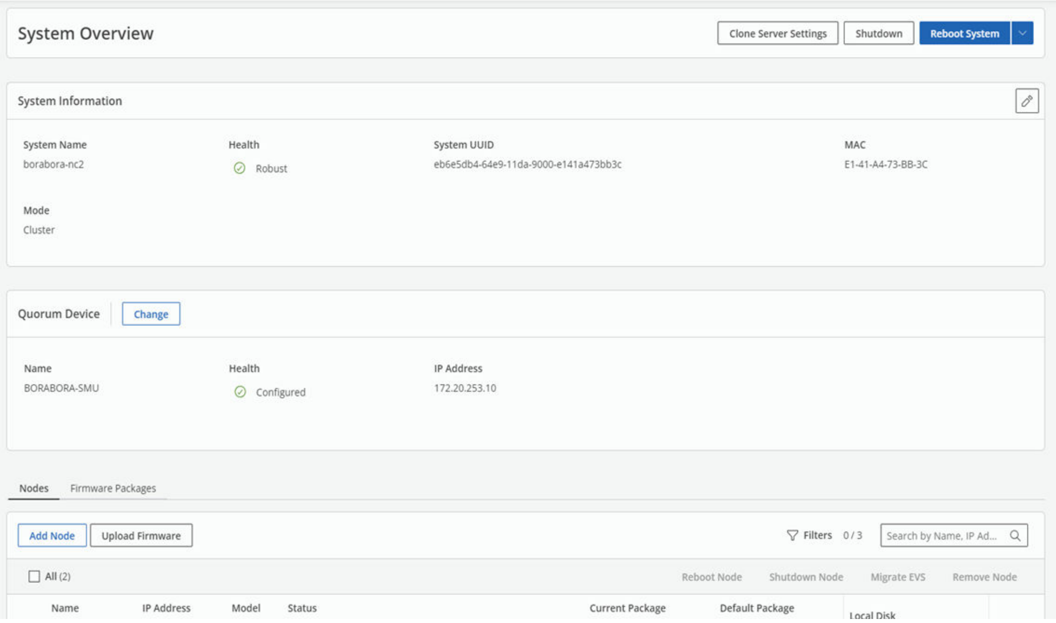
Configuring servers and nodes

Storage servers or server clusters that are administered by the VSP One File management software are referred to as managed servers. Only one managed server and its associated nodes can be managed at a time. To select a managed server, use the server list in the secondary header of the File Administrator GUI.

You can view overview information for a managed server and associated nodes in the **System Overview** pane. This pane shows information such as:

- The health, UUID, and mode (Stand-alone or Cluster) for the managed server.
- The quorum device and device status if the managed server is a cluster.
- The nodes that are associated with the managed server.
- Uploaded firmware packages.

To view server and node information, navigate to Configuration > System > System Overview.



System Information

System Name	Health	System UUID	MAC
borabora-nc2	✓ Robust	eb6e5db4-64e9-11da-9000-e141a473bb3c	E1-41-A4-73-BB-3C

Mode
Cluster

Name	Health	IP Address
BORABORA-SMU	✓ Configured	172.20.253.10

□ All (2)

Name	IP Address	Model	Status	Current Package	Default Package	Local Disk

Managing servers

The server mode, Stand-alone or Cluster, determines the tasks that you can complete for a managed server. Only one managed server can be managed at a time. To select a managed server, use the server list in the secondary header of the File Administrator GUI.

Note: To add or remove managed servers, use the System Administrator application as described in the *Hitachi Virtual Storage Platform One File Installation and Configuration Guide*.

Changing the server name

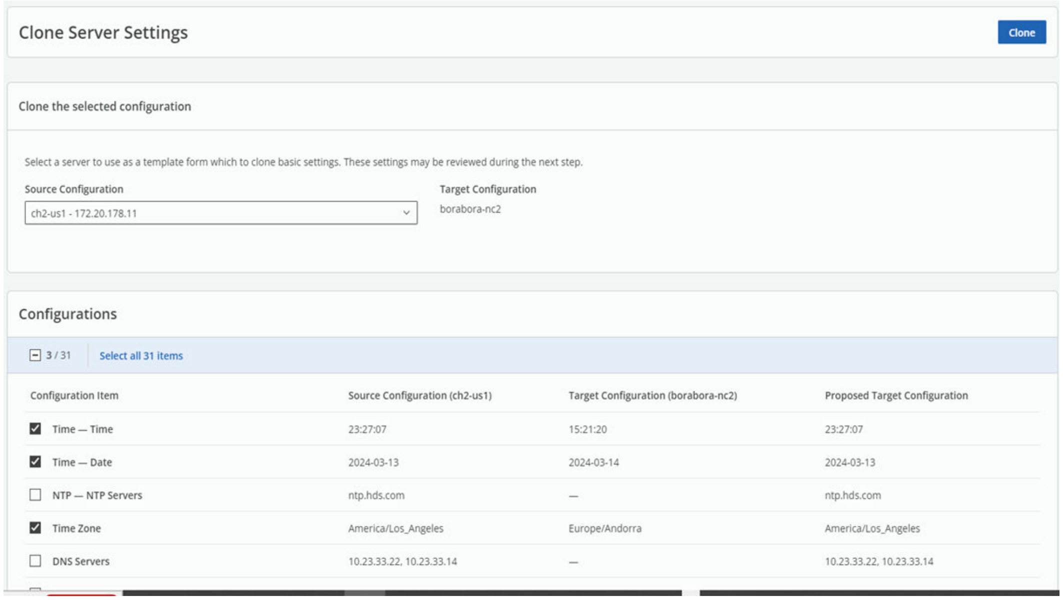
You can view configuration information for a managed server such as the server name, server health, UUID, MAC address, and mode (Stand-alone or Cluster). Of this information, you can change the server name.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. In the **System Information** pane, click the edit icon and change the server name in the **Server Name** box.
3. Click **Save**.

Cloning settings for a server

You can copy certain configuration settings from a source managed server to a target server.



Clone Server Settings

Clone the selected configuration

Select a server to use as a template form which to clone basic settings. These settings may be reviewed during the next step.

Source Configuration: ch2-us1 - 172.20.178.11

Target Configuration: borabora-nc2

Configurations

Configuration Item	Source Configuration (ch2-us1)	Target Configuration (borabora-nc2)	Proposed Target Configuration
☑ Time — Time	23:27:07	15:21:20	23:27:07
☑ Time — Date	2024-03-13	2024-03-14	2024-03-13
□ NTP — NTP Servers	ntp.hds.com	—	ntp.hds.com
☑ Time Zone	America/Los_Angeles	Europe/Andorra	America/Los_Angeles
□ DNS Servers	10.23.33.22, 10.23.33.14	—	10.23.33.22, 10.23.33.14

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. In the **System Overview** pane, click **Clone Server Settings**.
3. In the **Clone Server Settings** pane, select the server that you want to use as a source in the **Source Configuration** list.

   The target server is shown in the **Target Configuration** field.
4. In the **Configurations** pane, select the configuration items that you want to clone or click **All** to select all items.
5. Click **Clone**.

Result

A message shows the status of the server cloning process. When the process is complete, you must reboot the server to view the configuration changes.

Rebooting a server

For some server tasks, you must reboot the server to view updates. For example, to view configuration settings cloned from one server to another, you must reboot the target server.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. In the **System Overview** pane, select one of the following options to reboot the server:
   - For a server in **Stand-alone** mode, click **Reboot System**.
   - For a server in **Cluster** mode, click **Reboot System**, and then select one of the following options:
     - **Sequentially**: Nodes in the managed server cluster reboot one at a time.
     - **Simultaneously**: Nodes in the managed server cluster reboot at the same time.

3. Click **OK, Continue** to confirm.

Shutting down a server

When you want to shut down a server (for example, to replace a server with another) power off by using the shutdown process to help prevent data loss and unexpected errors. When a server is shut down, all associated cluster nodes are also shut down.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. In the **System Overview** pane, click **Shutdown**.
3. Click **Ok, Continue** to confirm.

Result

A message shows the status of the server shutdown process. If the process is successful, the server is powered off and requires a manual restart. All associated cluster nodes also require a manual restart.

Managing nodes

Administrators can configure a managed server as a standalone server or as a node in a cluster that lets multiple servers operate together as a single entity. The clustered nodes share storage under the centralized management of a single VSP One File instance and use a common namespace.

File services within the cluster are virtualized as EVS instances, and any EVS within the cluster can reside on, or be migrated to, any node within the cluster.

Viewing or changing a quorum device

A quorum device maintains cluster functions if a communication failure occurs between the nodes in a cluster. A quorum device is also used to restore the cluster registry, which contains the cluster configuration. All nodes in the cluster share the quorum device.

A quorum device is selected during the initial set up of the cluster. You can view information about the device or change the device at any time.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. In the **Quorum Device** pane, view the quorum device name, health status, and IP address or click **Change** to change the device.

Adding a node to a cluster

To add a node to a cluster, you must define a cluster node IP address. This IP address maintains heartbeat communication among cluster nodes and between the cluster nodes and the quorum device.

Important: The node must be the same hardware model as the nodes already in the cluster.

The number of nodes that you can add to a cluster depends on cluster licenses. To view license information, navigate to Configuration > System > License Keys.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. On the **Nodes** tab, click **Add Node**.

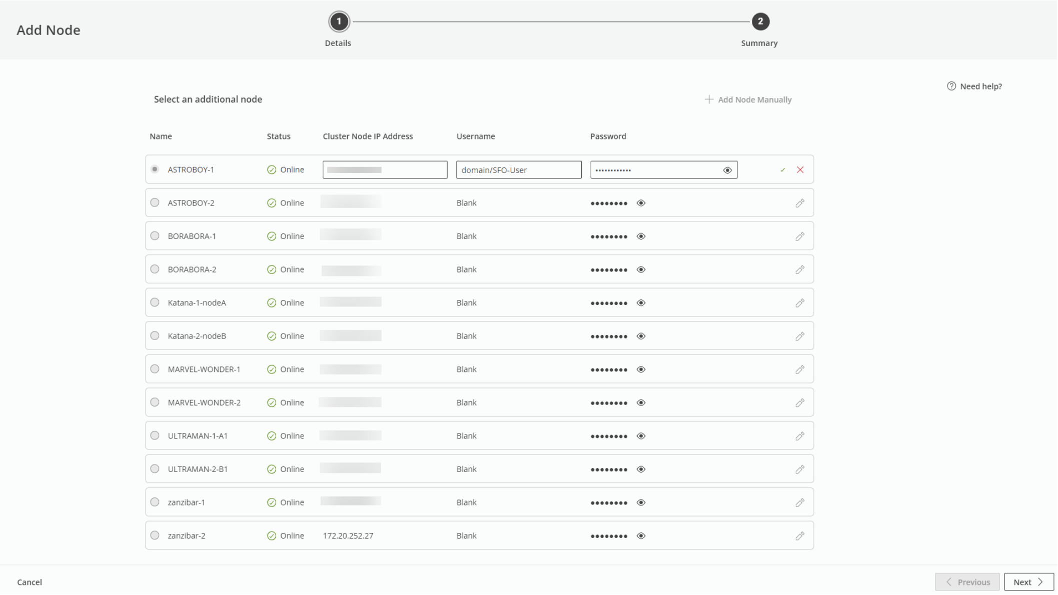
3. In the **Add Nodes** wizard, use one of the following options to select the node that you want to add, and then click **Next**:

   - To select a node that is currently managed by File Administrator, complete the following information:

     a. Select the node.

     b. In the **Cluster Node IP Address** box, use the provided IP address or enter another address.

     c. In the **Username** and **Password** boxes, enter the username and password for the node.



Add Node

Select an additional node

Name	Status	Cluster Node IP Address	Username	Password
● ASTROBOY-1	Online	[redacted]	domain/SFO-User	•••••••••••••
○ ASTROBOY-2	Online	[redacted]	Blank	••••••••
○ BORABORA-1	Online	[redacted]	Blank	••••••••
○ BORABORA-2	Online	[redacted]	Blank	••••••••
○ Katana-1-nodeA	Online	[redacted]	Blank	••••••••
○ Katana-2-nodeB	Online	[redacted]	Blank	••••••••
○ MARVEL-WONDER-1	Online	[redacted]	Blank	••••••••
○ MARVEL-WONDER-2	Online	[redacted]	Blank	••••••••
○ ULTRAMAN-1-A1	Online	[redacted]	Blank	••••••••
○ ULTRAMAN-2-B1	Online	[redacted]	Blank	••••••••
○ zanzibar-1	Online	[redacted]	Blank	••••••••
○ zanzibar-2	Online	172.20.252.27	Blank	••••••••

   - To select a node that is not currently managed by File Administrator, click **Add Node Manually**, complete the following information, and then click **Add**. The node is added to the list of nodes in the wizard where you can select it.

     a. In the **Joining Node Admin EVS IP address** box, enter the IP address for the admin EVS that is hosted by the node that you want to add.

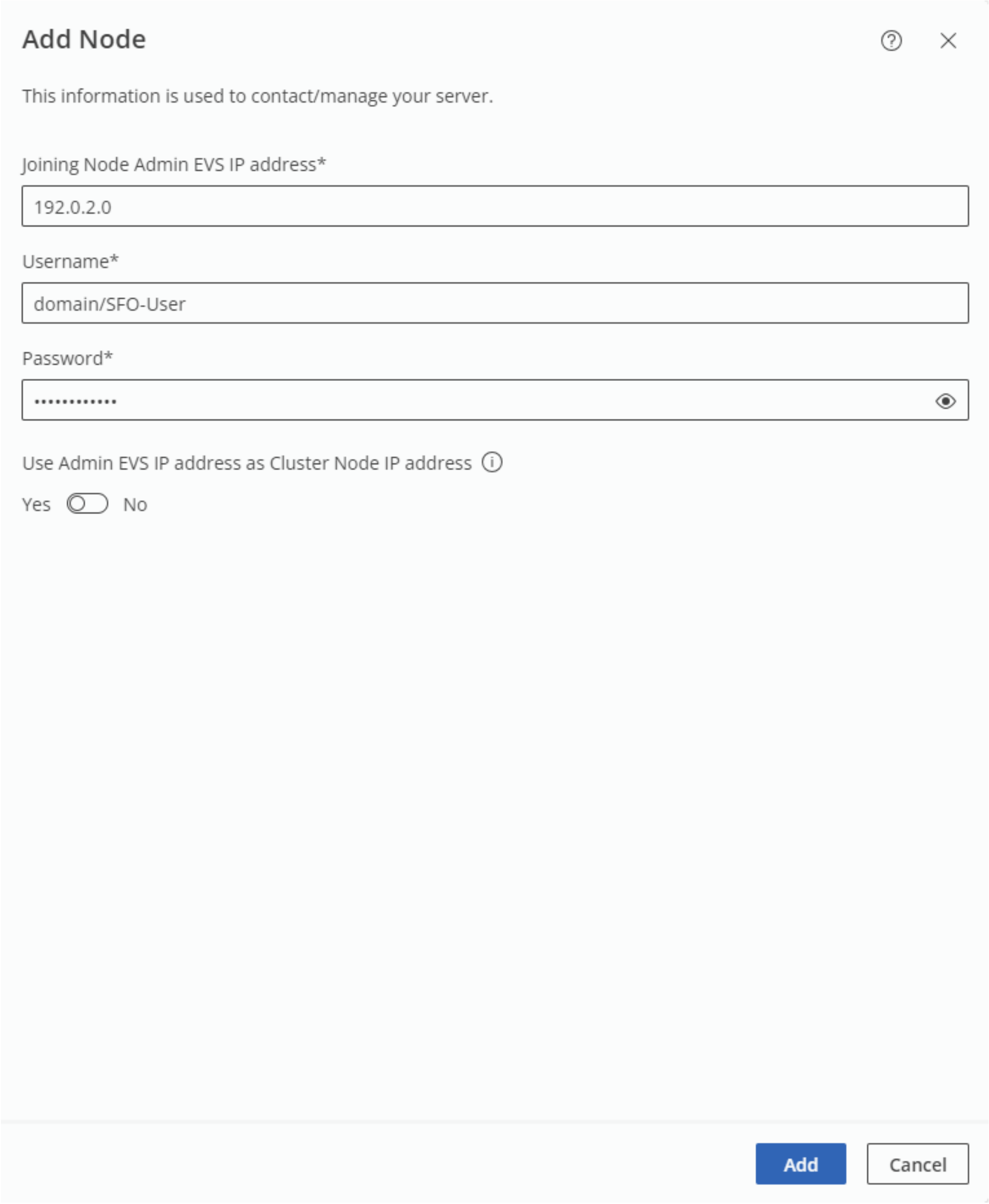
     b. In the **Username** and **Password** boxes, enter the username and password for the node.

     c. (Optional) To define a cluster node IP address that is different than the admin EVS IP address, set the **Use Admin EVS IP address as Cluster Node IP address** toggle switch to **No** and enter the following information:

        - Cluster node IP address

        - Cluster node subnet mask

The default value is **Yes**, which specifies that the admin EVS IP address is used as the cluster node IP address.



Add Node

This information is used to contact/manage your server.

Joining Node Admin EVS IP address*: 192.0.2.0

Username*: domain/SFO-User

Password*: ••••••••••••

Use Admin EVS IP address as Cluster Node IP address

Yes ○ No

4. In the **Summary** page, review the information for the node and cluster and all notifications, select the confirmation checkbox, and then click **Finish**.

Result

A message shows the status of the node addition process. If the process is successful, the node automatically reboots and joins the cluster.

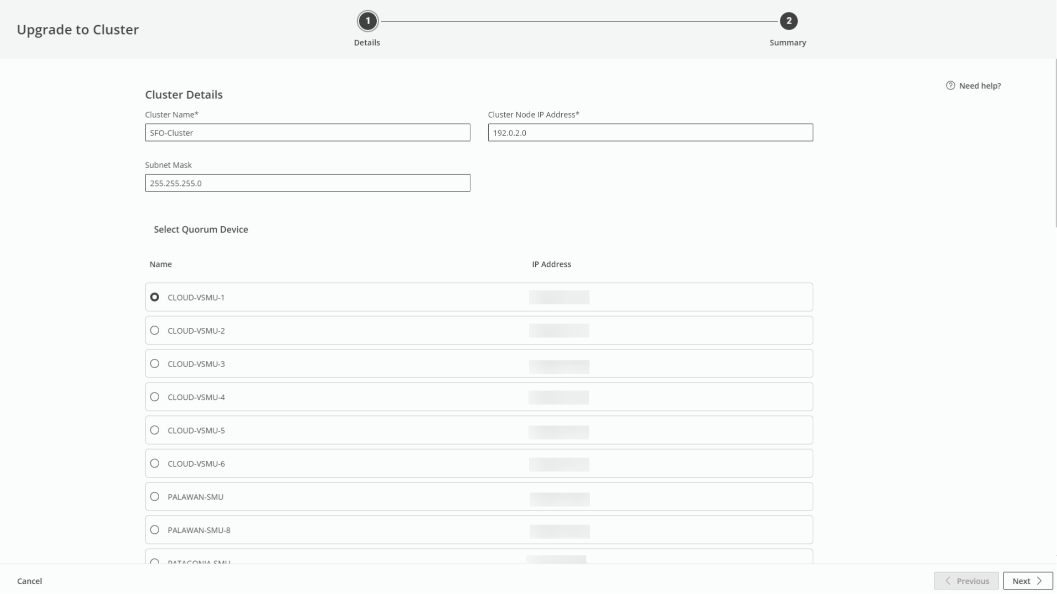
Upgrading a single node to a cluster

If the managed server mode is Stand-alone, you can upgrade the node to a cluster. When the upgrade is complete, the managed server status changes to Cluster.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. On the **Nodes** tab, click **Upgrade to Cluster**.
3. Click **Ok, Continue** to confirm that the node will require a reboot.
4. In the **Upgrade to Cluster** wizard, enter the following information, and then click **Next**:
    a. Enter the cluster name, IP address, and subnet mask of the cluster.
    b. Select a quorum device for the cluster.
    c. (Optional) Select a node to add to the cluster. If the node that you want to add is not shown in the list, click **Add Node Manually**, complete the following information, and then click **Add**. The node is then added to the list of nodes in the wizard.
        - In the **Joining Node Admin EVS IP address** box, enter the IP address for the admin EVS that is hosted by the node that you want to add.
        - In the **Username** and **Password** boxes, enter the username and password for the node.
        - (Optional) To define a cluster node IP address that is different than the admin EVS IP address, set the **Use Admin EVS IP address as Cluster Node IP address** toggle switch to **No** and enter the following information:
            - Cluster node IP address
            - Cluster node subnet mask

        The default value is **Yes**, which specifies that the admin EVS IP address is used as the cluster node IP address.



Cluster Details

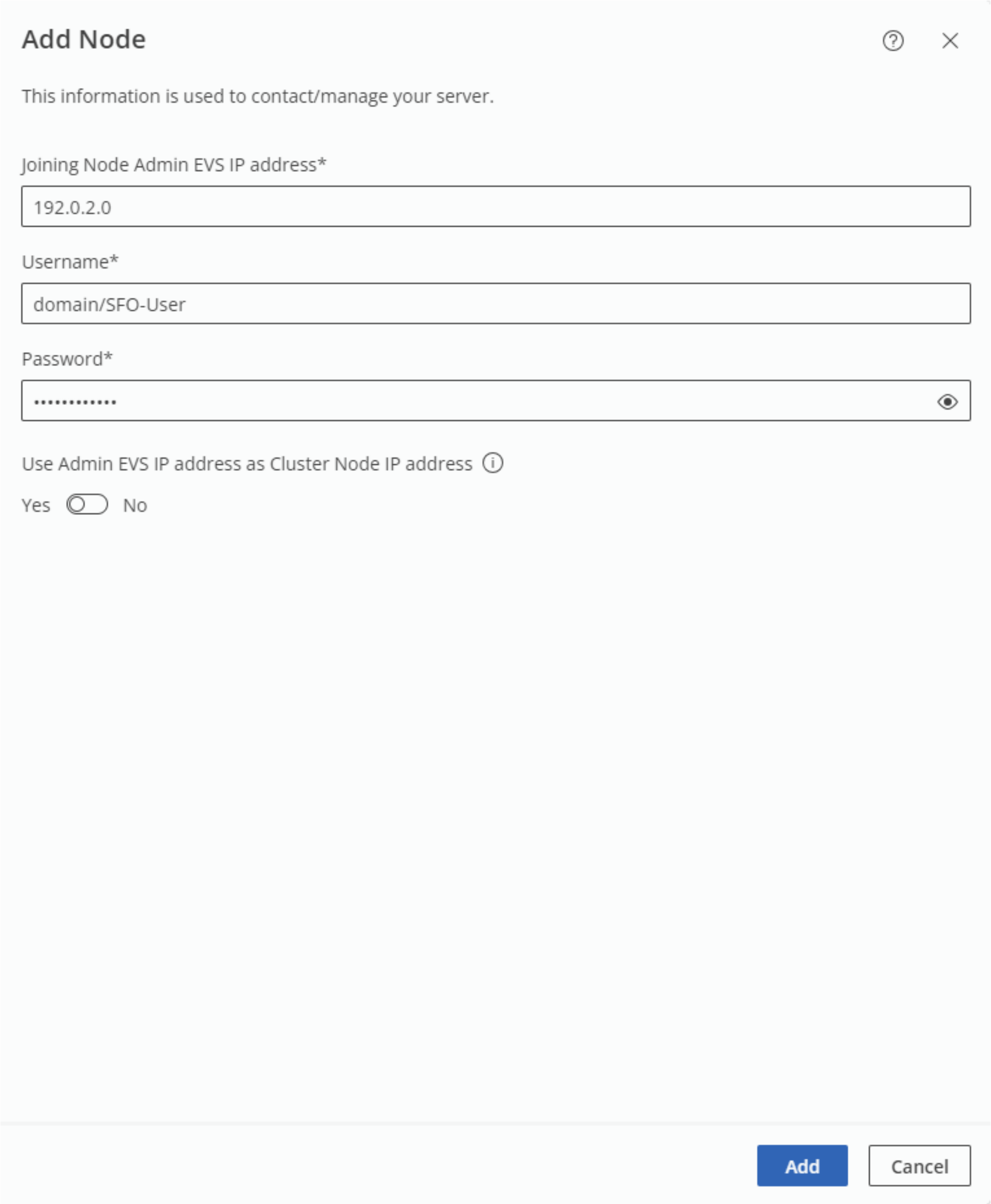
Cluster Name*: SFO-Cluster

Cluster Node IP Address*: 192.0.2.0

Subnet Mask: 255.255.255.0

Select Quorum Device

Name	IP Address
● CLOUD-VSMU-1	[redacted]
○ CLOUD-VSMU-2	[redacted]
○ CLOUD-VSMU-3	[redacted]
○ CLOUD-VSMU-4	[redacted]
○ CLOUD-VSMU-5	[redacted]
○ CLOUD-VSMU-6	[redacted]
○ PALAWAN-SMU	[redacted]
○ PALAWAN-SMU-8	[redacted]
○ PATAGONIA-SMU	[redacted]



Add Node

This information is used to contact/manage your server.

Joining Node Admin EVS IP address*

192.0.2.0

Username*

domain/SFO-User

Password*

••••••••••••

Use Admin EVS IP address as Cluster Node IP address

Yes ○ No

5. In the **Summary** page, review the new cluster configuration information, and then click **Finish**.

Result

A message shows the status of the node upgrade process. If the process is successful, the node automatically reboots and joins the cluster.

Removing a node from a cluster

You can remove a node from a cluster if the node has failed or is no longer needed.

Before you begin

Services hosted by the node must be migrated to a different node.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. On the **Nodes** tab, select the node or nodes that you want to remove, and then click **Remove Node**.
3. Click **OK, Continue** to confirm.

Result

A message shows the status of the node removal process. If the process is successful, the node is removed from the cluster and is configured as a standalone node.

EVS instances that were hosted by the removed node are automatically migrated to another cluster and details are provided in a confirmation message.

Migrating an EVS within a cluster

EVS migration occurs automatically as part of the failover resiliency of a cluster. You can also manually migrate EVS instances from one node to another within the same cluster.

Each node can host a maximum of 64 EVS instances. However, a cluster can host a maximum of 64 EVS instances from all nodes in the cluster.

> **Note:** When migrating an EVS, both the source and destination cluster must be running the same major firmware revision.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. On the **Nodes** tab, select the node or nodes that host the EVS that you want to migrate, and then click **Migrate EVS**.
3. In the **To** list, select the node that you want to migrate to.
4. Click **Migrate**.

Viewing nodes

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. Go to the **Nodes** tab.

   The following information is shown for each node:

Field/Item	Description
Name	The node name.
IP Address	The node IP address.

Field/Item	Description
Model	The node hardware model.
Status	The status of the node.
EVS	The EVS instances hosted by the node. Click an EVS to open the **EVS Details** page. To edit the EVS, see Modifying an EVS (on page 36).
Current Package	The firmware package that is currently in use for the node. If this package is different than the package in the **Default Package** field, reboot the node to update the firmware to the version in the default package.
Default Package	The default firmware package to be used for the node. You must reboot the node to update the firmware to the version in the default package.
Local Disk Free Space	The amount of free disk space on the node.
Local Disk Percentage	The percentage of the disk space used on the node.

Rebooting a node

For some tasks, you must reboot a node or nodes to view updates. For example, if you change the default firmware package for a single node, you must reboot the node for the change to take effect.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. On the **Nodes** tab, select the node or nodes that you want to reboot, and then click **Reboot Node**.
3. Click **Ok, Continue** to confirm.

Shutting down a node

You can shut down a node to safely end processes and close connections. Powering off a node by using the shutdown process helps to prevent data loss and unexpected errors. When a node in a cluster is shut down, other nodes in the cluster are still available.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. On the **Nodes** tab, select the node or nodes that you want to shut down, and then click **Shutdown Node**.
3. Click **Ok, Continue** to confirm.

Result

A message shows the status of the node shutdown process. If the process is successful, the node is powered off and requires a manual restart.

Monitoring node performance

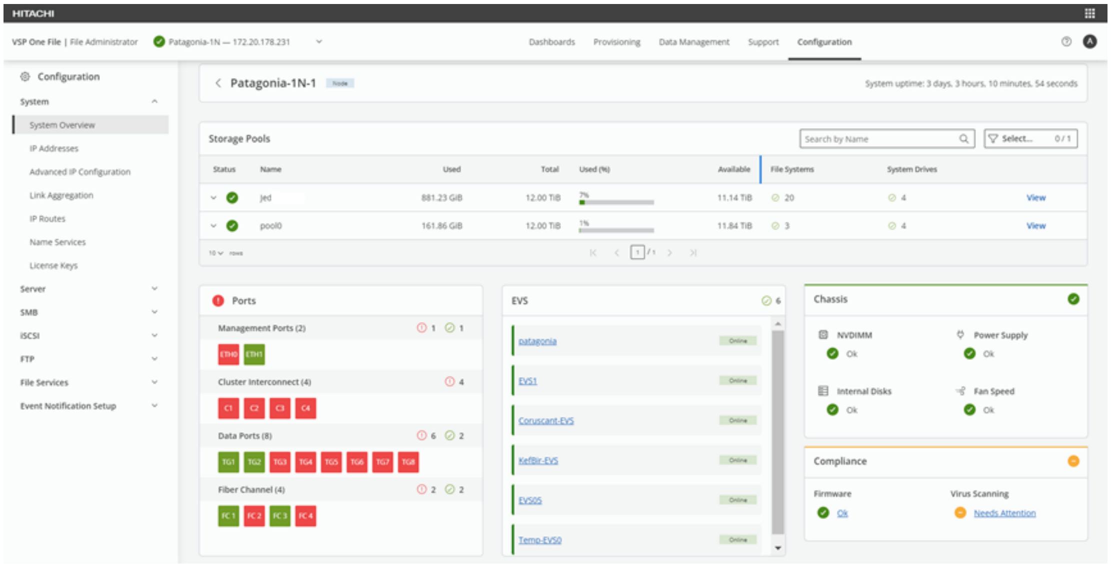
A dashboard that displays key resource information is available for each node. The dashboard contains multiple panels that report data associated with the node such as storage pools, ports, EVS instances, power consumption, and temperature status.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. On the **Nodes** tab, select the node that you want to monitor, and then click **View**.

Result

A dashboard is displayed for the node.



System uptime: 3 days, 3 hours, 10 minutes, 54 seconds

Storage Pools

Status	Name	Used	Total	Used (%)	Available	File Systems	System Drives	
✓	Jed	881.23 GiB	12.00 TiB	7%	11.14 TiB	20	4	View
✓	pool0	161.86 GiB	12.00 TiB	1%	11.84 TiB	3	4	View

Ports

Management Ports (2) ! 1 ✓ 1

Cluster Interconnect (4) ! 4

Data Ports (8) ! 6 ✓ 2

Fiber Channel (4) ! 2 ✓ 2

EVS ✓ 6

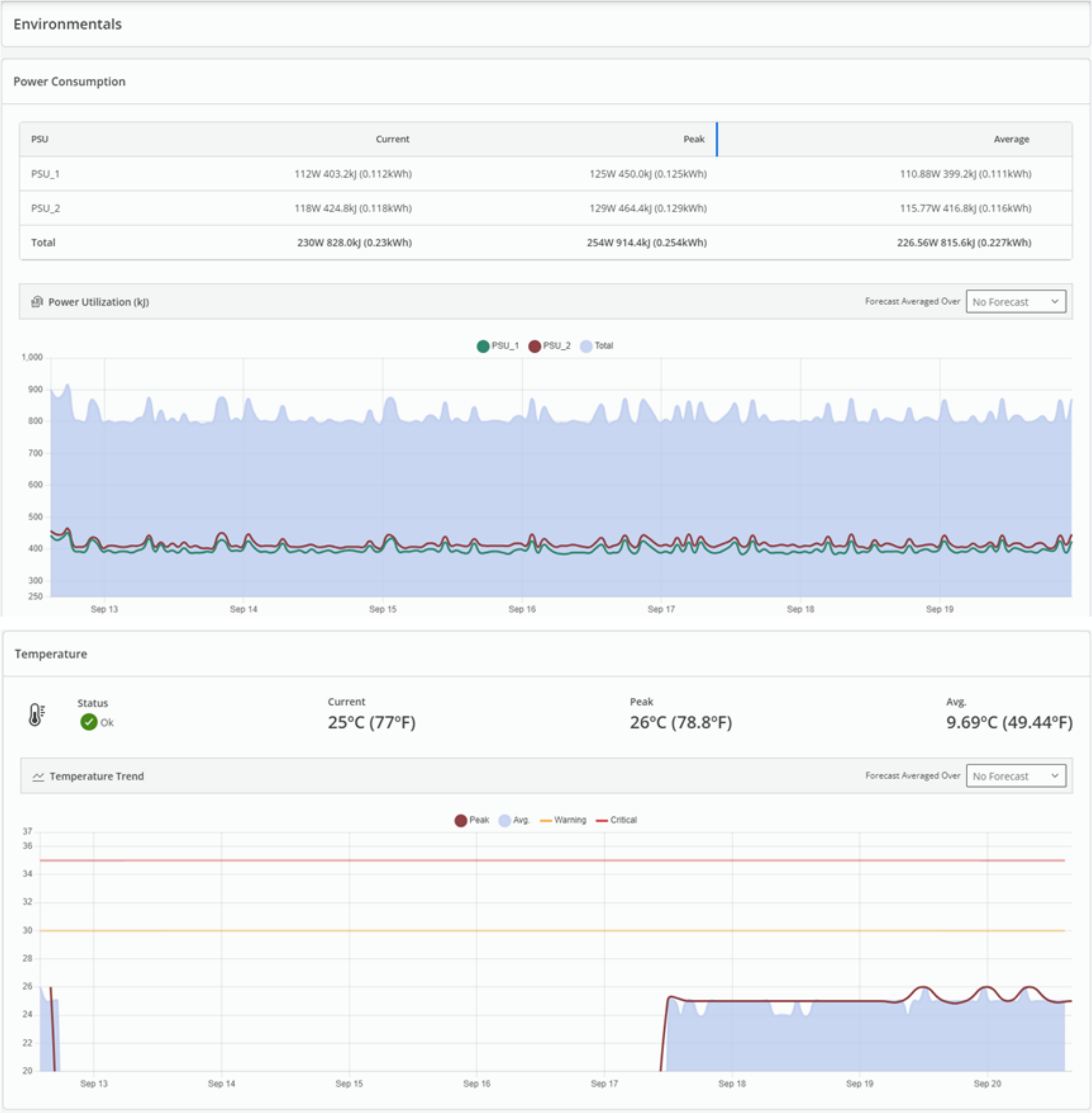
patagonia	Online
EVS1	Online
Coruscant-EVS	Online
KefBir-EVS	Online
EVS05	Online
Temp-EVS0	Online

Chassis ✓

NVDIMM: ✓ Ok
Power Supply: ✓ Ok
Internal Disks: ✓ Ok
Fan Speed: ✓ Ok

Compliance

Firmware: ✓ Ok
Virus Scanning: Needs Attention



Environmentals

Power Consumption

PSU	Current	Peak	Average
PSU_1	112W 403.2kJ (0.112kWh)	125W 450.0kJ (0.125kWh)	110.88W 399.2kJ (0.111kWh)
PSU_2	118W 424.8kJ (0.118kWh)	129W 464.4kJ (0.129kWh)	115.77W 416.8kJ (0.116kWh)
Total	**230W 828.0kJ (0.23kWh)**	**254W 914.4kJ (0.254kWh)**	**226.56W 815.6kJ (0.227kWh)**

Temperature

Status: Ok

Current: 25°C (77°F)

Peak: 26°C (78.8°F)

Avg.: 9.69°C (49.44°F)

The dashboard contains the following panels to report data by resource type:

- Storage Pools panel (on page 136)
- Ports panel (on page 138)
- EVS panel (on page 138)
- Chassis panel (on page 138)
- Compliance panel (on page 138)
- Power Consumption panel (on page 139)
- Temperature panel (on page 139)

Storage Pools panel

The **Storage Pool** panel displays data for the storage pools that are associated with a node. This panel includes the following information for each pool:

Status

The status of the storage pool that indicates the pool is OK or there is a warning.

Name

The name of the storage pool.

Used

The amount of storage that is used by the storage pool.

Total

The amount of storage that is allocated to the storage pool.

Used (%)

The amount of storage that is used by the storage pool displayed as a percentage. The percentage bar is color-coded to quickly alert you to the status of the storage usage.

- Green: The percentage of storage used is normal.
- Red: The percentage of storage used meets or exceeds the warning threshold set for the storage pool.

Available

The amount of storage space that is available.

File Systems

The number of file systems that are associated with the storage pool and the file system status.

System Drives

The number of system drives that are associated with the storage pool and the pool status.

Usage forecasting

You can forecast usage for a six month period. The forecast is based on the current usage data from a selected time period. To view forecast data in a graph, expand the storage pool row, and then select the time period that you want in the Forecast Average Over list. For example, if you select Last Month, the usage data for the last month is used to forecast usage for a six month period.

By default, this graph shows usage and when usage nears or meets the critical threshold. Click the Usage and Critical options to toggle to add or remove these metrics from the graph.

You can also view usage for each of the file systems that are associated with the storage pool by clicking File Systems for the graph. By default, the graph shows usage for all file systems. Click a file system label to add or remove the system from the graph.

Ports panel

The **Ports** panel displays the ports that are associated with the node. The ports are color-coded to alert you to the status of the port.

- Green: The port is up and operational.
- Yellow: There is a warning associated with the port.
- Red: The port is down or disabled.

EVS panel

The **EVS** panel displays the EVS instances that are assigned to the node and the status of each instance. To view information about an EVS, click the EVS link to open the details pane. You can view and edit the information as described in Modifying an EVS (on page 36).

Chassis panel

The **Chassis** panel displays the status of the following node chassis components:

NVDIMM

The status of the server NVDIMM devices. The status reflects a summary of the two devices.

Power Supply

The status of the cluster power supply units (PSUs).

Internal Disks

The status of the node internal hard disks.

Fan Speed

The status of the fans in the node chassis.

Compliance panel

The **Compliance** panel displays the status of the firmware images and virus scanning.

Firmware

The status of the installed firmware. To view and manage firmware packages, click the status text. For information about uploading and managing firmware, see Managing firmware (on page 140).

Virus Scanning

The status of the virus scanning engines for the EVS instances associated with the node. Click the status text to view the list of EVS instances and the number of associated virus scanning engines for each EVS, if applicable. To view detailed information about the virus scanning engines for an EVS, click View. For information about adding and managing virus scanning engines, see Virus scanning (on page 104).

Power Consumption panel

The **Power Consumption** panel shows the current, peak, and average power consumption for each power supply unit (PSU) in the node and the totals for the combined PSUs.

Usage forecasting

You can forecast usage for a six month period. The forecast is based on the current usage data from a selected time period. To view forecast data in a graph, select the time period that you want in the Forecast Average Over list. For example, if you select Last Month, the usage data for the last month is used to forecast usage for a six month period.

By default, the graph shows usage for all PSUs. Click a PSU label to add or remove the PSU from the graph.

Temperature panel

The **Temperature** panel displays the status of the node temperature and the current, peak, and average temperature.

Tremperature trending

You view the temperature trending for a six month period. The trend is based on the current temperature data for a selected time period. To view trend data in a graph, select the time period that you want in the Forecast Average Over list. For example, if you select Last Month, the temperature data for the last month is used to forecast temperatures for a six month period.

By default, the graph shows peak, average, warning, critical metrics. Click a metric label to add or remove the metric from the graph.

Managing block storage systems

If system drives in a storage system are shared by file and block storage pools, you can monitor the capacity for both pool types from Block Storage Pool panel in the Health dashboard. This single point of tracking capacity usage helps you to avoid performance issues such as the system slowing down as usage nears thresholds or halting if the system unexpectedly runs out of storage space.

For a description of the information displayed for block storage pools, see Block Storage Pool panel (on page 18).

Registering a block storage system

To monitor block storage pools from the Block Storage Pool panel in the Health dashboard, you must register the storage systems that are associated with the pools.

> **Important:** The block storage systems must be VSP One Block 20 or later systems.

Procedure

1. From the app switcher menu (⁝⁝⁝), select **System Administrator**.

2. Navigate to **Storage Subsystems**.
3. In the **Storage Subsystems** pane, click **Add Storage Subsystem**.
4. Enter the IP address, username, and password for the storage system, and then click **Add**.

Next steps

You can view the usage data for the storage pools associated with the storage system as described in Block Storage Pool panel (on page 18).

Modifying a block storage system

If the IP address, username, or password of a block storage system has changed, you can update the information to maintain connection to the system.

Procedure

1. From the app switcher menu (▦), select **System Administrator**.
2. Navigate to **Storage Subsystems**.
3. In the **Storage Subsystems** pane, identify the storage system that you want to modify, and then click **Edit**.
4. Update the storage system IP address, username, or password.

   To retain the existing password, leave the **Password** box blank.
5. Click **Save**.

Deleting a block storage system

If you delete a block storage system, you can no longer monitor the storage pools associated with the storage system in the Block Storage Pool panel of the Health dashboard.

Procedure

1. From the app switcher menu (▦), select **System Administrator**.
2. Navigate to **Storage Subsystems**.
3. In the **Storage Subsystems** pane, select the storage system or systems that you want to remove, and then click **Delete**.
4. Click **Delete** to confirm.

Managing firmware

Server hardware includes disk drives on which software and firmware images are loaded. You can upload firmware packages, view loaded packages, set a package as the default, or remove packages.

Uploading a firmware package

When you upload a firmware package, the package is installed on all nodes associated with the managed server.

Procedure

1. Navigate to **System** > **System Overview**.
2. On the **Firmware Packages** tab, click **Upload Firmware**.
3. In the **Upload Package** dialog box, select one of the following options to upload the package:
   - To add a file to upload, click **Choose File** and then drag and drop the file or click to upload the file.
   - To point to a file, click **URL** and then enter the file path.
4. Set the **Set as default package** toggle switch to **Yes** to set the package as the default or accept the default **No**.

   If you set the package as the default, you must reboot the server for the change to take effect.
5. Set the **Reboot the server** toggle switch to **Yes** to automatically reboot the server after the upgrade or accept the default **No**.

Next steps

A message shows the status of the upload process. You must reboot the server to change the currently used firmware package to the default package.

Viewing firmware packages

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. Go to the **Firmware** tab.

   The following information is shown for each package:

Field/Item	Description
Package	The firmware package tar file.
Not Installed on Cluster Nodes	Lists the nodes on which the firmware is not installed.
Install Status	The status of the installation.
Current	Specifies whether the firmware package is currently used. The values are **Yes** or **No**.
Default	Specifies whether the firmware package is the default package on the nodes. The values are **Yes** or **No**.

Setting a firmware package as the default

You can have multiple firmware versions installed on the nodes associated with a managed server. To select the version that you want to use for all of the nodes, set a firmware package as the default. You can change the firmware version for the nodes at any time by selecting another package as the default.

Procedure

1. Navigate to **System** > **System Overview**.
2. On the **Firmware Packages** tab, find the package that you want to set as the default, and then click **Set as default**.
3. Click **Ok, Continue** to confirm.

Next steps

A message shows the status of the default change. You must reboot the nodes to change the currently used firmware package to the default package.

Removing a firmware package

Before you begin

Ensure that the firmware package is not set as the current or default package for nodes associated with a managed server. To verify the package status, navigate to Configuration > System > System Overview. On the Nodes tab, confirm that the package is not listed in the Current Package or Default Package fields for the nodes.

Procedure

1. Navigate to **Configuration** > **System** > **System Overview**.
2. On the **Firmware Packages** tab, select the package or packages that you want to remove or click **All** to select all packages, and then click **Delete**.
3. Click **Delete** to confirm.

Registering the license

The license key is registered during the first time setup of the VSP One File management software. You can add additional license keys using File Administrator.

Before you begin

Obtain the VSP One File server license from your Hitachi Vantara representative.

Procedure

1. Navigate to **Configuration** > **System** > **License Keys**.
2. Click **Add File License**, and use one of the following options to add license keys.
   - Upload the `.txt` file that contains the license key.
   - Enter the license key, and then click **Add**.

3. Click **Add**.

Viewing license information

You can view information about the license, such as the total number of licenses, expiration, license type, universal NAS virtual capacity, and virtual storage capacity. You can also view the licensed services covered by each license key.

Procedure

1. Navigate to **Configuration** > **System** > **License Keys**.
   The **License Key** page displays an overview of all registered licenses.
2. To view details, select the license key, and then click **View.**
   The **License Key Details** page opens displaying the license information.

Server

Server tasks include configuring access to the VSP One File server, managing file services for the server, and enabling event notifications to be sent from the server.

Management access

Management access provides various configurations to prevent unauthorized access on the managed VSP One File server. The server can be configured to respond only to an authorized host configured through any one of the following protocols:

- SSC protocol
- Microsoft Volume Shadow Copy Service (VSS) protocol
- Simple Networking Management Protocol (SNMP)
- REST API protocol

Using management access, you can add new users and reset the login password of existing users on the server.

Configuring SSC access

You can enable or disable, and specify the hosts allowed to access the VSP One File server using the SSC protocol.

Procedure

1. Navigate to **Configuration** > **Server** > **Management Access**.
2. In the **Management Access** page, click the **Configuration** tab, and then click the edit icon for **SSC Access Configuration**.
3. In the **Edit SSC Access Configuration** dialog box, set the **Enable SSC Access** toggle switch to **Enabled**, and then complete the following information:

a. In the **Port Number** box, enter the port number that the VSP One File server uses to communicate through the SSC protocol. The default is port 206.

   SSC must be enabled on port 206 to perform upgrades, run diagnostics, and use accelerated data copy (ADC).

b. In the **Maximum Number of connections** box, enter the maximum number of simultaneous connections to the server. File Administrator supports a maximum of 10 simultaneous connections.

c. (Optional) To restrict SSC protocol access to allowed hosts, set the **Restrict Access To Allowed Host** toggle switch to **Yes**.

d. (Optional) In the **Allowed Hosts** box, enter the Hostname or IP address of the host that is allowed to access the VSP One File server using the protocol, and then click **Add**. To remove a host, click the delete icon.

   You can specify an IP address using the * character, for example, `10.168.*.*` or `172.*.*.*`.

4. Click **Save**.

Configuring VSS access

You can configure Microsoft Volume Shadow Copy Service (VSS) access on a VSP One File server or cluster to create snapshots of attached storage systems. Snapshots created by VSS are exported as iSCSI logical units.

Procedure

1. Navigate to **Configuration** > **Server** > **Management Access**.
2. In the **Management Access** page, click the **Configuration** tab, and then click the edit icon for **VSS Access Configuration**.
3. In the **Edit VSS Access Configuration** dialog box, set the **Enable VSS Access** toggle switch to **Enabled**, and then complete the following information:
   a. In the **Port Number** box, enter the port number that the VSP One File server uses to communicate through the VSS protocol. The default is port 202.

   b. In the **Maximum Number of connections** box, enter the maximum number of simultaneous connections to the server. File Administrator supports a maximum of five simultaneous connections.

   c. (Optional) To restrict VSS protocol access to allowed hosts, Set the **Restrict Access To Allowed Host** toggle switch to **Yes**.

   d. (Optional) In the **Allowed Hosts** box, enter the Hostname or IP address of the host that is allowed to access the VSP One File server using the protocol, and then click **Add**. To remove a host, click the delete icon.

      You can specify an IP address using the * character, for example, `10.168.*.*` or `172.*.*.*`.
4. Click **Save**.

Configuring REST API access

You can configure REST API access on the VSP One File server to enable applications to integrate with VSP One File server.

Procedure

1. Navigate to **Configuration** > **Server** > **Management Access**.
2. In the **Management Access** page, click the **Configuration** tab, and then click the edit icon for **RESTAPI Access Configuration**.
3. In the **RestAPI Access Configuration** dialog box, set the **RESTAPI Server** toggle switch to **Enabled**, and then complete the following information:
   a. In the **Port Number** box, enter the port number that the VSP One File server uses to communicate through the REST API protocol. The default is port 8444.
   b. In the **Maximum Number of connections** box, enter the maximum number of simultaneous connections to the server. File Administrator supports a maximum of 50 simultaneous connections.
   c. (Optional) To restrict protocol access to allowed hosts, set the **Restrict Access To Allowed Host** toggle switch to **Yes**.
   d. (Optional) In the **Allowed Hosts** box, enter the Hostname or IP address of the host that is allowed to access the VSP One File server using the protocol, and then click **Add**. To remove a host, click the delete icon.

      You can specify an IP address using the * character, such as: `10.168.*.*` or `172.*.*.*`.
4. Click **Save**.

Configuring SNMP access

You can enable or disable SNMP access, specify the version of SNMP for the VSP One File server to use, and specify the host access.

Procedure

1. Navigate to **Configuration** > **Server** > **Management Access**.
2. In the **Management Access** page, click the **Configuration** tab, and then click the edit icon for **SNMP Access Configuration**.
3. In the **SNMP Access Configuration** dialog box, complete the following information:
   a. From the **SNMP Protocol Support** list, select the version of the SNMP protocol that hosts must use when sending requests to the SNMP agent.
   b. Enter the port number that the VSP One File server uses to communicate through the SNMP protocol. The default is port 161.
   c. (Optional) To restrict SNMP protocol access to allowed hosts, set the **Restrict Access To Allowed Host** toggle switch to **Yes**.
   d. (Optional) In the **Allowed Hosts** box, enter the Hostname or IP address of the host that is allowed to access the VSP One File server using the protocol, and then click **Add**. To remove a host, click the delete icon.

      You can specify an IP address using the * character, for example, `10.168.*.*` or `172.*.*.*`.

4. In the **Allowed Communities** box, enter the community host string that gives access to the Management Information Base (MIB), and then click **Add**. To remove a host, click the delete icon.

   An example of a community string is public.

   The VSP One File server SNMP agent maintains a MIB that includes information about the VSP One File server hardware and software. The MIB is organized in a tree structure, with each item of data assigned a unique object identifier (OID). An example OID is 1.3.6.1.4.1.4242.1.1. The VSP One File server SNMP agent gives access to the VSP One File server MIB module, making management facilities available to the users beyond those listed in the MIB specification described in *RFC1213*. Click **SNMP MIB Modules** to download the VSP One File server MIB module locally.

5. Click **Save**.

Creating a VSP One File server user

You can add a normal user or a supervisor user on VSP One File server.

Procedure

1. Navigate to **Configuration** > **Server** > **Management Access**.
2. In the **Management Access** page, click the **Server Users** tab, and then click **Create User**.
3. In the **Create Server User** dialog box, complete the following information:
   a. Select one of the following access levels for the new user:
      - User
      - Supervisor

   b. Enter a username for the user.

      A username can be a combination of letters (a-z, A-Z), numbers (0-9), and special characters (_, ., -). An example username is Server_User-1

   c. Enter and confirm the user password.

      The password must be at least 8 characters and must contain at least one uppercase letter, number, and special character. An example password is Password@123.

4. Click **Save**.

Modifying a VSP One File server user login password

You can reset passwords for users on the VSP One File server. You cannot reset the password for the dev user.

Procedure

1. Navigate to **Configuration** > **Server** > **Management Access**.
2. In the **Management Access** page, click the **Server Users** tab.
3. Identify the user for the password reset, and then click **Edit**.
4. In the **Edit Server User** dialog box, complete the following information:

   a. Enter the old password of the user account.
   b. Enter and confirm the new user password.

      The password must be at least 8 characters and must contain at least one uppercase letter, number, and special character. An example password is Password@123.

5. Click **Save**.

Deleting a VSP One File server user

You can delete all users of the VSP One File server except the root, manager, and dev user.

Procedure

1. Navigate to **Configuration** > **Server** > **Management Access**.
2. In the **Management Access** page, click the **Server Users** tab.
3. Identify and select the user account that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Server settings

You can modify managed server settings configured during adding a managed server such as server name, location, and date and time. You can also view server information like model name, current software version, and serial number from server settings.

Modifying the server identification

You can modify the name, location, and contact information of a managed VSP One File server.

Procedure

1. Navigate to **Configuration** > **Server** > **Server Settings**.
2. In the **Server Setting** page, click the edit icon for **Server Identification**.
3. In the **Edit Server Identification Details** dialog box, modify the server name, location, and contact information. The server name, location, and contact can be in a combination of letters, numbers, and special characters. The location and contact support a maximum of 180 characters.
4. Click **Save**.

Modifying the server date and time

Modifying the server date and time is important for synchronization. Synchronization helps in accurate reporting of file access and modification times which results in proper data migration. NTP gives the best and most reliable method for maintaining the VSP One File server time accuracy.

When using NTP, the VSP One File server first verifies that the specified NTP servers are legitimate; then, over a period of a few hours, gradually adjusts its clock to the time provided by the NTP server. This gradual adjustment is normal, and is designed to minimize the effects of changing the server clock on services that use file timestamps.

Procedure

1. Navigate to **Configuration** > **Server** > **Server Settings**.
2. In the **Server Setting** page, click the edit icon for **Date and Time**.
3. Select the date, time, and the time zone of the server location and then to add a NTP server, enter the IP address or the host name of the NTP server and the click **Add**.

   You can add a maximum of five NTP servers. File Administrator compares all listed NTP server times to determine and set the most accurate time.
4. Click **Save**.

Modifying the server login security banner

The server login security banner is shown when you log in to the VSP One File server using SSH or a serial connection. You can enable or disable the server login security banner and modify the security banner content from File Administrator. The server login security banner is disabled by default.

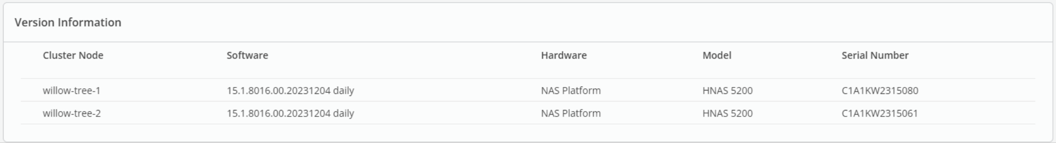
Procedure

1. Navigate to **Configuration** > **Server** > **Server Settings**.
2. In the **Server Setting** page, click the edit icon for **Security Banner Settings**.
3. In the **Security Banner Settings** dialog, set the **Login Security Banner** toggle switch to **Enabled**, and then modify the security banner text.
4. (Optional) To reset the login security banner to the default text, click **Reset to Default**.
5. Click **Save**.
6. Log out of the VSP One File management software, restart the web browser, and then log back in to view the new banner text.

Viewing the server version information

You can view information about the VSP One File server that you are using. This includes information such as software version, hardware type, and model for each node in the system.

To view server version information, click Configuration > Server > Server Settings and see Version Information.

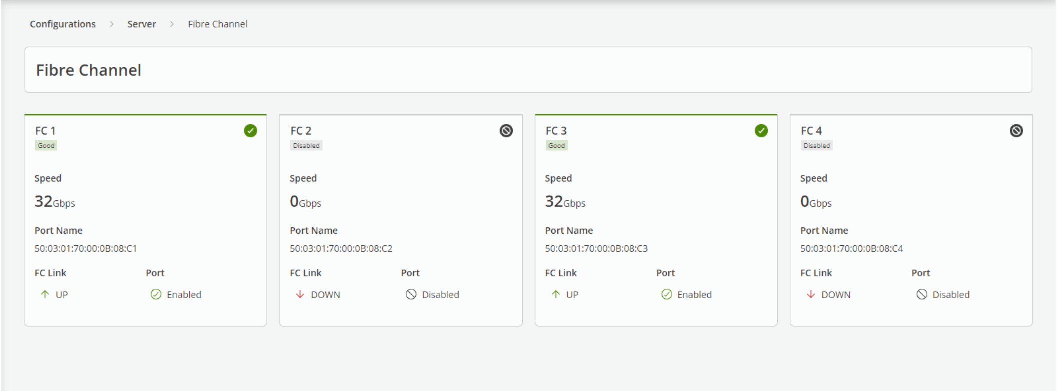


Version Information

Cluster Node	Software	Hardware	Model	Serial Number
willow-tree-1	15.1.8016.00.20231204 daily	NAS Platform	HNAS 5200	C1A1KW2315080
willow-tree-2	15.1.8016.00.20231204 daily	NAS Platform	HNAS 5200	C1A1KW2315061

Reviewing Fibre Channel report

File Administrator shows the Fibre Channel (FC) report for each port of a managed VSP One File server. To view the report, navigate to Configuration > Server > Fibre Channel.



Configurations > Server > Fibre Channel

Fibre Channel

FC 1 ✓
Good
Speed
32Gbps
Port Name
50:03:01:70:00:0B:08:C1
FC Link: ↑ UP
Port: ✓ Enabled

FC 2 ⊘
Disabled
Speed
0Gbps
Port Name
50:03:01:70:00:0B:08:C2
FC Link: ↓ DOWN
Port: ⊘ Disabled

FC 3 ✓
Good
Speed
32Gbps
Port Name
50:03:01:70:00:0B:08:C3
FC Link: ↑ UP
Port: ✓ Enabled

FC 4 ⊘
Disabled
Speed
0Gbps
Port Name
50:03:01:70:00:0B:08:C4
FC Link: ↓ DOWN
Port: ⊘ Disabled

The Fibre Channel page shows the following information:

Field	Description
Health of the FC port	The FC port health is one of the following values: ▪ Good - The port is healthy and functioning properly. ▪ Warning - The port is disabled, but the link is connected. ▪ Degraded - The port is enabled, but link is disconnected. ▪ Disabled - The port is disabled.
Connectivity speed of the FC port	The FC port speed is 4 Gbps or 8 Gbps or 16 Gbps or 32 Gbps.
FC port name	The name is a unique identifier associated with each FC port. An example of a port name is 50:03:01:70:00:0A:D8:61
Status of the FC link	The FC link status is Up (connected) or Down (disconnected).
Status of the FC port	The FC port status is Enabled or Disabled.

The following table shows the user actions required for the various FC port health status:

FC port health status	User actions
Good	No actions required.
Warning	Enable the FC port on the VSP One File server using the CLI command `fc-link <interface> enable`. An example: `fc-link 2 enable`. For more information, see the *VSP One File Server Command Reference*.
Degraded	Take the following actions to restore the link: ▪ If the FC cable is unplugged, plug in the FC cable. ▪ If the FC cable is damaged, change the FC cable.
Disabled	If you want to enable the FC port on the VSP One File server, use the CLI command `fc-link <interface> enable`. An example: `fc-link 2 enable`. For more information, see the *VSP One File Server Command Reference*.

Using SMB for Windows file access

Windows networks use the Server Message Block (SMB) protocol for file sharing between workstations and servers. The SMB protocol allows computers running Windows (and other compatible operating systems) to share resources over a network. It facilitates communication and data transfer between devices, enabling you to access shared files and resources seamlessly within a networked environment. This section contains information on using SMB with the NAS server.

SMB protocol support

The NAS server uses the same SMB protocols as Microsoft Windows, making it indistinguishable from a Windows file server.

The NAS server supports only the following SMB file-serving functions.

- Manipulation of shared resources, such as adding, listing, and deleting.
- Handling files, including reading, writing, creating, deleting, moving, and copying.
- Enabling file locking and byte-range locking.
- Implementing file access control using standard Windows ACLs.

- Managing file and directory attributes like read-only and archive.
- Automatically creating user home directories.

SMB requirements

Before you begin, you should have the following items ready to set up SMB for the NAS server:

- Apply SMB license key.
- Configure the NAS server using one of the following methods, based on the security model used on the SMB network.

Security model	Client authentication	Configuration method
Active Directory	Kerberos and NT4	Join Active Directory

If you connect the NAS server to an Active Directory, it functions similarly to being added to an NT domain. However, once it's part of the Active Directory, the server can verify clients using both the Kerberos protocol and the NT4 style authentication. Most newer Windows clients can handle both types of verification, but some older Windows clients only support NT4 style authentication.

- Supported clients: The NAS server supports platforms and clients that are compliant with SMB versions 1, 2, 2.1, and 3.
- Domain controller interaction: The storage server relies on Windows domain controllers to authenticate users and to obtain user information (for example, group membership). The NAS server automatically discovers and connects to the fastest and most reliable domain controllers. Because operating conditions can change over time, the NAS server selects the best domain controller every 10 minutes. By default, when authenticating clients in an Active Directory, the NAS server uses the time maintained by the domain controller, automatically adjusting for any clock inconsistencies.
- Dynamic DNS: The NAS server supports DNS and DDNS.

Supported SMB versions

The NAS server supports the SMB file sharing protocols with the following versions: SMB1, SMB2.0, SMB2.1, and SMB3. However, Microsoft® recommends SMB2.0 or later.

Supported SMB3 functionality for Hyper-V

The NAS server supports SMB3 functionality for Microsoft Hyper-V over SMB shares, including transparent failover, continuous availability, and shadow copies.

- **Continuous Availability:** Enables files that are opened using SMB3 on a continuously available share to survive network failures or cluster node failures. For example, if one cluster node fails, the client transparently reconnects to another cluster node without interruption to the client applications.

  If a continuously available share is changed from a cluster to a single server, and then back to a cluster, the server keeps the continuous availability of the share.

  > **Note:** For optimal SMB performance, enable continuous availability only when necessary, such as with Microsoft Hyper-V or Microsoft SQL server. If this feature is used, it is recommended to disable DDNS on the NAS server.

- **Persistent file handles:** Enables clients to transparently reconnect to disconnected SMB sessions. A persistent handle is preserved after a disconnection and blocks any attempts to open files while it waits for the client to reconnect.
- **VSS for SMB file shares:** The File Server Remote VSS (Volume Shadow Copy Service) Protocol (FSRVP) is a protocol for Windows Server that creates shadow copies of file shares on a remote computer. This protocol is most commonly deployed with Hyper-V and enables backup applications to create application-consistent backup and restore of VSS-aware applications storing data on network file shares.
- **Service Witness Protocol:** Enables a registered client to receive notification of any state changes on a continuously available server, without needing to wait for the connection to time out. This ensures that there is a fast notification and recovery time from an unplanned failure, such as a network loss.
- **SMB3 Multichannel:** Enables file servers to use multiple network connections simultaneously. This increases the network performance and availability of the file servers, and improves data throughput and fault tolerance. With SMB3 Multichannel, applications can utilize all available network bandwidth and increase resilience during network failures.

SMB3 Multichannel support

SMB3 Multichannel enables file servers to use multiple network connections simultaneously. This feature increases the network performance and availability of the file servers.

SMB3 Multichannel benefits include:

- Automatic configuration
- Client-side network processing on multiple CPU cores
- Increased data throughput
- Increased fault tolerance
- Resilience during network failures

SMB3 Multichannel is automatically enabled if the EVS is configured for version 3 of the SMB protocol.

SMB3 Encryption support

SMB Encryption provides end-to-end encryption of SMB data and protects against potential eavesdropping attacks on untrusted networks. Consider using SMB3 Encryption for any scenario in which sensitive data needs protection from man-in-the-middle (MITM) attacks.

SMB3 Encryption uses the Advanced Encryption Standard (AES)-CCM algorithm for both encryption and signing.

The main benefits of SMB3 Encryption are:

- No deployment requirements other than changing the SMB server settings.
- No dedicated hardware requirements unlike most storage area networks (SANs).
- Provides secure access to the server and shares.
- Protects data from eavesdropping attacks on untrusted networks.
- Provides end-to-end data encryption in-flight.

SMB3 Encryption is available only if the EVS is configured for version 3 of the SMB protocol.

Configuring SMB security

The SMB server integrates seamlessly into the existing domain and simplifies access control by performing all authentications against the existing domain user accounts.

Note: Only accounts that have been created in the domain or in a trusted domain can access the server.

When accessing a share, the SMB server checks the appropriate permissions. If access is granted at this level, standard file and directory access permissions apply.

The SMB server operates on a specific domain and can, optionally, join an Active Directory. It interacts with a domain controller (DC) in its domain to validate user credentials. The server supports Kerberos-based authentication to an Active Directory, as well as NTLM authentication. In addition to users belonging to its domain, the server allows connections from members of trusted domains.

The SMB server automatically grants administrator privileges to domain administrators who have been authenticated by the DC. In addition, local administration privileges can be assigned, including backup operator privileges to selected groups (or users).

Note: SMB can assign rights to machine (computer) accounts. A machine account is generated automatically by the operating system and registered in Active Directory. It can be used for authentication within a domain. A machine account authentication can be only done by an application which has built-in support. For example, Hyper-V server allows storing virtual machines on remote shares. Such shares should allow full access for the machine account of a computer running Hyper-V server.

Setting up SMB

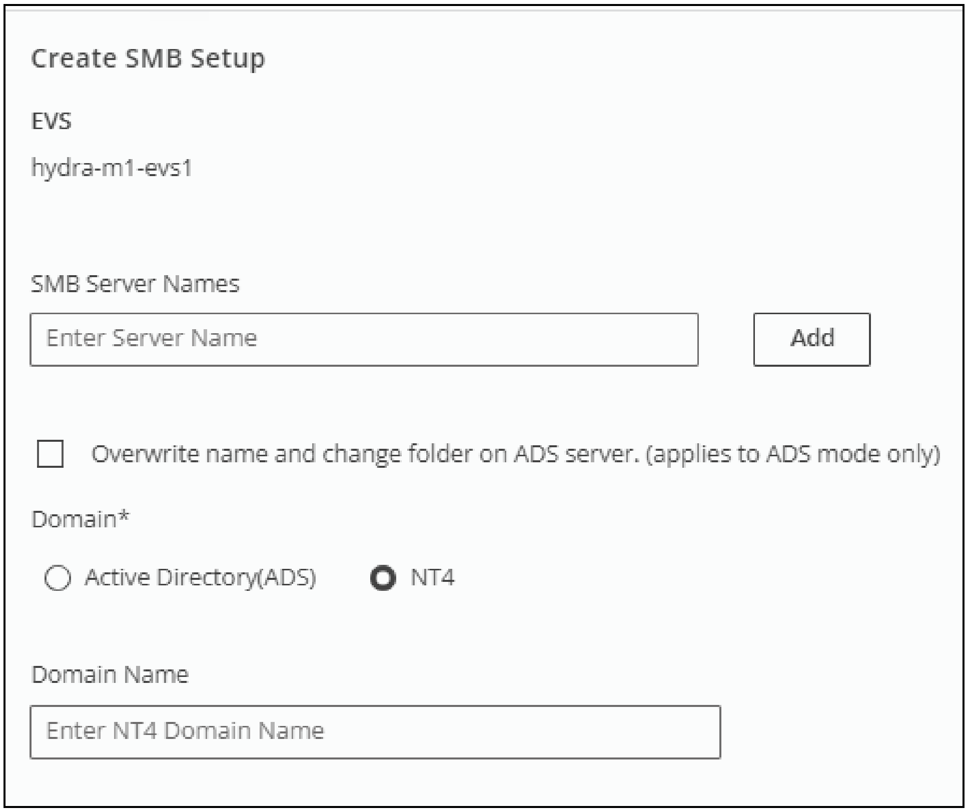
The SMB server can be configured with multiple SMB names to allow access for Windows clients. This is particularly useful in environments where multiple Windows servers are being consolidated.

To appear as a unique server on a Windows network, the SMB server performs the following for each configured SMB name:

- Allow administration through the Microsoft Server Manager (NT4) or Computer Management administrative tools.
- Register each SMB name as a server with the domain Master Browser so each name appears as a unique server in Network Neighborhood.
- Register each SMB name with DDNS and WINS for proper host name resolution.

Procedure

1. Navigate to **Configuration** > **SMB** > **SMB Setup**.
2. In the **SMB Setup** pane, select the EVS to which you want to add the SMB server name from the list of EVS instances.
3. Click **Create SMB Setup**.
4. In the **Create SMB Setup** dialog box, enter the following information:



Create SMB Setup

EVS

hydra-m1-evs1

SMB Server Names

Enter Server Name | Add

☐ Overwrite name and change folder on ADS server. (applies to ADS mode only)

Domain*

○ Active Directory(ADS) ● NT4

Domain Name

Enter NT4 Domain Name

a. In the **SMB Server Names** field, enter the SMB server name and click **Add**. You can add multiple server names.

   The name used by SMB users to access file services on the server. The maximum number of characters for the SMB server name in an Active Directory domain is 63, and in the NT4 domain is 15.

b. Select **Overwrite name and change folder on ADS server** to overwrite the folder name on the ADS server. This is applicable only when you use ADS as network directory service.

c. Under **Domain**, select **Active Directory (ADS)** or **NT4**.

   To use NT4 as network directory service, enter the NT4 domain name.

   To use ADS as network directory service, enter the following information:

Fields	Description
IP Address	The IP address of a domain controller within the Active Directory where the server will be configured.
DC Admin User	A user account must be a member of the Domain Administrators group to create a computer account in the Active Directory.
DC Admin Password	Password for the Domain Administrator user.
Folder	The location within the Active Directory where the computer account should be created. By default, the computer account is created in a folder called Computers within the Active Directory. If you want the account to be placed in a different folder, you need to specify that location.
DNS Suffix	Use this option only if you need to set a DNS suffix other than the Active Directory domain's primary DNS suffix. For example, set this if you have a disjoint domain.

5. Click **Create**.

Viewing SMB setup information

You can view the SMB setup information in the File Administrator.

Procedure

1. Navigate to **Configuration** > **SMB** > **SMB Setup**.
2. In the **SMB Setup** pane, select the EVS from the list of EVS instances to view the associated SMB server names.

   The following table describes the fields on the **SMB Setup** page:

Field	Description
Mode	
Security Mode	The configured security mode of the EVS.
Domain Name	The name of the domain in which the SMB server resides. The domain is set when the first SMB name is added.
ADS Domain	The domain where the SMB server is located.
DDNS	Indicates whether DDNS is enabled or disabled. By default, the SMB server is configured to use DDNS. To disable DDNS, click the edit icon, and set the **DDNS** toggle to **Disable**.
NetBIOS	
NetBIOS	When NetBIOS is enabled, it allows NetBIOS and WINS use on the SMB server. If the SMB server communicates by name with computers that use earlier Windows versions, this setting is required. By default, NetBIOS is disabled.
Configured SMB server details	
SMB Server Name	A list of SMB names added to the selected EVS.
Mode	Displays the mode for each SMB server name. Mode defines the authentication protocol used to communicate with the Windows network clients and domain controllers. The mode can be: ▪ **ADS**: The Microsoft's Active Directory Services communication protocol (Kerberos) is used to communicate with the Windows clients and domain controllers. ▪ **NT4**: The Windows NT4 communication protocol (NTLMSSP) is used to communicate with the Windows clients and domain controllers.
Disjoint	Indicates whether the DNS suffix matches the Active Directory domain primary DNS suffix. ▪ **no**: There is no disjoint namespace between the DNS and ADS. ▪ **yes**: There is a disjoint namespace between the DNS and ADS.

Deleting SMB server names

You can delete the SMB server name if it is no longer required.

When ADS SMB names are deleted, the corresponding computer account in the Active Directory is also deleted. Computer accounts in NT4 Domains must be deleted manually through Server Manager.

> **Caution:** SMB Name Deletion Alert! At least one SMB name must be configured on the server to support connections from Windows clients. As a result, if the last configured SMB name is removed, Windows clients are no longer able to access the server over SMB.

> **Note:** DNS entries do not de-register automatically after deleting a SMB server name, so the administrator must delete the SMB server name entry from DNS manually.

Procedure

1. Navigate to **Configuration** > **SMB** > **SMB Setup**.
2. In the **SMB Setup** pane, select the EVS from the list of EVS instances to view the associated SMB server names.
3. Select the SMB server name or names that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Configuring iSCSI

The NAS server supports the Internet Small Computer System Interface (iSCSI). iSCSI protocol enables block-level data transfer between requesting applications and iSCSI target devices.

To use iSCSI on NAS server, one or more iSCSI Logical Units (LUs) must be defined. iSCSI LUs are blocks of storage that are accessed through iSCSI targets. An Initiator can access the LU as a “local disk” through its target. Security mechanisms can be used to prevent unauthorized access to iSCSI targets.

To create iSCSI LUs, see Adding an iSCSI logical unit (on page 62).

iSCSI targets

An iSCSI target is a storage element accessible to iSCSI initiators. These targets appear to iSCSI initiators as different storage devices accessible over the network. The server supports a maximum of 32 iSCSI Targets per EVS and a maximum of 32 iSCSI sessions per Target.

Adding an iSCSI domain to an EVS

You have to add an iSCSI domain to an EVS before creating an iSCSI target.

Procedure

1. Navigate to **Configuration** > **iSCSI** > **iSCSI Target Domain**.
2. In the **iSCSI Targets** pane, select the EVS where you want to add an iSCSI domain from the list of EVS instances, and then click the edit icon.
3. Enter the EVS iSCSI domain name, and then click **Save**.

   The domain name is in `example.domain.com` format.

Adding an iSCSI target

Before you begin

- Make sure that the EVS iSCSI domain is added to the EVS where you are creating the iSCSI target.
- Make sure that at least one iSCSI logical unit is created and available.

Procedure

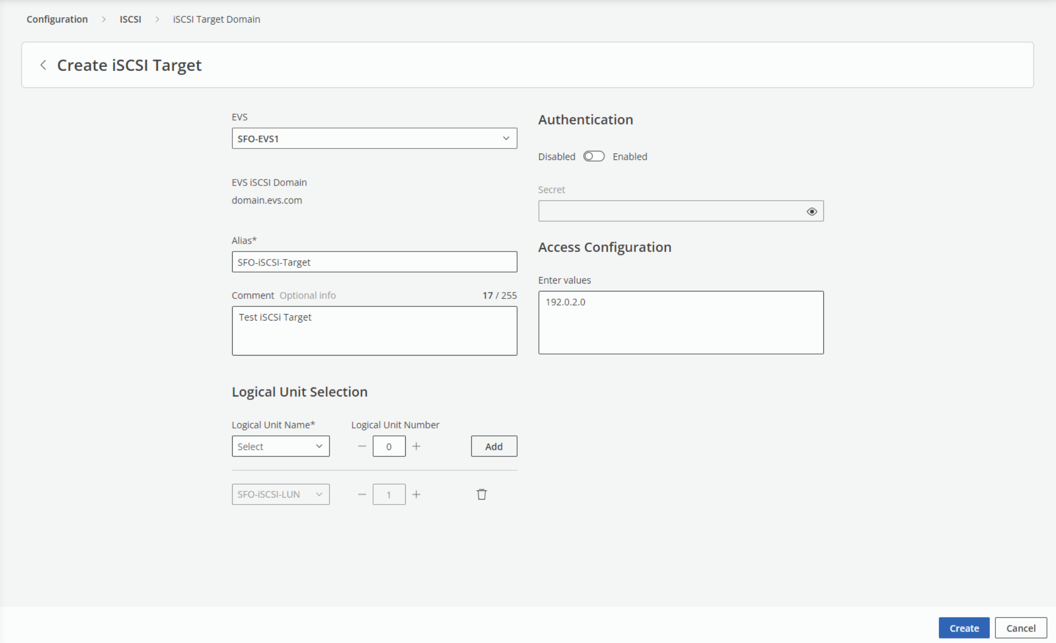
1. Navigate to **Configuration** > **iSCSI** > **iSCSI Target Domain** and click **Create Target**.
2. In the **Create iSCSI Target** pane, complete following information for the iSCSI target:
   a. Select the EVS where you want to create the iSCSI target.
   b. (Optional) Enable the iSCSI target authentication. If iSCSI target authentication is enabled, set an authentication password.

      By default, authentication is disabled. This setting is used to secure the iSCSI target. When authentication is disabled, iSCSI initiators are permitted to connect to the target and its logical units without verifying the target secret.
   c. Enter a name (alias) for the iSCSI target.

      This can be a maximum of 255 characters long.
   d. (Optional) Enter additional information about the iSCSI target and IP addresses for access configuration of the iSCSI target.

      If there are no IP addresses in access configuration, all clients can access the target. You can also add partial IP address or name using wild cards. For example: `10.168.*.*, *.company.com`. To deny access to a specific host, use the no_access or no access qualifier. For example, `10.1.2.38 (no_access)` which denies access to the host with the IP address `10.1.2.38`. To secure and control access to targets, follow these guidelines when specifying the IP addresses, Guidelines for entering values in the Access Configuration field (on page 211)
   e. Select an available iSCSI logical unit to connect with the iSCSI target, assign a logical unit number, and then click **Add**.

      You can add multiple iSCSI logical units with an iSCSI target. The logical unit number can be any number between 0 to 255.



EVS: SFO-EVS1

EVS iSCSI Domain: domain.evs.com

Alias*: SFO-iSCSI-Target

Comment Optional info 17 / 255: Test iSCSi Target

Authentication

Disabled ○ Enabled

Secret

Access Configuration

Enter values: 192.0.2.0

Logical Unit Selection

Logical Unit Name*: Select — Logical Unit Number: 0

SFO-iSCSI-LUN — 1

3. Click **Create**.

Modifying the properties of an iSCSI target

Note: Once set, the iSCSI Domain cannot be changed, but it is replaced if you later specify a new iSCSI target with a different iSCSI domain in the same EVS. The most recently specified iSCSI domain overrides all previously-specified iSCSI domains set for all previously added iSCSI targets in the EVS.

Procedure

1. Navigate to **Configuration** > **iSCSI** > **iSCSI Target Domain**.
2. In the **iSCSI Targets** pane, select the EVS associated with the target from the list of EVS instances.
3. Locate the target that you want to modify, and then click **View**.
4. In the target alias pane, modify the information that you want to change.
5. Click **Save**.

Deleting an iSCSI target

Deleting an iSCSI target removes access to its connected iSCSI logical units. When an iSCSI target is deleted, the iSNS database cannot find the iSCSI targets anymore, thus the iSCSI initiators cannot access the logical units as local hard drives.

Procedure

1. Navigate to **Configuration** > **iSCSI** > **iSCSI Target Domain**.
2. In the **iSCSI Targets** pane, select the EVS associated with the target from the list of EVS instances.
3. Select one or more targets that you want to delete, and then click **Delete**.

4. Click **Delete** to confirm.

Generating a new globally unique name for an iSCSI target

If you change an EVS iSCSI domain, then the globally unique names of the iSCSI targets does not change automatically, which might result in disconnecting the users. To make sure the users are not disconnected, you have to generate a new globally unique name.

Procedure

1. Navigate to **Configuration** > **iSCSI** > **iSCSI Target Domain**.
2. In the **iSCSI Targets** pane, select the EVS associated with the target from the list of EVS instances.
3. Select one or more targets for which you want to change the globally unique names, and then click **Generate New Globally Unique Names**.

   The globally unique name is in the `iqn.yyyy-mm.naming-authority:unique-name` format.

iSNS servers

The Internet Storage Name Service (iSNS) is a network database of iSCSI initiators and targets maintained on a iSNS server. If iSNS is configured, the NAS server can add its list of targets to iSNS server, which allows Initiators to easily find them on the network.

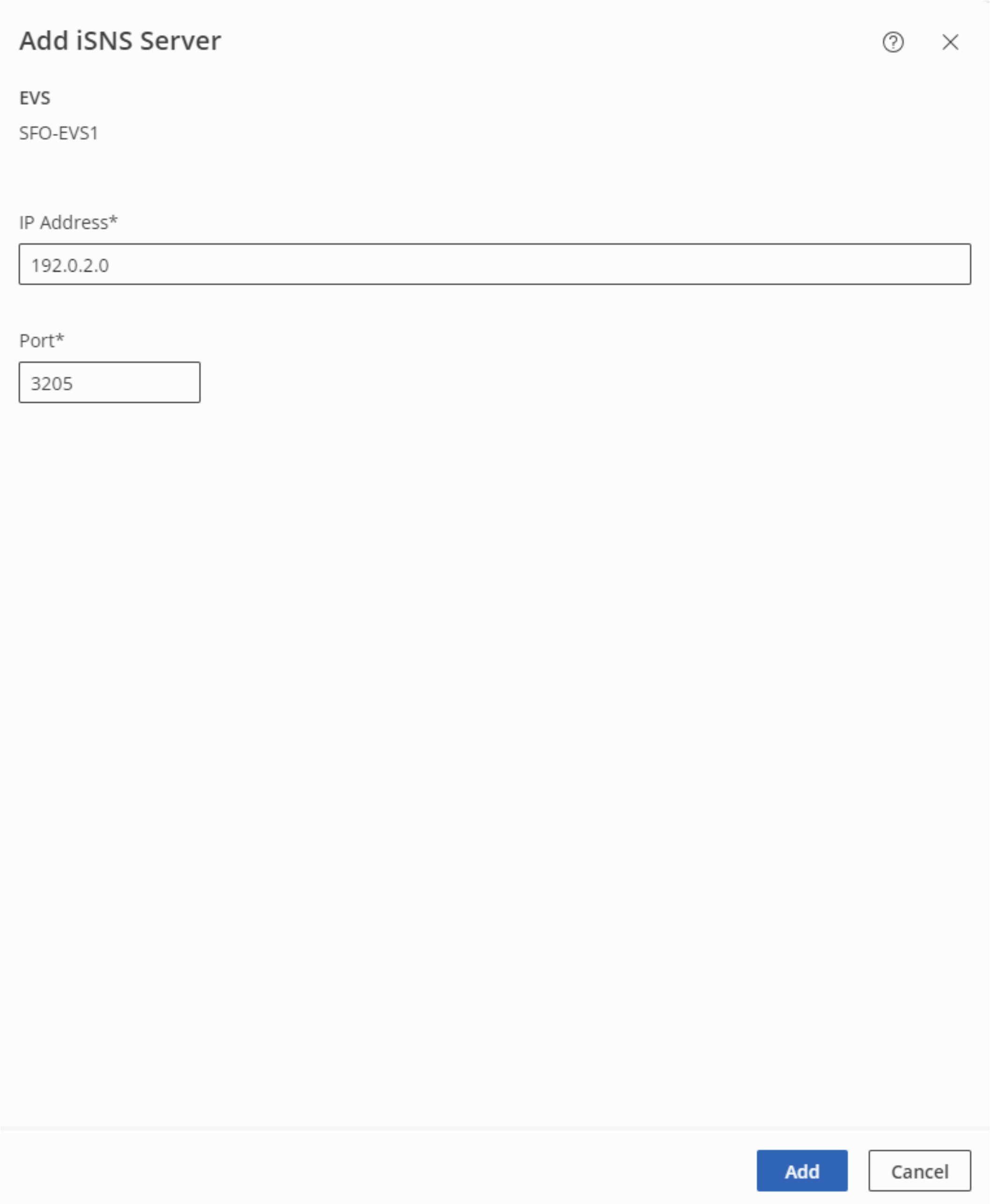
The NAS server registers its iSCSI targets with iSNS database when any of the following events occurs:

- A first iSNS server is added.
- An iSCSI target is added or deleted.
- The iSCSI service is started.
- The iSCSI domain is changed.
- A NAS server IP address is added or removed.

Adding an iSNS server

Procedure

1. Navigate to **Configuration** > **iSCSI** > **iSNS Server**.
2. In the **ISNS Servers** pane, select the EVS where you want to add a server from the list of EVS instances.
3. Click **Add iSNS Server**.
4. In the **Add iSNS Server** dialog box, add the iSNS server IP address and port number, and then click **Add**.



Add iSNS Server

EVS

SFO-EVS1

IP Address*

192.0.2.0

Port*

3205

Deleting an iSNS server

Procedure

1. Navigate to **Configuration** > **iSCSI** > **iSNS Server**.
2. In the **ISNS Servers** pane, select the EVS associated with the server from the list of EVS instances.
3. Select one or more server IP addresses that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Initiator authentication

The NAS server uses the Challenge Handshake Authentication Protocol (CHAP) to authenticate iSCSI initiators. CHAP requires a “shared secret” known by the initiator and the target. The NAS server also supports mutual authentication where the initiator authenticates the target on the server and the server authenticates the initiator.

To facilitate the mutual authentication process, the server must maintain a list of the initiators with which it can authenticate and the shared secret for each initiator.

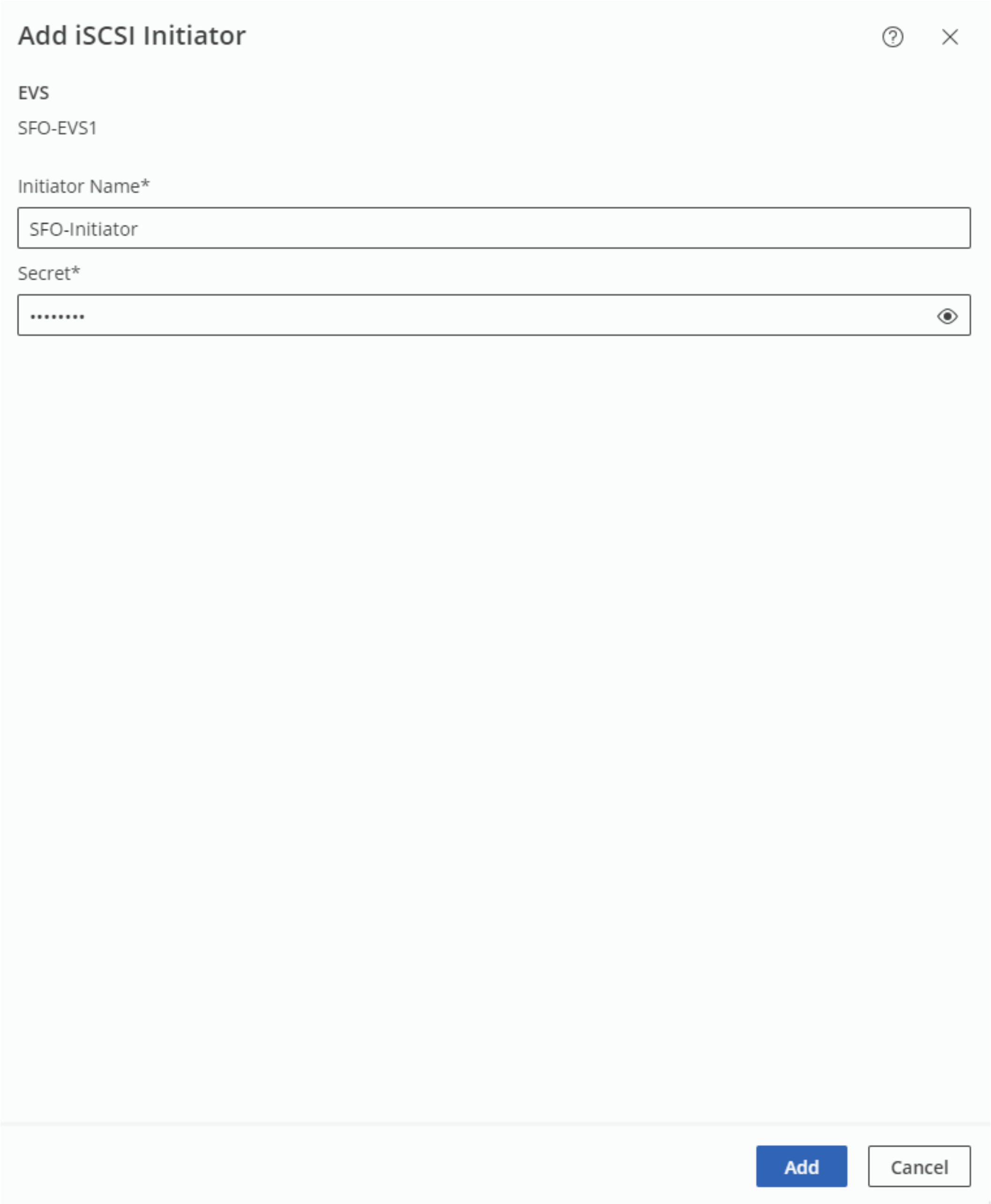
Adding initiator authentication

Procedure

1. Navigate to **Configuration** > **iSCSI** > **Initiator Authentication**.
2. In the **iSCSI Initiator Authentication** pane, select the EVS where you want to add the intiator from the list of EVS instances.
3. Click **Add iSCSI Initiator**.
4. In the **Add iSCSI Initiator** dialog box, enter the initiator name to identify the initiator with a globally unique name and the initiator secret (password) to secure the initiator from unauthorized access.

   The secret should be between 12 to 16 characters in length.

   > **Note:** If the secret is less than 12 characters and more than 16 characters in length, the initiators might not establish a successful connection.



Add iSCSI Initiator

EVS

SFO-EVS1

Initiator Name*

SFO-Initiator

Secret*

••••••••

5. Click **Add**.

Deleting an initiator authentication

Procedure

1. Navigate to **Configuration** > **iSCSI** > **Initiator Authentication**.
2. In the **iSCSI Initiator Authentication** pane, select the EVS associated with the initiator from the list of EVS instances.
3. Select one or more initiators that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Configuring FTP

Use FTP server to manage files and directories and control access to files.

File serving allows multiple clients to read or copy a file as it is being streamed over FTP to the server through any protocol (FTP, SMB, or NFS). If a client tries to copy a file while it is being written, the server provides only the data written until that point in time. The client is unable to modify, write, or lock the file.

FTP statistics are provided for the storage server in 10-second intervals, starting from the previous reboot of the server or the last reset of the statistics.

Configuring FTP preferences

Select the password authentication service and set a timeout to end inactive FTP sessions.

Procedure

1. Navigate to **Configuration** > **FTP** > **Configuration**.
2. Select **NT** or **NIS** as the password authentication service.

   If operating in UNIX or Mixed security mode, both NT and NIS password authentication are supported. If both services are enabled, the FTP user is authenticated against the configured NT domain first. If authentication fails, the server attempts to authenticate the user against the configured NIS domain.
3. Enter the session timeout value. The default is 15.

   The valid range is between 15 and 144000 minutes (14400 minutes = 10 days).
4. Select the option to enable read or write permissions for anonymous requests.
5. Click **Save**.

Adding an FTP user

Add an FTP user to allow anonymous logins to the mount point.

Procedure

1. Navigate to **Configuration** > **FTP** > **Users**.
2. In the **FTP Users** pane, select the EVS and file system where you want to add the user from the list of EVS instances.
3. Click **Create User**.
4. Enter the username. To allow anonymous logins to the mount point, specify the user name as `anonymous` or `ftp`.
   The password authentication service that you use determines whether users must log in with their NT domain name or UNIX user name.
5. Browse to the directory or specify the directory path where the user initiates a session upon logging in through FTP.

Note: Directories that are created automatically are owned by the root user and group (UID:0 / GID:0) and are accessible with full permissions (read, write, and execute). You must create these directories using the SMB or NFS protocols, or give the appropriate permissions explicitly after creating using this option.

6. To create the path automatically, select **Create path if it does not exist**.
7. Click **Create**.

Importing FTP users

You can import FTP users from a CSV or text file.

Before you begin

To import FTP users, prepare a file with user information:

- Each entry in the file must follow a specific syntax for username, file system, and initial directory. See the following example for syntax and sample values.

```
user_name file_system\initial_directory
DENIS Sales \Sales
```

- If the username or initial directory contains spaces, the entry must be enclosed within double quotes, and each entry must be separated by at least one space as shown in the following example:

```
"Mark Doe" Management "\mgmt\mark"
DENIS Sales \Sales
Andy Sales \Andy
John Tech "\tech\dirs\John"
```

- If you are unsure whether the initial directory exists, include the following option to automatically create the directory:

  ```
  ENSURE_PATH_EXISTS true
  ```

  This setting remains active until it is turned off by including the following option:

  ```
  ENSURE_PATH_EXISTS false
  ```

  In the following example, directories will be created automatically for the two entries until the option is turned off:

  ```
  "Mark Doe" Management "\mgmt\mark"
  ENSURE_PATH_EXISTS true
  DENIS Sales \Sales
  Andy Sales \Andy
  ENSURE_PATH_EXISTS false
  John Tech "\tech\dirs\John"
  ```

  > **Note:** Directories that are created automatically are owned by the root user and group (UID:0 / GID:0) and are accessible with full permissions (read, write, and execute). You must create these directories using the SMB or NFS protocols, or give the appropriate permissions explicitly after creating using this option.

- To include additional information about users, insert a comment in the file and precede it with the hash mark (#) as shown in the following example.

  ```
  # Users from the sales department
  Mark Management \mgmt\mark
  DENIS Sales "\Sales"
  Andy Sales "\Andy"
  John Tech \tech\dirs\John
  ```

Procedure

1. Navigate to **Configuration** > **FTP** > **Users**.
2. Click **Import Users**.
3. Upload the `.csv` or `.txt` file, and click **Import**.

Modifying FTP users

You can modify the file system, directory, and create the path automatically.

Procedure

1. Navigate to **Configuration** > **FTP** > **Users**.
2. In the **FTP Users** pane, select the EVS associated with the user from the list of EVS instances.

3. Locate the user that you want to modify, and then click **Edit**.
4. In the **FTP Users** pane, modify the information that you want to change.
5. Click **Save**.

Deleting an FTP user

Procedure

1. Navigate to **Configuration** > **FTP** > **Users**.
2. In the **FTP Users** pane, select the EVS associated with the user from the list of EVS instances.
3. Select one or more users that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

File Services

When a new VSP One File server is added in File Administrator, the file services like SMB, NFS, FTP, iSCSI, and CNS might be disabled. You can enable the required file services for the VSP One File server in File Administrator. If you do not use a file service, disable the file service.

Enabling file services

Procedure

1. Navigate to **Configuration** > **Files Services** > **Enable File Services**.
2. Click the edit icon, and then set all the file service toggle switches to **Enabled**.
3. Click **Save**.

User mappings and group mappings

When the file server is operating in either mixed or UNIX security mode, it requires mappings between UNIX, Windows, NFSv4, and Kerberos users and groups. For example, user John Doe could have a UNIX user account named `jdoe` and a Windows user account named `johnd`. These two user accounts are made equivalent by setting up a user mapping. Furthermore, the file server assumes that equivalent user and group names are the same for both environments. For example, if no explicit mapping is found for user `janed`, the server assumes that the UNIX user account named `janed` is the same as the Windows user account with the same name.

There are two steps to follow when setting up user and group mappings on the server:

- Specify the name and ID of each NFS user and group.

  > **Note:** This step is not required for Windows users or groups, as the server gets all of the information from the domain controller (DC).

- Map the NFS user (group) names to Windows NT user (group) names.

Windows access to a file created by a UNIX user (or vice-versa) is permitted when the UNIX name and Windows name are recognized as being the same user. However, NFS clients present an NFS operation to an NFS server with numerical UNIX User ID (UID) and UNIX Group ID (GID) as credentials. The server must map the UID and GID to a UNIX user or group name prior to verifying the UNIX to Windows name mapping.

The server uses the following methods to map from a numerical UNIX UID or GID to a UNIX user name or group name:

- If the server is configured to use the Network Information Service (NIS) no special configuration steps are needed; the server automatically retrieves the user (group) names and IDs from the NIS server.
- NFS user and group names can be added manually.
- NFS user and group names can be added by importing files. For example, the UNIX `/etc/passwd` file can be imported, providing the server with a mapping of user name to UID. The `/etc/groups` file should also be imported to provide the server with a mapping of Group name to GID.
- You can import the numerical ID to Name mappings directly from a NIS server or an LDAP server if one has been configured. Every time a UID is presented to the server, it will issue an NIS request to an NIS server to verify the mapping. This mapping can remain cached in the server for a configurable time. A cached ID to name binding for a User or Group will appear as Transient in the NFS Users or Groups list.

  Note: When a Windows user creates a file and the UNIX user or group mapping fails, the server sets the UID or the GID to 0 (root).

Each UNIX user name and numerical UID can be manually entered, along with its corresponding Windows user and domain name. Users configured manually will appear as permanent in the NFS users list.

Adding user or group mappings

Procedure

1. Navigate to **Configuration** > **File Services** > **User & Group Mappings**.
2. Select **Global Configuration** from the list of EVS security contexts, and then click **Add**.
3. In the **Add Mapping Type** dialog box, select one of the mapping types:
   - **User**
   - **Group**
4. Select the type of user or group from **NFSv2/3 Name**, **Unix ID**, **Windows Name**, **Windows ID**, **NFSv4** and **Kerberos**:
   - **Discover** - The server relies on information discovered from NIS servers, LDAP servers, or domain controllers for this mapping.
   - **Ignore** - The server does not retrieve information from NIS servers, LDAP servers, or domain controllers.
   - **Save to NAS server** - The server relies on information you provide.
5. Click **Add Mapping**.

Importing user or group mappings

You can import user or group mappings from a file stored on your machine or on a network drive, or from an NIS/LDAP server.

Procedure

1. Navigate to **Configuration** > **File Services** > **User & Group Mappings**.
2. Select **Global Configuration** from the list of EVS security contexts, and then click **Import**.
3. In the **Import Mappings** dialog box, select one of the import types:
    - **User Mapping**
    - **Group Mapping**
4. Select one of the import destination:
    - **File**
    - **NIS/LDAP**
5. To import from a file, select **File** to upload the file in **File Name**, and then click **Import**.
6. To import from a NIS/LDAP server, select **NIS/LDAP** to show the NIS or LDAP server that is contacted to import the mapping, and then click **Import**.

Modifying user or group mappings

In File Administrator, you can modify all fields in a user or group mappings.

Procedure

1. Navigate to **Configuration** > **File Services** > **User & Group Mappings**.
2. Select **Global Configuration** or an individual security context from the list of EVS security contexts.
3. Locate the user or group mapping that you want to modify, and then click **Edit**.
4. In the **User Mapping** or **Group Mapping** dialog box, edit the information that you want to change.
5. Click **Save**.

Deleting user or group mappings

Procedure

1. Navigate to **Configuration** > **File Services** > **User & Group Mappings**.
2. Select **Global Configuration** or an individual security context from the list of EVS security contexts.
3. Select one or more user or group mappings that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Domain mappings

Domain mappings provide the information to automatically map between Unix, Windows, NFSv4, and Kerberos users or groups. The domain mappings define how to map the domain or realm parts, assuming that equivalent users or groups of each type have the same name.

Creating a domain mapping

Procedure

1. Navigate to **Configuration** > **File Services** > **Domain Mappings**.
2. Select **Global Configuration** or an individual security context from the list of EVS security contexts, and then click **Add Domain Mapping**.
3. In the **Add Domain Mapping** dialog box, add the following information:
   a. If you want to map for Unix names, select **Map for Unix Names**.

      > **Note:** Only one mapping can map Unix names. If you try to add another domain mapping with the **Map for Unix Names** toggle to **Yes**, it will be disabled.

   b. Enter the **Windows Domain** name.
   c. Enter the **Kerberos Realm**.
   d. Enter the **NFSv4 Domain** name.
4. Click **Add**.

Modifying a domain mapping

Procedure

1. Navigate to **Configuration** > **File Services** > **Domain Mappings**.
2. Select **Global Configuration** or an individual security context from the list of EVS security contexts.
3. Locate the domain mapping that you want to modify, and then click **Edit**.
4. In the **Domain Mapping** dialog box, edit the information that you want to change.
5. Click **Save**.

Deleting a domain mapping

Before you begin

Make sure that the virtual volume is empty.

Procedure

1. Navigate to **Configuration** > **File Services** > **Domain Mappings**.
2. Select **Global Configuration** or an individual security context from the list of EVS security contexts.
3. Select one or more domain mappings that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Local groups

In a Windows domain, users and groups identify users (for example, `vsmith`) and groups of users (for example, `software`) on the network. Apart from the user-defined network group names (for example, `software`, `finance`, and `test`), Windows also supports a number of built-in or local groups with each providing various privileges and levels of access to the server on which they have been configured.

These groups exist on every Windows computer. They are not network groups, but are local to each computer. So, the user `vsmith` may be granted Administrator privileges on one computer and not on another.

On the server, the administrator can add users to any of the following local groups:

- **Root**: If a user is a member of the local Root group, the user bypasses all security checks, and can take ownership of any file in the file system.
- **Administrators**: If a user is a member of the local Administrators group, the user can take ownership of any file in the file system.
- **Audit Service Accounts:** If a user is a member of the Audit Service Accounts group, the server does not add any of their events to the audit log. However, the server does add events to the audit log for any user who is **not** a member of this group. These events consist of the Windows file access and deletion events which are recorded by the server.
- **Backup Operators**: If a user is a member of the local Backup Operators group, the user bypasses all security checks, but cannot take ownership of a file in the file system. The privilege to bypass all security checks in the file system is required for accounts that run backup or perform virus scans. Virus scanner servers that are a part of the Backup Operators group can, however, take ownership of any file in the file system.
- **Forced Groups**: If a user is a member of the local Forced Groups group, when the user creates a file, the user's defined primary group is overridden and the user account will be used to indicate the file creator's name.

Adding a local group or local group members

You can add a local group or local group members in an existing local group in File Administrator.

Procedure

1. Navigate to **Configuration** > **File Services** > **Local Groups**.
2. Select **Global Configuration** or an individual security context from the list of EVS security contexts, and then click **Add Local Group**.

> **Note:**
>
> - If an EVS uses the global configuration, any changes made to the global configuration settings will affect the EVS.
> - If an EVS uses an individual security context, changes made to the global configuration settings will not affect the EVS. To manage local groups for an EVS that uses an individual security context, you must select the EVS individual security context to make changes, even if those settings are the same as the settings used by the global security context.

3. In the **Add Local Group** dialog box, enter the local group name, and then click **Add**.
4. To add a new member to an existing local group:
   a. From the list of local groups, identify the local group to which you want to add a member, and then click **View**.
   b. In the group details page, click **Add Member**.
   c. In **Member Name**, enter the new member user name.

      To add more memebrs in a bulk, select **Add another member** checkbox.
   d. Click **Save**.

      To import members in a bulk from a locally saved .txt file, select **Import Users**.

Deleting a local group or local group members

Once created, local group names cannot be changed. To change a local group name, you must delete the local group, then create a new local group, and add members to the new local group. Deleting a local group is a two-stage process; you must delete all members of the group before you can delete the group itself.

You cannot delete default local groups.

Procedure

1. Navigate to **Configuration** > **File Services** > **Local Groups**.
2. Select **Global Configuration** or an individual security context from the list of EVS security contexts.

> **Note:**
>
> - If an EVS uses the global configuration, any changes made to the global configuration settings will affect the EVS.
> - If an EVS uses an individual security context, changes made to the global configuration settings will not affect the EVS. To manage local groups for an EVS that uses an individual security context, you must select the EVS individual security context to make changes.

3. To delete all members of the group:
   a. Identify the group and click **View**.
   b. Select all members of the group, and then click **Delete**.

      Alternatively, click the delete icon associated with the member name.
   c. Click **Delete** to confirm.

4. To delete the local group:
   a. Select the local group with recently deleted members, and then click **Delete**.
      Alternatively, click the delete icon associated with the local group.
   b. Click **Delete** to confirm.

File System Audit Policies

File system auditing monitors and records file access and modification operations performed through the SMB and NFSv3 protocols.

Modifying audit log consolidated cache configuration

You must configure the audit log consolidated cache for an EVS before adding a file system audit policy.

Procedure

1. Navigate to **Configuration** > **Files Services** > **File System Audit Policies**.
2. In the **File System Audit Policies** pane, select the EVS from the list of EVS instances, and then click the edit icon.
3. In the **Modify Audit Log Consolidated Cache** pane, modify the information that you want to change.
4. Click **Save**.

Adding a file system audit policy

Before you begin

Make sure that the audit log consolidated cache is configured for the EVS where the file system is located.

Create an audit policy for effective file system auditing.

Procedure

1. Navigate to **Configuration** > **Files Services** > **File System Audit Policies**.

2. Click **Add File System Audit**, complete the following information.
   - Select the EVS and associated file system for which you want to apply the audit policy.

     One of the following security modes is shown based on the configured security mode of the EVS:

     - **Mixed** (Windows and Unix)
     - **Unix** (supports Windows)
     - **Inherited**, the inherited security mode means the security mode is inherited from the EVS security mode and has not been manually changed.

     For more information on security modes, see Security modes (on page 177).
   - Allow access to audited protocols.
     - **SMB**: Access to SMB is always allowed.
     - **NFSv3**: Enable or disable NFSv3 protocols for audit.
   - Allow or deny access for unsupported Protocols.

     This setting determines if client computers are permitted to access the file system using a protocol that does not support auditing (such as NFSv2). Select on the following options:

     - **Deny Access**. Deny access to the file system using unauditable protocols (such as NFSv2).
     - **Allow Access**. Allows client access to the file system using unauditable protocols (such as NFSv2), but does not create any auditing events.

- Configure the audit log.

  Audit records, including audit log backups, are stored locally or to an external audit log server. To store records locally, set the **External** toggle to `No` and complete the following fields:

  - **Maximum Log File Size:** Specify the maximum size of the active audit log file in KiB or MiB. The default size is 512 KiB. The maximum log file size is 50 MiB.
  - **Log Roll Over Policy:** Specify the action when the active audit log file reaches the maximum file size.
    - **Wrap:** Deletes the oldest audit entry to make room for a new entry.
    - **New:** Creates a new active audit log file. This is the default.
  - **Directory:** Specify the directory in which the file system audit log files are saved. Use **Browse** to search for an existing directory, or enter the name of a directory to be created.
  - **File Name:** Specify the file name for the file system audit log. The file name must have an `.evt` extension. The default is `audit.evt`.
- Configure the backup policy for the audit log.
  - **Backup Interval (Minutes):** Specify the time in minutes between automatic backups of the active audit log. The backup interval must be between 5 and 14400 minutes (10 days). A value of 0 disables the automatic backups. The default is 0.
  - **Number of files to retain:** Specify the number of backup audit log files to retain. The default is **10**. The maximum number of files to retain is 50.

3. Click **Add**.

   The policy is enabled by default. To disable it, see Disabling a file system audit policy (on page 175).

Disabling a file system audit policy

When you create a file system audit policy, file system auditing is enabled by default. You can disable the file system audit policy to stop the file system auditing.

Procedure

1. Navigate to **Configuration** > **Files Services** > **File System Audit Policies**.
2. In the **File System Audit Policies** pane, select the EVS that is associated with the audit policy from the list of EVS instances.
3. Select the audit policy that you want to disable, and then click **Disable**.
4. Click **Yes, continue** to confirm.

Enabling a file system audit policy

You can enable a disabled file system audit policy to resume the file system auditing.

Procedure

1. Navigate to **Configuration** > **Files Services** > **File System Audit Policies**.
2. In the **File System Audit Policies** pane, select the EVS that is associated with the audit policy from the list of EVS instances.
3. Select the audit policy that you want to enable, and then click **Enable**.
4. Click **Yes, continue** to confirm.

Enabling audit log consolidated cache

You can enable the file system audit log consolidated cache for an EVS to report file system audit events to Windows clients.

Procedure

1. Navigate to **Configuration** > **Files Services** > **File System Audit Policies**.
2. In the **File System Audit Policies** pane, select the EVS that is associated with the cache from the list of EVS instances.
3. Cick **Enable Cache**.

Disabling audit log consolidated cache

You can disable the file system audit log consolidated cache for an EVS if you do not want to report file system audit events to Windows clients.

Procedure

1. Navigate to **Configuration** > **Files Services** > **File System Audit Policies**.
2. In the **File System Audit Policies** pane, select the EVS that is associated with the cache from the list of EVS instances.
3. Cick **Disable Cache**.

Modifying a file system audit policy

You can edit auditing information by modifying the file system audit policy.

Procedure

1. Navigate to **Configuration** > **Files Services** > **File System Audit Policies**.
2. In the **File System Audit Policies** pane, select the EVS associated with the policy from the list of EVS instances.
3. Locate the policy that you want to modify, and then click **View**.
4. In the policy name pane, click the edit icon, and modify the information that you want to change.
5. Click **Save**.

Deleting a file system audit policy

You can delete a file system audit policy if it is no longer required.

Procedure

1. Navigate to **Configuration** > **Files Services** > **File System Audit Policies**.
2. In the **File System Audit Policies** pane, select the EVS that is associated with the audit policy from the list of EVS instances.
3. Select one or more audit policies that you want to delete, and then click **Delete**.
4. Click **Delete** to confirm.

Security modes

Security modes are configured for each EVS, file system, and virtual volume. File system security mode and virtual volume security mode are configured when the file system and the virtual volume are created. You can view and switch the file system security mode of all EVS instances on a VSP One File server. The EVS security context should be set to global configurations which indicates that the security configuration is applied to all EVS instances in a VSP One File server.

The security modes are of two types:

- Unix security mode — When the VSP One File server is configured in UNIX security mode, it supports UNIX security definitions for SMB and NFS clients. All security settings are saved with UNIX file attributes. As a result, both NFS and SMB clients access files with UNIX security definitions.
- Mixed security mode — The mixed security mode supports both Windows and UNIX security definitions. In mixed security mode, each file (or directory) security is set up based on which user created, or which user last took ownership of the file (or directory). For a Windows user, the security definition is subject to Windows security rules; similarly, for a UNIX user, the security definition is subject to UNIX security rules.

Switching the file system security mode for EVS

You can switch the default file system security mode of all EVS instances only when the EVS security context is set to global configuration.

Procedure

1. Navigate to **Configuration** > **File Services** > **File System Security**.
2. In the **File System Security** pane, select **Global Configuration** from the list of EVS security contexts.
3. Click **Switch Mode**.
4. Click **Switch** to confirm.

Cluster name space

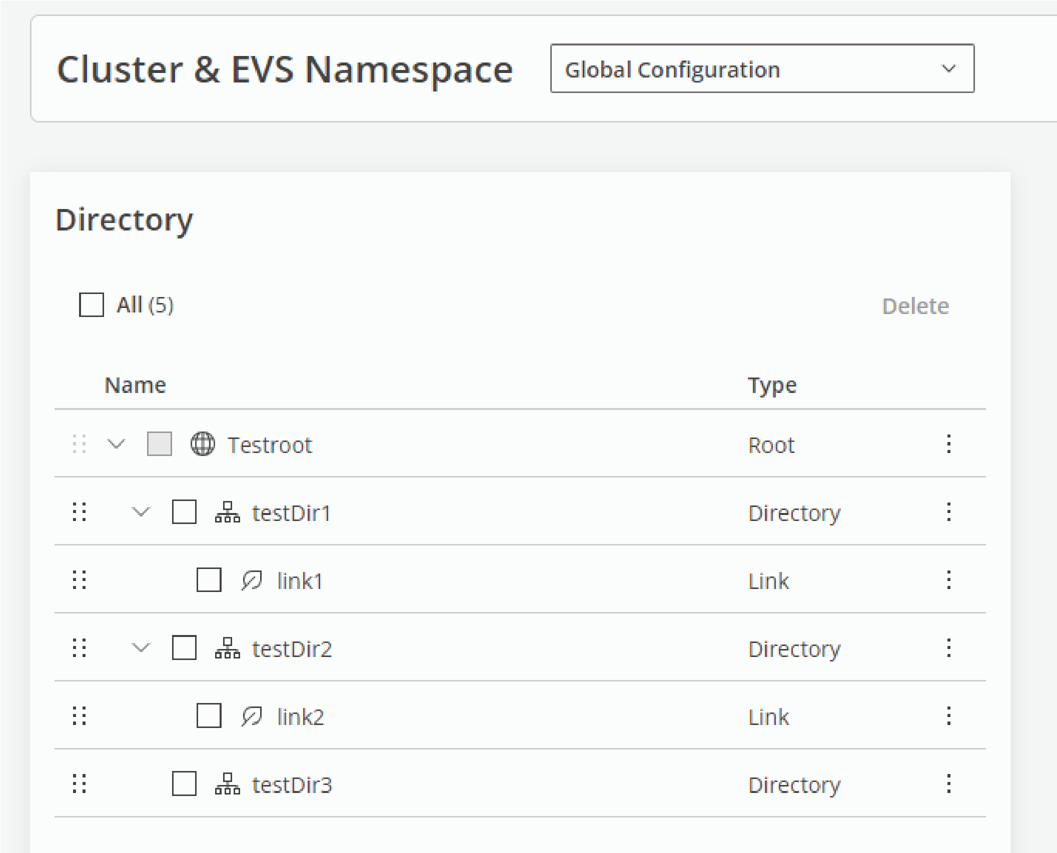
Important: A CNS is available only for EVS instances that use the global security context. You cannot complete the tasks in this section for EVS instances that use an individual security context.

The cluster name space (CNS) has a tree-like directory structure like a file system. The CNS virtual root and subdirectories provide access to file systems. You can view all of the configured directories and file system links in the File Administrator.

The following considerations help to simplify configuration and maintenance for a CNS:

- If there is only one CNS link to the file system, and there are no SMB shares or NFS exports on the file system, only a single link must be moved during a transfer of primary access.
- A CNS does not support hard links or move operations between the individual file systems. These operations are fully supported, but only within a single physical file system; that is, the part of the CNS tree under a file system link.
- Relocating file systems under the CNS might interrupt SMB access to the file system. To minimize interruption, relocate file systems when they are idle.
- Additional EVS instances causes unnecessary administrative overhead, and might lead to confusion. Use multiple EVS instances on the same cluster node only when you have data that should reside outside the cluster name space.
- When using a CNS, the recommended configuration is to have a single SMB share or NFS export at the root of the name space. If that configuration does not meet your requirements, the next best configuration is to have SMB shares or NFS exports pointing to individual directories in the name space. You should not configure SMB shares or NFS exports pointing to a path of the real file system unless it is necessary.

The following example shows a cluster name space tree structure:



Cluster & EVS Namespace

Global Configuration

Directory

□ All (5)

Delete

Name	Type
□ Testroot	Root
□ testDir1	Directory
□ link1	Link
□ testDir2	Directory
□ link2	Link
□ testDir3	Directory

- At the top of the name space the root directory is shown. In the example, the root directory is Testroot.
- Under the root directory are a number of subdirectories. In the example, one subdirectory has been created for each file system (testDir1, testDir2, and testDir3).
- Under each subdirectory is a file system link (link1 and link2). A file system link associates a directory with a specific file system.

Creating a CNS root directory

The first step required to configure CNS is to create the root directory.

Before you begin

Make sure that you select the appropriate EVS security context for the cluster name space.

Procedure

1. Navigate to **Configuration** > **File Services** > **CNS**.
2. In **CNS Root Label**, enter a label for the namespace, and then click **Apply**.

Creating CNS subdirectories

Subdirectories can be created under the root directory or under other subdirectories in the CNS tree. Subdirectories are optional, but they give structure to the CNS, allowing granular control over the organization of physical file system resources.

Before you begin

Make sure that a root directory is created for the name space.

Procedure

1. Navigate to **Configuration** > **File Services** > **CNS**.
2. From the more actions menu of the root directory, click **New Directory**.
3. In the **Create Directory** dialog box, enter a directory name, and then click **Create**.

   Note: The directory name must be between 2 and 255 characters long to be valid.

Creating a CNS file system link

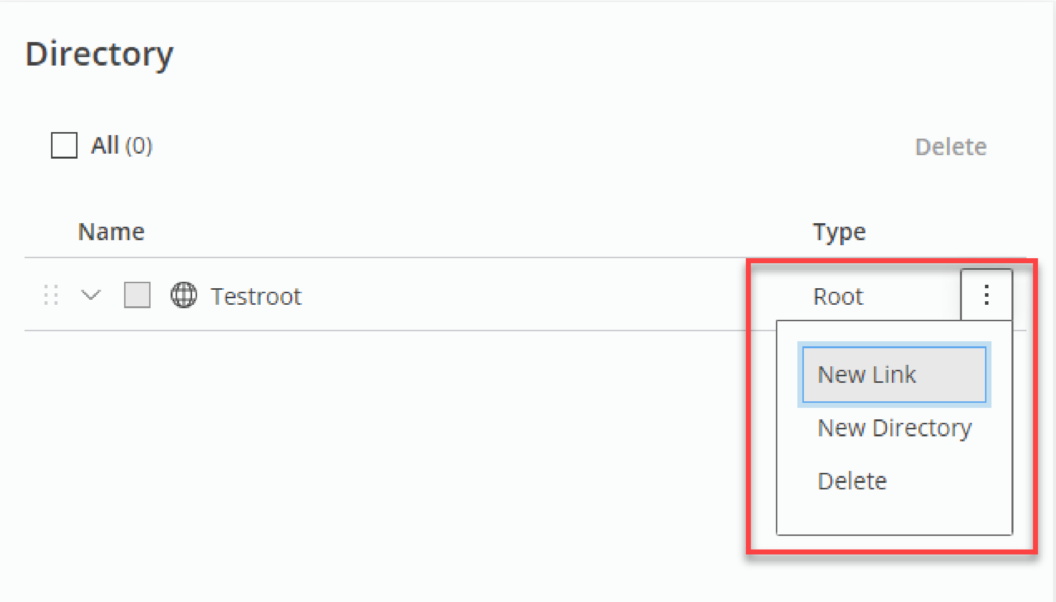
File system links make physical file systems accessible through the CNS. A file system link can be associated with either the root directory or a subdirectory. After creation, a file system link is displayed as a directory in the CNS. A network client navigating through CNS and into a file system link can see the contents of the directory.

Before you begin

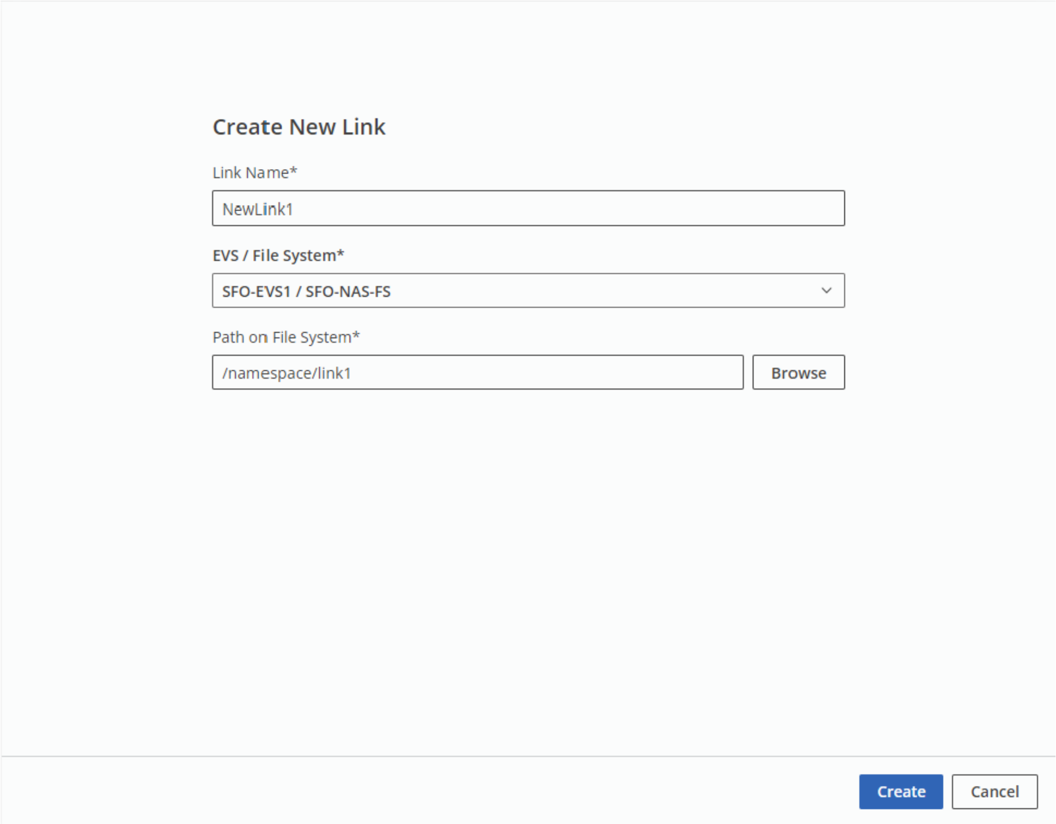
Make sure that a root directory is created for the name space.

Procedure

1. Navigate to **Configuration** > **File Services** > **CNS**.
2. From the more actions menu of the root directory, click **New Link**.



3. In the **Create New Link** dialog box, enter a file system link name, select the EVS and the file system for which the link is created, enter the path of the file system to be linked into the CNS, and then click **Create**.



Create New Link

Link Name*: NewLink1

EVS / File System*: SFO-EVS1 / SFO-NAS-FS

Path on File System*: /namespace/link1

Renaming a CNS subdirectory

Procedure

1. Navigate to **Configuration** > **File Services** > **CNS**.
2. From the CNS directory tree, identify the subdirectory to be renamed.
3. From the more actions menu, click **Edit**.
4. In the **Edit Directory** dialog box, enter a new name for the CNS directory, and then click **Save**.

Moving a CNS directory

Moving a CNS directory from one location in the CNS to another can be done at any time.

Procedure

1. Navigate to **Configuration** > **File Services** > **CNS**.
2. From the CNS directory tree, identify the subdirectory to be moved.
3. Drag and move the subdirectory to the new location in the CNS tree, then click **Save reorder**.

Modifying a CNS file system link

The name and location of a CNS file system link can be modified.

Procedure

1. Navigate to **Configuration** > **File Services** > **CNS**.
2. From the CNS directory tree, identify a file system link to modify.
3. From the more actions menu, click **Edit**.
4. As needed, change the link name or location.
    - To change the name of the file system link, enter the new link name and click **Save**.
    - To change the link location, identify the new location in the directory tree, drag the link to the new location, and then click **Save Reorder**.

Deleting a CNS file system link

Procedure

1. Navigate to **Configuration** > **File Services** > **CNS**.
2. From the CNS directory tree, select the file system link, and then click **Delete**.
3. Click **Delete** to confirm.

Deleting a CNS directory

Deleting a CNS directory permanently removes it and all of its subdirectories and file system links. Deleting CNS directories does not affect physical file systems on the server.

Procedure

1. Navigate to **Configuration** > **File Services** > **CNS**.
2. From the CNS directory tree, select the subdirectory, and then click **Delete**.
3. Click **Delete** to confirm.

Deleting a cluster name space

Before you begin

Make sure that there are no sub-directories and file system links present within the CNS root directory.

Deleting a CNS permanently erases it. Deleting a CNS does not affect the physical file systems accessible through the CNS. However, after the CNS is deleted, it might be necessary to restore access to the file system by sharing or exporting the file system through its EVS.

Procedure

1. Navigate to **Configuration** > **File Services** > **CNS**.
2. From the CNS directory tree, select the the root directory, and then click **Delete**.
3. Click **Delete** to confirm.

Event notification setup

You can configure the VSP One File server to send one of the following alert notification types to the users of File Administrator automatically when an event occurs:

- An email message, which the VSP One File server sends through an SMTP server.
- An SNMP trap, which notifies a central Network Management Station (NMS) of any events generated by the VSP One File server.
- A syslog alert, which is sent from the VSP One File server to a UNIX system log. The UNIX system must have its syslog daemon configured to receive remote syslog messages.

The best practice with any form of event notification is to set the notification frequency to Immediately for Severe events and send the alerts to at least two users.

Setting up email alerts

You can configure VSP One File server to send emails to specified recipients to alert them of system events. Setting up email alerts requires configuring SMTP servers to send out emails and setting up email profiles for distribution groups so that email recipients are notified.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **Email Alerts Setup**.
2. In the **Email Alerts Setup** page, click the edit icon.
3. Enter the Hostname or IP address of the SMTP server and the email address from which the alert email is sent to the recipient.

   The email address should specify a descriptive name that indicates the VSP One File sever or cluster from which the alert email is sent. If no name is configured, then the VSP One File server applies a default name. An example: administrator@<*servername*>.com.
4. Click **Save**.

Next steps

After setting up email alerts, add an email profile. For more information, see Adding an email profile (on page 183)

Adding an email profile

You can add email profiles to define different tiers of user responsibility for the VSP One File server. For example, you can create a profile in which recipients receive alerts only on Severe events; a second profile in which recipients receive alerts for only Severe and Warning events; and a third profile in which recipients receive alerts for all events. In a large user group, dividing these users into separate profiles saves time and simplifies event notification.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **Email Alerts Setup**.

2. In the **Email Alerts Setup** page, click **Add Email Profile**.
3. In the **Add Email Profile** page, complete the following information, and then click **Add**.
    a. To enable the email profile, set the **Enable Profile** toggle switch to **Yes**, and enter a profile name.

    A profile name can be a combination of letters (A-Z, a-z), numbers (0-9), and special characters.

    b. To allow the alert email to be sent in HTML format, set the **Send HTML Files** toggle switch to **Yes**.

    HTML emails are easier to read than plain text emails.

    c. To add recipients to the email profile, enter the email addresses of the recipients and press the enter key. Repeat this step to add multiple email addresses.

    d. To send a daily VSP One File server status email to recipients at midnight, set the **Send a Daily Status Email at Midnight** toggle switch to **Yes**.

    The daily status email contains logs of server performance, battery health, server health, and the current space usage of the file systems.

    e. To uuencode the attachments sent with alert emails when the VSP One File server restarts after an unplanned shutdown, set the **Uuencode Diagnostic Emails** toggle switch to **Yes**.

    Uuencoded email attachments contain diagnostic information that helps the recipients to identify the cause of the unplanned VSP One File server shutdown. By uuencoding the attachment, the email bypasses any virus scanning software at the recipient site.

    f. To exclude attachments from alert emails, set the **Exclude Attachments** toggle switch to **Yes**.

    g. To share server details in alert emails, set the **Disclose Server Details in Emails** toggle switch to **Yes**.

    Server details include restricted or confidential information like account names, IP addresses, and portions of user data.

    h. Enter a message to send as an alert email introduction.

    The introduction message is used to add information or comments to the body of the alert email.

    i. Enter the maximum size limit of an alert email in KiB.

    j. Based on the severity of the alert, select the frequency to send an alert email:

    - Immediate (An email is sent immediately when the event occurs. This option is intended for Severe events, but can be used for any event.)
    - Summary (An email is sent once or twice a day. This option is intended for Warning or Information events, but can be used for any event.)
    - Never (This is the default.)

    k. If the frequency is set to **Summary**, set the time to send the first summary. Optionally, set the time to send the second summary. The time is set in 24 hour format.

l. To send empty summary alert emails to the recipient, set the **Send Empty Summary Alert Emails** toggle switch to **Yes**.

   If there are no alerts, the VSP One File still sends out a summary email at the specified time.

m. To prevent alerts when the NDMP backup system generates an event, set the **Ignore NDMP Events in Immediate Emails** toggle switch to **Yes**.

Modifying an email profile

You can modify all information in an email profile except the profile name.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **Email Alerts Setup**.
2. In the **Email Alerts Setup** pane, locate the email profile that you want to modify, and then click **Edit**.
3. In the **Edit Email Profile** pane, edit the profile information.
4. Click **Save**.

Deleting an email profile

Alerts cannot be delivered if you delete an email profile. Make sure that you configure another profile to receive the alerts before deleting an existing profile.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **Email Alerts Setup**.
2. In the **Email Alerts Setup** pane, select the profile that you want to delete, and then click **Delete**.
3. Click **Delete** to confirm.

Setting up SNMP traps

You can set up an SNMP trap for VSP One File server to send an alert to an external system running an SNMP program when an event occurs.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **SNMP Traps Setup**.
2. In the **SNMP Traps Setup** page, click the edit icon.
3. Set the notification frequency for **Severe Alerts**, **Warning Alerts**, and **Information Alerts** to **Immediately**.
   - A Severe Alert indicates that a VSP One File server component has failed, which is a threat to the functioning of the server.
   - A Warning Alert indicates that a VSP One File server component requires attention, but it is not an immediate threat to the functioning of the server.
   - An Information Alert indicates that a VSP One File server component is operating normally.

4. Enter the port number that the server uses to send traps. The default port is 162.
5. To send a trap during an authentication failure, set the **Send traps upon authentication failure** toggle switch to **Yes.**

   An example of an authentication failure event is an SNMP host using an incorrect community string when sending a request.
6. Click **Save**.

Next steps

After setting up the SNMP traps, add trap recipients. For more information, see Adding SNMP trap recipients (on page 186).

Adding SNMP trap recipients

Add SNMP trap recipients for the traps sent by the VSP One File server.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **SNMP Traps Setup**.
2. In the **SNMP Traps Setup** page, click **Add** to add trap recipients.
3. Enter the Hostname or IP address of the SNMP host where the VSP One File server sends traps and the name of the SNMP community, and then click the check mark icon to save the trap recipients.

   Each SNMP host associates with an SNMP community. An SNMP community is a string that contains user credentials used to access data stored on other devices. An example of an SNMP community is `public`.

Deleting SNMP trap recipients

Deleting an SNMP trap disrupts the VSP One File server from sending alerts to hosts when an event occurs.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **SNMP Traps Setup**.
2. In the **SNMP Traps Setup** page, identify the SNMP trap recipient that you want to delete.
3. Select the SNMP trap, and then click **Delete**.
4. Click **Delete** to confirm.

Setting up syslog alerts

You can set up syslog alerts to send an alert from the VSP One File server to a UNIX system log when a severe or warning or information event occurs. The UNIX system must have its syslog daemon configured to receive remote syslog messages.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **Syslog Alerts Setup**.
2. In the **Syslog Alerts Setup** page, click the edit icon.

3. Set the notification frequency for **Severe Alerts**, **Warning Alerts**, and **Information Alerts** to **Immediately**.
   - A Severe Alert indicates that a VSP One File server component has failed, which is a threat to the functioning of the server.
   - A Warning Alert indicates that a VSP One File server component requires attention, but it is not an immediate threat to the functioning of the server.
   - An Information Alert indicates that a VSP One File server component is operating normally.
4. Click **Save**.

Next steps

After setting up syslog alerts, add syslog servers to receive alerts. For more information, see Adding syslog alerts server (on page 187)

Adding syslog alerts server

Add syslog servers to receive alerts from the VSP One File server.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **Syslog Alerts Setup**.
2. In the **Syslog Alerts Setup** page, click **Add** to add a syslog alert.
3. Enter the IP address or hostname of a syslog server where the VSP One File server sends the alerts, and then click the check mark icon to save the syslog alert.

Deleting syslog alerts server

Deleting a syslog alert server disrupts the VSP One File server from sending alerts to hosts when an event occurs.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **Syslog Alerts Setup**.
2. In the **Syslog Alerts Setup** page, select the syslog alert server that you want to delete, and then click **Delete**.
3. Click **Delete** to confirm.

Sending test notification

You can send a test email notification to the recipients defined for email notifications. Test notification setup send an alert immediately to all email recipients, regardless of notification frequency. The test notification setup is used to check the configuration of the email profile.

Procedure

1. Navigate to **Configuration** > **Event Notification Setup** > **Test Notification Setup**.

2. In the **Test Notification Setup** page, select the alert type to test:
   - Information
   - Warning
   - Severe
3. Type an alert message in the message box.

   The message box supports a maximum 255 characters.
4. Click **Send**.

Chapter 8: Network management

Network management includes configuring IP addresses and routes, grouping file-serving physical ports into link aggregations, and configuring name and directory services.

IP addresses

You can add, view, modify, or remove IP addresses in the VSP One File server network.

Viewing IP addresses

You can view information about the IP addresses that are in the VSP One File server network.

To view IP addresses, click Configuration > System > IP Addresses.

The following information is shown for each IP address:

Field/Item	Description
IP Address	The IP address of the administrative service, file service, or node.
Type	The type of the IP address: ▪ Administrative services: The IP address is for an administrative service. ▪ File services: The IP address is for a file service. ▪ Cluster Node: The IP address is for a node that can be a standalone node or a cluster node.
Label	The name of the Enterprise Virtual Server (EVS) or node that is assigned to the IP address.
Port	The interface (port) that is used by the IP address. One of the following values is shown: ▪ ag<*n*>: Identifies a file serving aggregation interface. ▪ eth-ag<*n*>: Identifies an aggregate Linux interface. ▪ ag<*n*>-vlan<*number*>: Identifies a VLAN interface. ▪ eth0 or eth1: Identifies a 10/100/1000 Ethernet non-file serving interface.

Adding an IP address

You can add an IP address for an administrative service, file service, or node (standalone or cluster).

Procedure

1. Navigate to **Configuration** > **System** > **IP Addresses**.
2. In the **IP Addresses** pane, click **Add IP Address**.
3. In the **Add IP Address** dialog box, complete the following information:
   - In the **EVS/Cluster Node** list, select the EVS or node that you want to assign to the IP address.

     The IP address type is specified for the EVS or node. For example, **EVS1 - File services** indicates that the EVS named EVS1 is a file service IP address.
   - In the **Port** list, select the interface that is used by the IP address.
   - Select the IP address type, **IPv4** or **IPv6**, and complete the associated information:
     - IPv4: Enter the IP address and select a netmask.
     - IPv6: Enter the IP address.
4. Click **Add**.

Modifying an IP address

Procedure

1. Navigate to **Configuration** > **System** > **IP Addresses**.
2. Select the IP address that you want to modify, and then click **Edit**.
3. In the **Edit IP Address** dialog box, you can update the following information:
   - In the **Port** list, select the port.
   - Select the IP address type, **IPv4** or **IPv6**, and modify the associated information:
     - IPv4: Enter the IP address and select a netmask.
     - IPv6: Enter the IP address.
4. Click **Save**.

Removing an IP address

Before you begin

> ⚠ **Caution:** Active connections end when the IP address is removed. Verify that the IP address is not in use.

Procedure

1. Navigate to **Configuration** > **System** > **IP Addresses**.

2. In the **IP Addresses** pane,
   - To delete static IP routes, select the IP address or addresses that you want to remove or click **All** to select all addresses, and then click **Delete**.
   - To remove dynamic IP routes, click **Flush Routes** to flush the cache.
3. Click **Delete** to confirm.

Advanced IP settings

Advanced settings are configured for the IP addresses that are in the VSP One File server network. These settings are the default values related to the IP network interfaces.

Viewing global IP settings

You can view the global settings for the IP addresses that are in the VSP One File server network. To view the settings, navigate to Configuration > System > Advanced IP Configuration.

Global Settings

The Global Settings pane shows the following settings:

Field/Item	Description
IP Reassembly Timer (Seconds)	The number of seconds before the server discards an incomplete IP datagram.
Ignore ICMP Echo Requests	Indicates whether Internet Control Message Protocol (ICMP) echo requests are ignored
Ignore ICMP Redirects	Indicates whether ICMP redirects are ignored.
TCP Keep Alive	Indicates whether a keepalive packet is sent when the system does not receive data or acknowledgment packets for a connection within the specified timeout period.
TCP Keep Alive Timeout (Seconds)	The number of seconds to keep a TCP connection alive.
TCP MTU	Specifies the size of the maximum transmission unit (MTU) in use for TCP packets when transmitting to a locally configured subnet.
Other Protocol MTU (Bytes)	Specifies the size of the MTU for protocols other than TCP when transmitting to a locally configured subnet.
ARP Cache Timeout (Seconds)	The number of seconds before the server removes an unused ARP entry from the caching table.

Field/Item	Description
IP MTU for Off-Subnet Transmits (Bytes)	The maximum IP packet size in use when transmitting to a different subnet.

Ports

The Ports pane shows the file service interfaces (ports) and whether default global settings or custom settings are used for each interface.

Modifying global IP settings

Procedure

1. Navigate to **Configuration** > **System** > **Advanced IP Configuration**.
2. In the **Global Settings** pane, click the edit icon.
3. Update the following settings, and then click **Save**:

Field/Item	Description
IP Reassembly Timer (Seconds)	Enter the number of seconds before the server discards an incomplete IP datagram. The default is **5**.
Ignore ICMP Echo Requests	Set the toggle switch to **Disabled** or **Enabled**. When enabled, this option instructs the system not to respond to Internet Control Message Protocol (ICMP) echo requests. The default is **Disabled**.
Ignore ICMP Redirects	Set the toggle switch to **Disabled** or **Enabled**. When enabled, this option instructs the system to ignore ICMP redirects. The default is **Disabled**.
TCP Keep Alive	Set the toggle switch to **Disabled** or **Enabled**. When enabled, this option instructs the system to send a keepalive packet when it has received no data or acknowledgment packets for a connection within the specified timeout period.
TCP Keep Alive Timeout (Seconds)	Enter the number of seconds to keep a connection alive. The default is **7200**.

Field/Item	Description
TCP MTU	Enter the size of the maximum transmission unit (MTU) in use for TCP packets when transmitting to a locally configured subnet. The valid range is 68 to 9600 bytes. For IPv6 traffic, this value must be 1280 or greater. The default is **1500**.
Other Protocol MTU (Bytes)	Enter the size of the MTU for protocols other than TCP when transmitting to a locally configured subnet. The valid range is 68 to 9600 bytes. For IPv6 traffic, this value must be 1280 or greater. The default is **1500**.
ARP Cache Timeout (Seconds)	Enter the number of seconds before the server removes an unused ARP entry from the caching table. The default is **60**.
IP MTU for Off-Subnet Transmits (Bytes)	Enter the maximum IP packet size in use when transmitting to a different subnet. The valid range is 68 to 9600 bytes. For IPv6 traffic, this value must be 1280 or greater. The default is **1500**.

Resetting global IP settings to default

Procedure

1. Navigate to **Configuration** > **System** > **Advanced IP Configuration**.
2. In the **Global Settings** pane, click the edit icon.
3. Click **Reset to Default**.
4. Click **Yes, Continue** to confirm.

Modifying global IP settings for a port

By default, global IP settings are applied to ports. You can modify some of these settings by port. The modified settings override the global settings.

There are two options available to modify the settings: Edit or Customize. The option that is available depends on whether the port is currently using global settings or customized settings.

Procedure

1. Navigate to **Configuration** > **System** > **Advanced IP Configuration**.
2. In the **Ports** pane, select the port that you want to modify, and then click **Edit** or **Customize** to update the following settings:

Field/Item	Description
Ignore ICMP Echo Requests	Set the toggle switch to **Disabled** or **Enabled**. When enabled, this option instructs the system not to respond to Internet Control Message Protocol (ICMP) echo requests. The default is **Disabled**.
IP MTU for Off-Subnet Transmits (Bytes)	Enter the maximum IP packet size in use when transmitting to a different subnet. The valid range is 68 to 9600 bytes. For IPv6 traffic, this value must be 1280 or greater. The default is **1500**.
TCP MTU	Enter the size of the maximum transmission unit (MTU) in use for TCP packets when transmitting to a locally configured subnet. The valid range is 68 to 9600 bytes. For IPv6 traffic, this value must be 1280 or greater. The default is **1500**.
IP MTU for Off-Subnet Transmits (Bytes)	Enter the maximum IP packet size in use when transmitting to a different subnet. The valid range is 68 to 9600 bytes. For IPv6 traffic, this value must be 1280 or greater. The default is **1500**.
Other Protocol MTU (Bytes)	Enter the size of the MTU for protocols other than TCP when transmitting to a locally configured subnet. The valid range is 68 to 9600 bytes. For IPv6 traffic, this value must be 1280 or greater. The default is **1500**.

3. Click **Save**.

Resetting global IP settings for a port

If IP settings for a port are customized, you can reset the settings to the global values.

Procedure

1. Navigate to **Configuration** > **System** > **Advanced IP Configuration**.
2. In the **Ports** pane, select the port that you want to reset to the global settings.
3. Click **Restore**.
4. Click **Yes, Continue** to confirm.

Link aggregations

Network clients use file-serving physical ports to access Enterprise Virtual Servers (EVSes) on cluster nodes. These ports are commonly grouped together in a link aggregation to increase redundancy and throughput of data.

The maximum number of ports that you can include in an aggregation is dependent on the number of physical ports provided by the storage platform. All ports in the aggregation must be of the same type and speed.

Link aggregations can increase bandwidth capability and create resilient and redundant links. Aggregations also provide load balancing, where the processing and communications activity is distributed across several links in a trunk.

An aggregation can be static or use Link Aggregation Control Protocol (LACP).

Using LACP for link aggregations

The VSP One File server manages the LACP relationship between switches. By using LACP, the server determines which ports are in use and can bring up alternative ports during a failure. For example, if the server does not receive LACP messages from the primary switch within the timeout period, the server can use the ports connected to the secondary switch instead.

Note: The server sends LACP data units set to ACTIVE. However, the switch can be in active or passive mode.

The server supports short (one second) and long (30 second) LACP timers. A short timeout is three seconds (three x one second). A long timeout is 90 seconds (three x 30 seconds). The link times out after three missed messages. Long timeouts are a best practice to upgrade upstream network devices without causing path failover on the server. The default setting is a short timeout. To change the timeout setting, use the applicable **`lacp-set-timeout`** CLI command as described in the command reference for the storage platform.

Viewing link aggregations

You can view link aggregations by navigating to Configuration > System > Link Aggregation.

The following information is shown for each aggregation:

Field/Item	Description
Name	The aggregation name (ag<*n*>).
Use LACP	Indicates whether the aggregation uses LACP. The values are Yes (LACP) or No (Static).
Ports	The ports in the aggregation group.

Field/Item	Description
Aggregation Status	The status for each port associated with the aggregation. The values are: ▪ OK ▪ Degraded ▪ Down ▪ Attached (the port is not configured for LACP)

Status

The Status pane shows the aggregation names, the associated ports, and the status of the ports by node.

Adding a link aggregation

Procedure

1. Navigate to **Configuration** > **System** > **Link Aggregation**.
2. Click **Add Link Aggregation**.
3. In the **Add Link Aggregation** dialog box, complete the following information:
   - In the **Name** list, select one of the available aggregations names. These are aggregation names that are not in use.
   - In the **Available Ports** list, select the ports that you want to add to the aggregation.
   - For the **Use LACP** option, select **Yes (LACP)** or **No (Static)**. For more information about this option, see Additional information about adding a link aggregation (on page 196).
   - For the **Port Load Balancing** option, select **Normal** or **Round Robin**. For more information about these options, see Additional information about adding a link aggregation (on page 196).
4. Click **Add**.

Additional information about adding a link aggregation

The following table describes the additional information about the fields that are required while creating a link aggregation:

Field/Item	Description
Use LACP	Indicates whether the aggregation supports LACP to manage the relationship between multiple switches. By using LACP, the server determines which ports are in use and can bring up alternative ports during a failure. For example, if the VSP One File server does not receive LACP messages from the primary switch within the timeout period, the server can use the ports connected to the secondary switch instead.
Port level Load Balancing	One of the following load balancing schemes that is used for all ports in the aggregation. ▪ Normal: The server routes all traffic for a given conversation through one of the physical ports in the appropriate aggregation. The server hash and routing functions determine which packets use which physical ports of the aggregation. For example, all traffic for a particular TCP connection is routed through the same physical port unless the port drops. ▪ Round robin: The packets making up the traffic are routed through the ports in sequential order. For example, the first packet goes down the first port, the second packet goes down the next port and so on until all ports are used. Then the traffic starts again at the first port. This routing scheme ensures that all the ports are equally used, to provide maximum link throughput. The disadvantage of round robin is that the clients must be able to handle out of order TCP traffic at high speed. The LACP specification (802.3ad) requires that an implementation follow the appropriate rules to minimize out-of-order traffic and duplicated packets. Round robin load balancing directly contravenes this requirement. However, there are situations where the server hash functions cannot balance the conversations across physical ports efficiently, which results in poor link utilization and reduced throughput. In these cases, round robin load balancing can improve link utilization and improve throughput.

Modifying a link aggregation

Procedure

1. Navigate to **Configuration** > **System** > **Link Aggregation**.
2. Locate the link aggregation that you want to modify, and then click **Edit**.

3. In the **Edit Link Aggregation Details** dialog box, you can update the following information:
   - In the **Available Ports** list, add or remove the ports in the aggregation.
   - For the **Use LACP** option, select **Yes (LACP)** or **No (Static)**.
   - For the **Port Load Balancing** option, select **Normal** or **Round Robin**.
4. Click **Save**.

Removing a link aggregation

Procedure

1. Navigate to **Configuration** > **System** > **Link Aggregation**.
2. Locate the aggregation that you want to remove, and then click the delete icon.
3. Click **Delete** to confirm.

IP routes

The VSP One File server supports the following options for routing IP traffic: default gateways, static routes, and dynamic routes.

Default gateways

Multiple default gateways are supported for routing IP traffic. When connected to multiple IP networks, add a default gateway for each network to which the server is connected. This configuration lets the server direct traffic through the appropriate default gateway by matching source IP addresses specified in outgoing packets with the gateway on the same subnet.

With multiple default gateways, the server routes IP traffic logically, reducing the need to specify static routes for every network that connects with a particular server.

Static routes

Static routing gives a fixed path for data in a network. When a server on a network is connected to additional networks through a router, communication between that server and the remote networks can be enabled by specifying a static route to each network.

Static routes are set up in a routing table. Each entry in the table consists of a destination network address, a gateway address, and a subnet mask. Entries for static routes in the server’s routing table are persistent, meaning that if a server is restarted, the routing table preserves the static routing entries.

Dynamic routes

Internet Control Message Protocol (ICMP) redirects and the Routing Information Protocol (RIP) are used to dynamically add routes to its route table.

ICMP redirects are a mechanism for routers to convey routing information back to the server. When one router detects that another router offers a better route to a destination, it sends the server a redirect that temporarily overrides the server's routing table. Being router-based, dynamic redirects do not require any configuration, but they can be viewed in the routing table.

The server supports ICMP router discovery, which lets the server discover the addresses of routers. ICMP routers periodically multicast their addresses; when the server receives these multicasts, it incorporates the routers into its routing table.

RIP lets the server automatically discover routes and then update routes in the routing table based on updates provided by other network devices.

The server stores dynamic host routes in its route cache for 10 minutes. When the time has elapsed, packets to a selected destination use the route specified in the routing table until the server receives another ICMP redirect.

Viewing IP routes

You can view the IP routes that are associated with the VSP One File server. To view the routes, navigate to Configuration > System > IP Routes.

The following information is shown for each route:

Field/Item	Description
Cluster Node Routing	When this option is disabled (the default behavior), the configured routes are propagated to all nodes in a cluster. If this option is enabled, it is possible to configure different routes for each node in a cluster. ⚠ **Caution:** If an EVS fails over to a node that is missing a required route, network traffic can no longer reach the required destination.
Destination	For a network route, this field shows the IP address and address prefix length of the destination. For a host route, this field shows only an IP address.
Gateway	The gateway IP address of the route.
Type	The type of route: ▪ Default: The route is set to gateway IP address. ▪ Network: The route is set to a specific network. ▪ Host: The route is set to a specific computer on the network.
Creation Type	The value Static indicates that the route was created manually. Dynamic indicates that the route was created by a switch.

Field/Item	Description
MTU	This value is the Maximum Transmission Unit (MTU), which is the largest size Ethernet frame that the server can send for the route.

Adding an IP route

You can add a gateway, network, or host IP route. These routes are static. The maximum possible number of static routes is 127.

Procedure

1. Navigate to **Configuration** > **System** > **IP Routes**.
2. Click **Add IP Route**.
3. In the **Add IP Route** dialog box, complete the following information:
   - In the **Route Type** list, select one of the following options:
     - **Default**: Select to set the gateway IP address of the route that is entered in the **Destination** box.
     - **Network**: Select to set a route to a specific network.
     - **Host**: Select to set a route to a specific computer on the network.

     The selected option determines which of the following options are available.
   - In the **Destination** box, enter the following information for the route destination:
     - If you selected the **Network** option, enter the IP address and select the address prefix length.
     - If you selected **Host**, enter only the IP address. Addresses that include numbers greater than 255, broadcast addresses, and unreachable gateways are not valid.
   - In the **Gateway** box, enter the gateway IP address for the route.
   - In the optional **MTU** box, enter the Maximum Transmission Unit (MTU). The MTU is the largest size Ethernet frame that the server can send for this route.

     This value must be between 68 and 9600 inclusive for IPv4 routes and between 1280 and 9600 inclusive for IPv6 routes. If the MTU is not specified, the server applies a default of 1500.
4. Click **Save**.

Removing an IP route

Procedure

1. Navigate to **Configuration** > **System** > **IP Routes**.
2. Select the route or routes that you want to remove.
3. Click **Delete** to confirm.

Name and directory services

Name and directory services support the location, administration, and management of network resources.

Name Services

The following name resolution methods are supported:

- Domain Name System (DNS)
- Windows Internet Naming Service (WINS)
- Network Information Service (NIS) and Lightweight Directory Access Protocol (LDAP)

These methods associate computer identifiers (for example, IP addresses) with computer (host) names. This association lets you to specify computer names rather than IP addresses in dialog boxes.

Directory services

The following directory service methods are supported:

- Lightweight Directory Access Protocol (LDAP)
- Network Information Service (NIS)

These services associate identifiers with users, groups, devices, volumes, folders, and other network resources. This functionality enables administrators to specify policies for access on a broad basis, rather than explicitly on a per-resource basis, and have this information accessible throughout the network.

Modifying the DNS or WINS name service

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. In the **Name Services** pane, select **Global Configuration** or an indvidual EVS from the EVS security contexts list.

   If an EVS inherits the global configuration, the option to modify the name service is not available. In this situation, you can modify the name service for only the global configuration.
3. On the **DNS and WINS** tab, click the edit icon.
4. Complete the following information:
   - In the **DNS Servers** box, enter the IP address, and then click **Add**. Repeat this step to add multiple addresses. To remove a server, click the delete icon.
   - In the **DNS Domain Name** box, enter the domain name.
   - In the **Domain Search Order** box, enter a domain suffix to use a search keyword, and then click **Add**. Repeat this step to add multiple suffixes. You can drag and move the suffixes to the order that you want.

- In the **WINS Server - Primary** box, enter the IP address of the primary WINS server.
- In the **WINS Server - Secondary** box, enter the IP address of the secondary WINS server (if available).

5. Click **Save**.

Modifying the name service order

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. In the **Name Services** pane, select **Global Configuration** or an indvidual EVS from the EVS security contexts list.

   If an EVS inherits the global configuration, the option to modify the name service order is not available. In this situation, you can modify the name service order for only the global configuration.
3. Click the **Ordering** tab, and then click the edit icon to change the server order.
4. To change the order, select the name services that you want in the **Available Name Services** box and click the arrow to move them to the **Selected Name Services** box.
5. Drag and move the name services in the **Selected Name Services** box to the order that you want.
6. Click **Save**.

Directory services

LDAP and NIS directory services associate identifiers with users, groups, devices, volumes, folders, and other network resources. This functionality enables administrators to specify policies for access on a broad basis, rather than explicitly on a per-resource basis, and have this information accessible throughout the network.

LDAP directory services

LDAP directory services provide user and group information retrieval, name service resolution, and FTP user authentication. Although LDAP and NIS directory services are supported, LDAP is more reliable and scalable than NIS and includes the following advantages:

- Improved accuracy, due to more frequent data synchronization of current and replicated data.
- Communications encryption using TLS.
- Authentication of connections to the LDAP database instead of anonymous access to NIS databases.

NIS directory services

NIS databases provide simple management and administration of Unix-based networks. These databases can provide details about users and groups, and also individual client machines (including the IP address and host name), to facilitate authentication for users logging in to clients on the network.

NIS directory services can provide the following features:

- NFS user and group account information retrieval.
- Name services for resolving host names to IP addresses.
- FTP user authentication.

Switching between NIS and LDAP directory services

You can change the directory service mode from LDAP to NIS or from NIS to LDAP.

> ⚠ **Caution:** You can temporarily lose connectivity to the server while switching between service modes.

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. In the **Name Services** pane, select **Global Configuration** or an indvidual EVS from the EVS security contexts list.

   If an EVS inherits the global configuration, the option to switch services is not available. In this situation, you can switch services for only the global configuration.
3. Click the **NIS / LDAP** tab.
4. Click **Switch to NIS** or **Switch to LDAP**.
5. Click **Yes, Continue** to confirm.

Result

The mode shown in the NIS / LDAP tab reflects the change to the server type.

Enabling NIS and LDAP directory services

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. In the **Name Services** pane, select **Global Configuration** or an indvidual EVS from the EVS security contexts list.

   If an EVS inherits the global configuration, the option to enable an LDAP or NIS directory service is not available. In this situation, you can enable a directory service for only the global configuration.
3. Click the **NIS / LDAP** tab.
4. Click **Enable NIS** or **Enable LDAP**.

Result

The mode shown in the NIS / LDAP tab reflects the enabled server type.

Disabling NIS and LDAP directory services

You can disable the use of directory services.

⚠ **Caution:** Use caution when disabling directory services because disabling these services prevents access to files.

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. In the **Name Services** pane, select **Global Configuration** or an indvidual EVS from the EVS security contexts list.

   If an EVS inherits the global configuration, the option to disable the directory services is not available. In this situation, you can disable the services for only the global configuration.
3. Click the **NIS / LDAP** tab.
4. Click **Disable NIS and LDAP**.
5. Click **Yes, Disable** to confirm.

LDAP servers

Modifying the LDAP configuration settings

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. In the **Name Services** pane, select **Global Configuration** or an indvidual EVS from the EVS security contexts list.

   If an EVS inherits the global configuration, the option to modify the LDAP configuration settings is not available. In this situation, you can modify the settings for only the global configuration.
3. Click the **NIS / LDAP** tab and confirm that **LDAP Mode** is shown, and then click the edit icon.
4. Complete the following information:

   - In the **Domain name** box, enter the LDAP domain name.
   - In the **Username** box, enter the username of the administrator who has rights and privileges for this LDAP server. The name can be up to 256 characters in length.
   - In the **Password** box, enter the password for the username.

- Set the **TLS** switch to **Disabled** or to **Enabled** to enable secure communication with the LDAP server.
- In the **Schema** list, select one of the following schemas for use by the LDAP server:
  - **MS Active Directory**: Configures the server to operate with Microsoft Active Directory 2012 and later using the default Active Directory schema.
  - **MS Identify Management for Unix**: Deprecated by Microsoft.
  - **MS Services for Unix**: Deprecated by Microsoft.
  - **RFC-2307**: Defines a standard convention for the storage and retrieval of user and group mapping information from an LDAP server. If the site uses the RFC 2307 (or RFC 2307bis) schema, and you configure the storage server/cluster to support both mixed mode operations and LDAP services, it is assumed that you have already loaded the RFC 2307 schema into the directory, and that you have already provisioned the user objects appropriately. This is the default.

5. Click **Save**.

Adding an LDAP server

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. Click the **NIS / LDAP** tab and confirm that **LDAP Mode** is shown.
3. Click **Add**.
4. In the **Add LDAP Server** dialog box, complete the following information:
   - In the **Server IP Address** box, enter the IP address for the LDAP server.
   - In the **Port** box, enter the standard port number to use for communication with the LDAP server. The default value is 389.
   - In the **TLS Port** box, enter the secure port to use for communication with the LDAP server. The default value is 636.
5. Click **Add**.

Modifying an LDAP server

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. Click the **NIS / LDAP** tab and confirm that **LDAP Mode** is shown.
3. Select the LDAP server that you want to modify, and then click **Edit**.
4. In the **Edit LDAP Server** dialog box, modify the following information:
   - In the **Server IP Address** box, enter the IP address for the LDAP server.
   - In the **Port** box, enter the standard port number to use for communication with the LDAP server. The default value is 389.
   - In the **TLS Port** box, enter the secure port to use for communication with the LDAP server. The default value is 636.

5. Click **Save**.

Removing an LDAP server

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. Click the **NIS / LDAP** tab and confirm that **LDAP Mode** is shown.
3. Select the server or servers that you want to remove or click **All** to select all servers, and then click **Delete**.
4. Click **Delete** to confirm.

NIS servers

Modifying the NIS configuration settings

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. In the **Name Services** pane, select **Global Configuration** or an indvidual EVS from the EVS security contexts list.

   If an EVS inherits the global configuration, the option to modify the NIS configuration settings is not available. In this situation, you can modify the settings for only the global configuration.
3. Click the **NIS / LDAP** tab and confirm that **NIS Mode** is shown, and then click the edit icon.
4. Complete the following information:
   - In the **Domain** box, enter the name of the NIS domain for which the system is a client. The maximum number of characters is 64.
   - In the **Rebind** box, the frequency of attempts to connect to configured NIS servers. Enter a value from 1 to 15 minutes.
   - In the **Timeout** box, enter a time from 100 to 10,000 milliseconds to wait for a response from an NIS server when verifying the domain for servers. The default value is 300 milliseconds.
   - Set the **Broadcast for Servers** switch to **Disabled** or to **Enabled** to discover the available NIS servers on the network. The servers must be in the same NIS domain and present on the server's network.
5. Click **Save**.

Adding a NIS server

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. Click the **NIS / LDAP** tab and confirm that **NIS Mode** is shown.
3. Click **Add**.

4. In the **Add NIS Server** dialog box, complete the following information:
   - In the **Server IP address** box, enter the IP address for the NIS server.
   - In the **Priority** box, enter the priority level for the selected NIS server (the lowest value is highest priority). If the NIS domain contains multiple servers, the system attempts to bind to the server with the highest priority level whenever it performs a rebind check. The following options are available: **low (3)**, **medium (2)**, and **high (1)**.
5. Click **Add**.

Modifying a NIS server

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. Click the **NIS / LDAP** tab and confirm that **NIS Mode** is shown.
3. Select the NIS server that you want to modify, and then click **Edit**.
4. In the **Edit NIS Server** dialog box, update the following information:
   - In the **Server IP address** box, enter the IP address for the NIS server.
   - In the **Priority** box, enter the priority level for the selected NIS server (the lowest value is highest priority). If the NIS domain contains multiple servers, the system attempts to bind to the server with the highest priority level whenever it performs a rebind check. The following options are available: **low (3)**, **medium (2)**, and **high (1)**.
5. Click **Save**.

Removing a NIS server

Procedure

1. Navigate to **Configuration** > **System** > **Name Services**.
2. Click the **NIS / LDAP** tab and confirm that **NIS Mode** is shown.
3. Select the server or servers that you want to remove or click **All** to select all servers, and then click **Delete**.
4. Click **Delete** to confirm.

Chapter 9: Logs

Use logs to detect, troubleshoot, and fix errors or failures.

Downloading diagnostic logs

File Administrator allows you to download diagnostic log files to investigate and resolve errors or failures.

Procedure

1. Navigate to **Support** > **Troubleshooting** > **Diagnostic Logs**.
2. Select the devices for which diagnostics are required.
   - **Managed NAS Servers**
   - **System Administrator**

   You can download diagnostics for **Managed NAS Servers** and **System Administrator** together.

   If you want to download diagnostics for **Managed NAS Servers** you have to select **Include All Managed Servers** to download all managed NAS servers diagnostic logs or **Include Only the Currently Managed Server** to download only the selected managed server diagnostic logs.
3. Click **Prepare Logs**.

Result

File Administrator downloads the diagnostic log file. An example of the diagnostic file name is `diagnostics_YYYY_MM_DD_<current time>+0000.zip`, where DD, MM and YYYY is the date, month and year when the diagnostic file is downloaded.

Event logs

You can configure the VSP One File server to show comprehensive event logging and automated alert notification. The server continuously monitors temperature, fans, power supply units, and disk drives. Each time an event occurs, for example, a disk failure or a possible breach of security, the server records it in an event log. The event log can be saved as a permanent record. The event log is used in trend and fault analysis.

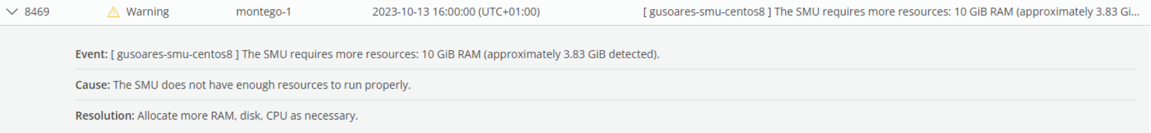
The automated alert notification is sent by the server according to a predefined severity categories (Severe, Warning, Information), including daily summary. When automated alert notification is enabled, the system notifies selected personnel when an event is generated, based on the level of severity of the event. Automated alert notification helps users to proactively monitor the health of the server and address problems with the server.

The event log can contain a maximum of 10,000 events. When the event log limit is reached, each new event replaces the oldest event in the log.

Displaying and filtering event logs

Procedure

1. Navigate to **Support** > **Logs** > **Event Logs**.
2. Search an event log with an event ID or event description or by using the **Filter**.
3. Set the filter for severity level of the events, event category type, cluster node for which you want to display the log, and date range you want to view.
4. Click an event to display its details, cause, and resolution.



8469 Warning montego-1 2023-10-13 16:00:00 (UTC+01:00) [gusoares-smu-centos8] The SMU requires more resources: 10 GiB RAM (approximately 3.83 Gi...

Event: [gusoares-smu-centos8] The SMU requires more resources: 10 GiB RAM (approximately 3.83 GiB detected).

Cause: The SMU does not have enough resources to run properly.

Resolution: Allocate more RAM, disk, CPU as necessary.

5. Select **Server Time** to view the time of occurrence of the event logs in the server location timezone.

   By default, File Administrator shows the event logs in local time.
6. Click **Download** to download the log as a csv file to your computer.

FTP audit logging

FTP audit logging is managed individually for each EVS. When enabled, it maintains an audit log that tracks user activity performed through the FTP protocol for all file systems within the EVS. The audit log is generated to monitor user activity and record events whenever a user performs the following actions:

- Logging in or out.
- Renaming or deleting a file.
- Retrieving, appending, or storing a file.
- Creating or removing a directory.

Additionally, it logs occurrences of session timeouts.

Upon accessing the **FTP Audit Logs** page for this first time, you will encounter a list of EVS instances with a disabled status. This status indicates that the configuration has not yet been set up. To initiate FTP audit logging, configure the settings for each EVS. For more information, see Enabling and configuring FTP audit logging (on page 210).

If you have previously configured FTP audit logging, the FTP Audit Logs page will display the current settings and status for each EVS. From this page, you can disable audit logging or modify the settings.

FTP events are logged in a text file, where each event is represented by a tab-delimited line. Each line includes the date, time, username, client IP address, and command description. The most recent file is named `ftp.log`, while older files follow the naming convention `ftp<n>.log`, with *n* increasing as additional files are created.

To view FTP audit logs, use a text editor. If the logging directory is within an NFS export or SMB share, access the directory and open the log file. Alternatively, if the logging directory is accessible through FTP, download and open the file using a text editor.

Enabling and configuring FTP audit logging

You can enable and configure FTP audit logging.

Procedure

1. Navigate to **Support** > **Logs** > **FTP Audit Logs**.
2. Locate the EVS to enable and configure FTP audit logging, and then click **Edit**.
   - Set the **Audit Logging** toggle to **Enabled**.
   - Select a file system to store the audit log files.
   - Specify the maximum number of records per log file. When this limit is reached, a new log file is created. By default, each log file contains up to 10000 records.

     FTP events are logged in a text file, where each event is represented by a tab-delimited line. Each line includes the date, time, username, client IP address, and command description.
   - Specify the maximum number of log files. When the number of log files reaches its limit, the oldest log file is automatically deleted to create space for new ones. By default, the file system maintains up to 10 log files.

     The most recent file is named `ftp.log`, while older files follow the naming convention `ftp<n>.log`, with *n* increasing as additional files are created.
   - Enter the directory path within the selected file system.
   - Select the **Create path if it does not exist** option to automatically create the directory .

   > **Note:**
   >
   > Automatically created directories are owned by the root user and group (UID:0 / GID:0) and have full permissions (read, write, and execute). You can create these directories using the SMB or NFS protocols, or explicitly grant the appropriate permissions after creation using this option.
3. Click **Save**.

Appendix A: Guidelines for entering values in the Access Configuration field

To secure and control access to shared resources, follow these guidelines when specifying the IP addresses of the clients that can access them.

IP address and domain specification

Use the following IP address and domain specification guidelines to enter the IP addresses of the clients to configure access to SMB shares, NFS exports, and iSCSI targets.

Value	Description
Blank or `*`	All clients can access the shared resources.
Specific addresses or name. Examples: Example: `192.0.2.0`, `client.dept.example.com`	Clients with specified names or addresses can access the shared resources.
A range of addresses using Classless Inter-Domain Routing (CIDR) notation. Example: `192.0.2.0/24`	Clients with an IP address within the specified IP address range (10.168.20.0 to 10.168.20.255) can access the shared resources.
Partial addresses or name using wildcards Example: `192.0.*.*`	Clients with matching names or addresses can access the shared resources.

IP address export qualifiers

You can append the following qualifiers to IP addresses when specifying client access.

Qualifier	Description	Applicable to
read_write, readwrite, rw	Grants read and write access. This is the default setting.	SMB shares and NFS exports
read_only, readonly, ro	Grants read-only access.	SMB shares and NFS exports

Qualifier	Description	Applicable to
noaccess, no_access	Denies the specified clients access.	SMB shares, NFS exports, and iSCSI targets
root_squash, rootsquash	Maps user and group IDs of 0 to the anonymous user or group. This is the default setting.	NFS exports
no_root_squash, norootsquash	Turns off root squashing.	NFS exports
all_squash, allsquash	Maps all user IDs and group IDs to the anonymous user or group.	NFS exports
no_all_squash, noallsquash	Turns off all squashing. This is the default setting.	NFS exports
secure	Requires requests to originate from an IP port lower than 1024. Access to such ports is normally restricted to administrators of the client machine. To turn this off, use the **`insecure`** option.	NFS exports
insecure	Turns off the **`secure`** option. This is the default setting.	NFS exports
anon_uid, anonuid	Explicitly sets an anonymous user ID.	NFS exports
anon_gid, anongid	Explicitly sets an anonymous group ID.	NFS exports
(sec=<mode>)	Specifies the NFS security flavor, where <mode> is a colon delimited list of allowed security flavors (sys:krb5:krb5i:krb5p).	NFS exports

The following qualifiers are examples:

- **`10.1.2.38(ro)`**

  Grants read-only access to the client with IP address 10.1.2.38.

- **`10.1.2.0/24(ro)`**

  Grants read-only access to all clients with an IP address in the range 10.1.2.0 to 10.1.2.255.

- **`yourcompanydept(ro)`**

  Grants read-only access to all members of the NIS group.

- **`*.mycompany.com(ro, anonuid=20)`**

  Grants read-only access to all clients with a computer name that ends in .mycompany.com. All squashed requests are treated as if they originated from user ID 20.

- **`10.1.*.* (readonly, allsquash, anonuid=10, anongid=10)`**

  Grants read-only access to all the matching clients with IP address beginning with 10.1. All requests are squashed to the anonymous user, which is explicitly set as user ID 10 and group ID 10.

- The order that the entries are specified is important.

  `*(ro)`

  `10.1.2.38(rw)`

  The first grants read-only access to all clients, the second line grants read/write access to the specified client. These lines must be transposed to grant write access to 10.1.2.38.

- **`10.1.1.*(sec=sys),10.1.2.*(sec=krb5:krb5i:krb5p),*(sec=krb5p)`**
  - Clients in the 10.1.1.* subnet use **`sys`** authentication.
  - Clients in the 10.1.2.* subnet to use **`krb5`**, **`krb5i`**, or **`krb5p`**.
  - All other clients use **`krb5p`**.

  Note: To improve system performance, specify client access IP address or IP address ranges before specifying host name or NIS netgroups.

Specifying clients by name

The following list describes how to specify clients by name rather than by IP address in SMB shares and NFS exports.

- **Full Qualified Domain Name Required**

  To specify the fully qualified domain name of the client. For example, use **`aclient.dept.example.com`** instead of **`aclient`**.

- **Leading Wildcard Allowed**

  To specify a partial name, a single wildcard located at the start of the name can be used.

  You can use a single wildcard (*) at the beginning of a name to specify a partial name or pattern.

- **Export Options Change Requires Remount**

  When the client mounts the shared resource, it determines which option to apply to a specific client. Subsequent changes to DNS, WINS, or NIS that resolve the client's IP address to a different computer name are only applied when the client unmounts and remounts the share or export.

- **Name Service Order is Significant**.

  The application of share or export options to a client's mount request may be affected by the order in which the system applies DNS, WINS, and NIS information to resolve IP addresses. The first service that can resolve the client name (in the name order sequence) supplies the name and searches configuration options for the share or export.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact