Hewlett Packard Enterprise

HPE StoreOnce VSA System User Guide

For StoreOnce software version 4.1.3

Abstract

This document is the user guide for the Hewlett Packard Enterprise StoreOnce VSA System and is intended for users who install, operate, and maintain the StoreOnce System. Always check www.hpe.com/info/storeonce/docs for the most current documentation, including localized versions (PDF) for your product.

Part Number: BB954-80094a
Published: January 2020
Edition: 1

© Copyright 2018, 2019 Hewlett Packard Enterprise Development LP

Notices

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

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

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

Notice for OpenSSL

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (**http://www.openssl.org**)

Acknowledgments

Intel®, Itanium®, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

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

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

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

UNIX® is a registered trademark of The Open Group.

Contents

Getting started....10
What's new in HPE StoreOnce Systems 4.1.1.... 10
FAQ....10
Logging in to the StoreOnce Management Console.... 11
User interface quick tour.... 11
Selecting a system to view and manage (federation).... 12
StoreOnce Management Console supported browsers.... 12
Using the StoreOnce First Time Setup wizard.... 13

About StoreOnce Systems....14
StoreOnce VSA....14
Security features.... 14

Federations....17
About federations....17
Standalone federation example.... 17
Overlapping federations example.... 18
Viewing federation health....19
Viewing federation members....20
Creating federations....20
Adding systems to federations....21
Removing systems from federations....21
Selecting a system to view and manage (federation).... 22

Dashboards.... 23
Viewing system dashboards.... 23
Viewing federation dashboards....23
Capacity efficiency terms.... 24
Editing system information....24

Data services overview....25
Viewing data services.... 25

StoreOnce Catalyst data services.... 26
About StoreOnce Catalyst.... 26
Stores....26
Viewing StoreOnce Catalyst stores....27
StoreOnce Catalyst stores screens and properties....27
Creating StoreOnce Catalyst stores....42
Editing StoreOnce Catalyst stores.... 42
Deleting StoreOnce Catalyst stores....43
Cloud Bank stores....43
Viewing Cloud Bank stores.... 43
Cloud Bank stores screens and properties.... 43

Cloud Bank stores service providers and properties....56
Tips for working with Cloud Bank stores....57
Creating Cloud Bank stores....60
Connecting Cloud Bank stores....60
Deleting Cloud Bank stores....61
Detaching Cloud Bank stores....61
Disconnecting Cloud Bank stores....62
Editing Cloud Bank stores....62
Exporting encryption keys for Cloud Bank stores....62
Clients....63
Integrating backup applications with StoreOnce Catalyst clients overview....63
Adding StoreOnce Catalyst clients to StoreOnce Systems....64
Adding StoreOnce Catalyst client access for StoreOnce Catalyst stores....64
Deleting StoreOnce Catalyst clients for StoreOnce Systems....64
Editing StoreOnce Catalyst clients for StoreOnce Systems....64
Editing client access for StoreOnce Catalyst stores....65
Editing client public access for StoreOnce Catalyst stores....65
Items....65
Viewing StoreOnce Catalyst items....65
Viewing StoreOnce Catalyst items related-sessions....66
Deleting StoreOnce Catalyst items....66
Backup/restore and copy sessions....66
Viewing StoreOnce Catalyst backup/restore sessions....67
StoreOnce Catalyst stores backup/restore properties....67
Viewing Catalyst copy sessions....69
Catalyst stores copy properties....69
Comparing StoreOnce Catalyst backup/restore sessions....73
Canceling StoreOnce Catalyst copy sessions....74
Comparing StoreOnce Catalyst copy sessions....74
Pausing and resuming outbound copy sessions....74
StoreOnce Catalyst over Fibre Channel....75
Viewing StoreOnce Catalyst Fibre Channel device settings....75
StoreOnce Catalyst Fibre Channel settings and properties....75
StoreOnce Catalyst over Fibre Channel client considerations....77
StoreOnce Catalyst over Fibre Channel zoning considerations....78
Configuring StoreOnce Catalyst over Fibre Channel....79
Editing StoreOnce Catalyst Fibre Channel settings....79
StoreOnce Catalyst Fibre Channel number of devices per login....79
Editing StoreOnce Catalyst Fibre Channel device login settings....80
Editing StoreOnce Catalyst Fibre Channel target device settings....80
StoreOnce Catalyst settings....81
Viewing StoreOnce Catalyst settings....81
Viewing StoreOnce Catalyst Fibre Channel device settings....81
Bandwidth limits (StoreOnce Catalyst)....81
Adding StoreOnce Catalyst clients to StoreOnce Systems....84
Configuring StoreOnce Catalyst proxy server settings....84
Editing StoreOnce Catalyst Fibre Channel settings....84
Editing StoreOnce Catalyst Fibre Channel target device settings....85
Pausing and resuming outbound copy sessions....85

VT library data services....86
VT libraries and multiple Fibre Channel ports....86
VT libraries....86
Viewing VT libraries....86
VT Libraries screens and properties....87

Viewing VT library details....94
Viewing VT libraries interface information....94
VT library interface device properties....95
Creating VT libraries....96
Editing VT libraries....97
Tips for editing VT libraries....97
Deleting VT libraries....98
VT library emulation types....98
VT library tape drives....99
Changing the number of VT library tape drives....100
VT library cartridges....100
Viewing VT libraries cartridge information....100
VT library cartridge properties....100
Viewing VT libraries slot mappings detail....101
Changing the number of VT library cartridge slots....102
Creating VT library cartridges....102
Editing VT library barcodes....102
Tips for editing VT library barcodes....103
Editing VT library cartridges....103
Deleting VT library cartridges....104
Erasing VT library cartridges....104
Moving VT library cartridges....105
Unloading VT library cartridges....105
VT replication....105
VT libraries replication overview....106
Viewing VT replication mappings....106
VT replication screens and properties....107
Viewing VT replication slot mappings....110
Adding replication permissions for target VT libraries....111
Creating replication mappings for source VT libraries....111
Editing replication mappings for source VT libraries....112
Editing replication permissions for target VT libraries....112
Editing replication public access for target VT libraries....112
Editing replication slot mappings for source VT libraries....113
Deleting replication mappings for source VT libraries....113
Making replication target VT libraries visible to hosts....113

NAS data services....115
NAS shares....115
Viewing NAS shares....115
NAS shares screens and properties....115
Viewing NAS shares detail....121
Creating NAS shares....121
Editing NAS shares....121
Tips for editing NAS shares....122
Deleting NAS shares....122
NAS CIFS shares....122
NFS shares....130
Replicating NAS shares....131
Restarting NAS share replication jobs....131
NAS replication....131
NAS shares replication overview....132
Viewing NAS replication mappings....132
NAS replication screens and properties....133
Viewing NAS replication file information....136

Adding replication permissions for target NAS shares....137
Adding replication target systems....137
Creating replication mappings for source NAS shares....137
Editing replication mappings for source NAS shares....138
Editing replication permissions for target NAS shares....138
Editing replication public access for target NAS shares....138
Deleting replication mappings for source NAS shares....139
Recovering replicating NAS shares over a WAN....139
NAS settings....140
Viewing NAS settings....140
Adding and deleting NAS CIFS Active Directory users and groups....140
Adding, editing, and deleting NAS CIFS users....141
Adding, editing, and deleting NAS NFS hosts....141
Editing NAS CIFS settings....141
Editing NAS NFS settings (browsability)....142
Joining and leaving NAS CIFS Active Directories....142

Replication data services....143
Viewing replication settings....143
Bandwidth limits (replication)....143
Viewing replication bandwidth limits....144
Bandwidth limit properties (replication)....144
Editing replication general bandwidth limit settings....145
Editing replication bandwidth limiting windows settings....146
Editing replication maximum concurrent job settings....146
Blackout windows (replication)....147
Viewing replication blackout windows....147
Blackout window properties....147
Editing replication blackout window settings....148
Event history (replication)....148
Viewing replication event history....149
Event history properties....149
Clearing replication events....150
Editing replication out of sync notification....150
Partner systems (replication)....150
Viewing replication partner systems....150
Partner system properties....151
Adding replication target systems....152
Editing and deleting replication target systems....152
Locating replication serial numbers....152
Pausing replication....152
Permissions (replication)....152
Viewing replication event history....153
Adding replication permissions for target systems....153
Removing replication permissions for target systems....153
Resuming replication....154

Reports....155
Reports overview....155
Report content categories....155
Viewing online reports....156

Event log....157

Viewing event logs..... 157
Manually deleting events..... 157
Managing automatic event deletion..... 157

Restart, shutdown, and upgrade..... 158
Restarting and shutting down StoreOnce systems..... 158
Upgrade overview..... 158
Upgrading StoreOnce Systems..... 158

System settings.....160
Viewing the StoreOnce software version..... 160
Viewing warranty serial numbers..... 160
StoreOnce VSA licensing.....160
Obtaining StoreOnce and AutoPass license server licenses..... 162
Viewing StoreOnce licenses.....162
License Management screen and properties..... 163
Adding StoreOnce Standalone licenses.....165
Deleting StoreOnce Standalone licenses.....165
Adding Enterprise licenses.....165
Connecting Enterprise license servers.....166
Disconnecting Enterprise license servers..... 166
Removing Enterprise licenses.....167
Unlicensed mode..... 167
Editing system date and time.....168
Editing system information.....168
Editing user preferences.....168
Capacity units..... 168
Using the StoreOnce First Time Setup wizard.....169
Updating StoreOnce system information..... 169

Hardware settings.....170
Storage..... 170
Viewing storage.....170
Configuring storage.....170
Rescanning storage..... 170
Unconfiguring storage.....170
Editing storage capacity thresholds..... 171
Networking.....171
StoreOnce networking features overview..... 171
Networking concepts.....172
Viewing the active network configuration..... 172
Editing the active network configuration.....173
Activating network configurations.....173
Adding, editing, and deleting port sets.....174
Adding, editing, and deleting subnets..... 175
Adding, editing, deleting static routes..... 177
Adding and deleting encryption links.....178
Editing DNS servers.....179
Pinging systems.....180
Using traceroute.....180
Fibre Channel..... 180
StoreOnce VSA and Fibre Channel support..... 180
Viewing Fibre Channel port settings and properties.....180

Fibre Channel settings and properties 181
Editing Fibre Channel port settings 182

User management settings 183
User roles and types 183
Adding, editing, and deleting users and groups 184
Adding directory servers 184
Removing directory servers 185
Configuring password policies 185

Security settings 186
Certificates 186
Certificate Authority (CA) 186
Viewing security certificates 186
Replacing default certificates - overview 186
Generating certificate signing requests (CSR) 187
Importing security certificates 188
Removing CA security certificates 189
Key Manager 189
Viewing the Key Manager mode 190
Backing up Key Manager configurations 190
Restoring Key Manager configurations 190
Enrolling with an External Key Manager 191
Generating External Key Manager certificate signing requests 192
Renewing External Key Manager certificates 193
Withdrawing from an External Key Manager 194
EKM enrollment common errors 194
Data in Flight encryption guidelines 194
Login Banner 196
Enabling and disabling StoreOnce login banners 196
Sessions 196
Viewing sessions 196
Configuring session timeout policy 196
Initialisation Console credentials 196
Initialisation Console user name and password 196
Changing the Initialisation Console user password 197
Data at Rest encryption guidelines 197

Support settings 199
Remote Support 199
Configuring remote support 199
Viewing the temporary support password mode 200
Sending test events 200
Log Collection 200
Viewing log collections 201
Generating, downloading, and removing log collections 201
Temporary support passwords 201
Viewing the temporary support password mode 202
Changing the temporary support password mode 202
Exporting temporary support password ciphertext 202
Changing temporary support password ciphertext 202

Notification settings....203
Notifications....203
Viewing email alerts....203
Editing SMTP settings....203
Adding SMTP subscriptions....203
Editing and deleting SMTP subscriptions....203
Sending test email....204
SNMP....204
Viewing and configuring SNMP....204
Editing SNMP agent setups....204
Adding SNMP trapsinks....204
Editing and deleting SNMP trapsinks....205
Adding SNMP users....205
Editing and deleting SNMP users....205
Testing SNMP agents....206
Remote Logging Server....206
Adding remote logging servers....206
Editing and deleting remote logging servers....206

Best practices....207
Data services best practices....207
StoreOnce Catalyst best practices....207
StoreOnce Catalyst over Fibre Channel best practices....208
StoreOnce Catalyst via Micro Focus Data Protector best practices....208

Troubleshooting....209
All member systems in a federation are unreachable....209
Backup application connection issues....209
NAS CIFS timeout issues....210
NAS NFS stale handle error....210
Obtaining log collections....211
Password issues....211
Reported capacity shows an unexpected drop....211
Restarting data services....212

StoreOnce websites....213

Support and other resources....214
Accessing Hewlett Packard Enterprise Support....214
Accessing updates....214
Customer self repair....215
Remote support....215
Warranty information....215
Regulatory information....216
Documentation feedback....216

Getting started

What's new in HPE StoreOnce Systems 4.1.1

HPE StoreOnce Systems 4.1.1 includes the following new or enhanced features, compared to 4.1.0.

General

- A new Resources tile is added to the System Dashboard.
- New information added for configuring a directory server and accepting a Trust Certificate.

StoreOnce Federations

Expanded information about removing a StoreOnce system from a Federation.

FAQ

General

Can I upgrade older versions of HPE StoreOnce Systems to software version 4.1?

No. Older StoreOnce Systems cannot be upgraded to version 4.1.

Replication

- **Is StoreOnce Gen4 replication compatible with StoreOnce Gen3 replication?**

  Yes.
- **Is StoreOnce Gen4 replication compatible with StoreOnce Gen2 replication?**

  No.
- **Does StoreOnce Gen4 support creating new replication target devices (NAS share or VT library) from a source StoreOnce System?**

  No. You must first create a new target device on the target StoreOnce System, and then grant permission to source StoreOnce Systems to replicate to the target device. Learn more: **NAS shares replication overview** on page 132 and **VT libraries replication overview** on page 106.

Licensing

- **Is StoreOnce Gen4 licensing different than StoreOnce Gen3 licensing?**

  Yes. For example:

  - StoreOnce Gen4 Catalyst and replication do not require licenses to use
  - StoreOnce Gen4 Secure Erase does not require a license to use
  - StoreOnce VSA supports Enterprise licensing from HPE AutoPass License servers
- **Do StoreOnce Gen4 Systems support HPE StoreOnce all-inclusive licensing?**

  Yes.
- **Are HPE Cloud Bank Storage licensing and Encryption licensing part of all-inclusive licensing?**

No. Cloud Bank storage licenses are capacity-based and must be purchased separately. Encryption licenses may also be purchased to enable data at rest and data in flight encryption.

Logging in to the StoreOnce Management Console

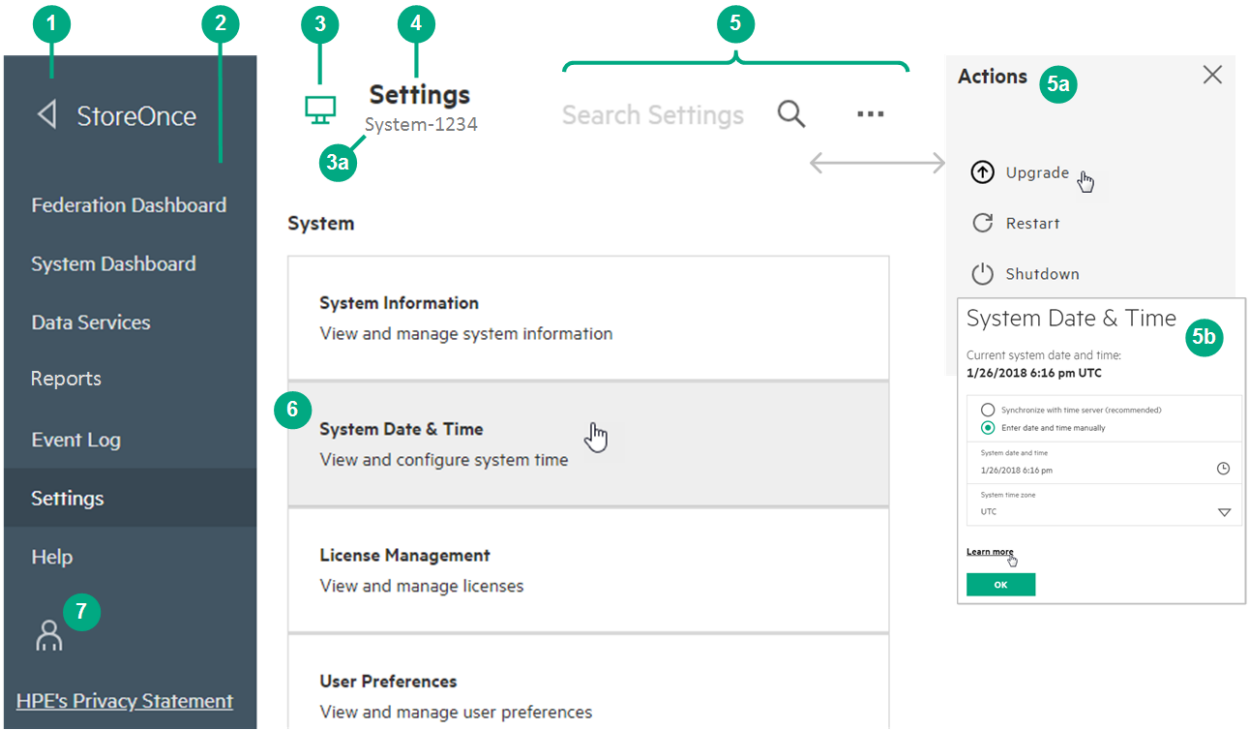
Procedure

1. Browse to the StoreOnce system. You can use the IP Address or Fully Qualified Domain Name, **https://<IP address or FQDN>**. The StoreOnce Management Console **Log In** screen opens.
2. Enter your user name and password and click **Log In**.

- If you log in to a StoreOnce System that is a federation lead, the **Federation Dashboard** is displayed. Learn more: **About federations** on page 17.
- If you log in to a StoreOnce System that is not a federation lead, the **System Dashboard** is displayed.

User interface quick tour

The HPE StoreOnce Management Console user interface includes the following key features:



Main menu icon (1). Clicking the main menu icon exposes and hides the main menu. When the main menu is hidden, more of the viewing area is available for screens, menus, and dialogs.

Main menu (2). The main menu provides quick access to the major areas and features in the user interface. The main menu is exposed by default. If you do not see the main menu, click the main menu icon (1) to expose it.

System selector (3). Clicking the change-system icon ( ) opens the **System Management** screen where you can choose the system whose information is displayed in the screens and dialogs. The name of the selected system (3a) is displayed under the screen names.

TIP: The System Management screen displays multiple systems only when you are logged in to the lead system of a StoreOnce federation. Learn more: **About federations** on page 17.

Screens (4). The screen area displays tabular and graphic information. Many screens include menu icons (▪▪▪). Clicking menu icons opens **Actions** menus on the right side of the screen. Some screens include **Filters** ( ), **Search** ( ), clickable graphics, and Information icons ( ) that link to more detailed information.

Flyout menus and dialogs (5). The right side of screens is the flyouts area. The flyout area is where you can display menus and dialogs that are normally hidden. This quick tour shows that on the Settings screen you can display an **Actions** menu (5a) and the System Date & Time dialog (5b) in the flyout area. Many flyouts include **Learn more** links.

Panels (6). Several screens include clickable panels that provide quick access for viewing information and using action dialogs.

User icon (7). Clicking the user icon shows your login user name and enables you to log out.

Selecting a system to view and manage (federation)

If you are logged in to a StoreOnce federation lead system, you can select any member system to view and manage. The name of the system that is being viewed and managed appears under the screen names. Learn more: **User interface quick tour** on page 11.

TIP: StoreOnce federations are user-specified configurations that allow multiple StoreOnce Systems to be managed from a single system. Learn more: **About federations** on page 17.

Procedure

1. While viewing a screen, click the change-system icon ( ). The **System Management** screen opens.
2. On the **System Management** screen, click the system that you want to view and manage. The screen that you were viewing changes to show that the system you selected is now being managed.

Example

While viewing the Settings screen for System A, you want to view and change the settings for System B.

1. On the **Settings** screen, click the change-system icon ( ). The **System Management** screen opens.
2. On the **System Management** screen, click System B. The **Settings** screen changes to show that you are now viewing and managing System B.

StoreOnce Management Console supported browsers

For the most current compatibility information including browser versions, see the *HPE StoreOnce Support Matrix*.

- Internet Explorer
- Mozilla Firefox
- Google Chrome

Using the StoreOnce First Time Setup wizard

The StoreOnce First Time Setup wizard guides you through the steps to set up a recently installed StoreOnce System.

Procedure

1. Browse to the recently installed StoreOnce System. The First Time Setup wizard is automatically displayed.

   TIP: If a StoreOnce System has already been set up, its First Time Setup wizard is not displayed.

2. The setup steps include:

   - Setting the **Administrator Password**.
   - Setting the **Console Password**.
   - Setting basic **System Information** such as the system name (host name), location, and contact information.
   - Setting the **System Date & Time**. You can set the date and time manually, or synchronize the date and time with a network time server.
   - Configuring **Storage**. The wizard detects the factory installed storage. The wizard also enables you to configure additional storage capacity that you might have installed. The wizard also reports issues with additional storage, for example, when additional storage is not installed in the correct location.
   - Configuring **Remote Support**.

About StoreOnce Systems

StoreOnce VSA

The StoreOnce VSA software provides the flexibility of StoreOnce Systems as virtual systems. StoreOnce VSA software can be Installed into vSphere, Hyper-V, or Microsoft Azure environments. Backup and recovery applications use StoreOnce VSA as a backup target, just like StoreOnce hardware platforms.

For information on hypervisor support with StoreOnce software versions, see the *HPE Data Availability, Protection, and Retention Compatibility Matrix*.

The StoreOnce VSA is available to purchase by license. The base license includes up to 4 TB of usable capacity.

Deploying the VSA

See the *StoreOnce VSA Deployment and Configuration Guide* for more information and instructions on deploying StoreOnce VSA Systems.

Security features

The StoreOnce System offers the security features of Data at Rest Encryption, Data in Flight Encryption, and Secure Erase. Data at Rest and Data in Flight Encryption can be applied using a Security license. Secure Erase is available without a license.

Data at Rest Encryption

When enabled, Data at Rest Encryption protects data at rest on a stolen, discarded, or replaced disk from forensic attack.

If the Security license is already applied, you can enable Data at Rest Encryption when creating a StoreOnce Catalyst store, VT library, and NAS share. Once enabled, encryption is automatically performed on the data before it gets written to disk. Encryption cannot be disabled once it is configured.

IMPORTANT: When encrypting Catalyst stores, NAS shares, or VT libraries, HPE recommends backing up internal and external encryption key stores. For information on backing up external keys, see **Backing up Key Manager configurations** on page 190.

Data in Flight Encryption

Data in Flight Encryption is used to secure network links between data centers for low-bandwidth Catalyst Copy or VT library and NAS replication. StoreOnce does not support Data In Flight Encryption for direct backup to StoreOnce Systems over a local network, due to performance impacts.

When enabled, Data in Flight Encryption protects in-transit data from attack using the IPsec protocol. The data can be moving between two StoreOnce Systems over a WAN. Or, moving between a StoreOnce System and a backup server over a LAN or WAN.

Data in Flight Encryption encrypts the data traffic to all the Catalyst stores using that IP connection. Therefore, it may have an impact on performance.

IMPORTANT:

Data in Flight Encryption is not supported for IPv6 subnets.

Key Managers

The StoreOnce System can use a local or an external key manager to manage keys for Data at Rest and Data in Flight Encryption. The local key manager is used unless the system has been configured to use an external key manager. Two external key manager products are supported: Micro Focus Enterprise Secure Key Manager and Gemalto SafeNet KeySecure. At any time, you can configure the StoreOnce System to use the local or external key manager. You cannot use both key manager types at the same time.

When using the local key manager, the local key store contains the encryption keys used for Data at Rest Encryption or Data in Flight Encryption. HPE recommends backing up the local key store and saving it securely offsite in case the original key store becomes corrupted. Keep only the latest version of the key store.

For example, after the creation or deletion of:

- Catalyst stores, VT libraries, or NAS shares
- Data in Flight Encryption links

When using an external key manager, the local key store contains only the credentials required to authenticate the external key manager. HPE recommends backing up the local key store after a StoreOnce System has been successfully configured to use the external key manager. The external key manager stores and manages all the encryption keys used for Data in Flight Encryption and Data at Rest Encryption.

Secure Erase

You can enable Secure Erase for all store types except Cloud Bank stores. This feature allows secure erasure of data that was backed up as part of a regular backup job. For example, you may have unintentionally backed up confidential data and need make sure that it has been securely erased.

IMPORTANT:

- Secure Erase increases system overhead and reduces performance. HPE recommends enabling Secure Erase immediately prior to expiring a backup from the backup application. And disabling Secure Erase it immediately afterward. Do not leave Secure Erase enabled for long periods of time.
- To remove data immediately, be sure that the backup application is configured correctly. You may need to revise rotation and retention policies to ensure that the data is expired.
- HPE recommends using the backup application to delete data when using Secure Erase.

Secure Erase can only be enabled after the StoreOnce Catalyst store, VT library, or NAS share is created. Enable Secure Erase by editing the store, VT library, or NAS share. Once you enable Secure Erase, all data written to disk will be securely erased upon data deletion.

The Secure Erase overwrites data to be deleted with a sequence of 0, 1 or pseudo random data. The sequence depends on the number of overwrite passes. You can configure Secure Erase to overwrite the data to be deleted with either one, three, five, or seven passes. The amount of time required to complete the Secure Erase increases with the number of overwrite passes.

When Secure Erase is enabled (for Catalyst stores, VT libraries, or NAS shares), data is securely deleted. Work with the backup application to trigger the Secure Erase, for example by forcing the format of a VT library cartridge. The backup application sends the request to delete the data and the deletion is carried out as part of the Housekeeping function. You can trigger Secure Erase manually by deleting:

- A StoreOnce Catalyst object or whole store
- VT library cartridge, or whole VT library
- NAS share.

Only data chunks (processed portions of user data) that are not referenced by any other items can be securely erased. If an item references a data chunk that is not marked for Secure Erase, the referenced data chunk will not be erased.

Federations

About federations

StoreOnce federations allow you to manage multiple StoreOnce systems from a single system. The managing system in a federation is called the federation lead system, and the other systems in the federation are called member systems.

Lead systems. When logged in to a lead system, you can manage not only that system, but you can also manage any of the member systems in the federation. For example, from the lead system you can create StoreOnce Catalyst stores on any member systems in the federation.

The Federation Dashboard screen on a lead system displays aggregated information about the federation. For example, the dashboard shows the total number of StoreOnce Catalyst stores in the federation.

Member systems. When logged in to a member system, you can manage the system as usual. However, you cannot manage other systems in the federation from a member system.

The Federation Dashboard on a member system indicates that the system is part of federation. The dashboard does not display aggregated information about the federation.

General guidelines

- A federation can include up to 20 systems. The maximum includes the member systems and the lead system.
- A federation can have only one lead system.
- A system can be member in more than one federation.
- A system can be a member in one system and also be the lead system in another federation.
- Each member system in a federation must be able to communicate with the lead system. Member systems in a federation do not need to be able to communicate with other member systems.

Networking guidelines

- HPE strongly recommends using static IP addresses, rather than DHCP. If DHCP is used, and IP addresses change, the trust relationships between systems will fail.

  WARNING: If the IP address of the lead system in a federation is changed, access to all member systems in federation will be lost. To re-establish access, each member system must be removed and readded to the federation.

- It is not a requirement that member systems and the lead system in a federation reside on the same network. However, the network route between federation lead and members must be robust.

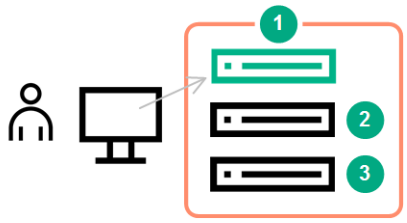
  HPE recommends setting up a federation as a separate network. The network can be a VLAN network, a physical-port network, or mixed.

- To add a StoreOnce system to a federation, you must enter its properly formatted IPv4 or IPv6 address. You cannot use a Fully Qualified Domain Name (FQDN).

Standalone federation example

Scenario

Your organization has three StoreOnce Gen4 Systems: System1, System2, and System3. There is a need to create a federation that includes the three StoreOnce systems. System1 is chosen to be the lead system for managing the federation.



The following are high-level step descriptions. For detail steps, see **Adding systems to federations** on page 21.

1. Browse to System1, the intended lead system, and log in.
2. Add System2

   (To create the federation, you can add any intended member system. In this example System2 is added.)

   a. On the Federation Dashboard for System1, open the Add dialog.

   b. On the Add dialog, enter the system address and administrator credentials for System2.

   c. When System2 is added, the federation is created. System1 is the lead and System2 is a member, reporting to System1.

3. Add System3

   a. On the Federation Dashboard for System1, open the Add dialog.

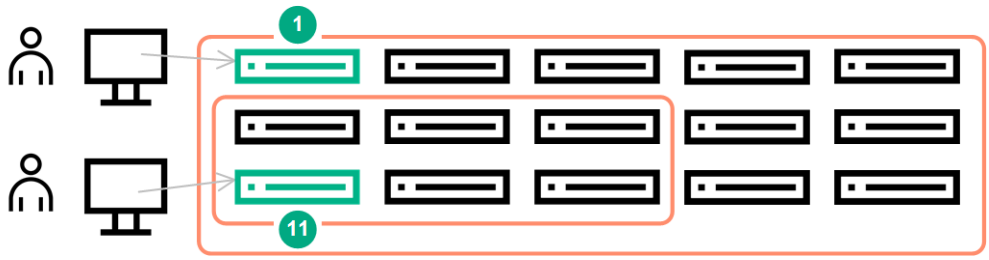
   b. On the Add dialog, enter the system address and administrator credentials for System3.

   c. System3 is added to the federation, reporting to System1.

Overlapping federations example

Scenario

Your organization has 15 StoreOnce Gen4 Systems. There is a need to have two federations for managing systems and viewing aggregated information. One federation will include all 15 StoreOnce Systems. A second federation is an overlapping federation that will include six regional group StoreOnce Systems.



System1 is chosen to be the lead system for the federation of all 15 StoreOnce systems. System11 is chosen to be the lead system for the federation of six regional group StoreOnce Systems.

The two federations can be created in any order. In this example, the federation of all 15 systems is created first. The following are high-level step descriptions for creating the two federations.

Create the federation of all 15 StoreOnce Systems

1. Browse to System1, the intended lead system for the federation of all 15 StoreOnce Systems, and log in.
2. To add the 14 other StoreOnce Systems, repeat the following substeps:
   a. On the Federation Dashboard for System1, open the Add dialog.
   b. On the Add dialog, enter the system address and administrator credentials for the StoreOnce System to be added.

Create the federation of six regional group StoreOnce Systems

1. Browse to System11, the intended lead system for the federation of the six regional group systems, and log in.
2. To add the five other StoreOnce Systems in the regional group, repeat the following substeps:
   a. On the Federation Dashboard for System11, open the Add dialog.
   b. On the Add dialog, enter the system address and administrator credentials for the StoreOnce System to be added.

Viewing federation health

Procedure

1. Browse to a lead system in the federation and log in.
2. On the main menu, select **Federation Dashboard**.

   The federation health is summarized in the **Health Status** panel.
3. On the Federation Dashboard, do one of the following:
   - To view the health of all reachable federation members, click the title **Health Status** above the graphic. The **System** *(All Systems)* screen displays a list of all reachable systems in the federation and their health.
   - To view the health of federation systems that have a specific status, click the status on the graphic or legend. For example, clicking the Warning status on the graphic opens the **System** *(All Systems)* screen and displays the reachable federation systems that have a Warning status.

   There are three status options that are specific to federation members:

- Unreachable: There is an issue with the member system, and it cannot send status updates to the lead. For example, there is a network problem or the system is powered off.
- Address Inconsistent: The IP address that the member uses for the federation connection has changed since it became a federation member. While the member can talk to the lead, the lead cannot talk to the member. HPE recommends removing the member and adding it back with the new, correct IP address.
- Synchronizing: Shown only during lead initialization. The member is reachable but the lead has not yet received system data from it. Once the lead receives the member data, the status will change.

Viewing federation members

Procedure

1. Log in to the lead system in the federation.
2. On the main menu, select **Federation Dashboard**.

   a. To see a list of systems in the federation, click the change-system icon ( ) in the upper left corner of the screen. The **System Management** screen displays the list of systems in the federation.

   b. To see a list of only the member systems, or to add and remove member systems from the federation, click the manage-federation icon ( ) in the upper right corner of the screen. The **Federation Management** screen has tabs for **Members** and **Leads**.

Creating federations

Prerequisites

- HPE strongly recommends using static IP addresses, rather than DHCP. Learn more: **About federations** on page 17.
- HPE recommends that you follow the network guidelines for federations. Learn more: **About federations** on page 17.
- Before you create a federation, determine the StoreOnce System that will be the lead system and the systems that will be members.

Procedure

1. Browse to the system that will be the lead system and log in.
2. On the main menu, select **Federation Dashboard**, and then do one of the following:

   - Click the plus icon (+).
   - Click the federation management edit icon ( ) in the upper right corner of the screen. On the **Federation Management** screen, **Members** tab, expand the **Actions** menu and select **Add**.

3. On the **Add system to federation** dialog, enter the required information for one of the member systems and click **OK**.

   The dialog will close and a federation will be created. At that point, the federation will consist of a lead system and the one member system.

You can continue to use the **Add system to federation** dialog to add systems as members. Or, you can add systems later. Learn more: **Adding systems to federations** on page 21

Adding systems to federations

You can add systems to an existing StoreOnce federation. Learn more: **About federations** on page 17.

HPE strongly recommends using static IP addresses, rather than DHCP. If DHCP is used, and IP addresses change, the trust relationships between systems will fail.

WARNING: If the IP address of the lead system in a federation is changed, access to all member systems in federation will be lost. To re-establish access, each member system must be removed and readded to the federation.

Procedure

1. Browse to the lead system in the federation and log in.
2. On the main menu, select **Federation Dashboard**, and then do one of the following:
   - Click the plus icon (+).
   - Click the federation management edit icon ( ) in the upper right corner of the screen. On the **Federation Management** screen, **Members** tab, expand the **Actions** menu and select **Add**.

   The **Add system to federation** dialog opens.

Removing systems from federations

Prerequisites

IMPORTANT: If you plan to decommission the lead system in a federation, you must remove all the member systems first. You cannot remove the lead system from a federation from a member system.

Procedure

1. Browse to a system in the federation and log in.
2. On the main menu, select **Federation Dashboard**, and then click the manage-federation icon ( ) in the upper right corner of the screen.
3. To remove a **member** system, do the following:
   a. On the **Federation Management** screen, **Members** tab, select the system.
   b. Expand the **Actions** menu and select **Remove**.
   c. On the **Remove** dialog, select the check box to acknowledge that you want to remove the system.
   d. Click **Remove** to complete the action.
4. To remove a **lead** system, do the following:
   a. On the **Federation Management** screen, **Lead** tab, select the system.
   b. Expand the **Actions** menu and select **Remove**.

c. On the **Remove** dialog, select the check box to acknowledge that you want to remove the system.

d. Click **Force Remove** to complete the action.

Selecting a system to view and manage (federation)

If you are logged in to a StoreOnce federation lead system, you can select any member system to view and manage. The name of the system that is being viewed and managed appears under the screen names. Learn more: **User interface quick tour** on page 11.

TIP: StoreOnce federations are user-specified configurations that allow multiple StoreOnce Systems to be managed from a single system. Learn more: **About federations** on page 17.

Procedure

1. While viewing a screen, click the change-system icon ( ). The **System Management** screen opens.
2. On the **System Management** screen, click the system that you want to view and manage. The screen that you were viewing changes to show that the system you selected is now being managed.

Example

While viewing the Settings screen for System A, you want to view and change the settings for System B.

1. On the **Settings** screen, click the change-system icon ( ). The **System Management** screen opens.
2. On the **System Management** screen, click System B. The **Settings** screen changes to show that you are now viewing and managing System B.

Dashboards

Viewing system dashboards

Procedure

1. On the main menu, select **System Dashboard**.

   TIP: If you are logged in to a federation lead system, the most recently viewed system dashboard is displayed. To select a different system dashboard, click the change-system icon ().

2. The **System Dashboard** screen summarizes the system properties on panels for **Health Status**, **System Information**, **Data Services**, **Storage Utilisation**, and **Resources**.

   - You can click the hyperlinked panel titles to display more information. For example, clicking the title Data Services opens the Data Services screen.
   - You can also click some graphic titles and graphic elements to display more information. For example, clicking the Catalyst Stores title above the graphic opens the Catalyst Stores screen and displays all stores. Or, clicking the Warning status on the graphic opens the Catalyst Stores screen and displays only stores that have a Warning status.
   - To update system information, click the edit icon () on the **System Information** panel. Learn more: **Editing system information** on page 24.
   - To customize which tiles are displayed on the dashboard, click the view options icon ().

Viewing federation dashboards

TIP: The Federation Dashboard screen displays the aggregated properties of a federation only when you are logged in to a federation lead system.

Learn more: **About federations** on page 17.

Procedure

1. Log in to the lead system in the federation and log in.
2. On the main menu, select **Federation Dashboard**.
3. The **Federation Dashboard** screen summarizes the properties of the StoreOnce Systems in the federation.

   - You can click the panel titles to display more information. For example, clicking Data Services opens the Data Services screen.
   - You can also click some graphic titles and graphic elements to display more information. For example, clicking the Catalyst Stores title above the graphic opens the Catalyst Stores screen and displays all stores. Or, clicking the Warning status on the graphic opens the Catalyst Stores screen and displays only stores that have a Warning status.

- To customize which tiles are displayed in the dashboard, click the view options icon ().
- To add a system to the federation, click the plus icon (+). The **Add system to federation** dialog opens.

4. To open the **System Management** screen, click the change-system icon () in the upper left corner of the screen. The System Management screen displays a list of systems in the federation and their connection status.

5. To open the **Federation Management** screen, click the manage-federation icon () in the upper right corner of the screen. The Federation Management screen includes tabs for federation **Members** and **Leads**. Each tab shows a list of systems and their connection status. The screen also enables you to add or remove systems from the federation.

Capacity efficiency terms

- **Capacity Savings**: The amount of capacity saved (as a percentage) by deduplicating the data.
- **Deduplication Ratio**: The total amount of data written by the backup application (before deduplication) divided by the actual capacity used after deduplication.
- **Size on Disk**: The amount of disk space used to store all the deduplicated data.
- **User Data Stored**: The amount of data written by the backup application before the data was deduplicated.

Editing system information

You can edit the system name. You can also view and edit optional information such as a contact name, phone number, and email address.

Procedure

1. Do one of the following:

   - On the main menu, select **System Dashboard**, and then click the edit icon () on the **System Information** panel.
   - On the main menu, select **Settings**, and then click the **System Information** panel.

Data services overview

Viewing data services

Procedure

1. On the main menu, select **Data Services**. The **Data Services** screen summarizes the data service categories.

   Learn more:

   - **Viewing StoreOnce Catalyst stores** on page 27
   - **Viewing Cloud Bank stores** on page 43
   - **Viewing VT libraries** on page 86
   - **Viewing NAS shares** on page 115
   - **Viewing VT replication mappings** on page 106
   - **Viewing NAS replication mappings** on page 132

2. You can use the **Settings** menu to view and change data services settings.

   Learn more:

   - **Viewing StoreOnce Catalyst settings** on page 81
   - **Viewing NAS settings** on page 140

StoreOnce Catalyst data services

Licensing requirements

- The security features of Data at Rest Encryption and Data in Flight Encryption require a Security license.
- Cloud Bank Storage is a licensed feature. Licensing is based on capacity in 1 TB increments. Licenses are required for the capacity of data written to the Cloud Bank Storage stores. If you use the Cloud Bank Storage Detach feature, additional licenses are needed for the capacity of the detached Stores.

About StoreOnce Catalyst

StoreOnce Catalyst is a StoreOnce function that allows StoreOnce supported backup applications to:

- Back up data to a target store on the StoreOnce System. Deduplication may occur on the media server, backup/database server, or StoreOnce System to ensure efficient use of the available bandwidth.
- Copy jobs between StoreOnce Systems. Configuration occurs within the StoreOnce supported backup application, making StoreOnce Catalyst an attractive alternative to using the replication function on the StoreOnce System. Copy jobs are initiated from the StoreOnce supported application and have none of the complexities of replication mapping.
- **IMPORTANT:** If StoreOnce Catalyst operations pass through a firewall, the network administrator must open (TCP) ports 9387 (Command protocol) and 9388 (Data protocol). Opening these ports allows the StoreOnce Catalyst traffic to pass to and from the StoreOnce Systems.

StoreOnce supported backup applications

StoreOnce Catalyst is a backup application-integrated solution. For a list of StoreOnce supported backup applications, see the *HPE StoreOnce Support Matrix* **https://www.hpe.com/Storage/StoreOnceSupportMatrix**.

Benefits of StoreOnce Catalyst

- The StoreOnce supported backup application is in full control of data for the full life cycle of the backup data.
- The StoreOnce supported backup application has full visibility of all items and jobs on the StoreOnce System.
- Deduplication can occur on either the media server or StoreOnce System which ensures efficient use of the available bandwidth.
- There is no enforced limit on the number of StoreOnce Catalyst items within a store.
- Copy jobs are initiated from the StoreOnce supported application and have none of the complexities of replication mapping.
- If StoreOnce Catalyst device types are used, space reclamation is more automated and easier to implement from within the StoreOnce supported backup application.

Stores

Viewing StoreOnce Catalyst stores

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, do one of the following:
   - To view all stores, click the title **Catalyst Stores** above the graphic.
   - To view stores that have a specific status, click the status on the graphic. For example, clicking the Warning status on the graphic opens the **Catalyst Stores** screen and displays only stores that have a Warning status.
3. On the **Catalyst Stores** screen, click the StoreOnce Catalyst store.
   The screen for an individual StoreOnce Catalyst store includes tabs for **Overview**, **Details**, **Permissions**, **Items**, **Backup/Restore**, **Outbound Copy**, and **Inbound Copy**.

StoreOnce Catalyst stores screens and properties

Catalyst Stores screen (all stores)

TIP: In the list view, columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).

Property	Description
Store Name	The name of the store on the source StoreOnce system.
Status	The status of the Catalyst store. OK, Warning, Critical.
User Data Stored	The amount of data that you have backed up, reconciled with the logical data recorded on the StoreOnce supported backup application.
Size On Disk	The physical disk space consumed on disk (actual size after deduplication).
Dedupe Ratio	The ratio of duplicate data against new data identified in the data job.
More properties	
Number Of Items	The number of items in the Catalyst store.

Table Continued

Property	Description
Physical Storage Quota	The quota for the amount of data written to disk after deduplication. If the quota is enabled, and the quota limit is reached, backups will fail to prevent the quota from being exceeded. The quota allows you to partition the physical capacity of the StoreOnce System between various users. Applications with a better deduplication ratio can store more data. **TIP:** If you need capacity management, HPE recommends configuring StoreOnce supported backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state. Using quotas and client permissions to control client access to the Catalyst store defines how much space a particular user can use on the StoreOnce System.

Table Continued

Property	Description
Logical Storage Quota	The quota for the amount of data sent to the disk before deduplication. If the quota is enabled and the quota limit is reached, backups will fail to prevent the quota from being exceeded. A quota allows you to provide a service to back up a particular amount of user data. The logical data size of a Catalyst item is updated at every 1 GB of physical data stored or when a Catalyst item is closed. In backups with high deduplication ratios, a logical data size quota can be exceeded before the Catalyst store prevents further backups. The physical data size quota, which updates more frequently, is not affected. For example, if a logical data quota size is set to 1 TB and the backup has a deduplication ratio of 10:1, the logical data size quota can be exceeded by 10 GB. **TIP:** If you need capacity management, HPE recommends configuring backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state. Using quotas and client permissions to control client access to Catalyst stores defines how much space a particular user can use on the StoreOnce System.
Encryption	Indicates whether the Catalyst store data is encrypted. Shows as Not Licensed if there is no encryption license on the StoreOnce System. If encryption is licensed, shows as Enabled or Disabled.
Secure Erase Mode	The availability of HPE Secure Erase. Shows as None or the number of Secure Erase passes.

Catalyst Stores screen (individual store), Overview tab

Property	Description
Status bar	The status of the Catalyst store. Shows as Online, Down, or Error.
Store Dedupe Ratio	The deduplication ratio achieved on the data on the Catalyst store.
User Data Stored	The amount of user data stored on the Catalyst store.
Size on Disk	The actual size used on disk after deduplication.
Items	The number of items in the Catalyst store.

Table Continued

Property	Description
Logical Storage Quota	The quota for the amount of data sent to the disk before deduplication. If the quota is enabled and the quota limit is reached, backups will fail to prevent the quota from being exceeded. A quota allows you to provide a service to back up a particular amount of user data. The logical data size of a Catalyst item is updated at every 1 GB of physical data stored or when a Catalyst item is closed. In backups with high deduplication ratios, a logical data size quota can be exceeded before the Catalyst store prevents further backups. The physical data size quota, which updates more frequently, is not affected. For example, if a logical data quota size is set to 1 TB and the backup has a deduplication ratio of 10:1, the logical data size quota can be exceeded by 10 GB. **TIP:** If you need capacity management, HPE recommends configuring backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state. Using quotas and client permissions to control client access to Catalyst stores defines how much space a particular user can use on the StoreOnce System.
Physical Storage Quota	The quota for the amount of data written to disk after deduplication. If the quota is enabled, and the quota limit is reached, backups will fail to prevent the quota from being exceeded. The quota allows you to partition the physical capacity of the StoreOnce System between various users. Applications with a better deduplication ratio can store more data. **TIP:** If you need capacity management, HPE recommends configuring StoreOnce supported backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state.

Property	Description
	Using quotas and client permissions to control client access to the Catalyst store defines how much space a particular user can use on the StoreOnce System.

Catalyst Stores screen (individual store), Details tab

Property	Description
Store Name	Name of the Catalyst store.
Description	A text description of the share (optional).
System Serial Number	The unique serial number generated automatically by the StoreOnce System.
System Name	Name of the StoreOnce System.
Created	The date and time that the Catalyst store was created.
Number of Catalyst Items	The number of items in the Catalyst store.
Security	
Store Encryption	Indicates whether the Catalyst store data is encrypted. Shows as Not Licensed if there is no encryption license on the StoreOnce System. If encryption is licensed, shows as Enabled or Disabled.
Secure Erase Mode	The availability of HPE Secure Erase. Shows as None or the number of Secure Erase passes.
Data Immutability Retention	The selected Immutable Period, or "No Limit" if the feature is disabled. The Data Immutability feature prevents backup applications from modifying or deleting Catalyst items during the immutable period. The Data Immutability feature prevents the backup application from modifying or deleting StoreOnce Catalyst items during the Immutable Period. However, StoreOnce administrators can still delete the store through the StoreOnce System. When using Data Immutability, it is essential that the backup application administrator is not also a StoreOnce administrator. Data Immutability is often used on a secondary or tertiary StoreOnce System where you can more easily implement administrator separation. The Immutable Period includes a one hour grace period. For the first hour after a backup completes, you can delete a Catalyst item. After the grace period ends, the Immutable Period begins. When you enable the Data Immutability feature, you specify the number of days for the Immutable Period. The default is 30. The Immutable Period begins when the item is tagged as Complete by the backup application.

Table Continued

Property	Description
Client Password Policy	The client password policy can be either SHA-1 or SHA-256. The policy relates to how the client password is transferred between a Catalyst client and a StoreOnce System. Not all Catalyst supported backup applications support SHA-256 mode. For a list of StoreOnce supported backup applications, see the *HPE StoreOnce Support Matrix* **https://www.hpe.com/Storage/StoreOnceSupportMatrix**.
Storage Quotas	
Physical Storage Quota	The quota for the amount of data written to disk after deduplication. If the quota is enabled, and the quota limit is reached, backups will fail to prevent the quota from being exceeded. The quota allows you to partition the physical capacity of the StoreOnce System between various users. Applications with a better deduplication ratio can store more data. **TIP:** If you need capacity management, HPE recommends configuring StoreOnce supported backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state. Using quotas and client permissions to control client access to the Catalyst store defines how much space a particular user can use on the StoreOnce System.

Table Continued

Property	Description
Logical Storage Quota	The quota for the amount of data sent to the disk before deduplication. If the quota is enabled and the quota limit is reached, backups will fail to prevent the quota from being exceeded. A quota allows you to provide a service to back up a particular amount of user data. The logical data size of a Catalyst item is updated at every 1 GB of physical data stored or when a Catalyst item is closed. In backups with high deduplication ratios, a logical data size quota can be exceeded before the Catalyst store prevents further backups. The physical data size quota, which updates more frequently, is not affected. For example, if a logical data quota size is set to 1 TB and the backup has a deduplication ratio of 10:1, the logical data size quota can be exceeded by 10 GB.  **TIP:** If you need capacity management, HPE recommends configuring backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state. Using quotas and client permissions to control client access to Catalyst stores defines how much space a particular user can use on the StoreOnce System.
Transfer Policies	
Primary (Default) Transfer Policy	The default transfer policy for the server. Media servers can be configured individually to use the most efficient transfer policy. As long as the two transfer policies have different values, the media server will determine which is the most bandwidth efficient transfer policy to use. • High: all data is sent from the media server and deduplicated on the StoreOnce System. Also called target-side deduplication. • Low: the media server deduplicates the data and sends only unique data. Also called source-side deduplication.
Secondary Transfer Policy	Generally, the opposite of the primary transfer policy so the media server can determine which policy is most appropriate. However, you can enforce the transfer policy used by the media servers by setting both the primary and secondary transfer policies to the same value.
Session History	

Table Continued

Property	Description
Backup/Restore History	The number of days that the history of the backup/restore jobs is saved.
Copy History	The number of days that the history of the copy jobs is saved.

Catalyst Stores screen (individual store), Permissions tab

Property	Description
Public Access	
Public Access (state of)	Enabled or disabled. If enabled, all clients have unrestricted access to all Catalyst stores. **TIP:** The more secure approach is to disable Public Access and instead assign individual client identifier access.
Client Access	
Client Name	The Catalyst client name that is provided to the StoreOnce supported backup applications when connecting to StoreOnce Catalyst. The client name and password are used to authenticate access to Catalyst stores.
Description	A description of the Catalyst client (optional).
Client Access (state)	Enabled or disabled. If enabled, you assign permissions when configuring clients and stores. HPE recommends enabling client access for increased data security.

Catalyst Stores screen (individual store), Items tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).
- To display all item properties in a **Details** flyout, click the information icon ( ) for the item.

IMPORTANT: Users with the Administrator role can delete individual items. However, HPE recommends that you use the StoreOnce supported backup application remove items. Using the backup application will ensure integrity with the backup application catalog. Deleting items using the StoreOnce Management Console should only be done as a last resort.

Property	Description
Modified	The date and time that the item in the Catalyst store was modified.
Item	The name of the item within the data job. The name is created by the StoreOnce supported backup application. Each data job can have multiple items.
Tag List	A list of tags or marks defined by the backup application that are used to filter items.
Logical Data Size	The amount of data sent to the device before deduplication.
More properties	
Created	The date and time that the item in the Catalyst store was created.

Catalyst Stores screen (individual store), Backup/Restore tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().
- To display the properties in a **Details** flyout, click the information icon ().

Property	Description
Status	Status of the data job item, which may be: • Running: In progress • Completed: The item has completed successfully, this status does not mean the entire data job has completed, only the item, and does not reconcile with the backup application job completion status. • Cancelled: The Status Information provides more details. For example, the data connection has been lost between the StoreOnce System and the media server. (This situation is unlikely to occur). • Unexpected error: The StoreOnce System experienced a problem while processing the item. • Insufficient disk space: It will be necessary to clear some disk space or add storage. • Link failure: IP connectivity has been lost and the backup application must retry the job. • System shutdown: The backup application system has been shut down. **IMPORTANT:** HPE recommends that you use the backup application to clean up incomplete or orphaned items before retrying the job.
Started	Date and time that the data job started.
Item	The name of the item within the data job. This name is created by the backup application. Each data job may have multiple items.
Logical Data Written	The amount of user data that was written. This amount reconciles with information in the backup application log. A backup job can span multiple items.
Logical Data Read	The amount of user data that was read.
More properties	
Status Information	Information which explains the reason for the status that is reported.
Ended	Date and time that the data job ended.
Write Duration	The length of time that data was written.
Read Duration	The length of time that data was read.
Clone Duration	The length of time that data was being cloned.
Backup Application	The StoreOnce supported backup application that created the item.
Client Name	Name that identifies the client application that created the item.
Client Address	The IP address of the server that created the item.

Table Continued

Property	Description
Deduplication Ratio	The deduplication ratio achieved on the data on the Catalyst store.
Logical Data Cloned	The amount of data that was cloned.
Logical Write Throughput	The rate that at which data was actually written. This rate is typically less than the write bandwidth.
Logical Read Throughput	The rate at which data was actually read. This rate is typically less that the read bandwidth rating.
Logical Clone Throughput	The rate at which data was cloned.
Write Bandwidth	The theoretical maximum rate that data could be written, without regard to practical considerations.
Read Bandwidth	The theoretical maximum rate that data could be read, without regard to practical considerations.
Transport Protocol	Indicates whether the copy was performed using Fibre Channel, TCP-IP, or the StoreOnce Internal Network.
Total Data Transferred	The total amount of data transferred in the job.

Catalyst Stores screen (individual store), Outbound Copy tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).
- To display the properties in a **Details** flyout, click the information icon ( ).

Property	Description
Status	The status of the outbound copy job, which may be Queued, Paused, Running, Cancelled, or Completed.
Queued	The date and time the job was put in the queue.
Source Item	The name of the item within the data job. This name is created by the backup application. Each data job may have multiple items.
Source Item Size	The size of the source item.
Percentage Completed	The percentage of the copy job that has been completed.
More properties	

Table Continued

Property	Description
Status Information	Information which explains the reason for the status that is reported.
Backup Application	The StoreOnce supported backup application that created the item.
Started	Date and time that the data job started.
Ended	Date and time that the data job ended.
Duration	The amount of time taken to copy the data.
Estimated Completion	The estimated completion time, if the copy job is still running.
Client Address	The IP address of the server that created the item.
Client Name	The client that initiated the outbound copy job. The client name is defined in the StoreOnce supported backup application.
Source Item Last Modified	The date and time that the source item was last modified. **TIP:** This information is useful if you need to check whether the source item might have been modified during the copy attempt. An error message is also generated if the source item is modified while copying.
Source Item Copy Offset	This value identifies where the data to be copied occurs within the source item.
Source Item Copy Size	This value identifies the size of the data to be copied within the source item.
Target Address	The IP address of the target server. The target is the other StoreOnce System to which the job is being copied from this StoreOnce System. All target details are specified by the backup application when the outbound copy job is created.
Target Store Name	The name of the target Catalyst store on the StoreOnce System to which the data is being copied.
Target Item	The name of the target item on the StoreOnce System to which the dat is being copied. All item names are defined by the StoreOnce supported backup application.
Target Item Copy Offset	This value identifies where the data to be copied occurs within the target item.

Table Continued

Property	Description
Copy Throughput	The rate that at which data was actually copied. This rate is typically less than the theoretical maximum bandwidth.
Transport Protocol	Indicates whether the copy was performed using Fibre Channel, TCP-IP, or the StoreOnce Internal Network.
Data Copied	The amount of data copied. This value matches the source item data size.
Total Bandwidth	The theoretical maximum rate that data could be copied without regard to practical considerations.
Total Bandwidth Saving	The percentage of bandwidth saved. The % bandwidth saving depends on whether the Catalyst store has been configured for source-side deduplication with a low-bandwidth transfer policy, or target-side deduplication with a high-bandwidth transfer policy.
Unsuccessful Retry Attempts	The number of retry attempts that were unsuccessful. **TIP:** If there are multiple unsuccessful attempts, a network link may be down or a blackout window may be scheduled.
Next Copy Attempt Time	The date and time for the next copy attempt.
Copy Marked for Cancellation	Indicates whether the user has cancelled the copy job.

Catalyst Stores screen (individual store), Inbound Copy tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).
- To display the properties in a **Details** flyout, click the information icon ( ).

Property	Description
Status	The status of the outbound copy job, which may be Queued, Paused, Running,Cancelled, or Completed.
Queued	The date and time the job was put in the queue.
Source Item	The name of the item within the data job. This name is created by the backup application. Each data job may have multiple items.

Table Continued

Property	Description
Source Item Size	The size of the source item.
Percentage Completed	The percentage of the copy job that has been completed.
More properties	
Status Information	Information which explains the reason for the status that is reported.
Backup Application	The StoreOnce supported backup application that created the item.
Started	Date and time that the data job started.
Ended	Date and time that the data job ended.
Duration	The amount of time taken to copy the data.
Estimated Completion	The estimated completion time, if the copy job is still running.
Client Address	The IP address of the server that created the item.
Client Name	The client that initiated the inbound copy job. The client name is defined in the StoreOnce supported backup application.
Source Address	The IP address of the source server. The source is the StoreOnce System from which the data is being copied to this StoreOnce System.
Source Store Name	The name of the source Catalyst store on the StoreOnce System from which the data is being copied.
Source Item Last Modified	The date and time that the source item was last modified.  **TIP:** This information is useful if you need to check whether the source item might have been modified during the copy attempt. An error message is also generated if the source item is modified while copying.
Source Item Copy Offset	This value identifies where the data to be copied occurs within the source item.
Source Item Copy Size	This value identifies the size of the data to be copied within the source item.
Target Item	The name of the target item on the StoreOnce System to which the dat is being copied. All item names are defined by the StoreOnce supported backup application.

Table Continued

Property	Description
Target Item Copy Offset	This value identifies where the data to be copied occurs within the target item.
Copy Throughput	The rate that at which data was actually copied. This rate is typically less than the theoretical maximum bandwidth.
Transport Protocol	Indicates whether the copy was performed using Fibre Channel, TCP-IP, or the StoreOnce Internal Network.
Data Copied	The amount of data copied. This value matches the source item data size.
Total Bandwidth	The theoretical maximum rate that data could be copied without regard to practical considerations.
Total Bandwidth Saving	The percentage of bandwidth saved. The % bandwidth saving depends on whether the Catalyst store has been configured for source-side deduplication with a low-bandwidth transfer policy, or target-side deduplication with a high-bandwidth transfer policy.
Copy Marked for Cancellation	Indicates whether the user has cancelled the copy job.

Creating StoreOnce Catalyst stores

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, expand the **Actions** menu and select **Create**.

   The **Create** dialog enables you to specify the following:

   - **Catalyst store name**
   - **Security Settings**
   - **Advanced Settings**

Editing StoreOnce Catalyst stores

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, click the store.
4. On the screen for the Catalyst store, expand the **Actions** menu and select **Edit**.

The **Edit** dialog allows you to specify the following:

- **Security Settings**
- **Advanced Settings**

Deleting StoreOnce Catalyst stores

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, click the store.
4. On the screen for the Catalyst store, expand the **Actions** menu and select **Delete**.

Cloud Bank stores

Viewing Cloud Bank stores

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, do one of the following:
   - To view all Cloud Bank stores, click the title **Cloud Bank Stores** above the graphic.
   - To view Cloud Bank stores for a specific status, click the status on the graphic. For example, clicking the Warning status on the graphic opens the **Cloud Bank Stores** screen and displays only Cloud Bank stores that have a Warning status.
3. On the **Cloud Bank Stores** screen, click the Cloud Bank store.
   The screen for an individual Cloud Bank store includes tabs for **Overview**, **Details**, **Permissions**, **Items**, **Backup/Restore**, **Outbound Copy**, and **Inbound Copy**.

Cloud Bank stores screens and properties

Cloud Bank Stores screen (all stores)

TIP: In the list view, columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).

Property	Description
Store Name	The name of the Cloud Bank store on the source StoreOnce system.
Status	The status of the Cloud Bank store. OK, Warning, Critical.

Table Continued

Property	Description
User Data Stored	The amount of data that you have backed up, reconciled with the logical data recorded on the StoreOnce supported backup application.
Size In Cloud	The size of the Catalyst store on the Cloud Bank service provider. This is the space consumed after deduplication.
Dedupe Ratio	The ratio of duplicate data against new data identified in the Cloud Bank store.
More properties	
Size on Disk	The actual size used on disk after deduplication.
Number Of Items	The number of items in the Catalyst store.
Physical Storage Quota	The quota for the amount of data written to disk after deduplication. If the quota is enabled, and the quota limit is reached, backups will fail to prevent the quota from being exceeded. The quota allows you to partition the physical capacity of the StoreOnce System between various users. Applications with a better deduplication ratio can store more data. **TIP:** If you need capacity management, HPE recommends configuring StoreOnce supported backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state. Using quotas and client permissions to control client access to the Catalyst store defines how much space a particular user can use on the StoreOnce System.

Table Continued

Property	Description
Logical Storage Quota	The quota for the amount of data sent to the disk before deduplication. If the quota is enabled and the quota limit is reached, backups will fail to prevent the quota from being exceeded. A quota allows you to provide a service to back up a particular amount of user data. The logical data size of a Catalyst item is updated at every 1 GB of physical data stored or when a Catalyst item is closed. In backups with high deduplication ratios, a logical data size quota can be exceeded before the Catalyst store prevents further backups. The physical data size quota, which updates more frequently, is not affected. For example, if a logical data quota size is set to 1 TB and the backup has a deduplication ratio of 10:1, the logical data size quota can be exceeded by 10 GB.  **TIP:** If you need capacity management, HPE recommends configuring backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state. Using quotas and client permissions to control client access to Catalyst stores defines how much space a particular user can use on the StoreOnce System.
Encryption	Indicates whether the Catalyst store data is encrypted. Shows as Not Licensed if there is no encryption license on the StoreOnce System. If encryption is licensed, shows as Enabled or Disabled.
Estimated Time	After a **Connect** action is started, this property shows the estimated time until the Cloud Bank store will be reconnected.

Cloud Bank Stores screen (individual store), Overview tab

Property	Description
Status bar	The status of the Catalyst store. Shows as Online, Down, or Error.
Store Dedupe Ratio	The deduplication ratio achieved on the data on the Catalyst store.
User Data Stored	The amount of user data stored on the Catalyst store.

Table Continued

Property	Description
Size in Cloud	The size of the Catalyst store on the Cloud Bank service provider. This is the space consumed after deduplication.
Size on Disk	The size of the Catalyst store on the StoreOnce System. This is the space consumed after deduplication.
Items	The number of items in the Catalyst store.

Table Continued

Property	Description
Logical Storage Quota	The quota for the amount of data sent to the disk before deduplication. If the quota is enabled and the quota limit is reached, backups will fail to prevent the quota from being exceeded. A quota allows you to provide a service to back up a particular amount of user data. The logical data size of a Catalyst item is updated at every 1 GB of physical data stored or when a Catalyst item is closed. In backups with high deduplication ratios, a logical data size quota can be exceeded before the Catalyst store prevents further backups. The physical data size quota, which updates more frequently, is not affected. For example, if a logical data quota size is set to 1 TB and the backup has a deduplication ratio of 10:1, the logical data size quota can be exceeded by 10 GB. **TIP:** If you need capacity management, HPE recommends configuring backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state. Using quotas and client permissions to control client access to Catalyst stores defines how much space a particular user can use on the StoreOnce System.
Physical Storage Quota	The quota for the amount of data written to disk after deduplication. If the quota is enabled, and the quota limit is reached, backups will fail to prevent the quota from being exceeded. The quota allows you to partition the physical capacity of the StoreOnce System between various users. Applications with a better deduplication ratio can store more data. **TIP:** If you need capacity management, HPE recommends configuring StoreOnce supported backup applications that have quotas to reroute to another device or to postpone backups. Rerouting will prevent backups from failing unexpectedly. When a Catalyst store reaches its quota, the status of the store changes to “Online - Critical.” The Catalyst store status will change to “Fault.” Restores from that store are permitted, but new backups will fail. To remedy, increase the quota or expire backups. When the quota is no longer met, the Catalyst store status and the overall Catalyst status will return to the “Running” state. Using quotas and client permissions to control client access to the Catalyst store defines how much space a particular user can use on the StoreOnce System.

Cloud Bank Stores screen (individual store), Details tab

Property	Description
Store Name	Name of the Catalyst store.
Description	A text description of the share (optional).
System Serial Number	The unique serial number generated automatically by the StoreOnce System.
System Name	Name of the StoreOnce System.
Created	The date and time that the Catalyst store was created.
Number of Catalyst Items	The number of items in the Catalyst store.
Security	
Store Encryption	Indicates whether the Catalyst store data is encrypted. Shows as Not Licensed if there is no encryption license on the StoreOnce System. If encryption is licensed, shows as Enabled or Disabled.
Secure Erase Mode	The availability of HPE Secure Erase. Shows as None or the number of Secure Erase passes.
Cloud Bank Storage	
Cloud Service Provider	Name of the Cloud Bank service provider.
Access Key	The access key (user name) of the cloud storage.
Host	The host IP address of the cloud storage.
Proxy	Option which determines whether connection to Azure is routed through an HTTP proxy or not.
SSL	Indicates whether encrypted communication with the Cloud Bank service provider is used.
Self-signed SSL Certificate	Indicates whether a self-signed SSL certificate is used.
Signature Version	Select either v2 or v4 signature authentication with S3 connections. HPE recommends v4.
Bucket Name	The bucket name of the cloud storage.
Transfer Policies	

Table Continued

Property	Description
Primary (Default) Transfer Policy	The default transfer policy for the server. Media servers can be configured individually to use the most efficient transfer policy. As long as the two transfer policies have different values, the media server will determine which is the most bandwidth efficient transfer policy to use. • High: all data is sent from the media server and deduplicated on the StoreOnce System. Also called target-side deduplication. • Low: the media server deduplicates the data and sends only unique data. Also called source-side deduplication.
Secondary Transfer Policy	Generally, the opposite of the primary transfer policy so the media server can determine which policy is most appropriate. However, you can enforce the transfer policy used by the media servers by setting both the primary and secondary transfer policies to the same value.
Session History	
Backup/Restore History	The number of days that the history of the backup/restore job is saved.
Copy History	The number of days that the history of the copy job is saved.

Cloud Bank Stores screen (individual store), Permissions tab

Property	Description
Public Access	
Public Access (state of)	Enabled or disabled. If enabled, all clients have unrestricted access to all Catalyst stores. **TIP:** The more secure approach is to disable Public Access and instead assign individual client identifier access.
Client Access	
Client Name	The Catalyst client name that is provided to the StoreOnce supported backup applications when connecting to StoreOnce Catalyst. The client name and password are used to authenticate access to Catalyst stores.
Description	A description of the Catalyst client (optional).
Client Access (state)	Enabled or disabled. If enabled, you assign permissions when configuring clients and stores. HPE recommends enabling client access for increased data security.

Cloud Bank Stores screen (individual store), Items tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().
- To display the properties in a **Details** flyout, click the information icon ().

IMPORTANT: Users with the Administrator role can delete individual items. However, HPE recommends that you use the StoreOnce supported backup application remove items. Using the backup application will ensure integrity with the backup application catalog. Deleting items using the StoreOnce Management Console should only be done as a last resort.

Property	Description
Modified	The date and time that the item in the Catalyst store was modified.
Item	The name of the item within the data job. The name is created by the StoreOnce supported backup application. Each data job can have multiple items.
Tag List	A list of tags or marks defined by the backup application that are used to filter items.
Logical Data Size	The amount of data sent to the device before deduplication.
More properties	
Created	The date and time that the item in the Catalyst store was created.

Cloud Bank Stores screen (individual store), Backup/Restore tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().
- To display the properties in a **Details** flyout, click the information icon ().

Property	Description
Status	Status of the data job item, which may be: • Running: In progress • Completed: The item has completed successfully, this status does not mean the entire data job has completed, only the item, and does not reconcile with the backup application job completion status. • Cancelled: The Status Information provides more details. For example, the data connection has been lost between the StoreOnce System and the media server. (This situation is unlikely to occur). • Unexpected error: The StoreOnce System experienced a problem while processing the item. • Insufficient disk space: It will be necessary to clear some disk space or add storage. • Link failure: IP connectivity has been lost and the backup application must retry the job. • System shutdown: The backup application system has been shut down. **IMPORTANT:** HPE recommends that you use the backup application to clean up incomplete or orphaned items before retrying the job.
Started	Date and time that the data job started.
Item	The name of the item within the data job. This name is created by the backup application. Each data job may have multiple items.
Logical Data Written	The amount of user data that was written. This amount reconciles with information in the backup application log. A backup job can span multiple items.
Logical Data Read	The amount of user data that was read.
More properties	
Status Information	Information which explains the reason for the status that is reported.
Ended	Date and time that the data job ended.
Write Duration	The length of time that data was written.
Read Duration	The length of time that data was read.
Clone Duration	The length of time that data was being cloned.
Backup Application	The StoreOnce supported backup application that created the item.
Client Name	Name that identifies the client application that created the item.
Client Address	The IP address of the server that created the item.

Table Continued

Property	Description
Deduplication Ratio	The deduplication ratio achieved on the data on the Catalyst store.
Logical Data Cloned	The amount of data that was cloned.
Logical Write Throughput	The rate that at which data was actually written. This rate is typically less than the write bandwidth.
Logical Read Throughput	The rate at which data was actually read. This rate is typically less that the read bandwidth rating.
Logical Clone Throughput	The rate at which data was cloned.
Write Bandwidth	The theoretical maximum rate that data could be written, without regard to practical considerations.
Read Bandwidth	The theoretical maximum rate that data could be read, without regard to practical considerations.
Transport Protocol	Indicates whether the copy was performed using Fibre Channel, TCP-IP, or the StoreOnce Internal Network.
Total Data Transferred	The total amount of data transferred in the job.

Cloud Bank Stores screen (individual store), Outbound Copy tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().
- To display the properties in a **Details** flyout, click the information icon ().

Property	Description
Status	The status of the outbound copy job, which may be Queued, Paused, Running, Cancelled, or Completed.
Queued	The date and time the job was put in the queue.
Source Item	The name of the item within the data job. This name is created by the backup application. Each data job may have multiple items.
Source Item Size	The size of the source item.
Percentage Completed	The percentage of the copy job that has been completed.
More properties	

Table Continued

Property	Description
Status Information	Information which explains the reason for the status that is reported.
Backup Application	The StoreOnce supported backup application that created the item.
Started	Date and time that the data job started.
Ended	Date and time that the data job ended.
Duration	The amount of time taken to copy the data.
Estimated Completion	The estimated completion time, if the copy job is still running.
Client Address	The IP address of the server that created the item.
Client Name	The client that initiated the outbound copy job. The client name is defined in the StoreOnce supported backup application.
Source Item Last Modified	The date and time that the source item was last modified. **TIP:** This information is useful if you need to check whether the source item might have been modified during the copy attempt. An error message is also generated if the source item is modified while copying.
Source Item Copy Offset	This value identifies where the data to be copied occurs within the source item.
Source Item Copy Size	This value identifies the size of the data to be copied within the source item.
Target Address	The IP address of the target server. The target is the other StoreOnce System to which the job is being copied from this StoreOnce System. All target details are specified by the backup application when the outbound copy job is created.
Target Store Name	The name of the target Catalyst store on the StoreOnce System to which the data is being copied.
Target Item	The name of the target item on the StoreOnce System to which the dat is being copied. All item names are defined by the StoreOnce supported backup application.
Target Item Copy Offset	This value identifies where the data to be copied occurs within the target item.

Table Continued

Property	Description
Copy Throughput	The rate that at which data was actually copied. This rate is typically less than the theoretical maximum bandwidth.
Transport Protocol	Indicates whether the copy was performed using Fibre Channel, TCP-IP, or the StoreOnce Internal Network.
Data Copied	The amount of data copied. This value matches the source item data size.
Total Bandwidth	The theoretical maximum rate that data could be copied without regard to practical considerations.
Total Bandwidth Saving	The percentage of bandwidth saved. The % bandwidth saving depends on whether the Catalyst store has been configured for source-side deduplication with a low-bandwidth transfer policy, or target-side deduplication with a high-bandwidth transfer policy.
Unsuccessful Retry Attempts	The number of retry attempts that were unsuccessful. **TIP:** If there are multiple unsuccessful attempts, a network link may be down or a blackout window may be scheduled.
Next Copy Attempt Time	The date and time for the next copy attempt.
Copy Marked for Cancellation	Indicates whether the user has cancelled the copy job.

Cloud Bank Stores screen (individual store), Inbound Copy tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).
- To display the properties in a **Details** flyout, click the information icon ( ).

Property	Description
Status	The status of the outbound copy job, which may be Queued, Paused, Running,Cancelled, or Completed.
Queued	The date and time the job was put in the queue.
Source Item	The name of the item within the data job. This name is created by the backup application. Each data job may have multiple items.

Table Continued

Property	Description
Source Item Size	The size of the source item.
Percentage Completed	The percentage of the copy job that has been completed.
More properties	
Status Information	Information which explains the reason for the status that is reported.
Backup Application	The StoreOnce supported backup application that created the item.
Started	Date and time that the data job started.
Ended	Date and time that the data job ended.
Duration	The amount of time taken to copy the data.
Estimated Completion	The estimated completion time, if the copy job is still running.
Client Address	The IP address of the server that created the item.
Client Name	The client that initiated the inbound copy job. The client name is defined in the StoreOnce supported backup application.
Source Address	The IP address of the source server. The source is the StoreOnce System from which the data is being copied to this StoreOnce System.
Source Store Name	The name of the source Catalyst store on the StoreOnce System from which the data is being copied.
Source Item Last Modified	The date and time that the source item was last modified.  **TIP:** This information is useful if you need to check whether the source item might have been modified during the copy attempt. An error message is also generated if the source item is modified while copying.
Source Item Copy Offset	This value identifies where the data to be copied occurs within the source item.
Source Item Copy Size	This value identifies the size of the data to be copied within the source item.
Target Item	The name of the target item on the StoreOnce System to which the dat is being copied. All item names are defined by the StoreOnce supported backup application.

Table Continued

Property	Description
Target Item Copy Offset	This value identifies where the data to be copied occurs within the target item.
Copy Throughput	The rate that at which data was actually copied. This rate is typically less than the theoretical maximum bandwidth.
Transport Protocol	Indicates whether the copy was performed using Fibre Channel, TCP-IP, or the StoreOnce Internal Network.
Data Copied	The amount of data copied. This value matches the source item data size.
Total Bandwidth	The theoretical maximum rate that data could be copied without regard to practical considerations.
Total Bandwidth Saving	The percentage of bandwidth saved. The % bandwidth saving depends on whether the Catalyst store has been configured for source-side deduplication with a low-bandwidth transfer policy, or target-side deduplication with a high-bandwidth transfer policy.
Copy Marked for Cancellation	Indicates whether the user has cancelled the copy job.

Cloud Bank stores service providers and properties

StoreOnce Cloud Bank store supported cloud service providers are **Azure**, **AWS** (Amazon Web Services), **Scality**, and **S3 Compatible**.

The following information is required to use StoreOnce Cloud Bank store actions with the supported cloud service providers.

Azure Cloud Services

Property	Description
Storage Account Name	The storage account name can be found on the Azure account portal.
Access Key	The access key is used to authenticate the storage account name. The key can be found on the Azure account portal.
Container Name	Name of the container on Azure that contains the Cloud Bank store objects.
Proxy	Option which determines whether connection to the service provider is routed through an HTTP proxy or not.

AWS (Amazon Web Services)

Property	Description
Access Key	The access key can be found on the AWS account portal.
Secret Key	The secret key is used to authenticate the access key. It can be found on the AWS account portal.
Bucket Name	Name of the bucket on AWS that contains the Cloud Bank store objects.
Proxy	Option which determines whether connection to Azure is routed through an HTTP proxy or not.

Scality and S3 Compatible

Property	Description
Host	Host address of the service provider. For example, *s3server.domain.net*.
Port	The host port for the service provider. Typically 443.
SSL	Option that specifies whether communication with the service provider is encrypted or not. HPE recommends enabling SSL.
Signature Version	Method of authentication to use. HPE recommends v4 for most situations. In some cases, it may be necessary to use v2 for compatibility.
Access Key	Similar to a user name. It can be found on the service provider account portal.
Secret Key	Similar to a password. It is used to authenticate the access key. It can be found on the service provider account portal.
Bucket Name	Name of the bucket on the service provider that contains the Cloud Bank store objects.
Proxy	Option which determines whether connection to the service provider is routed through an HTTP proxy or not.

Tips for working with Cloud Bank stores

Creating Cloud Bank stores

StoreOnce Secure Erase Mode is not supported on Cloud Bank stores.

When you create a Cloud Bank store with the **Create Store** dialog, the StoreOnce System verifies that:

- The StoreOnce System can connect to your selected cloud service provider.
- The cloud service provider account and credentials information that you provide are valid.

- The bucket or container that you want to use exists.
- The SSL certificate can be authenticated.

Connecting Read/Write to Cloud Bank stores

- **IMPORTANT:**
  - Connecting read/write can only be done 24 hours after disconnecting or detaching the Cloud Bank store.
  - It is only possible to connect a Cloud Bank store to a StoreOnce System which is running a StoreOnce version equal or newer than the StoreOnce version used to last write to the Cloud Bank store.

- You must have sufficient Cloud Bank storage read/write capacity licensed on the StoreOnce System.
- Only one StoreOnce System at a time can connect read/write to a particular Cloud Bank store.
- When connected read/write, changes in a Cloud Bank store (such as new, changed, or deleted items) can take time to become consistent in the cloud.

Connecting Read-Only to Cloud Bank stores

- **IMPORTANT:**
  - When connected read-only to a Cloud Bank store that is connected read/write to another StoreOnce System, be sure that enough time has passed before attempting to use new backups.
  - It is only possible to connect a Cloud Bank store to a StoreOnce System which is running a StoreOnce version equal or newer than the StoreOnce version used to last write to the Cloud Bank store.

- Connecting read-only allows a Cloud Bank store to be read by multiple StoreOnce Systems. After connection, the Cloud Bank store remains read-only on the StoreOnce system. If the Cloud Bank store is connected read/write to another StoreOnce System, the read-only connection will refresh from the cloud periodically.
- To connect read-only, the Cloud Bank store must have been detached by a StoreOnce System, or connected read/write, within the past 60 days.

Disconnecting Cloud Bank stores

- Disconnecting a Cloud Bank store removes the store from a StoreOnce System and leaves the data in the cloud in a read/write state. This state allows a Cloud Bank store to be migrated between StoreOnce Systems or used to test cloud connection functionality.

- **WARNING:** If a Cloud Bank store is encrypted, be sure that you have exported and saved the encryption key before disconnecting. The encryption key is required to connect to another StoreOnce System.

- To disconnect, the StoreOnce System must be connected read/write to the Cloud Bank store.

- **WARNING:** If you do not reconnect a StoreOnce System read/write to the Cloud Bank store within 60 days, the Cloud Bank store cannot be connected to any StoreOnce System. Thus, the data can no longer be recovered.

- After disconnecting, for the first 24 hours, you can only connect a StoreOnce System read-only to the Cloud Bank store.

Editing Cloud Bank stores

If modifying cloud service provider settings for a Cloud Bank store, the StoreOnce system will verify the connectivity and credentials. If any of the connectivity tests fail, the Cloud Bank store is not changed.

Detaching Cloud Bank stores

- Detaching removes a Cloud Bank store from a StoreOnce System and leaves detached Cloud Bank store in a read-only state.

- **WARNING:** If a Cloud Bank store is encrypted, be sure that you have exported and saved the encryption key before detaching. The encryption key is required to connect to another StoreOnce System.

- Detaching is only possible if there is enough Detach Capacity licensed on the StoreOnce System.

- **IMPORTANT:** Once detached, connect read/write is no longer possible. No further data can be written to this store from a StoreOnce System. However, the bucket or container permissions in the cloud service provider remain unchanged.

- Detaching requires a StoreOnce Cloud Bank Storage Detach license. Once detach is complete, the StoreOnce Cloud Bank Storage Detach license is reduced by the store size in the cloud. The equivalent value of detach capacity that is used is released from the Cloud Bank storage read/write capacity. The newly available read/write capacity is available for new or existing Cloud Bank stores.

Deleting Cloud Bank stores

If the Cloud Bank store is connected read/write:

- **WARNING:** The data in the cloud service provider storage is marked as deleted. The data can no longer be recovered to any StoreOnce System.

- The Cloud Bank store is removed from the StoreOnce System, but the bucket or container in the cloud service provider remains. You can delete the bucket or container using the management interface of the cloud service provider.

If the Cloud Bank store is connected read-only:

- Any other StoreOnce Systems connected to this Cloud Bank store will continue to operate.
- If you want to delete the Cloud Bank store from the cloud, HPE recommends first removing the Cloud Bank store from all connected StoreOnce Systems. Then deleting the bucket or container using the management interface of the cloud service provider.

Configuring firewalls for Cloud Bank

Cloud Bank connections require connectivity between the StoreOnce and the Cloud Service Provider. In some cases users might need to alter their firewall configurations to allow traffic to flow through their firewall to the end points. If using an S3 Compatible service provider, or Scality, this might be the Host address specified when configuring the Cloud Bank store, for instance. For AWS and Azure service providers, they use a range of addresses depending on the regions used. Further details of the IP address ranges for AWS can be found here: **AWS IP address ranges**. Further details of the Azure Datacenter IP ranges can be found here: **Azure Datacenter IP address ranges**. Depending on the configuration, it is also likely that ports 80 or 443 would need to be configured on the firewall.

S3 Compatible Cloud Bank stores

For a list of supported S3 Compatible service providers see the StoreOnce Support Matrix. See **StoreOnce websites** for the link to this resource.

When using self-signed SSL certificates for S3 Compatible service provider Dell EMC ECS, the SSL certificate provided must be in the StoreOnce Cloud Bank required format. Cloud Bank expects a Common Name field in the Subject field of an SSL certificate to be present and match the DNS. The default certificate which ships with ECS is incompatible with Cloud Bank. For details of working with ECS certificates refer to the “Certificates” chapter of the **ECS Administration Guide**.

Creating Cloud Bank stores

Only users with the Administrator role can create and manage Cloud Bank stores. See also **Tips for working with Cloud Bank stores** on page 57. For service provider information, see **Cloud Bank stores service providers and properties** on page 56.

Prerequisites

You need the following to create a Cloud Bank store:

- A connection that allows the StoreOnce System to contact the cloud service provider.
- Account name and credentials to access the cloud service provider.
- Name of the bucket or container on the cloud to connect to the Catalyst store.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Cloud Bank Stores** above the graphic.
3. On the **Cloud Bank Stores** screen, expand the **Actions** menu and select **Create**.

   The **Create** dialog enables you to specify the following:

   - **Service Provider Settings**
   - **Security Settings**
   - **Advanced Settings**

Connecting Cloud Bank stores

Only users with the Administrator role can create and manage Cloud Bank stores. See also **Tips for working with Cloud Bank stores** on page 57.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Cloud Bank Stores** above the graphic.
3. On the **Cloud Bank Stores** screen, click the Cloud Bank store.
4. On the screen for the Cloud Bank store, expand the **Actions** menu and select **Connect**.
5. On the **Connect** dialog, provide the required information for the cloud service provider and click **Connect**.

   If the cloud service provider is configured with a self-signed SSL certificate, details about the connection are displayed. To continue, confirm the trust for the service provider. Or, cancel the connection.

6. After the connecting:
   - Details of the Cloud Bank store are displayed. The store name, description, number of items, last access date, and other details are displayed.

     IMPORTANT: Before proceeding, review the details to verify that the Cloud Bank store is the correct store to attach to the StoreOnce System.

   - If the Cloud Bank Store is encrypted, and the StoreOnce System does not have the encryption key, an encryption key request is displayed. To continue, the encryption key file must be uploaded.
7. If the Cloud Bank store is not the correct store, cancel the connect action. Otherwise, select **Connect Read Only** or **Connect Read Write**.

Deleting Cloud Bank stores

Only users with the Administrator role can create and manage Cloud Bank stores. See also **Tips for working with Cloud Bank stores** on page 57.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Cloud Bank Stores** above the graphic.
3. On the **Cloud Bank Stores** screen, click the Cloud Bank store.
4. On the screen for the Cloud Bank store, expand the **Actions** menu and select **Delete**.

Detaching Cloud Bank stores

Only users with the Administrator role can create and manage Cloud Bank stores. See also **Tips for working with Cloud Bank stores** on page 57.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Cloud Bank Stores** above the graphic.

3. On the **Cloud Bank Stores** screen, click the Cloud Bank store.
4. On the screen for the Cloud Bank store, expand the **Actions** menu and select **Detach**.

Disconnecting Cloud Bank stores

Only users with the Administrator role can create and manage Cloud Bank stores. See also **Tips for working with Cloud Bank stores** on page 57.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Cloud Bank Stores** above the graphic.
3. On the **Cloud Bank Stores** screen, click the Cloud Bank store.
4. On the screen for the Cloud Bank store, expand the **Actions** menu and select **Disconnect**.

Editing Cloud Bank stores

Only users with the Administrator role can create and manage Cloud Bank stores. See also **Tips for working with Cloud Bank stores** on page 57.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Cloud Bank Stores** above the graphic.
3. On the **Cloud Bank Stores** screen, click the Cloud Bank store.
4. On the screen for the Cloud Bank store, expand the **Actions** menu and select **Edit**.

   The **Edit** dialog enables you to specify the following:

   - **Service Provider Settings**
   - **Security Settings**
   - **Advanced Settings**

Exporting encryption keys for Cloud Bank stores

IMPORTANT: To allow an encrypted Cloud Bank store to be accessed by a different StoreOnce System, its encryption key is required. HPE recommends that you export the encryption key and securely store it.

The encryption key password must comply with the following criteria:

- A minimum of 15 characters, and a maximum of 32 characters.
- A minimum of 1 uppercase character, and 1 lowercase character.
- A minimum of 1 numeric character, and 1 special character.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Cloud Bank Stores** above the graphic.
3. On the **Cloud Bank Stores** screen, click the Cloud Bank store.
4. On the screen for the Cloud Bank store, expand the **Actions** menu and select **Export Key**.
5. Enter a password for encrypting the exported key.

Clients

Integrating backup applications with StoreOnce Catalyst clients overview

Many backup applications include features that integrate with StoreOnce Catalyst. The integration allows users of supported backup applications to perform StoreOnce Catalyst backup/restore and copy operations from the backup application user interface. StoreOnce Catalyst clients are key components of the integration. StoreOnce Catalyst clients are permissions-centric clients on StoreOnce Systems that allow you to control the access that backup applications have with StoreOnce Catalyst stores.

This overview outlines how to create StoreOnce Catalyst clients, and how to use the clients to control backup application access to StoreOnce Catalyst stores.

Prerequisites

This overview assumes that the StoreOnce Catalyst stores that will be used with backup applications exist. If you have not created the stores, see **Creating StoreOnce Catalyst stores** on page 42.

Procedure

Create StoreOnce Catalyst clients for use with backup applications

1. Create named StoreOnce Catalyst clients for controlling backup application access to StoreOnce Catalyst stores. Lean more: **Adding StoreOnce Catalyst clients to StoreOnce Systems** on page 64.

   For example, you might create StoreOnce Catalyst clients on a StoreOnce System that have the names *west division* and *east division*. Your backup applications could then be configured to associate their backup/restore and copy actions with those StoreOnce Catalyst clients.

Add the StoreOnce Catalyst clients to individual StoreOnce Catalyst stores

2. Add the named StoreOnce Catalyst clients to specific StoreOnce Catalyst stores. Adding named StoreOnce Catalyst clients to individual StoreOnce Catalyst stores enables you to control the backup applications that have permission to interact with the StoreOnce Catalyst stores. Learn more: **Adding StoreOnce Catalyst client access for StoreOnce Catalyst stores** on page 64.

   For example, you might add the StoreOnce Catalyst client *west division* to several StoreOnce Catalyst stores, and add the StoreOnce Catalyst client *east division* to other StoreOnce Catalyst stores.

   Alternately, if you want less specific control, you can allow **Public Access** for a StoreOnce Catalyst store. Public Access allows any named StoreOnce Catalyst client to access the StoreOnce Catalyst store. Learn more: **Editing client public access for StoreOnce Catalyst stores** on page 65.

Configure your backup applications

3. After you have created StoreOnce Catalyst clients and added them to StoreOnce Catalyst stores, you can configure supported backup applications to interact with the stores.

TIP: To configure supported backup applications, you will need the IP address of the StoreOnce System, and the names and passwords for the StoreOnce Catalyst clients.

Adding StoreOnce Catalyst clients to StoreOnce Systems

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Permissions** tab.
3. Expand the **Actions** menu and select **Add**.

Adding StoreOnce Catalyst client access for StoreOnce Catalyst stores

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, select the StoreOnce Catalyst store.
4. On the screen for the StoreOnce Catalyst store, click the **Permissions** tab.
5. On the **Client Access** panel, expand the **Actions** menu and select **Add**.

Deleting StoreOnce Catalyst clients for StoreOnce Systems

WARNING: If you delete a StoreOnce Catalyst client for a StoreOnce System, data protection software that uses the client will no longer have access to StoreOnce Catalyst stores on the system.

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Permissions** tab.
3. Click the StoreOnce Catalyst client, and then expand the **Actions** menu and select **Remove**.

Editing StoreOnce Catalyst clients for StoreOnce Systems

You can edit StoreOnce Catalyst client descriptions and passwords. You cannot change the names of StoreOnce Catalyst clients.

Procedure

1. Navigate to the **Catalyst Settings** screen.

If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.

2. On the **Catalyst Settings** screen, click the **Permissions** tab.
3. Click the StoreOnce Catalyst client, and then expand the **Actions** menu and select **Edit**.

Editing client access for StoreOnce Catalyst stores

StoreOnce Catalyst client access to a StoreOnce Catalyst store is enabled when the client is added to the store. You can later disable and enable access by editing the client permissions for the store.

TIP: If **Public Access** to a StoreOnce Catalyst store is enabled, then individual StoreOnce Catalyst client access cannot be edited.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, select the StoreOnce Catalyst store.
4. On the screen for the StoreOnce Catalyst store, click the **Permissions** tab.
5. Click the StoreOnce Catalyst client, and then expand the **Actions** menu and select **Edit**.

Editing client public access for StoreOnce Catalyst stores

When **Public Access** to a StoreOnce Catalyst store is enabled, any named StoreOnce Catalyst client on the StoreOnce system can be used by a supported backup application to access the store.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, select the StoreOnce Catalyst store.
4. On the screen for the StoreOnce Catalyst store, click the **Permissions** tab.
5. On the **Public Access** panel, click the edit icon ( ).

Items

Viewing StoreOnce Catalyst items

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, select the StoreOnce Catalyst store.

4. On the screen for the StoreOnce Catalyst store, click the **Items** tab. A list of items in the store is shown.
5. To view details of an item, click its information icon ().

Viewing StoreOnce Catalyst items related-sessions

You can view the sessions that are related to an item in a StoreOnce Catalyst store.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, click the StoreOnce Catalyst store.
4. On the screen for the StoreOnce Catalyst store, click the **Items** tab.
5. Select the item and then expand the **Actions** menu and select **Show Backup/Restore Sessions**, **Show Outbound Copy Sessions**, or **Show Inbound Copy Sessions**.

Deleting StoreOnce Catalyst items

WARNING: Deleting items from the StoreOnce Catalyst store will permanently delete the data. HPE recommends using the backup application to delete items. Using the backup application will ensure that the backup application catalog is updated.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, select the StoreOnce Catalyst store, and then click the **Items** tab.
4. Select the item, and then expand the **Actions** menu and select **Delete** .

Backup/restore and copy sessions

About Job types

Different backup applications can use different terminology for data transfers.

From a StoreOnce Catalyst perspective, if data is being moved between the StoreOnce System and a media server or application server, it is a *data job*. If the transfer is between two StoreOnce Systems, it is a StoreOnce Catalyst *copy* job.

Data jobs

For data jobs, the backup application is responsible for the data movement.

If the number of data jobs starts getting high, the StoreOnce System can be loaded heavily. You can see jobs failing to start, or running slowly (although the aggregate performance across the many jobs will still be high) due to insufficient resources being available.

Copy jobs

For copy jobs, the StoreOnce System is responsible for all data movement (although the process is initiated by the backup application software).

If the number of copy jobs gets high (close to the maximum concurrent jobs), copies will not fail. Copy activities happen under the control of the StoreOnce System and it will optimize the queuing and running of jobs based on the resources available.

TIP: The **Maximum Concurent Jobs** value is not guaranteed in all cases.

Viewing StoreOnce Catalyst backup/restore sessions

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, select the StoreOnce Catalyst store, and then click the **Backup/ Restore** tab.
4. To view the details for a backup/restore session, click its information icon ( ).

StoreOnce Catalyst stores backup/restore properties

Catalyst Stores screen (individual store), Backup/Restore tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).
- To display the properties in a **Details** flyout, click the information icon ( ).

Property	Description
Status	Status of the data job item, which may be: • Running: In progress • Completed: The item has completed successfully, this status does not mean the entire data job has completed, only the item, and does not reconcile with the backup application job completion status. • Cancelled: The Status Information provides more details. For example, the data connection has been lost between the StoreOnce System and the media server. (This situation is unlikely to occur). • Unexpected error: The StoreOnce System experienced a problem while processing the item. • Insufficient disk space: It will be necessary to clear some disk space or add storage. • Link failure: IP connectivity has been lost and the backup application must retry the job. • System shutdown: The backup application system has been shut down. **IMPORTANT:** HPE recommends that you use the backup application to clean up incomplete or orphaned items before retrying the job.
Started	Date and time that the data job started.
Item	The name of the item within the data job. This name is created by the backup application. Each data job may have multiple items.
Logical Data Written	The amount of user data that was written. This amount reconciles with information in the backup application log. A backup job can span multiple items.
Logical Data Read	The amount of user data that was read.
More properties	
Status Information	Information which explains the reason for the status that is reported.
Ended	Date and time that the data job ended.
Write Duration	The length of time that data was written.
Read Duration	The length of time that data was read.
Clone Duration	The length of time that data was being cloned.
Backup Application	The StoreOnce supported backup application that created the item.
Client Name	Name that identifies the client application that created the item.
Client Address	The IP address of the server that created the item.

Table Continued

Property	Description
Deduplication Ratio	The deduplication ratio achieved on the data on the Catalyst store.
Logical Data Cloned	The amount of data that was cloned.
Logical Write Throughput	The rate that at which data was actually written. This rate is typically less than the write bandwidth.
Logical Read Throughput	The rate at which data was actually read. This rate is typically less that the read bandwidth rating.
Logical Clone Throughput	The rate at which data was cloned.
Write Bandwidth	The theoretical maximum rate that data could be written, without regard to practical considerations.
Read Bandwidth	The theoretical maximum rate that data could be read, without regard to practical considerations.
Transport Protocol	Indicates whether the copy was performed using Fibre Channel, TCP-IP, or the StoreOnce Internal Network.
Total Data Transferred	The total amount of data transferred in the job.

Viewing Catalyst copy sessions

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, select the Catalyst store, and then click the **Outbound Copy**, or **Inbound Copy** tab.

   Each tab shows the appropriate list of copy sessions.
4. To view the details for a copy session, click its information icon ( ).

Catalyst stores copy properties

Catalyst Stores screen (individual store), Outbound Copy tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).
- To display the properties in a **Details** flyout, click the information icon ( ).

Property	Description
Status	The status of the outbound copy job, which may be Queued, Paused, Running, Cancelled, or Completed.
Queued	The date and time the job was put in the queue.
Source Item	The name of the item within the data job. This name is created by the backup application. Each data job may have multiple items.
Source Item Size	The size of the source item.
Percentage Completed	The percentage of the copy job that has been completed.
More properties	
Status Information	Information which explains the reason for the status that is reported.
Backup Application	The StoreOnce supported backup application that created the item.
Started	Date and time that the data job started.
Ended	Date and time that the data job ended.
Duration	The amount of time taken to copy the data.
Estimated Completion	The estimated completion time, if the copy job is still running.
Client Address	The IP address of the server that created the item.
Client Name	The client that initiated the outbound copy job. The client name is defined in the StoreOnce supported backup application.
Source Item Last Modified	The date and time that the source item was last modified.  **TIP:** This information is useful if you need to check whether the source item might have been modified during the copy attempt. An error message is also generated if the source item is modified while copying.
Source Item Copy Offset	This value identifies where the data to be copied occurs within the source item.
Source Item Copy Size	This value identifies the size of the data to be copied within the source item.

Table Continued

Property	Description
Target Address	The IP address of the target server. The target is the other StoreOnce System to which the job is being copied from this StoreOnce System. All target details are specified by the backup application when the outbound copy job is created.
Target Store Name	The name of the target Catalyst store on the StoreOnce System to which the data is being copied.
Target Item	The name of the target item on the StoreOnce System to which the dat is being copied. All item names are defined by the StoreOnce supported backup application.
Target Item Copy Offset	This value identifies where the data to be copied occurs within the target item.
Copy Throughput	The rate that at which data was actually copied. This rate is typically less than the theoretical maximum bandwidth.
Transport Protocol	Indicates whether the copy was performed using Fibre Channel, TCP-IP, or the StoreOnce Internal Network.
Data Copied	The amount of data copied. This value matches the source item data size.
Total Bandwidth	The theoretical maximum rate that data could be copied without regard to practical considerations.
Total Bandwidth Saving	The percentage of bandwidth saved. The % bandwidth saving depends on whether the Catalyst store has been configured for source-side deduplication with a low-bandwidth transfer policy, or target-side deduplication with a high-bandwidth transfer policy.
Unsuccessful Retry Attempts	The number of retry attempts that were unsuccessful. **TIP:** If there are multiple unsuccessful attempts, a network link may be down or a blackout window may be scheduled.
Next Copy Attempt Time	The date and time for the next copy attempt.
Copy Marked for Cancellation	Indicates whether the user has cancelled the copy job.

Catalyst Stores screen (individual store), Inbound Copy tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().
- To display the properties in a **Details** flyout, click the information icon ().

Property	Description
Status	The status of the outbound copy job, which may be Queued, Paused, Running,Cancelled, or Completed.
Queued	The date and time the job was put in the queue.
Source Item	The name of the item within the data job. This name is created by the backup application. Each data job may have multiple items.
Source Item Size	The size of the source item.
Percentage Completed	The percentage of the copy job that has been completed.
More properties	
Status Information	Information which explains the reason for the status that is reported.
Backup Application	The StoreOnce supported backup application that created the item.
Started	Date and time that the data job started.
Ended	Date and time that the data job ended.
Duration	The amount of time taken to copy the data.
Estimated Completion	The estimated completion time, if the copy job is still running.
Client Address	The IP address of the server that created the item.
Client Name	The client that initiated the inbound copy job. The client name is defined in the StoreOnce supported backup application.
Source Address	The IP address of the source server. The source is the StoreOnce System from which the data is being copied to this StoreOnce System.
Source Store Name	The name of the source Catalyst store on the StoreOnce System from which the data is being copied.

Table Continued

Property	Description
Source Item Last Modified	The date and time that the source item was last modified. **TIP:** This information is useful if you need to check whether the source item might have been modified during the copy attempt. An error message is also generated if the source item is modified while copying.
Source Item Copy Offset	This value identifies where the data to be copied occurs within the source item.
Source Item Copy Size	This value identifies the size of the data to be copied within the source item.
Target Item	The name of the target item on the StoreOnce System to which the dat is being copied. All item names are defined by the StoreOnce supported backup application.
Target Item Copy Offset	This value identifies where the data to be copied occurs within the target item.
Copy Throughput	The rate that at which data was actually copied. This rate is typically less than the theoretical maximum bandwidth.
Transport Protocol	Indicates whether the copy was performed using Fibre Channel, TCP-IP, or the StoreOnce Internal Network.
Data Copied	The amount of data copied. This value matches the source item data size.
Total Bandwidth	The theoretical maximum rate that data could be copied without regard to practical considerations.
Total Bandwidth Saving	The percentage of bandwidth saved. The % bandwidth saving depends on whether the Catalyst store has been configured for source-side deduplication with a low-bandwidth transfer policy, or target-side deduplication with a high-bandwidth transfer policy.
Copy Marked for Cancellation	Indicates whether the user has cancelled the copy job.

Comparing StoreOnce Catalyst backup/restore sessions

You can compare backup/restore sessions for a StoreOnce Catalyst store.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.

3. On the **Catalyst Stores** screen, select the StoreOnce Catalyst store, and then click the **Backup/ Restore** tab.
4. Select two backup/restore sessions, and then click the compare icon ( ).

Canceling StoreOnce Catalyst copy sessions

You can cancel active outbound and inbound copy sessions for a StoreOnce Catalyst store.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, click the StoreOnce Catalyst store.
4. On the screen for the StoreOnce Catalyst store, click the **Outbound Copy** tab or **Inbound Copy** tab, as appropriate.
5. Click the check box for the copy session, and then expand the **Actions** menu and select **Cancel**.

Comparing StoreOnce Catalyst copy sessions

You can compare outbound and inbound copy sessions for a StoreOnce Catalyst store.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **Catalyst Stores** above the graphic.
3. On the **Catalyst Stores** screen, click the StoreOnce Catalyst store.
4. On the screen for the StoreOnce Catalyst store, click the **Outbound Copy** tab or **Inbound Copy** tab, and then expand the **Actions** menu and select **Compare**.

Pausing and resuming outbound copy sessions

You can pause and resume outbound copy sessions on a StoreOnce System.

WARNING: All outbound copy sessions on a StoreOnce System are paused. No further data is copied until outbound copy sessions are resumed.

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Bandwidth Limits** tab.
3. On the **Outbound Copy Sessions Bandwidth Limiting Windows** panel, expand the **Actions** menu and select **Pause Copy Sessions** or **Resume Copy Sessions**, as appropriate.

StoreOnce Catalyst over Fibre Channel

TIP: The Fibre Channel Settings are only relevant to certain StoreOnce System models and are only available if the StoreOnce System supports Fibre Channel.

If StoreOnce Catalyst over Fibre Channel is supported on the StoreOnce System, the Fibre Channel settings are available. StoreOnce Catalyst over Fibre Channel functions in the same way as StoreOnce Catalyst over Ethernet. StoreOnce supported backup applications do not perceive a difference.

However, some configuration is required to set up the backup and restore connections between the ports on the StoreOnce System and the ports on the client servers. The configuration is done using the Fibre Channel settings screen and actions.

When using StoreOnce Catalyst over Fibre Channel:

- Backups are supported on StoreOnce Catalyst over a Fibre Channel interface and over Ethernet networks.
- StoreOnce System to StoreOnce System connectivity through optimized StoreOnce Catalyst copy jobs is supported over both Ethernet and Fibre Channel.
- Administrator client privileges are required to run StoreOnce Catalyst over Fibre Channel because it accesses OS-specific device files associated with StoreOnce Catalyst over Fibre Channel devices.

Viewing StoreOnce Catalyst Fibre Channel device settings

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Fibre Channel** tab.

   The Fiber Channel tab shows identifier information and a list of target devices and initiator devices.
3. To view details of a Fibre Channel target or initiator device, click its information icon ( ).

StoreOnce Catalyst Fibre Channel settings and properties

TIP: Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).

Setting	Description
Fibre Channel	
Identifier	The Fibre Channel address of the StoreOnce System.

Table Continued

Setting	Description
Identifier Alias	An alias for the Fibre Channel address to make it easier to identify the StoreOnce System in the backup application. The alias must begin with the “COFC-” prefix and cannot contain any special characters except a hyphen (-).
Target Devices	
Device Name	The name of the Catalyst over Fibre Channel port.
Status	The status of the port and its current speed.
FC Address	The Fibre Channel address of the Catalyst over Fibre Channel device. Or Down if not connected.
World Wide Node Name	Generated automatically by the StoreOnce System and used for Fibre Channel zoning for Fibre Channel target devices. Zone with the Copy Source Fibre Channel target World Wide Name or the Fibre Channel client Fibre Channel port WWN for backup/restore.
Number of Devices per Login	The number of client Fibre Channel ports zoned with that StoreOnce Catalyst over Fibre Channel port. The number is accurate as of the last reboot. If a client Fibre Channel port is unzoned, the Fibre Channel logins are not removed.
More properties	
World Wide Port Name	Generated automatically by the StoreOnce System and used for Fibre Channel zoning for Fibre Channel target devices. Zone with the Copy Source Fibre Channel target World Wide Name or the Fibre Channel client FC port WWN for backup/restore.
Number of Logins	The number of client Fibre Channel ports zoned with that StoreOnce Catalyst over Fibre Channel port. The number is accurate as of the last reboot. If a client Fibre Channel port is unzoned, the Fibre Channel logins are not removed.
Initiator Devices	
Device Name	The name of the Catalyst over Fibre Channel port.
Status	The status of the port and its current speed.
FC Address	The Fibre Channel address of the Catalyst over Fibre Channel device. Or Down if not connected.

Table Continued

Setting	Description
World Wide Node Name	Generated automatically by the StoreOnce System and used for Fibre Channel zoning for Fibre Channel target devices. Zone with the Copy Source Fibre Channel target World Wide Name or the Fibre Channel client Fibre Channel port WWN for backup/restore.
Number of Devices per Login	The number of client Fibre Channel ports zoned with that StoreOnce Catalyst over Fibre Channel port. The number is accurate as of the last reboot. If a client Fibre Channel port is unzoned, the Fibre Channel logins are not removed.

StoreOnce Catalyst over Fibre Channel client considerations

Windows clients

Administrator permissions are required to run StoreOnce Catalyst over Fibre Channel backups.

StoreOnce Catalyst over Fibre Channel presents a device type of “Processor.” In Windows Device Manager, these devices are shown as “Other Devices.” After zoning the devices or changing the Number of Devices per Initiator Port, right-click “Other Devices.” Then select “Scan for hardware changes” to detect the new devices.

Linux clients

StoreOnce Catalyst over Fibre Channel presents a device type of “Processor.” On Linux, these devices files are created in `/dev/sg*`. By default, `/dev/sg*` devices are accessible by root users only. If backups are run as a nonroot user, first grant the backup user permissions to access these device files using a Linux `udev` rule.

The `lsscsi --generic` command can be used to determine which `/dev/sg*` device files belong to StoreOnce Catalyst over Fibre Channel.

AIX clients

- StoreOnce Catalyst over Fibre Channel presents a device type of “Sequential” on AIX. These device files are created in `/dev/rmt*`. After zoning the devices, or changing the Number of Devices per Initiator Port, you must scan for device file changes. You can scan by executing the `cfgmgr` command on AIX as a root user.
- By default, `/dev/rmt*` device files are accessible by root users only. Running backups as a nonroot user requires an additional one-time configuration step of running `storeonce-cofc-passthrough-install.sh`. This installation script must be run as root and can be found in the backup application installation `bin` directory. This step is only required when backups will not be run as a root user.
- When using StoreOnce Catalyst over Fibre Channel on AIX, an additional configuration step is required in the StoreOnce Management Console. Find the WWPN of the client AIX Fibre Channel port. On the Fibre Channel Settings tab, set the Emulation Mode to AIX. After changing the emulation, you must scan for device file changes by executing the `cfgmgr` command on AIX as a root user.
- HPE recommends setting Delayed I/O Failure (`fc_err_recov=delayed_fail`) and Disabled Dynamic Tracking (`dyntrk=no`) on StoreOnce Catalyst over Fibre Channel AIX media/backup servers. These options are not compatible with IBM Spectrum Protect. Be sure that StoreOnce Catalyst over Fibre Channel and IBM Spectrum Protect do not use the same media/backup server.

HP-UX clients

StoreOnce Catalyst over Fibre Channel presents a device type of “Processor.” On HP-UX, these devices files are created in `/dev/pt/ptX`. After zoning the devices or changing the Number of Devices per Initiator Port, scan for device file changes. Execute the `ioscan -fnC /dev/pt` command as a root user. By default, `/dev/pt/ptX` devices are accessible by root users only. If backups are run as a nonroot user, first grant the backup user permissions to access these device files using `chmod o +rwx /dev/pt/pt*`.

For finer grained permissions, determine which `/dev/pt/ptX` device files relate to StoreOnce Catalyst over Fibre Channel using:

```
/usr/sbin/scsimgr -p get_attr all_lun -a device_file -a dev_type -a pid | grep StoreOnce
```

Then use `chmod o+rwx` on the appropriate devices.

Solaris clients

StoreOnce Catalyst over Fibre Channel presents a device type of “Processor.” On Solaris, these devices files are created in `/dev/scsi/processor/*`. After zoning the devices or changing the Number of Devices per Initiator Port, scan for device file changes. Execute the following commands as a root user. These operations will not affect Fibre Channel devices already configured on the Solaris system.

- `add_drv -vi scsiclass,03 sgen`
- `update_drv -vai scsiclass,03 sgen`

By default, `/dev/scsi/processor/*` devices are accessible by root users only. If backups are run as a nonroot user, first grant the backup user permissions to access these device files using `chmod -R o +rwx /dev/scsi/processor/*`.

For finer grained permissions, determine which `/dev/scsi/processor/*` device files relate to Catalyst over Fibre Channel using:

```
for i in /dev/scsi/processor/*; do echo $i; ls $i; luxadm inq $i | egrep "Vendor|Product"; echo; done
```

Then use `chmod -R o+rwx` on the appropriate devices.

StoreOnce Catalyst over Fibre Channel zoning considerations

Important: Nonoptimal Fibre Channel SAN zoning can lead to a lack of Fibre Channel connectivity. HPE recommends the following:

- Zone every backup/media server with at least two Fibre Channel ports and at least two StoreOnce node Fibre Channel ports across different Fibre Channel cards. Ideally, they are also zoned across different SANs. Multiple connections allow for higher availability. If a connection is broken, StoreOnce Catalyst over Fibre Channel will automatically attempt to connect on a different path without failing the backup. The backup will fail from a lack of connection only if no paths are available from the media/backup server or to the StoreOnce. Zone StoreOnce Catalyst Copy over Fibre Channel source and destination copy devices the same way.
- StoreOnce Catalyst Copy over Fibre Channel is a two-way protocol. Zone the source Initiator WWN with the destination target WWN, and zone the destination Initiator WWN with the source target WWN. The source and destination must be able to communicate with each other over Fibre Channel.

- Use small Fibre Channel zones limiting the number of Fibre Channel ports in each zone.
- StoreOnce Catalyst over Fibre Channel does not use or rely on any external multipath drivers. Connections are balanced using StoreOnce Catalyst over Fibre Channel internal algorithms. Catalyst over Fibre Channel ignores installed multipath drivers.

Configuring StoreOnce Catalyst over Fibre Channel

For an overview, see **StoreOnce Catalyst over Fibre Channel** on page 75.

IMPORTANT: Running StoreOnce Catalyst over Fibre Channel requires Administrator privileges to access OS-specific device files associated with StoreOnce Catalyst over Fibre Channel devices.

Prerequisites

- Client HBAs, switches, Fibre Channel driver, and firmware versions are supported. See the *HPE StoreOnce Support Matrix* **https://www.hpe.com/Storage/StoreOnceSupportMatrix**.
- Media/database servers can communicate with the StoreOnce System over a Fibre Channel network.
- Any network segregation, such as zoning, is set up to handle required connectivity between the StoreOnce System and servers.

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Fibre Channel** tab.

Editing StoreOnce Catalyst Fibre Channel settings

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Fibre Channel** tab.
3. On the **Fibre Channel** panel, click the edit icon ( ).

StoreOnce Catalyst Fibre Channel number of devices per login

The Number of Devices per Login determines the number of concurrent backup/restore and copy connections allowed from:

- A single client Fibre Channel port to a single StoreOnce Fibre Channel port.
- A source StoreOnce Fibre Channel port to a destination StoreOnce Fibre Channel port.

The Number of Devices per Login does not relate to how many total sessions can be established over a StoreOnce port. Each client port to StoreOnce port relationship will present the Number of Devices per Login. The setting applies to all StoreOnce Catalyst supported client operating systems and to StoreOnce Catalyst Copy over Fibre Channel.

The default number is 20. If you need multiple concurrent backup/copy streams, increase the Number of Devices per Login. The maximum allowed is 256 devices per client Fibre Channel port login. After increasing, you must run a device file rescan on the client for the change to be recognized. If you decrease the number, client operating systems will not delete StoreOnce Catalyst over Fibre Channel device files after a rescan. Operating systems only clear outdated device files on a reboot.

Calculate the number of paths available from one particular client or source StoreOnce node to a destination StoreOnce System using this formula:

```
number of a client's ports zoned to a StoreOnce System * number of StoreOnce
System ports zoned to that client * devices per initiator count
```

Table 1: Example relationships between Device per Login and Number of Connections

Per Client	StoreOnce System	Devices per Initiator Port	Number of concurrent backup/restore/copy sessions [1]
1 port zoned to	4 ports	1	4
2 ports zoned to	4 ports	1	8
2 ports zoned to	2 ports	4	16
2 ports zoned to	4 ports	8	64

[1] Per client Fibre Channel port to StoreOnce port relationship, and source StoreOnce port to destination StoreOnce port for StoreOnce Catalyst copy.

Editing StoreOnce Catalyst Fibre Channel device login settings

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Fibre Channel** tab.
3. On the **Target Devices** panel, click the target device, and then click the edit icon ( ).
4. On the **Edit Devices** dialog, use the **Number of Devices per Login** selector to change the setting.

Editing StoreOnce Catalyst Fibre Channel target device settings

Procedure

1. Navigate to the **Catalyst Settings** screen.

If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.

2. On the **Catalyst Settings** screen, click the **Fibre Channel** tab.
3. On the **Target Devices** panel, click the target device, and then click the edit icon ( ).

StoreOnce Catalyst settings

Viewing StoreOnce Catalyst settings

The **Catalyst Settings** screen allows you to view and manage StoreOnce Catalyst settings.

Procedure

1. Do one of the following:
   - On the main menu, select **Data Services**. On the **Data Services** screen, expand the **Actions** menu and select **Catalyst Settings**.
   - On the main menu, select **Settings**. On the **Settings** screen, under **Data Services**, click the **Catalyst Settings** panel.
2. The **Catalyst Settings** screen includes tabs for **Permissions**, **Bandwidth Limits**, **Fibre Channel**, and **Proxy Server**.

Viewing StoreOnce Catalyst Fibre Channel device settings

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Fibre Channel** tab.

   The Fiber Channel tab shows identifier information and a list of target devices and initiator devices.
3. To view details of a Fibre Channel target or initiator device, click its information icon ( ).

Bandwidth limits (StoreOnce Catalyst)

Users with the Administrator role can establish and edit StoreOnce Catalyst bandwidth limits.

Bandwidth limits can be used to avoid saturating the WAN with low-bandwidth replication and to free up bandwidth for other processes and applications. You can establish a general bandwidth limit, and limits for one or two windows for each day of the week. Each window can have a different bandwidth limit.

- To establish or edit a general bandwidth limit, see **Editing Catalyst general bandwidth limits** on page 83.
- To establish or edit a bandwidth limits for specific day of the week and time windows, see **Editing Catalyst bandwidth limiting windows** on page 83.

IMPORTANT:

- Catalyst bandwidth limits apply to all outbound copy jobs a StoreOnce System. The limits cannot be applied to individual outbound jobs.
- When a bandwidth limiting window is enabled, it overrides the general bandwidth limit at the day and time the window is active.

- HPE recommends:
  - A minimum of 2Mb/s per concurrent copy job.
  - At least 512Kbps per concurrent job is required for reliable operation.

Viewing Catalyst bandwidth limits

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Bandwidth Limits** tab.

Bandwidth limit properties (Catalyst)

Catalyst Settings screen, Bandwidth Limits tab

Property	Description
Status	
System Time	The current time on the StoreOnce System.
Current Bandwidth Limit	The current Catalyst copy bandwidth limit in Kb/s. No Limit indicates that no bandwidth restrictions are currently active.
Source Jobs Bandwidth Limiting Windows	
General Bandwidth Limit	Limit in Kb/s. No Limit indicates that the general bandwidth limit is not enabled.
Restriction table	
Day	Day of the week
First Restriction Limit	Catalyst copy bandwidth restriction in Kb/s. Dashes indicate that the restriction is not enabled.

Table Continued

Property	Description
First Restriction Time	Catalyst copy restriction start and end time. Dashes indicate that the restriction is not enabled.
Second Restriction Limit	Catalyst copy bandwidth restriction in Kb/s. Dashes indicate that the restriction is not enabled.
Second Restriction Time	Catalyst copy restriction start and end time. Dashes indicate that the restriction is not enabled.
Maximum Jobs	
Maximum Concurrent Source Jobs	The maximum number of source jobs that can run concurrently.
Maximum Concurrent Target Jobs	The maximum number of target jobs that can run concurrently.  **TIP:** If you are running backups at the same time as replication, the default value of the target jobs can be reduced. Reducing the value helps avoid using too much WAN bandwidth and overloading the target StoreOnce System.

Editing Catalyst general bandwidth limits

Only an administrator can add bandwidth limiting windows.

For more information, see **Bandwidth limits (StoreOnce Catalyst)** on page 81.

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Bandwidth Limits** tab.
3. On the **Outbound Copy Sessions Bandwidth Limiting Windows** panel, expand the **Actions** menu and select **Edit General Bandwidth Limit**.

   On the edit dialog, do one of the following:

   - Manually enter a bandwidth limit.
   - Use the built-in **Bandwidth Limit Calculator** to determine and apply a limit.

Editing Catalyst bandwidth limiting windows

You can use bandwidth limiting to avoid saturating the WAN with low-bandwidth replication and to free up bandwidth for other processes and applications. The limits apply to all outbound copy jobs from a StoreOnce System.

For more information, see **Bandwidth limits (StoreOnce Catalyst)** on page 81.

IMPORTANT: Restriction times are in system local time, not in UTC. If the time zone of the StoreOnce System is changed after restrictions are added, you must change the restriction times accordingly.

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Bandwidth Limits** tab.
3. On the **Day/Restriction** table, click a day of the week, and then expand the **Actions** menu and select **Edit Bandwidth Limiting Windows**.

   On the edit dialog, do one of the following:

   - Manually enter a bandwidth limit.
   - Use the built-in **Bandwidth Limit Calculator** to determine and apply a limit.

Adding StoreOnce Catalyst clients to StoreOnce Systems

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Permissions** tab.
3. Expand the **Actions** menu and select **Add**.

Configuring StoreOnce Catalyst proxy server settings

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Proxy Server** tab.
3. On the **Proxy Server** panel, click the edit icon ( ).

Editing StoreOnce Catalyst Fibre Channel settings

Procedure

1. Navigate to the **Catalyst Settings** screen.

If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.

2. On the **Catalyst Settings** screen, click the **Fibre Channel** tab.
3. On the **Fibre Channel** panel, click the edit icon ( ).

Editing StoreOnce Catalyst Fibre Channel target device settings

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Fibre Channel** tab.
3. On the **Target Devices** panel, click the target device, and then click the edit icon ( ).

Pausing and resuming outbound copy sessions

You can pause and resume outbound copy sessions on a StoreOnce System.

WARNING: All outbound copy sessions on a StoreOnce System are paused. No further data is copied until outbound copy sessions are resumed.

Procedure

1. Navigate to the **Catalyst Settings** screen.

   If necessary, see **Viewing StoreOnce Catalyst settings** on page 81.
2. On the **Catalyst Settings** screen, click the **Bandwidth Limits** tab.
3. On the **Outbound Copy Sessions Bandwidth Limiting Windows** panel, expand the **Actions** menu and select **Pause Copy Sessions** or **Resume Copy Sessions**, as appropriate.

VT library data services

VT Library licensing requirements

- No licensing is required for VT Library emulations, unless using the Security features Data at Rest Encryption, Data in Flight Encryption, and Secure Erase.
- VT Library replication requires a license on the target site, but only if replication is used.
- Replication encryption using IPsec is part of the Security license.

VT libraries and Fibre Channel settings

For information about Fibre Channel settings, see the following System settings topics:

- **Viewing Fibre Channel port settings and properties** on page 180
- **Fibre Channel settings and properties** on page 181
- **Editing Fibre Channel port settings** on page 182

VT libraries and multiple Fibre Channel ports

When creating a VT library, you can select one or multiple Fibre Channel ports for the Library controller virtual robotics interface.

The Fibre Channel settings identify both the HBA card and the port number that will be used. For example, HBA-6.Port1 is Port 1 on the Fibre Channel card in slot 6.

Tape drives within a VT library can only appear on one Fibre Channel port. If you select multiple ports for the library robotics controller, the tape drives are automatically assigned. The assignments distribute the tape drives evenly across the Fibre Channel ports to ensure best performance and failover.

After creating a VT library, you can change its tape drive assignments on the **Interface Information** tab, **Edit Device** dialog of the VT library. See **Editing VT libraries** on page 97.

VT libraries

Viewing VT libraries

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, do one of the following:
   - To view all VT libraries, click the title **VT Libraries** above the graphic.
   - To view VT libraries that have a specific status, click the status on the graphic. For example, clicking the Warning status on the graphic opens the **VT Libraries** screen and displays only libraries that have a Warning status.
3. The **VT libraries** screen shows the VT libraries on the StoreOnce System.

TIP:

- In the list view, columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().
- To create a VT library, expand the **Actions** menu and select **Create Library**. (You must be logged in with an administrator role). See **Creating VT libraries** on page 96.

4. On the **VT Libraries** screen, click the VT library.
   The screen for an individual VT library includes tabs for **Overview**, **Details**, **Interface Information**, **Cartridges**, and **Replication Permissions**.

   Some of the properties and settings on the **Interface Information**, **Cartridges**, and **Replication Permissions** tabs can be edited. (You must be logged in with an administrator role).

VT Libraries screens and properties

VT Libraries screen (all libraries)

TIP: In the list view, columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().

Property	Description
Name	The name of the VT library. HPE recommends using a name that identifies the host or backup job with which it is associated.
Status	The device status. Offline, starting, stopping, online. (This status is not the status of the connection.)
User Data Stored	The amount of user data stored on the VT library.
Size on Disk	The actual size used on disk after deduplication.
Dedupe Ratio	The deduplication ratio achieved on the data on the VT library.
Replication Role	The role of the VT library. Non-replicating, Replication Source, or Replication Target.
More properties	
Number of Cartridges	The number of cartridge slots in the VT library. The number of slots available depends upon the type of VT library emulation. Each slot is automatically populated with a new cartridge upon creation. The cartridge capacity corresponds to the type of tape drive emulation.

Table Continued

Property	Description
Protocol	The port type. Fibre Channel or iSCSI.
Physical Storage Quota	This quota is for the amount of data written to disk after deduplication. The minimum quota size is 50 GB. If the quota is enabled and the quota limit is reached, backups will fail to prevent the quota from being exceeded. The quota allows you to partition the physical capacity of the StoreOnce System between various users. When a library reaches its quota, the status of the library will change to “Critical”. Restores from that library are permitted but new backups will fail. When the quota is no longer met, either by increasing the quota or by expiring backups, the library status returns to the “OK” state. **TIP:** If capacity management is required, HPE recommends configuring backup applications with quotas to reroute to another device or to postpone backups to prevent backups from failing unexpectedly.
Logical Storage Quota	This quota is for the amount of data a user sends to the device before deduplication. The minimum quota size is 50 GB. If the quota is enabled and the quota limit is reached, backups will fail to prevent the quota from being exceeded. This approach allows you to provide a service to back up a particular amount of user data. For example, set this quota when you charge customers per TB of user data protected. When a library reaches its quota, the status of the library will change to “Critical”. Restores from that library are permitted but new backups will fail. When the quota is no longer met, either by increasing the quota or by expiring backups, the library status returns to the “OK” state. **TIP:** If capacity management is required, HPE recommends configuring backup applications with quotas to reroute to another device or to postpone backups to prevent backups from failing unexpectedly.
Encryption	This feature requires a StoreOnce Security Pack license before encryption can be enabled. Encryption cannot be enabled or disabled once a library is created. It can only be enabled at library creation. If enabled, encryption is performed before writing data to disk for this library.
Secure Erase Mode	This feature requires a StoreOnce Security pack license before it can be enabled. To enable, select the number of preferred Overwrite Passes for deleted data (1, 3, 5, or 7 — The default selection of “None” disables secure erase). You cannot select Secure Erase while creating a library, but after the library is created, you can activate this feature. (Requires a Security pack license.) See **Security features** on page 14.

VT Libraries (individual library), Overview tab

Property	Description
Dedupe Ratio	The deduplication ratio achieved on the data on the VT library.
User Data Stored	The amount of user data stored on the VT library.
Size on Disk	The actual size used on disk after deduplication.

VT Libraries screen (individual library), Details tab

Property	Description
Library Name	The name of the VT library. HPE recommends using a name that identifies the host or backup job with which it is associated.
Replication Role	The role of the VT library. Non-replicating, Replication Source, or Replication Target.
Creation Time	The date and time the VT library was created.
Media Changer Protocol	The port type. Fibre Channel or iSCSI.
Storage Quotas	
Physical Storage Quota	This quota is for the amount of data written to disk after deduplication. The minimum quota size is 50 GB. If the quota is enabled and the quota limit is reached, backups will fail to prevent the quota from being exceeded. The quota allows you to partition the physical capacity of the StoreOnce System between various users. When a library reaches its quota, the status of the library will change to “Critical”. Restores from that library are permitted but new backups will fail. When the quota is no longer met, either by increasing the quota or by expiring backups, the library status returns to the “OK” state.  **TIP:** If capacity management is required, HPE recommends configuring backup applications with quotas to reroute to another device or to postpone backups to prevent backups from failing unexpectedly.

Table Continued

Property	Description
Logical Storage Quota	This quota is for the amount of data a user sends to the device before deduplication. The minimum quota size is 50 GB. If the quota is enabled and the quota limit is reached, backups will fail to prevent the quota from being exceeded. This approach allows you to provide a service to back up a particular amount of user data. For example, set this quota when you charge customers per TB of user data protected. When a library reaches its quota, the status of the library will change to “Critical”. Restores from that library are permitted but new backups will fail. When the quota is no longer met, either by increasing the quota or by expiring backups, the library status returns to the “OK” state.  **TIP:** If capacity management is required, HPE recommends configuring backup applications with quotas to reroute to another device or to postpone backups to prevent backups from failing unexpectedly.
Security	
Library Encryption	This feature requires a StoreOnce Security Pack license before encryption can be enabled. Encryption cannot be enabled or disabled once a library is created. It can only be enabled at library creation. If enabled, encryption is performed before writing data to disk for this library.
Secure Erase Mode	This feature requires a StoreOnce Security pack license before it can be enabled. To enable, select the number of preferred Overwrite Passes for deleted data (1, 3, 5, or 7 — The default selection of “None” disables secure erase). You cannot select Secure Erase while creating a library, but after the library is created, you can activate this feature. (Requires a Security pack license.) See **Security features** on page 14.
Emulation	
Library Emulation	The type of emulation for the VT library. The library emulation type determines the available embedded tape drives and cartridge slots. For example, if you select MSL G3 Series (2x24), the device emulates an MSL2024 Library with two embedded tape drives and a possible total of 24 cartridge slots. StoreOnce Systems support a number of emulation types. See **VT library emulation types** on page 98. Consult your backup application technical support information for information about device types they support.

Table Continued

Property	Description
Drive Emulation	The drive emulation type (LTO–2, 3, 4, 5 or 6) determines the default capacity of the newly created cartridges within the VT library device and the inquiry string information provided to the backup application. Tape cartridge capacities can be changed individually at any time but cannot be reduced to smaller than the current used size. If you selected D2DBS Generic for the Library Emulation, Ultrium VT is an option for drive emulation. This emulation is a generic Ultrium device which is clearly identifiable as virtual. Where supported by the backup application, Hewlett Packard Enterprise recommends that D2DBS Generic and Ultrium VT are used in preference to the other emulation types. All drives on a VT library configured with the IBM-TS3500 emulation type will use the IBM-LTO3 drive emulation type. Drives on a library configured with IBM-TS3500 IBMi will use the IBM-LTO5 drive emulation type. If the library is changed to a different emulation type, the drives will change to the default drive emulation type of LTO4. If you edit this property, the new setting applies only to the next drives that are created within the library. It is not retrospectively applied to existing drives.
Number of Slots	The number of cartridge slots in the VT library. The number of slots available depends upon the type of VT library emulation. Each slot is automatically populated with a new cartridge upon creation. The cartridge capacity corresponds to the type of tape drive emulation.
Number of Drives	The default number of drives is determined by the type of emulation selected. The number of drives can only be set during VT library creation. After VT library creation, you can add and remove drives **IMPORTANT:** If increasing the number of drives, do not exceed the maximum number of libraries and drives that a host can physically access.
Default Cartridge Size	The default size of tape cartridges in the VT library. This property can only be set when creating a VT library.
Barcode	

Table Continued

Property	Description
Barcode Template	A barcode is an 8– or 6–character, alpha-numeric, unique identifier for a cartridge within the StoreOnce System. Backup applications normally track cartridges using barcodes, but may also alias a cartridge with another name in its database. (IBM emulations only support 8–character barcodes.) By default, barcodes are generated automatically but may be determined by a barcode template created when a VT library is created. If using barcode templates, the barcode template: • Must be unique and must not start with the letters “CLN” or “DG” because these combinations are reserved designations for cleaning and diagnostic cartridges. • Can have a prefix of up to three alpha-numeric characters, a start value, and a suffix of up to two alpha-numeric characters. Any unspecified prefix or suffix characters will increase the length of the variable field of the barcode. • Should be a minimum of 6 characters. Valid ASCII characters are A-Z, a-z, 0–9. Barcodes are always displayed as eight characters with letters in capitals, regardless of the size selected. However, if the number of barcode characters is set to 6, only the rightmost six characters are visible to the backup software. For example, barcode 1ABCDEFG will truncate to BCDEFG. (Truncated barcode characters are shown in brackets. You can modify the barcode template after a VT library is created.
Number of Barcode Characters	Barcodes for the library can display six or eight characters. The StoreOnce System generates barcodes automatically for cartridges. When entering a barcode manually, eight characters are required. If the 6–character barcode is selected, the StoreOnce System will truncate to six characters, removing two characters of an 8–character barcode. For example, barcode 1ABCDEFG will truncate to BCDEFG. The barcode is displayed with the truncated characters in brackets on the Cartridges tab (1A)BCDEFG.
Prefix	Barcode prefix. One to three alpha-numeric characters.
Start Value	Starting value for the next barcode.
Suffix	Barcode suffix. One to two alpha-numeric characters.
Next Barcode	Create the barcode with the next sequential value.
Backup Application Details	

Table Continued

Property	Description
Backup Application	The name and information about the backup application that is used to back up to the VT library. The information is optional, but is recommended as an aid to HPE support troubleshooting. The information has no impact on performance or deduplication efficiency.
Data Type	The type of data being protected by the backups to this VT library. The information is optional, but is recommended as an aid to HPE support troubleshooting. The information and has no impact on performance or deduplication efficiency.

VT Libraries screen (individual library), Interface Information tab

TIP: Columns for the most often viewed properties are shown by default. To remove columns, click the column selector icon ( ).

Property	Description
Name	The name of the VT library interface device. There is an entry for the Medium Changer, and for each of the configured tape drives.
Status	The device status. Offline, starting, stopping, online. (This status is not the status of the connection.)
Protocol	Fibre Channel or iSCSI.
Serial Number	This number is a unique serial number for the device. It is generated automatically by the StoreOnce System and cannot be edited.
iSCSI Alias	The alias is generated automatically by the StoreOnce System for iSCSI devices.

VT Libraries screen (individual library), Cartridges tab

TIP: Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).

Property	Description
Location	Cartridge slot number, tape drive number, mail slot number
Barcode	The alpha-numeric unique identifier for a cartridge within the StoreOnce System.
Mapped Slot	Indicates whether the slot is included in a replication mapping.

Table Continued

Property	Description
Used Size	The used capacity.
Cartridge Size	The default size of tape cartridges in the VT library. This property can only be set when creating a VT library.
More properties	
Write Protected	Whether write protection is enabled for disabled for a cartridge slot.
Last Written	Date and time data was last written to the tape drive or mail slot.

VT Libraries screen (individual library), Replication Permissions tab

Property	Description
Replication Serial Number (and access)	The replication serial number that is automatically generated by the StoreOnce System. This replication serial number is used for all replication jobs. The replication serial number does not change. The replication serial number for a StoreOnce System is different than its serial number. When Public Access is allowed, any StoreOnce System can participate in replication of the VT library.

Viewing VT library details

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT Library.
4. On the **VT Libraries** screen for the library, click the **Details** tab.

Viewing VT libraries interface information

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT Library.
4. On the **VT Libraries** screen for the library, click the **Interface Information** tab.

VT library interface device properties

VT Library, Fibre Channel Device
The following properties can appear on the **Edit Device** dialog when a VT library uses a Fibre Channel interface.

Property	Description
Device Name	The name of the VT library interface device. There is an entry for the Medium Changer, and for each of the configured tape drives.
Status	The status of the port, which may be OK, Down, Warning, Error, or Not Used. Warnings occur if the port is not available or is down. They also appear if the system is unable to obtain Speed information. Errors occur if there is a fault or the system cannot obtain the link status.
Protocol	Fibre Channel or iSCSI.
Device Serial Number	This number is a unique serial number for the device. It is generated automatically by the StoreOnce System and cannot be edited.
FC Address	The Fibre Channel addresses of the device. The address is shown for each FC Port for which the device is configured. Or, shows "Down" if the port is not connected.
Number of Logins	Fibre Channel libraries show the number of logins for each device in the library. Libraries split across multiple ports have multiple entries.
Port	Defines the Fibre Channel port to which each media changer or drive is connected.
World Wide Node Name	Provided when the device is created and is globally unique. You can change this setting, if necessary, but not to any names used by libraries or drives on the local StoreOnce System.
World Wide Port Name	Generated automatically by the StoreOnce System and used for Fibre Channel zoning for Fibre Channel devices. You can change this setting, if necessary, but not to any names used by libraries or drives on the local StoreOnce System. Libraries split across multiple ports have multiple entries.

VT Library, iSCSI Device
The following properties can appear on the VT Libraries **Interface Information** tab when a VT library uses an iSCSI interface.

Property	Description
Name	The name of the VT library interface device. There is an entry for the Medium Changer, and for each of the configured tape drives.
Status	The device status (not the state of the connection): Offline, starting, stopping, online.
Protocol	iSCSI
Serial Number	The serial number is a unique identifier for the device. It is generated automatically by the StoreOnce System and cannot be edited.
iSCSI Alias	The Alias is generated automatically by the StoreOnce System for iSCSI devices.

Creating VT libraries

Only users with the administrator role can create VT libraries.

- To reduce Fibre Channel traffic, and complexity with backup application configurations, HPE recommends the following:
  - Create only the VT libraries that you need.
  - When creating a VT library, configure only the number of tape cartridges that you are likely to need. Later, you can add cartridge slots to expand the VT library. You can also remove empty cartridge slots without deleting the whole VT library.

    For more information, see **Security features** on page 14.
- To enable Data at Rest or Data in Flight encryption for a VT library, you must do it when creating the library. To see the settings, click the **Security Settings** edit icon ( ).

  The encryption features require an HPE StoreOnce encryption license. If the license is not installed, *Not Licensed* is displayed.
- After the VT library has been created, you can edit the library and enable Secure Erase.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, expand the **Actions** menu and select **Create**.

   The **Create Library** dialog allows you to specify the following:

   - **Library name**
   - **Interface Information** (iSCSI port, Fibre Channel port, or no port)
   - **Security Settings**
   - **Emulation Settings**

- **Barcode Settings**
- **Backup Application Details**
- **Advanced Settings**

Editing VT libraries

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.
4. On the screen for the VT library, expand the **Actions** menu and select **Edit**.

   The **Edit** dialog allows you to specify the following:

   - **Interface Information** (iSCSI port, Fibre Channel port, or no port)
   - **Security Settings**
   - **Emulation Settings**
   - **Barcode Settings**
   - **Backup Application Details**
   - **Advanced Settings**

Tips for editing VT libraries

Users with the administrator role can edit the following settings:

- **Interface Information**

  WARNING: Changing the Media Changer Port configuration does not automatically reassign tape drives that might become incorrectly configured.

  For example, if you change a Fibre Channel multiple port configuration to a single port, you must manually correct tape drives that become connected to an incorrect port. (When the status shows ready and restarted.)

- **Security Settings**: After a VT library is created, and the correct HPE StoreOnce license is applied, Secure Erase Mode can be enabled and disabled. To enable, select the number of Overwrite Passes (1, 3, 5, or 7).

  When enabled, Secure Erase securely erases confidential data that might have been unintentionally backed up.

- **Emulation Settings**:
  - You cannot change the Library Emulation type to a type that has smaller maximum values. For example, you cannot change to an emulation that has a smaller number of tape cartridges.
  - Changing the cartridge size (by changing the emulation type) only changes newly added cartridges. The change does not change the size of cartridges that are already created.

- Deleting tape cartridges. You cannot delete tape cartridges by editing the Emulation Settings.

  TIP: To delete tape cartridges, see **Deleting VT library cartridges** on page 104.

- Deleting cartridges by reducing the number of slots. This reduction only removes the highest numbered empty slots. Once the delete operation reaches a slot number that contains a cartridge, it will not allow further reduction, even if previous slots are empty.

- **Barcode Settings**: Number of Reported Barcode Characters and Barcode Template.
- **Backup Application Details**: Backup Application and Type.
- **Advanced Settings**: Storage Quotas.

Deleting VT libraries

Only users with the administrator role can delete VT libraries.

WARNING: All data on the VT library will be deleted.

- The deduplication store for the VT library will also be deleted.
- If Secure Erase is enabled for this VT library, the data will be deleted securely.
- It may take some time to delete all the files and free space on the StoreOnce System.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.
4. On the screen for the VT library, expand the **Actions** menu and select **Delete**.

VT library emulation types

StoreOnce Systems emulate a range of physical tape devices.

D2DBS Generic

If supported by your backup application, D2DBS Generic is the preferred emulation type. D2DBS Generic does not emulate physical library types and is clearly identifiable as a StoreOnce device. It is the most flexible emulation type available; however, backup application support varies by software vendor.

If you have selected D2DBS Generic for the Library Emulation Type, you will be able to select Ultrium VT for the tape drive emulation. Ultrium VT is a generic Ultrium device which is clearly identifiable as virtual. Back up application support for Ultrium VT is common, but not as complete as the D2DBS library type, so it is not possible to use it with all backup software.

NOTE: VERITAS prefers their customers use this emulation type with BackupExec and NetBackup.

EML E Series

An enterprise tape library solution that allows you to configure tape drives per node and cartridges per library.

ESL E Series

An enterprise tape library solution that allows you to configure tape drives per node and cartridges per library.

IBM-TS3500

A tape library device that appears as a native IBM TS3500 device in a TSM environment to allow use of standard IBM drivers. The emulation type is configured at the library level. Therefore, all tape drives on a library configured with the IBM-TS3500 emulation type will use the IBM-LTO3 tape drive emulation type. When the library is then changed to a different emulation type, the tape drives will change to the new emulation type.

MSL G3 Series (2x24)

A tape library device with a maximum of two embedded Ultrium tape drives and 24 cartridge slots. Used when implementing rotation schemes which involve simultaneous backup jobs to two devices. This emulation type is widely supported by backup applications.

MSL G3 Series (4x48)

A tape library device with a maximum of four embedded Ultrium tape drives and 48 cartridge slots. Used when implementing rotation schemes which involve simultaneous backup jobs to more than two devices or jobs that use many cartridges devices. This emulation type is widely supported by backup applications.

MSL G3 Series (8x96)

A tape library device with a maximum of eight embedded Ultrium tape drives and 96 cartridge slots.

Flexible emulation

The ESL, EML, and D2DBS emulations are flexible because they allow you to configure many tape drives per library. The main benefits are that many tape drives allows:

- More concurrent streams on backups which are throttled due to host application throughput, such as multiple streamed backups from a database.
- A single library (and therefore deduplication store) to contain similar data from backups that must run in parallel to increase deduplication ratio.

If using these flexible emulation types, consider the following factors:

- An important consideration when configuring VT library devices is that the library and each tape drive that you configure for it counts as a separate device. There are practical limitations on the number of devices that each host and Fibre Channel switch or HBA can access.
- The total device value also applies to NAS shares and StoreOnce Catalyst stores. If you configure the full value as VT library devices, you will not be able to configure any NAS shares or StoreOnce Catalyst stores for that StoreOnce System.

VT library tape drives

Changing the number of VT library tape drives

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the library.
4. On the screen for the VT library, expand the **Actions** menu and select **Edit**.
5. On the **Edit** dialog, click the **Emulation Settings** panel.
6. On the **Emulation Settings** dialog, you can increase or decrease the number of tape drives.

VT library cartridges

Viewing VT libraries cartridge information

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT Library.
4. On the **VT Libraries** screen for the library, click the **Cartridges** tab.

VT library cartridge properties

VT Libraries screen (individual), Cartridges tab

TIP: Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().

Property	Description
Location	The location information is based on your selection of **Type** on the **Cartridges** tab. • **Slots**: Location shows the cartridge slot number. • **Drives**: Location shows the tape drive number. • **Mail slot**: Location shows the mail slot number. A mail slot is a dedicated slot. It holds a cartridge that is ready for exporting to or importing from physical tape. Mail slots are not used with StoreOnce Systems. **TIP:** • When all columns for a slot show dashes, it indicates that the slot does not contain a cartridge. • To create a cartridge for an empty slot, see **Creating VT library cartridges** on page 102.
Barcode	The alpha-numeric unique identifier for a cartridge within the StoreOnce System. For details, see Barcode properties section of the **VT Libraries screens and properties** on page 87 topic.
Mapped Slot	Indicates whether the slot is included in a replication mapping.
Used Size	The used capacity.
Cartridge Size	The default size of tape cartridges in the VT library. This property can only be set when creating a VT library.
More properties	
Write Protected	Whether write protection is enabled for disabled for a cartridge slot.
Last Written	Date and time data was last written to the tape drive or mail slot.

Viewing VT libraries slot mappings detail

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Replication** above the graphic.
3. On the **VT Replication** screen, click the mapping.
4. On the **VT Replication** screen for the mapping, select the **Slot Mapping** tab.

   A list of source and target slot mappings is shown.
5. To view the details for a slot mapping, click its information icon ( ).

Changing the number of VT library cartridge slots

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the library.
4. On the screen for the VT library, expand the **Actions** menu and select **Edit**.
5. On the **Edit** dialog, click the **Emulation Settings** panel.
6. On the **Emulation Settings** dialog, you can increase or decrease the number of cartridge slots.

Creating VT library cartridges

Only users with the administrator role can create cartridges.

TIP: The Create Cartridges action creates cartridges in all empty slots in a VT library.

IMPORTANT:

- If you create a cartridge in an empty slot, ensure that the backup application inventories it (adds it to its database or catalog). Otherwise, the backup application cannot access the new cartridge.
- If you create a cartridge in an empty mail slot, use the backup application to move the blank new cartridge to an empty cartridge slot without requiring an inventory. This approach saves processing time.

Prerequisites

To create cartridges in a VT library, the VT library must have at least one empty slot or mail slot.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.
4. On the screen for the VT library, click the **Cartridges** tab, and then select **Slots** or **Mail Slot** for the **Type**.

   A list of slots or mail slots is displayed.
5. On the **Type** panel, expand the **Actions** menu and select **Create Cartridges**.
6. On the Create Cartridges dialog, select the cartridge size, and click **Create**.
7. After the action completes, restart the backup application services to ensure that the application sees the new cartridges.

Editing VT library barcodes

You can change the number or reported bar code characters for a VT library. You can also change the barcode template for a VT library.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the library.
4. On the screen for the library, expand the **Actions** menu and select **Edit**.
5. On the **Edit** dialog, **Barcode Settings** panel, click the edit icon ().

Tips for editing VT library barcodes

The barcodes for multiple cartridges within a VT library can be changed according to a user-defined template. The template can contain a prefix, suffix, or both.

General

- All characters in a barcode must be alpha-numeric (A-Z, 0–9). All alphabetic characters are capitalized upon application (regardless of how they are entered).
- A barcode template results in restricted barcode prefixes of CLN or DG being created.
- A barcode template cannot be applied to a range of slots with one or more empty slots.

Barcode format

- **Prefix**: Defines the first letter or numerical value for the barcodes. Accepts up the three characters.
- **Start Value**: Defines the numerical value of the first barcode value.
- **Suffix**: Defines the suffix letter or numerical value for the barcodes. Accepts up to two characters.

IMPORTANT:

- The values you choose for prefix, suffix, and starting value limit how many barcodes can be generated.

  For example, if you enter a two-character prefix and two-character suffix, you are limited to three alpha-numeric characters for the variable portion. If the starting value for the variable portion is 000, the choice would limit the amount of barcodes to 46656.
- If six-character barcodes are selected, the leading characters of the barcode will not be reported to the backup application. These characters might be part of the barcode prefix specified.

Editing VT library cartridges

You can edit cartridges by specifying a slot or mail slot. The properties that can be changed include the cartridge barcode, maximum size, and write protection.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.

4. On the screen for the VT library, click the **Cartridges** tab, and then select **Slots** or **Mail Slot** for the **Type**.

   A list of slots or mail slots is displayed.

5. Click the slot or mail slot, and then expand the **Actions** menu on the **Type** panel and select **Edit**.

Deleting VT library cartridges

WARNING: Deleting a cartridge permanently deletes all data on the cartridge.

HPE recommends using the data protection software to erase cartridges prior to deleting the cartridge. This approach ensures that the application catalog is updated.

Only users with the administrator role can delete cartridges from a VT library.

- You can delete cartridges by specifying a slot or mail slot.
- You cannot delete cartridges that are currently in drives that are mapped for replication. Or that are in the delete pending, erase pending, or creating state.

TIP: You can also delete cartridges by using the Edit Library, Emulation Settings dialog, and reducing the number of slots.

However, that approach only removes the highest slots with no or blank cartridges. Once the delete operation reaches a slot that contains a cartridge with data, it will not reduce the number further. Even if lower numbered slots are blank. First, use the Cartridges tab, Erase Cartridges dialog to reconfigure the slots to a blank state.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.
4. On the screen for the VT library, click the **Cartridges** tab, and then select **Slots** or **Mail Slot** for the **Type**.

   A list of slots or mail slots is displayed.

5. Click the slot or mail slot, and then expand the **Actions** menu on the **Type** panel and select **Delete**.

Erasing VT library cartridges

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.
4. On the screen for the VT library, click the **Cartridges** tab, and then select **Slots** or **Mail Slot** for the **Type**.

A list of slots or mail slots is displayed.

5. Click the slot or mail slot, and then expand the **Actions** menu and select **Erase**.

Moving VT library cartridges

Moving cartridges is useful to realign the VT library configuration with the backup application. For example, if the library and backup application become out of sync. Or if the backup application does not support a Move Medium command.

- You can move a cartridge to an empty slot or empty mail slot.
- You cannot move cartridges that are in the delete pending, erase pending, or create state.

Prerequisites

To move cartridges, the VT library must have at least one empty slot or tape drive.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.
4. On the screen for the VT library, click the **Cartridges** tab, and then select **Slots** or **Mail Slot** for the **Type**.

   A list of slots or mail slots is displayed.
5. Click the slot or mail slot, and then expand the **Actions** menu and select **Move**.

Unloading VT library cartridges

Unloading cartridges is useful to realign the VT library configuration with the backup application. For example, if the library and backup application become out of sync.

- You can unload all loaded cartridges from the tape drives in a VT library.
- You cannot unload cartridges that are in the delete pending, erase pending, or create state.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.
4. On the screen for the VT library, click the **Cartridges** tab.
5. On the **Type** panel, expand the **Actions** menu and select **Unload All**.

VT replication

The following topics are specific to VT replication. For general replication settings that apply to both VT and NAS replication, see **Viewing replication settings** on page 143.

VT libraries replication overview

TIP: Multiple source StoreOnce Systems can replicate VT libraries to a single target StoreOnce System. This approach, known as fan-in, provides consolidation benefits.

- Only users with the Administrator role can create and manage VT library replication mappings.
- You can only map and replicate VT libraries of the same version.

Prerequisites

This overview assumes that the source and target VT libraries exist. If you have not created the source and target VT libraries, see **Creating VT libraries** on page 96.

Procedure

Create partner systems relationship

1. On the source StoreOnce System, create a partner system relationship between the source and target systems. Lean more: **Adding replication target systems** on page 137.

   TIP: After a partner system relationship between systems has been created, you do not need to perform this step again.

Establish system-level replication permission

2. On the target StoreOnce system, establish replication permission between the source system and the target system. Learn more: **Adding replication permissions for target systems** on page 153.

   TIP: After system-level replication permission has been established between systems, you do not need to perform this step again.

Establish VT library replication permission

3. On the target StoreOnce system, select the target VT library and establish replication permission for the library. Learn more: **Adding replication permissions for target VT libraries** on page 111.
4. On the target StoreOnce system, turn on (allow) replication to the target VT library. Learn more: **Editing replication permissions for target VT libraries** on page 112.

Create VT Library replication mapping

5. On the source system, select the source VT library and create replication mapping for the library. Learn more: **Creating replication mappings for source VT libraries** on page 111.

Viewing VT replication mappings

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, do one of the following:

- To view all VT replication mappings, click the title **VT Replication** above the graphic.
- To view VT replication mappings that have a specific status, click the status on the graphic. For example, clicking the Warning status on the graphic opens the **VT Replication** screen and displays only VT replication mappings that have a Warning status.

3. On the **VT Replication** screen, click the VT replication mapping.
   The screen for an individual VT replication mapping includes tabs for **Overview**, **Details**, and **Slots Mapping**.

VT replication screens and properties

VT Replication screen (all mapping)

TIP: In the list view, columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().

Property	Description
Status	Replication status. Synchronised, Synchronising, or Pending Synchronisation.
Source Name	Name of the source StoreOnce System.
Source Device	The name of the source VT library.
Target Name	Name of the target StoreOnce System.
Target Device	The name of the target VT library.
More properties	
Mapping Type	Replication Source or Replication Target
Name	Name that the StoreOnce System assigned to the replication mapping.
Hours Out of Sync	Number of hours that the replication mapping has been out of sync.
Recovery Active	Indicates whether data recovery is active.
Slots In Sync	The number of mapped VT library slots that are in sync.
Slots Out Of Sync	The number of mapped VT library slots that are out of sync.

VT Replication screen (individual mapping), Overview tab

Property	Description
Status bar	Replication status. Synchronised, Synchronising, or Pending Synchronisation.
Replication Source graphic	
Source Name	Name of the source StoreOnce System.
Source Device Name	The name of the source VT library.
Replication Summary graphic	
Number of Slots in Sync	The number of mapped VT library slots.
Number of mapped Slots	The number of mapped VT library slots that are in sync.
Replication Direction Arrow	The direction of replication. An arrow pointing from target to source indicates data recovery.
Average Throughput	Average throughput of the replication mapping in b/s.
Bandwidth Used	Bandwidth used for the replication mapping in Kb/s.
Replication Target graphic	
Target Name	Name of the target StoreOnce System.
Target Device Name	The name of the target VT library.

VT Replication screen (individual mapping), Details tab

Property	Description
Recovery Active	Indicates whether data recovery is active. (The replication direction is from target to source.)
Average Throughput	Average throughput of the replication mapping in b/s.
Bandwidth Used	Bandwidth used for the replication mapping in Kb/s.
Percentage Bandwidth Saved	The percentage of bandwidth saved during the replication job. The saving depends upon whether the device has been configured for source-side deduplication with a low-bandwidth transfer policy. Or with target-side deduplication with a high-bandwidth transfer policy.

Table Continued

Property	Description
Mapped Slots	Number of mapped slots.
Mapping Type	Replication source or target.
Out Of Sync Entries	
Number of Hours Out of Sync	Number of hours that the replication mapping has been out of sync.
Number of Slots Out Of Sync	Total number of mapped slots in the replication mapping that are out of sync.
Number of Slots Out Of Sync (Warning)	Number of mapped slots in the replication mapping that are out of sync, with a status of Warning.
Number of Slots Out Of Sync (Critical)	Number of mapped slots in the replication mapping that are out of sync, with a status of Critical.
Source and Target Details	
Library Name	The name of the VT library.
Replication Address	IP address of the StoreOnce System.
Replication Serial Number	Replication serial number of the StoreOnce System.
Total Slots	Total cartridge slots in the VT library.
User Data Stored	The amount of user data stored on the VT library.
Size on Disk	The actual size used on disk after deduplication.

VT Replication screen (individual mapping), Slots Mapping tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).
- To display all slot mapping properties in a **Details** flyout, click the information icon ( ) for the slot mapping.

Property	Description
Source Slot	Cartridge slot number in the source VT library.
Target Slot	Cartridge slot number in the target VT library.
Barcode	Bar code of the cartridge. The barcode is the same on the source and target.
Status	Status of the replication job.
User Data Stored	The amount of user data stored on the VT library.
More Properties	
Cartridge Size	The size of tape cartridges in the VT library.
Marked for Recovery	Indicates whether the data recovery option for the VT library is enabled.
Job Size	The amount of data in the replication job.
Duration	The length of time for the replication job to complete.
Time Start Sync	The date and time when synchronisation was started.
Last Sync Time	The date and time when the last synchronisation was completed.
Time Out of Sync	The amount of time that the replication mapping was out of sync.
Progress	The percentage of progress for the replication job.
Throughput	The replication job throughput in b/s.
Bandwidth Utilization	The replication job bandwidth in Kb/s.
Bandwidth Savings	The percentage of bandwidth savings for the replication mapping.

Viewing VT replication slot mappings

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Replication** above the graphic.
3. On the **VT Replication** screen, click the replication mapping.
4. On the screen for the VT replication mapping, click the **Slots Mapping** tab.

A list of slots is shown. To view more detail, click the information icon ( ) for the slot mapping.

Adding replication permissions for target VT libraries

Prerequisites

- The system level replication permission for the source StoreOnce system must have been previously added to the target StoreOnce system. Learn more: **VT libraries replication overview** on page 106.
- You know the replication serial number of the source StoreOnce system. Learn more: **Locating replication serial numbers** on page 152.

Procedure

1. On the main menu of the target StoreOnce system, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.
4. On the screen for the VT library, click the **Replication Permissions** tab.

   A list shows the source system replication permissions for the target VT library.
5. To add a source system to the list, expand the **Actions** menu and select **Add**.
6. On the **Add** dialog, paste in the replication serial number of the source StoreOnce System.

   When the action is complete, the replication serial number of the source StoreOnce System is added to the list.

Creating replication mappings for source VT libraries

Procedure

1. On the main menu of the source StoreOnce System, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Replication** above the graphic.
3. On the **VT Replication** screen, expand the **Actions** menu and select **Create**.

   The **Create** dialog enables you to specify the following:

   - **Source Library**
   - **Target System**
   - **Target Library**
   - **Mapped Slots**
   - **Target Library Data Recovery Option**

Editing replication mappings for source VT libraries

Procedure

1. On the main menu of the source StoreOnce System, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Replication** above the graphic.
3. On the **VT Replication** screen, click the VT library replication mapping.
4. On the screen for the VT library replication mapping, expand the **Actions** menu and select **Edit**.

Editing replication permissions for target VT libraries

Editing the replication access permission enables you to allow or disallow replication access to a target VT library.

Prerequisites

In this procedure, you must know the replication serial number of the source StoreOnce system. Learn more: **Locating replication serial numbers** on page 152.

Procedure

1. On the main menu of the target StoreOnce system, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the target VT library.
4. On the screen for the target VT library, click the **Replication Permissions** tab.

   A list shows the system replication serial numbers for the target VT library.
5. In the replication permissions list, click the replication serial number of the source StoreOnce System. Then, expand the **Actions** menu and select **Allow Replication**.

   On the **Edit Replication Access** dialog, you can allow or disallow replication to the target VT library.

Editing replication public access for target VT libraries

You can allow or disallow public access for replicating to a target VT library. When public access is allowed, any StoreOnce System can participate in replication to the target VT library.

Procedure

1. On the main menu of the target StoreOnce, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Libraries** above the graphic.
3. On the **VT Libraries** screen, click the VT library.
4. On the screen for the VT library, click the **Replication Permission** tab.
5. Click the **Public Access** item, and then expand the **Actions** menu and select **Allow Replication**.
6. On the **Edit Replication Access** dialog, you can allow or disallow public access replication to the target VT library.

Editing replication slot mappings for source VT libraries

Procedure

1. On the main menu of the source StoreOnce System, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Replication** above the graphic.
3. On the **VT Replication** screen, click the replication mapping.
4. On the screen for the replication mapping, expand the **Actions** menu and select **Edit**.
5. On the **Edit** dialog, **Mapped Slots** panel, click the edit icon ().

Deleting replication mappings for source VT libraries

Procedure

1. On the main menu of the source StoreOnce System, select **Data Services**.
2. On the **Data Services** screen, click the title **VT Replication** above the graphic.
3. On the **VT Replication** screen, click the VT replication mapping.
4. On the screen for the VT replication mapping, expand the **Actions** menu and select **Delete**.

Making replication target VT libraries visible to hosts

For an overview of VT libraries replication, see **VT libraries replication overview** on page 106.

Replication target VT libraries with Media Changer Port type "No Port" are not visible to hosts. You can make them visible by changing the Media Changer Port to iSCSI or Fibre Channel. Making a target VT library visible allows a backup application to:

- Move cartridges from storage slots to drives in the VT library.
- Perform read and verify operations on cartridges (but not write).
- Perform load and unload operations on tape devices.

Why make target VT libraries visible?

It can be useful to make a target VT library visible to:

- Confirm that replication is working correctly.
- Check the integrity of the replicated backup by doing a test restore.
- Use a backup application to perform manual tape copy jobs (sometimes called tape offload) to any tape device on the network.

⚠ **WARNING:** If a backup application can see both the source and target VT libraries, the application cannot distinguish between them. The reason is that the barcodes in the source and target VT libraries are duplicated in the two locations.

IMPORTANT: You cannot change data on a target VT library cartridge. You can only load it temporarily to a physical tape device to read it.

Best practices

WARNING: Failure to follow best practices can cause instability or damage your backup system and data. Cartridges can be marked as unusable or the backup application can attempt to write to target cartridges.

Procedure

1. Verify that no replication jobs to the selected target cartridge are in progress.
2. Verify that no backup jobs to the mapped source cartridges are scheduled.
3. Verify that the backup application media server is not in the same cell or domain as the source cartridge.
4. Import the data on the target cartridge into the backup application. This operation must be repeated after *each* replication operation to the cartridge.
5. Perform the desired operation on the cartridge, which may be:
   a. Verify the cartridge using the backup application, either with a verify command or by performing a restore.
   b. Copy the cartridge to a physical tape device connected to the media server.

Making a target device visible

- Create the replication mapping as normal. See **VT libraries replication overview** on page 106.
- From the host that has access to the target VT library, edit the target VT library. See **Editing VT libraries** on page 97.
- Click the **Interface Information** panel.
- On the **Interface Information** dialog, select the appropriate Fibre Channel or iSCSI configuration for the **Media Changer Port**. Click **OK** and then click **Update**.
- Make the target VT library visible from other hosts. Configure the Fibre Channel fabric to make the host visible. Target visibility persists even if the power fails or if the replication mapping is removed.

To remove visibility to the target VT library, reset the **Media Changer Port** to None.

NAS data services

IMPORTANT: The StoreOnce network share is intended to be used only by backup applications that “back up to disk”. Do not use the NAS target device as a drag-and-drop general file store, unless seeding a StoreOnce System for replication.

NAS licensing requirements

- No licensing is required for StoreOnce NAS emulations unless using Encryption of Data at Rest.
- If StoreOnce NAS replication is used, a license on the target StoreOnce System is required. Self-replication does not require a license.

Protocol Support

- NFS version 3 is supported over IPv4 and IPv6.
- NFS version 4 is not supported.
- SMB versions 2 and 3 supported over IPv4 only.
- SMB version 1 is not supported due to security vulnerabilities.

NAS shares

Viewing NAS shares

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, do one of the following:
   - To view all NAS shares, click the title **NAS Shares** above the graphic.
   - To view shares that have a specific status, click the status on the graphic. For example, clicking the Warning status on the graphic opens the **NAS Shares** screen and displays only shares that have a Warning status.
3. On the **NAS Shares** screen, click the NAS share.
   The screen for an individual NAS share includes tabs for **Overview**, **Details**, **Network Paths**, **Permissions**, and **Replication Permissions**.

NAS shares screens and properties

NAS Shares screen (all shares)

In the list view, columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().

Property	Description
Name	Name of the NAS share.
Status	The status of the share. Online, offline, not started, failed to start, stopping, creating, or deleting
User Data Stored	The amount of user data stored on the NAS share.
Size on Disk	The actual size used on disk after deduplication.
Dedupe Ratio	The deduplication ratio achieved on the data on the NAS share. All NAS shares have deduplication enabled. Deduplication on NAS shares cannot be disabled.
Replication Role	The replication role of the NAS share. Non-Replicating, Replication Source, or Replication Target.
More properties	
Number of Files	The number of files and directories on the NAS share.
Protocol	CIFS (Common Internet File System) or NFS (Network File System)
Physical Storage Quota	This quota is for the amount of data written to disk after deduplication. If the quota is enabled and the limit is reached, backups will fail to prevent the quota from being exceeded. The quota allows you to partition the physical capacity of the StoreOnce System between various users (and users with a better deduplication ratio can store more data). When a NAS share reaches its quota, the status of the share will change to “Physical Quota Reached”. Restores from that share are permitted but new backups will fail. When the quota is no longer met, either by increasing the quota or by expiring backups, the share status returns to the “OK” state. If you use this feature in conjunction with client permissions to control of client access to the share, you can effectively define how much space a particular user is allowed to use on the StoreOnce System. With many users using the same system, this approach allows you to control how much disk space is available to individual users. **TIP:** If capacity management is required, Hewlett Packard Enterprise recommends configuring backup applications with quotas to reroute to another device or to postpone backups to prevent backups from failing unexpectedly.

Table Continued

Property	Description
Logical Storage Quota	This quota is for the amount of data a user sends to the device before deduplication. If the quota is enabled and the quota limit is reached, backups will fail in order to prevent the quota from being exceeded. This allows you to provide a service to back up a particular amount of user data. For example, set this when you charge customers per TB of user data protected. When a NAS share reaches its quota, the status of the share will change to “Logical Quota Reached”. Restores from that share are permitted but new backups will fail. When the quota is no longer met, either by increasing the quota or by expiring backups, the share status returns to the “OK” state. If you use this feature in conjunction with Client-Permissions to control a client’s access to the share, you can effectively define how much space a particular user is allowed to use on the . With many users using the same system, this allows you to control how much disk space is available to individual users. **NOTE:** If capacity management is required, Hewlett Packard Enterprise recommends configuring backup applications with quotas to reroute to another device or to postpone backups to prevent backups from failing unexpectedly.
Encryption	Indicates whether the NAS share data is encrypted. Shows as Not Licensed if there is no encryption license on the StoreOnce System. If encryption is licensed, shows as Enabled or Disabled.
Secure Erase Mode	The availability of HPE Secure Erase. Shows as Disabled or the number of Secure Erase passes.

NAS Shares screen (individual share), Overview tab

Property	Description
Status bar	The status of the NAS share. Shows as Online, Down, or Error.
Share Dedupe Ratio	The deduplication ratio achieved on the data on the NAS share. All NAS shares have deduplication enabled. Deduplication on NAS shares cannot be disabled.
User Data Stored	The amount of user data stored on the NAS share.
Size on Disk	The actual size used on disk after deduplication.

NAS Shares screen (individual share), Details tab

Property	Description
Name	Name of the NAS share.
Description	A text description of the share (optional).
Access Protocol	CIFS (Common Internet File System) or NFS (Network File System)
Replication Role	The replication role of the NAS share. Non-Replicating, Replication Source, or Replication Target.
Share Version	NAS shares can be configured as version 2 (default) or version 1. The primary difference is the maximum number of items permitted per share. (An item is a file or a directory) • Version 1 NAS shares: 25,000 items • Version 2 NAS shares: 1,000,000 items Also, version 2 NAS shares are optimized to improve performance with Commvault backup software. Version 1 NAS shares are only recommended for replication compatibility with legacy StoreOnce systems that only support version 1 NAS shares. Once configured, you can change the NAS share version from 1 to 2 but you cannot change from 2 to 1. The maximum number of NAS shares depends upon the product model and the number of other devices (including VT libraries and StoreOnce Catalyst stores) already created.
Number of Files/ Directories	The number of files and directories on the NAS share.
Write Protection	Used to prevent further backup to the share. If enabled, any backup jobs currently using that share will fail.
Security	
Encryption Enabled	Indicates whether the NAS share data is encrypted. Shows as Not Licensed if there is no encryption license on the StoreOnce System. If encryption is licensed, shows as Enabled or Disabled.
Secure Erase Mode	The availability of HPE Secure Erase. Shows as None or the number of Secure Erase passes.
Storage	

Table Continued

Property	Description
Physical Storage Quota	This quota is for the amount of data actually written to disk after deduplication. If the quota is enabled and the quota limit is reached, backups will fail in order to prevent the quota from being exceeded. The quota allows you to partition the physical capacity of the StoreOnce System between various users (and users with a better deduplication ratio can store more data). When a NAS share reaches its quota, the status of the share will change to “Physical Quota Reached”. Restores from that share are permitted but new backups will fail. When the quota is no longer met, either by increasing the quota or by expiring backups, the share status returns to the “OK” state. If you use this feature in conjunction with client permissions to control a client’s access to the share, you can effectively define how much space a particular user is allowed to use on the StoreOnce System. With many users using the same system, this allows you to control how much disk space is available to individual users.  **TIP:** If capacity management is required, Hewlett Packard Enterprise recommends configuring backup applications with quotas to reroute to another device or to postpone backups to prevent backups from failing unexpectedly.
Logical Storage Quota	This quota is for the amount of data a user sends to the device before deduplication. If the quota is enabled and the quota limit is reached, backups will fail in order to prevent the quota from being exceeded. This allows you to provide a service to back up a particular amount of user data. For example, set this when you charge customers per TB of user data protected. When a NAS share reaches its quota, the status of the share will change to “Logical Quota Reached”. Restores from that share are permitted but new backups will fail. When the quota is no longer met, either by increasing the quota or by expiring backups, the share status returns to the “OK” state. If you use this feature in conjunction with Client-Permissions to control a client’s access to the share, you can effectively define how much space a particular user is allowed to use on the . With many users using the same system, this allows you to control how much disk space is available to individual users.  **TIP:** If capacity management is required, Hewlett Packard Enterprise recommends configuring backup applications with quotas to reroute to another device or to postpone backups to prevent backups from failing unexpectedly.
Backup Details	

Table Continued

Property	Description
Backup Application	The name and information about the backup application that is used to back up to the NAS share. The information is optional, but is recommended as an aid to HPE support troubleshooting. The information has no impact on performance or deduplication efficiency.
Data Type	The type of data being protected by the backups to this NAS share. The information is optional, but is recommended as an aid to HPE support troubleshooting. The information and has no impact on performance or deduplication efficiency.

NAS Shares screen (individual share), Network Paths tab

Property	Description
Path	The network paths used to access the configured NAS share.

NAS Shares screen (individual share), Permissions tab

Property	Description
Access Protocol	CIFS (Common Internet File System) or NFS (network file system).
Authorisation	
Authorisation mode	Authorisation mode applies only to CIFS NAS shares. The modes are: None, User, or AD (Active Directory). • None mode provides a simple CIFS server configuration that allows creation of shares with no authorization. Any user or computer can mount and access the shares. • User mode secures CIFS shares so they can be accessed only by specified users. The users must have local account credentials on the StoreOnce System. • Active Directory mode secures CIFS shares so they can be accessed only by specified users or groups. The users or groups must be within an Active Directory domain to the CIFS server.
User Access	
User Name (and access)	Name of a user for the NAS share. Access to a NAS share can be enabled and disabled for the user.

NAS Shares screen (individual share), Replication Permissions tab

Property	Description
Replication Serial Number (and access)	The replication serial number that is automatically generated by the StoreOnce System. This replication serial number is used for all replication jobs. The replication serial number does not change. The replication serial number for a StoreOnce System is different than its serial number. When Public Access is allowed, any StoreOnce System can participate in replication of the NAS share.

Viewing NAS shares detail

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS** above the graphic.
3. On the **NAS Shares** screen, click the NAS share.
4. On the **NAS Shares** screen for the share, click the **Details** tab.

Creating NAS shares

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS** above the graphic.
3. On the **NAS Shares** screen, expand the **Actions** menu and select **Create**.

   The **Create** dialog allows you to specify the following:

   - **NAS Share Name**
   - **Access Protocol** (CIFS or NFS)
   - **Security Settings**
   - **Backup Application Details**
   - **Advanced Settings**

Editing NAS shares

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS** above the graphic.

3. On the **NAS Shares** screen, click the share.
4. On the screen for the share, expand the **Actions** menu and select **Edit**.

   The **Edit** dialog allows you to specify the following:

   - **Security Settings**
   - **Backup Application Details**
   - **Advanced Settings**

Tips for editing NAS shares

- Users with the administrator role can edit the following:
  - **Security Settings**: Secure Erase Mode. You can enable Secure Erase and select the number of Overwrite Passes. This property does not appear until after the NAS share is created.
  - **Backup Application Details**: Backup Application and Type
  - **Advanced Settings**: Description, Write Protection, and Storage Quotas. Write protection prevents access initially, or protects data after it has been backed up.
- Data at Rest Encryption cannot be edited. This feature is only enabled or disabled at the time of NAS share creation.
- You cannot change the NAS share name after it is created.

  If a NAS share is converted from Read/Write to Read Only, any open items will be forced closed, which may result in inconsistencies if they are being written to by a backup application. The user will be warned that this could occur before the change is made.
- The Network Path tab is not available for when you select **Edit**. However, if you display the Network Paths tab, you can copy the share path if required. If your StoreOnce System is configured on a Virtual LAN, this tab will display all the VLAN IP addresses available for that share.

Deleting NAS shares

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS Shares** above the graphic.
3. On the **NAS Shares** screen, click the share.
4. On the screen for the share, expand the **Actions** menu and select **Delete**.

NAS CIFS shares

Overview of creating backup target shares that Windows users can access.

Procedure

1. Confirm or select the NAS CIFS authentication mode for the StoreOnce System. See **Selecting NAS CIFS authentication modes** on page 123.
2. Create NAS CIFS shares on the StoreOnce System. See **Creating NAS shares** on page 121.
3. Define access rights to the NAS CIFS shares. Do one of the following:

   - If you are using User authentication:
     - Add local user accounts for the StoreOnce System. See **Adding NAS CIFS local users** on page 124.
     - Enable or disable user access to individual shares. See **Editing NAS CIFS shares user access** on page 125.
   - If you are using Active Directory authentication, configure the Active Directory server and the StoreOnce System. See **NAS CIFS Active Directory authentication overview** on page 125

NAS CIFS authentication modes

The CIFS authentication mode is a setting for all NAS CIFS shares on a StoreOnce System.

- **None**. Provides a simple CIFS server configuration that allows for the creation of shares with no authentication. Any user or computer can mount and access the shares created on the StoreOnce System with this setting.

  This mode is the default authentication mode for the CIFS server where all the Shares configured have its Permission disabled. Because this mode is the default, there is no user action required to activate this mode. Proceed to mounting the share on your Windows client.
- **User**. Secures CIFS shares so they can be accessed only by specified users. The users must have local account credentials on the StoreOnce System.

  Once the CIFS server authentication mode is set to user, you can use the **Permissions** tab of the share to add and remove users. You can also edit the access for specific users.
- **Active Directory**. Secures CIFS shares so they can be accessed only by specified users or groups. The users or groups must be within an Active Directory domain to the CIFS server.

Prerequisites:

- Domain Name
- Domain Controller on supported server. See the *HPE StoreOnce Support Matrix* **https://www.hpe.com/Storage/StoreOnceSupportMatrix**.
- A user account on the Domain Controller, which is the Domain Administrator or delegated user with Domain Administrative rights.
- A user account on the server running DNS to add entries.
- The system time on the StoreOnce System must be correct and in sync with the domain controller.

Selecting NAS CIFS authentication modes

The CIFS authentication mode is a setting for all NAS CIFS shares on a StoreOnce System. Learn more: **NAS CIFS authentication modes** on page 123.

WARNING: If you change the CIFS authentication mode:

- Running backups and restores will fail.
- To make the new setting take effect on the client, log out of the client and then log back in.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Server** tab.
3. On the **Settings** panel, click the edit icon ( ).
4. On the **CIFS Settings** dialog, select the **Authentication Mode**, and then click **Update**.

NAS CIFS server user authentication mode

Adding NAS CIFS local users

Prerequisites

The CIFS server authentication mode for the StoreOnce System is set to user.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Server** tab.
3. On the **Users** panel, expand the **Actions** icon and select **Add User**.
4. On the **Add User** dialog, enter a user name and the password that you want to use.

   - The user name can be up to 64 characters.
   - The password must be at least eight characters long and can include special characters.
   - The password can comply with the Windows strong password requirements: uppercase letters (A,B,C) or lowercase letters (a,b,c) or numbers (0,1,2,3,4,5,6,7,8,9) or symbols (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /).
5. Click **Add**.

   The new user is added to the list in the Users panel. By default, new users are added to a StoreOnce System with Access to NAS CIFS shares disabled.

TIP: To enable access to a specific NAS CIFS share, navigate to the share and click the **Permissions** tab. Then select the user and click its edit icon ( ).

Changing NAS CIFS local user passwords

Prerequisites

The CIFS server authentication mode is set to user.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Server** tab.
3. On the **Users** panel, select the user, and then expand the **Actions** icon and select **Edit User**.
4. On the **Edit User** dialog, enter and confirm the new password, and then click **Update**.

   The new password takes effect immediately.

Deleting NAS CIFS local users

Prerequisites
The CIFS server authentication mode is set to user.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Server** tab.
3. On the **Users** panel, select the user, and then expand the **Actions** icon and select **Remove User**.

Editing NAS CIFS shares user access

You can enable and disable access by specific users to individual NAS CIFS shares.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS** above the graphic.
3. On the **NAS Shares** screen, click the CIFS NFS share.
4. On the **NAS Shares** screen for the NAS CIFS share, click the **Permissions** tab.
5. On the **User Access** panel, click the user, and then click the edit icon ( ). The **Edit User Access** dialog opens. Enable of disable **Access**.

Active Directory authentication mode

NAS CIFS Active Directory authentication overview

Process overview:

Procedure

1. **Adding StoreOnce Systems to Active Directory domains** on page 126
2. **Granting Active Directory domain users access to NAS CIFS shares** on page 127

3. **Adding Active Directory users as local administrators to the StoreOnce CIFS server** on page 128
4. **Adding Active Directory groups as local administrators to the StoreOnce CIFS server** on page 129

Adding StoreOnce Systems to Active Directory domains

- To add a StoreOnce System, you must know the Active Directory domain name and the credentials of an Active Directory user that has permission to add the StoreOnce System to the domain.
- **WARNING:** To add a StoreOnce System, you must use the StoreOnce **Join** action. Joining or leaving an Active Directory domain will cause running backup and restore jobs on a StoreOnce System to fail. Do not perform this procedure if the StoreOnce System has backup or restore jobs running.

Prerequisites

- **IMPORTANT:**
  - Verify that the StoreOnce System has an entry in the DNS server. The DNS entry is required so the StoreOnce System can be resolved by referring to its qualified domain name. (StoreOnce Systems do not automatically add themselves to DNS server configurations during network configuration.).

    If the StoreOnce System does not have a DNS entry, you must manually create the entry before proceeding.
  - StoreOnce port sets and DNS entries on the **Networking** screen must be configured correctly. The networking settings must allow the StoreOnce System contact the Active Directory server and resolve its host name.
  - The system time on StoreOnce System and the Active Directory server must be in sync.

Procedure

On the StoreOnce System

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Server** tab.
3. On the **CIFS Server** tab, click the edit icon ( ) on the **Settings** panel.
4. On the **CIFS Settings** dialog, select **Active Directory** for the **Authentication Mode**.
5. Enter the name of the Active Directory **Domain** to which you want to join the StoreOnce System, and then click **Update**.

   The **Join Active Directory** dialog opens.
6. On the **Join Active Directory** dialog, enter the user name and password to join the Active Directory domain, and then click **Join**.

- The StoreOnce System is added to the domain and the **CIFS Server** tab displays the Active Directory information. (Joining can take some time, depending on topology and domain size.).
- The **Local Administrators** panel shows the domain users that can be delegated to manage the CIFS Server of the StoreOnce System. To add local administrators, see **Adding and deleting NAS CIFS Active Directory users and groups** on page 140.

On a Windows domain management system

7. Verify that there is an entry for the StoreOnce CIFS server.

   On a Windows server that is used to perform Active Directory domain configuration, launch the **Active Directory Users and Computers** management tool. For example, enter `dsa.msc` in the Windows **Run command**. Or from a PC with the Microsoft **Remote Server Administration Tools** installed, launch from **Administrative Tools**).

Granting Active Directory domain users access to NAS CIFS shares

This procedure uses the Windows Computer Management Console to grant Active Directory domain users access to StoreOnce NAS CIFS shares.

Prerequisites

The CIFS server authentication mode for the StoreOnce System is set to Active Directory.

Procedure

Microsoft Management Console

1. On the Windows client, open the Microsoft Management Console (MMC). For example, select **Start** > **Run** > **mmc**.
2. From the MMC menu, browse through **FileAdd/Remove Snap-in**.
3. The **Add or Remove Snap-ins** window opens. Browse through the list of **Available Snap-ins** and search for **Shared Folders**.
4. Select the **Shared Folders** snap-in.
5. Click **Add**. The **Shared Folders** window opens.
6. Select **Another Computer** and enter the fully qualified domain name of the StoreOnce System. This step can also be done by clicking **Browse** and searching for the StoreOnce System.
7. In the **View** section of the window, select **Shares**. Complete the snap-in configuration by clicking **Finish**.
8. Click **OK** to complete the snap-in addition.

   The snap-in is now added to the MMC console. This setting can be saved for future management of the StoreOnce System NAS CIFS shares.

9. Expand the **Shares** list to see the shares configured on the StoreOnce System.
10. Select the share you want to assign domain users or groups to access. Right-click on the share and select **Properties**.

    The **Share Properties** screen will open. A new share created will have no users or groups assigned to it.

11. Select the **Share Permissions** tab and click **Add**.

12. Enter the domain user name to be added. Verify by the domain user name by clicking **Check Names**. Once the user is verified, click **OK**.
13. Assign the permission you want the domain user to have for this share.
14. Click **OK** to confirm the changes.

    It is now possible to access the newly created share from any Windows server on the domain using the credentials of anyone who has permission to access the share. If a permitted user is logged into Windows, access to the share is granted automatically with those permissions.

    IMPORTANT: When switching from None or User authentication mode to Active Directory authentication mode, HPE recommends logging out and then back in to the Windows client where the share is mounted. This approach ensures that the new authentication settings of the CIFS server are enforced.

    NOTE: The StoreOnce System does not support creating shares from Windows Computer Management Consoles. Shares must be created from the StoreOnce Management Console.

    The StoreOnce System only supports the Shared Folders utility within the Windows Computer Management. Any other Windows Computer Management utilities are not supported.

Adding Active Directory users as local administrators to the StoreOnce CIFS server

After a StoreOnce System is added to an Active Directory domain, the **Local Administrators** panel is displayed on the **CIFS server** tab of the **NAS Settings** screen.

- The **Local Administrators** panel allows you to add Active Directory domain users or groups with administrator privileges to the CIFS server. Adding users or groups using the StoreOnce Management Console provides a way of implementing Delegated Administration, which is not available for the StoreOnce device from the Active Directory Management tool.
- Users are added using the Active Directory login name. This name is available from the user account information from the Active Directory Management tool. (Right-click the domain user from the domain controller, select **Properties**, and check the domain user account information.)

  Both user login formats are accepted. For example, <domain_user@domain> or <domain \domain_user>. The user is resolved against the domain controller database.
- **IMPORTANT:** When adding Active Directory domain users through a StoreOnce Management Console, the users are automatically added as Local Administrators. (Even if they are not administrator users on the Active Directory domain.)

Prerequisites

- The StoreOnce System has been added to an Active Directory domain.
- The user or group to be added must already exist in the Active Directory domain.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Servers** tab.

3. On the **Local Administrators** panel, expand the **Actions** menu and select **Add Users or Groups**
4. On the **Add Users or Groups** dialog, enter the user name in the **Member Name** box, and then click **Add**.

   The user is added to the list of local administrators.

Adding Active Directory groups as local administrators to the StoreOnce CIFS server

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Servers** tab.
3. On the **Local Administrators** panel, expand the **Actions** menu and select **Add Users or Groups**
4. On the **Add Users or Groups** dialog, in the group name in the **Member Name** box, and then click **Add**.

   The group is added to the list of local administrators.

Deleting Active Directory users or groups as local administrators of the StoreOnce CIFS server

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Servers** tab.
3. On the **Local Administrators** panel, select the **Member**, and then expand the **Actions** menu and select **Delete Users or Groups**
4. On the **Delete Members** dialog, click the acknowledgment check box, and then click **Delete**.

   The user or group is deleted from the list of local administrators.

Leaving Active Directory domains

You may want a StoreOnce System to leave Active Directory domains to:

- Temporarily leave, then rejoin the StoreOnce System to the same Active Directory domain.
- Join the StoreOnce System to a different Active Directory domain.
- Change the StoreOnce System to another CIFS server authentication mode.

⚠ **WARNING:** Leaving an Active Directory domain prevents the member users and groups from accessing NAS CIFS shares on the StoreOnce System.

Prerequisites

The StoreOnce System is joined to an Active Directory.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Server** tab.
3. On the **Settings** panel, expand the **Actions** menu and select **Leave Active Directory**.

NFS shares

Overview of configuring backup target shares that UNIX and Linux servers can access.

1. Add NFS hosts to the StoreOnce System. These hosts are the servers that mount the NAS NFS shares. See **Adding NAS NFS server hosts** on page 130.
2. Create NAS NFS shares on the StoreOnce System. See **Creating NAS shares** on page 121.

   TIP: When NAS NFS shares are created, read/write access is enabled for all hosts. If you want to restrict access, you must edit the access property of the share.
3. Enable or disable host access by editing the access type on individual NAS NFS shares. See **Editing NAS NFS shares host access** on page 131.

Adding NAS NFS server hosts

This procedure adds a NAS NFS host to a StoreOnce System.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **NFS Servers** tab.
3. On the **Host List** panel, expand the **Actions** menu and select **Add Host**.
4. On the **Add Host** dialog, enter the name that you want to use for the host (required) and a description (optional). Click **Add**.

   The new NAS NFS server host is added to the list.

Editing NAS NFS settings (browsability)

NAS NFS settings include an NFS browsability setting. The setting allows you to enable or disable browsability to NFS shares.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **NFS Server** tab.
3. On the **Settings** panel, click the edit icon ( ).

Editing NAS NFS shares host access

In the list of hosts, the * (asterisk) host name represents any/all hosts.

IMPORTANT: To restrict host access to specific hosts, you should first set the access type for any/all hosts to No Access, and then add individual hosts and their access types.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS** above the graphic.
3. On the **NAS Shares** screen, click the NAS NFS share.
4. On the **NAS Shares** screen for the NAS NFS share, click the **Permissions** tab.
5. On the **Host List** panel, click the host, and then click the edit icon ( ). The **Edit Host Access** dialog opens.

Replicating NAS shares

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS** above the graphic.
3. On the **NAS Shares** screen, click the panel for the specific NAS share.
4. On the **NAS Shares** screen for the specific share, select **Start Replication** on the **Actions** menu.

Restarting NAS share replication jobs

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS** above the graphic.
3. On the **NAS Shares** screen, click the panel for the specific NAS share.
4. On the **NAS Shares** screen for the specific share, click the **Replication Info** tab, and then click the information icon ( ) for the share mapping.
5. On the **Share Mapping** screen for the share, click the **File Details** tab, and then click the information icon ( ) for the file.
6. On the **File Details** dialog, click the **Restart Job** button.

NAS replication

The following topics are specific to NAS replication. For replication settings that apply to both NAS replication and VT replication, see **Viewing replication settings** on page 143.

NAS shares replication overview

TIP: NAS replication requires a 1:1 relationship from a source StoreOnce System to a target StoreOnce System. Replicating from multiples sources to a single target (fan-in) is not supported with NAS replication. (Fan-in is supported for VT replication and StoreOnce Catalyst replication.)

Prerequisites

This overview assumes that the source and target NAS shares exist. If you have not created the source and target NAS shares, see **Creating NAS shares** on page 121.

Procedure

Create partner systems relationship

1. On the source StoreOnce System, create a partner system relationship between the source and target system. Lean more: **Adding replication target systems** on page 137.

   TIP: After a partner system relationship has been created, you do not need to perform this step again.

Establish system-level replication permission

2. On the target StoreOnce system, establish replication permission between the source system and the target system. Learn more: **Adding replication permissions for target systems** on page 153.

   TIP: After system-level replication permission has been established, you do not need to perform this step again.

Establish NAS share replication permission

3. On the target StoreOnce system, select the target NAS share and establish replication permission for the share. Learn more: **Adding replication permissions for target NAS shares** on page 137.
4. On the target StoreOnce system, turn on (allow) replication to the target NAS share. Learn more: **Editing replication permissions for target NAS shares** on page 138.

Create NAS share replication mapping

5. On the source system, select the source NAS share and create replication mapping for the share. Learn more: **Creating replication mappings for source NAS shares** on page 137.

Viewing NAS replication mappings

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, do one of the following:

   - To view all NAS replication mappings, click the title **NAS Replication** above the graphic.
   - To view NAS replication mappings that have a specific status, click the status on the graphic. For example, clicking the Warning status on the graphic opens the **NAS Replication** screen and displays only NAS replication mappings that have a Warning status.

3. On the **NAS Replication** screen, click the NAS replication mapping.

The screen for an individual NAS replication mapping includes tabs for **Overview**, **Details**, and **File Information**.

NAS replication screens and properties

NAS Replication screen (all mapping)

TIP: In the list view, columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).

Property	Description
Status	Replication status. Synchronised, Synchronising, or Pending Synchronisation.
Source Name	Name of the source StoreOnce System.
Source Device	The name of the source NAS share.
Target Name	Name of the target StoreOnce System.
Target Device	The name of the target NAS share.
More properties	
Mapping Type	Replication Source or Replication Target
Name	Name that the StoreOnce System assigned to the replication mapping.
Hours Out of Sync	Number of hours that the replication mapping has been out of sync.
Recovery Active	Indicates whether data recovery is active.
Entries In Sync	The number of mapped NAS share entries that are in sync.
Entries Out Of Sync	The number of mapped NAS share entries that are out of sync.
Protocol	CIFS (Common Internet File System) or NFS (Network File System)

NAS Replication screen (individual mapping), Overview tab

Property	Description
Status bar	Replication status. Synchronised, Synchronising, or Pending Synchronisation.
Replication Source graphic	
Source Name	Name of the source StoreOnce System.
Source Device Name	The name of the source NAS share
Replication Summary graphic	
Entries in Sync	The number of mapped entries.
Mapped Entries	The number of mapped entries that are in sync.
Replication Direction Arrow	The direction of replication. An arrow pointing from target to source indicates data recovery.
Average Throughput	Average throughput of the replication mapping in b/s.
Bandwidth Used	Bandwidth used for the replication mapping in Kb/s.
Replication Target graphic	
Target Name	Name of the target StoreOnce System.
Target Device Name	The name of the target NAS share.

NAS Replication screen (individual mapping), Details tab

Property	Description
Recovery Active	Indicates whether data recovery is active. (The replication direction is from target to source.).
Average Throughput	Average throughput of the replication mapping in b/s.
Bandwidth Used	Bandwidth used for the replication mapping in Kb/s.
Percentage Bandwidth Saved	The percentage of bandwidth saved during the replication job. The saving depends upon whether the device has been configured for source-side deduplication with a low-bandwidth transfer policy. Or with target-side deduplication with a high-bandwidth transfer policy.

Table Continued

Property	Description
Mapping type	Replication source or target.
Out of Sync Entries	
Number of Hours Out of Sync	Number of hours that the replication mapping has been out of sync.
Number of Entries Out Of Sync	
Number of Entries Out Of Sync (Warning)	Number of mapped entries in the replication mapping that are out of sync, with a status of Warning.
Number of Entries Out Of Sync (Critical)	Number of mapped entries in the replication mapping that are out of sync, with a status of Critical.
Source and Target Details	
Share Name	The name of the NAS share.
Replication Address	IP address of the StoreOnce System.
Replication Serial Number	Replication serial number of the StoreOnce System.
Total Entries	Total number of entities in the NAS share.
User Data Stored	The amount of user data stored on the NAS share.
Size on Disk	The actual size used on disk after deduplication.

NAS Replication screen (individual mapping), File Information tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().
- To display the properties in a **Details** flyout, click the information icon ().

Property	Description
Entry	NAS share entry number.
Type	Directory or file.

Table Continued

Property	Description
File Name	Name of the directory or file.
Status	Replication status. Synchronised, Synchronising, or Pending Synchronisation.
More properties	
Marked For Recovery	Indicates whether the data recovery option for the NAS share is enabled.
File Size	Size of the file.
Duration	The length of time for the replication job to complete.
Time Start Sync	The date and time when synchronisation was started.
Last Sync Time	The date and time when the last synchronisation was completed.
Time Out of Sync	The amount of time that the replication mapping was out of sync.
Progress Phase 1	The percentage of progress for the replication job in phase 1. Phase 1 replicates the main file data.
Progress Phase 2	The percentage of progress for the replication job in phase 2. Phase 2 replicates internally written write-in-place data that is associated with a file.
Progress Phase 3	The percentage of progress for the replication job in phase 3. Phase 3 replicates metadata that is associated with a file.
Throughput	The replication job throughput in b/s.
Bandwidth Utilization	The replication job bandwidth in Kb/s.
Bandwidth Savings	The percentage of bandwidth savings for the replication mapping.

Viewing NAS replication file information

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS Replication** above the graphic.
3. On the **NAS Replication** screen, click the replication mapping.
4. On the screen for the NAS replication mapping, click the **File Information** tab.

A list of files is shown.

5. To view the details for a file, click its information icon ().

Adding replication permissions for target NAS shares

Prerequisites

To add replication permissions:

- The system level replication permission for the source StoreOnce system must have been previously added to the target StoreOnce system. Learn more: **NAS shares replication overview** on page 132.
- You know the replication serial number of the source StoreOnce system. Learn more: **Locating replication serial numbers** on page 152.

Procedure

1. On the main menu of the target StoreOnce system, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS Shares** above the graphic.
3. On the **NAS Shares** screen, click the NAS share.
4. On the screen for the NAS share, click the **Replication Permissions** tab.

   A list shows the source system replication permissions for the target NAS share.
5. To add a source system to the list, expand the **Actions** menu and select **Add**.
6. On the **Add** dialog, paste in the replication serial number of the source StoreOnce System.

   When the action is complete, the replication serial number of the source StoreOnce System is added to the list.

Adding replication target systems

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Partner Systems** tab.
3. Expand the **Actions** menu and select **Add**.

Creating replication mappings for source NAS shares

Procedure

1. On the main menu of the source StoreOnce System, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS Replication** above the graphic.
3. On the **NAS Replication** screen, expand the **Actions** menu and select **Create**.

   The **Create** dialog enables you to specify the following:

- **Source Share**
- **Target System**
- **Target Share**
- **Target Share Data Recovery Option**

Editing replication mappings for source NAS shares

Procedure

1. On the main menu of the source StoreOnce System, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS Replication** above the graphic.
3. On the **NAS Replication** screen, click the NAS share replication mapping.
4. On the screen for the NAS share replication mapping, expand the **Actions** menu and select **Edit**.

Editing replication permissions for target NAS shares

Editing the replication access permission enables you to allow or disallow replication access to a target NAS share.

Prerequisites

In this procedure, you must know the replication serial number of the source StoreOnce system. Learn more: **Locating replication serial numbers** on page 152.

Procedure

1. On the main menu of the target StoreOnce system, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS Shares** above the graphic.
3. On the **NAS Shares** screen, click the target NAS share.
4. On the screen for the target NAS share, click the **Replication Permissions** tab.

   A list shows the source system replication serial numbers for the target NAS share.
5. In the replication permissions list, click the replication serial number of the source StoreOnce System. Then, expand the **Actions** menu and select **Allow Replication**.

   On the **Edit Replication Access** dialog, you can allow or disallow replication to the target NAS share.

Editing replication public access for target NAS shares

You can allow or disallow replication access for a NAS share. When public access is allowed, any StoreOnce System can participate in replication of the NAS share.

Procedure

1. On the main menu of the target StoreOnce System, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS Shares** above the graphic.
3. On the **NAS Shares** screen, click the target NAS share.

4. On the screen for the target NAS share, click the **Replication Permissions** tab.
5. Click the **Public Access** item, and then expand the **Actions** menu and select **Allow Replication**.
6. On the **Edit Replication Access** dialog, you can allow or disallow replication to the target NAS share.

Deleting replication mappings for source NAS shares

Procedure

1. On the main menu of the source StoreOnce System, select **Data Services**.
2. On the **Data Services** screen, click the title **NAS Replication** above the graphic.
3. On the **NAS Replication** screen, click the NAS replication mapping.
4. On the screen for the NAS replication mapping, expand the **Actions** menu and select **Delete**.

Recovering replicating NAS shares over a WAN

In this scenario, a remote source site has lost its host servers and StoreOnce System. New server hardware has been purchased and installed at the site, and the administrator must recover data to a new server. A new StoreOnce system has not been installed at the remote site.

The administrator plans to recover data over a WAN from a StoreOnce System at a data center. (Which will take a long time.)

Before the failure, a replication mapping existed between the source NAS share (at the remote site) and the target NAS share (at the data center). After the failure, the replication mapping still exists, but the source NAS share is missing at the remote site. The target NAS share on the StoreOnce System at the data center is still in target-share mode. It has not had its replication mapping removed.

TIP:

- The following procedure retains the ability to back up to the target NAS share. If backing up to the target NAS share is not required, an easier solution might be to recover data directly from the target NAS share, which is read-only.
- Recovering high volumes of data over a WAN can take a long time. Recovering data at the data center is much faster. And once recovered, the recovered data can be transported to the remote site.

WARNING: If you replace the storage disks on a source StoreOnce System — and keep the system — the source to target mapping will still exist. Therefore, **you must remove the replication mapping before performing a recovery**.

If the replication mapping is not removed, the blank source NAS share (on the replacement storage disks) will overwrite the target NAS share. Effectively losing backup data on both the source and target NAS shares.

Procedure

1. On the target StoreOnce System in the data center, remove the replication mapping.

a. Navigate to the **NAS Replication** screen. See **Viewing NAS replication mappings** on page 132

b. Select the NAS replication mapping.

c. Remove the replication mapping. See **Deleting replication mappings for source NAS shares** on page 139

2. The target NAS share at the data center becomes a nonreplicating NAS share.
3. Make sure that the backup application is targeting the newly nonreplicating NAS share at the data center. Recover the data using the backup application at the data center.
4. At this point, there is no source StoreOnce System at the remote site. If one is installed at a later date, reverse recover the data and configure the replication mapping.

NAS settings

Viewing NAS settings

The **NAS Settings** screen allows you to view and manage NAS settings.

Procedure

1. Do one of the following:

   - On the main menu, select **Data Services**. On the **Data Services** screen, expand the **Actions** menu and select **NAS Settings**.
   - On the main menu, select **Settings**. On the **Settings** screen, under **Data Services**, click the **NAS Settings** panel.

2. The **NAS Settings** screen includes tabs for **CIFS Server** and **NFS Server**.

Adding and deleting NAS CIFS Active Directory users and groups

NAS CIFS Active Directory users and groups (if any) are listed on the **Local Administrators** panel of the **CIFS Server** tab of the **NAS Settings** screen.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.

2. On the **NAS Settings** screen, click the **CIFS Servers** tab.
3. Scroll to the **Local Administrators** panel.

   TIP: If the **Local Administrators** panel is not displayed, click the edit icon ( ) on the **Settings** panel. Then use the **CIFS Settings** dialog to set the **Authentication mode** to **Active Directory**.

4. On the **Local Administrators** panel, do one of the following:

- To add a CIFS Active Directory user, expand the **Actions** menu and select **Add Users or Groups**.
- To delete a CIFS user or group, select the user or group and then expand the **Actions** menu and select **Delete Users or Groups**. The **Delete Members** dialog opens.

Adding, editing, and deleting NAS CIFS users

Prerequisites

To display the CIFS server **Users** panel and **Actions** menu, the **Authentication Mode** must be set to **User** on the **CIFS Settings** dialog.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Servers** tab.
3. On the **Users** panel, do one of the following:

   - To add a CIFS user, expand the **Actions** menu and select **Add**.
   - To edit or delete a CIFS user, select the user, and then expand the **Actions** menu and select **Edit** or **Delete**.

Adding, editing, and deleting NAS NFS hosts

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **NFS Servers** tab.
3. On the **Host List** panel, do one of the following:

   - To add an NFS host, expand the **Actions** menu and select **Add**.
   - To edit or delete an NFS host, select the host and then expand the **Actions** menu and select **Edit** or **Delete**.

Editing NAS CIFS settings

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.
2. On the **NAS Settings** screen, click the **CIFS Server** tab.
3. On the **Settings** panel, click the edit icon ().

Editing NAS NFS settings (browsability)

NAS NFS settings include an NFS browsability setting. The setting allows you to enable or disable browsability to NFS shares.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.

2. On the **NAS Settings** screen, click the **NFS Server** tab.
3. On the **Settings** panel, click the edit icon ().

Joining and leaving NAS CIFS Active Directories

Prerequisites

To display Active Directory actions on the **NAS Settings** screen, the **Authentication Mode** must be set to **Active Directory** on the **CIFS Settings** dialog.

Procedure

1. Navigate to the **NAS Settings** screen.

   If necessary, see **Viewing NAS settings** on page 140.

2. On the **NAS Settings** screen, click the **CIFS Server** tab.
3. On the **Settings** panel, expand the **Actions** menu and select **Join Active Directory** or **Leave Active Directory**, as appropriate.

Replication data services

Replication data services include replication mapping for VT libraries and NAS shares, and general replication settings.

Replication Mapping

Replication mapping is available for source and target VT libraries and NAS shares.

- To view VT replication mapping, see **Viewing VT replication mappings** on page 106.
- To view NAS replication mapping, see **Viewing NAS replication mappings** on page 132.

Replication Settings

General replication settings include: Partner Systems, Bandwidth Limits, Blackout Windows, Event History, and Permissions.

To view replication settings, see **Viewing replication settings** on page 143.

Viewing replication settings

Procedure

1. Do one of the following:
   - On the main menu, select **Data Services**. On the **Data Services** screen, expand the **Actions** menu and select **Replication Settings**.
   - On the main menu, select **Settings**. On the **Settings** screen, under **Data Services**, click the **Replication Settings** panel.
2. The **Replication Settings** screen includes tabs for **Partner Systems**, **Bandwidth Limits**, **Blackout Windows**, **Event History**, and **Permissions**.

Bandwidth limits (replication)

Users with the Administrator role can establish and edit replication bandwidth limits.

Bandwidth limits can be used to avoid saturating the WAN with low-bandwidth replication and to free up bandwidth for other processes and applications. You can establish a general bandwidth limit, and limits for one or two windows for each day of the week. Each window can have a different bandwidth limit.

- To establish or edit a general bandwidth limit, see **Editing replication general bandwidth limit settings** on page 145.
- To establish or edit a bandwidth limits for specific day of the week and time windows, see **Editing replication bandwidth limiting windows settings** on page 146.

IMPORTANT:

- Replication bandwidth limits apply to all outbound replication jobs a StoreOnce System. The limits cannot be applied to individual outbound jobs.
- When a bandwidth limiting window is enabled, it overrides the general bandwidth limit at the day and time the window is active.

- HPE recommends:
  - A minimum of 2Mb/s per concurrent replication job.
  - At least 512Kbps per concurrent job is required for reliable operation.

Viewing replication bandwidth limits

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Bandwidth Limits** tab.

Bandwidth limit properties (replication)

Replication Settings screen, Bandwidth Limits tab

Property	Description
Status	
System Time	The current time on the StoreOnce System.
Current Bandwidth Limit	The current replication bandwidth limit in Kb/s. No Limit indicates that no bandwidth restrictions are currently active.
Source Jobs Bandwidth Limiting Windows	
General Bandwidth Limit	Limit in Kb/s. No Limit indicates that the general bandwidth limit is not enabled.
Restriction table	
Day	Day of the week
First Restriction Limit	Replication bandwidth restriction in Kb/s. Dashes indicate that the restriction is not enabled.

Table Continued

Property	Description
First Restriction Time	Replication restriction start and end time. Dashes indicate that the restriction is not enabled.
Second Restriction Limit	Replication bandwidth restriction in Kb/s. Dashes indicate that the restriction is not enabled.
Second Restriction Time	Replication restriction start and end time. Dashes indicate that the restriction is not enabled.
Maximum Jobs	
Maximum Concurrent Source Jobs	The maximum number of source jobs that can run concurrently.
Maximum Concurrent Target Jobs	The maximum number of target jobs that can run concurrently. **TIP:** If you are running backups at the same time as replication, the default value of the target jobs can be reduced. Reducing the value helps avoid using too much WAN bandwidth and overloading the target StoreOnce System.

Editing replication general bandwidth limit settings

You can use bandwidth limiting to avoid saturating the WAN with low-bandwidth replication and to free up bandwidth for other processes and applications. The limits apply to all outbound replication jobs from a StoreOnce System. Learn more: **Bandwidth limits (replication)** on page 143.

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Bandwidth Limits** tab.
3. On the **Source Jobs Bandwidth Limiting Windows** panel, expand the **Actions** menu and select **Edit General Bandwidth Limit**.

   On the Edit General Bandwidth Limit dialog opens.
4. To enable or disable the limit, click the **General Bandwidth Limit** toggle.
5. When enabled, you can manually enter a bandwidth limit, or use the built-in **Bandwidth Limit Calculator** to determine and apply a limit.

TIP: The recommended bandwidth limit is a calculation of (Max WAN Speed) x (Max Desired WAN Usage%).

6. To save your edits, click **Update**.

Editing replication bandwidth limiting windows settings

You can use bandwidth limiting to avoid saturating the WAN with low-bandwidth replication and to free up bandwidth for other processes and applications. The limits apply to all outbound replication jobs from a StoreOnce System. Learn more: **Bandwidth limits (replication)** on page 143.

IMPORTANT: Restriction times are in system local time, not in UTC. If the time zone of the StoreOnce System is changed after restrictions are added, you must change the restriction times accordingly.

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.

2. On the **Replication Settings** screen, click the **Bandwidth Limits** tab.
3. On the **Source Jobs Bandwidth Limiting Windows** panel, click the day of the week (for example, Monday) on the restriction table, and then expand the **Actions** menu and select **Edit Bandwidth Limiting Windows**.
4. On the **Edit Bandwidth Limiting Windows** dialog, click the **Restriction 1** toggle.
   - Manually enter a bandwidth limit, or use the built-in **Bandwidth Limit Calculator** to determine and apply a limit.

     TIP: The recommended bandwidth limit is a calculation of (Max WAN Speed) x (Max Desired WAN Usage%).

   - Enter or select a **Restriction Time**.
5. If you want to set another restriction time, click the **Restriction 2** toggle and complete the entries.
6. When ready, click **Update**. The bandwidth limiting window for the selected day of the week is added to the restriction table.

Editing replication maximum concurrent job settings

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.

2. On the **Replication Settings** screen, click the **Bandwidth Limits** tab.
3. On the **Maximum Jobs** panel, click the edit icon ( ).

Blackout windows (replication)

Users with the Administrator role can specify times when replication cannot occur. Fo example during planned maintenance, or heavy network traffic.

- Blackout windows for a StoreOnce System apply regardless of whether the system is a replication source or target.
- Any running jobs for replication mappings that involve the StoreOnce System are automatically paused during a blackout window.
- You can configure multiple blackout windows for a StoreOnce System.

To establish or edit blackout windows, see **Editing replication blackout window settings** on page 148.

Viewing replication blackout windows

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Blackout Windows** tab.

Blackout window properties

Replication Settings screen, Blackout Windows tab

Property	Description
Status	
System Time	The current time on the StoreOnce System.
Blackout Windows	Indicates whether blackout windows are active or inactive. When blackout windows are active, no replication can occur.
Source Jobs Blackout Windows, Restriction table	
Day	Day of the week
First Restriction Time	Replication restriction start and end time. Dashes indicate that the restriction is not enabled.
Second Restriction Time	Replication restriction start and end time. Dashes indicate that the restriction is not enabled.

Editing replication blackout window settings

Users with the Administrator role can specify times when replication cannot occur. For example, during planned maintenance or heavy network traffic. Learn more: **Blackout windows (replication)** on page 147.

IMPORTANT: Restriction times are in system local time, not in UTC. If the time zone of the StoreOnce System is changed after restrictions are added, you must change the restriction times accordingly.

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Blackout Windows** tab.
3. On the **Source Jobs Blackout Windows** panel, click the day of the week (for example, Monday) on the restriction table, and then expand the **Actions** menu and select **Edit Blackout Window**.
4. On the **Edit Blakout Window** dialog, click the **Restriction 1** toggle, and then Enter or select a **Restriction Time**.
5. If you want to set another restriction time, click the **Restriction 2** toggle and complete the entries.
6. When ready, click **Update**. The blackout window for the selected day of the week is added to the restriction table.

Event history (replication)

The Event History tab includes the following:

- The **Out of Sync Notifications** panel that shows the warning and critical out-of-sync settings.

  The settings establish the amount of time (in hours) that a replication mapping can be out of sync before an out-of-sync event is generated.

  When an out-of-sync event is generated, an entry is added to the StoreOnce System event Log. Also, depending on the StoreOnce System configuration, an SNMP trap is triggered and email is sent.
- The **Events** panel that shows a list of significant replication events.

  The list includes the date and time, severity status, and associated messages. The most recent event is at the top of the list.

  TIP: The replication event history is maintained even if the StoreOnce System is power cycled.

See also:

- **Clearing replication events** on page 150.
- **Editing replication out of sync notification** on page 150.

Viewing replication event history

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.

2. On the **Replication Settings** screen, click the **Event History** tab.

   The Event History tab includes panels for:

   - **Events**

     To filter the list of events, click the filter icon ( ). You can filter on the event severity (Info, Warning, Error), event message text, and event date and time.

   - **Out of Sync Notifications**

3. To view the details of an event, click its information icon ( ).

Event history properties

Replication Settings screen, Event History tab

Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).

Property	Description
Out of Sync Notifications	
Out of Sync Warning	Indicates the amount of time that a replication mapping can be out of sync before an out-of-sync warning event is generated.
Out of Sync Critical	Indicates the amount of time that a replication mapping can be out of sync before an out-of-sync critical event is generated.
Events	
Severity	The severity level of the replication event (Information, Warning, Error).
Event Category	StoreOnce category of the replication event. For example, a *Cartridge data job event*.
Time	Date and time that the replication event occurred.
Message	The replication event message. For example, *Data job for a cartridge has completed successfully*.

Table Continued

Property	Description
More properties	
Reason	Reason that the replication event occurred. For example, *Starting Job to synchronise Cartridge Data in Target Slot with Source Slot*.
Source Library/Share Name	Name of the source VT library or NAS share that is involved in the replication event.
Target Library/Share Name	Name of the target VT library or NAS share that is involved in the replication event.
Source Slot/Entry ID	Source VT library Slot or NAS share Entry ID that is involved in the replication event.
Target Slot/Entry ID	Target VT library Slot or NAS share Entry ID that is involved in the replication event.

Clearing replication events

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Event History** tab.
3. Click the clear icon ( ).

Editing replication out of sync notification

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Event History** tab.
3. On the **Out of Sync Notification Settings** panel, click the edit icon ( ).

Partner systems (replication)

Viewing replication partner systems

Procedure

1. Navigate to the **Replication Settings** screen.

If necessary, see **Viewing replication settings** on page 143.

2. On the **Replication Settings** screen, click the **Partner Systems** tab.

Partner system properties

Replication Settings screen (all), Partner Systems tab

The **Partner Systems** tab displays the replication status of all source and target devices that are configured on the StoreOnce System.

Columns for the most often viewed settings are shown by default. To add or remove columns, click the column selector icon ().

Setting	Description
System Name	The name of the StoreOnce System.
Status	The health of the StoreOnce System.
System Type	System replication type: source or target.
Replication Address	The IP address of the StoreOnce System.
Replication Serial Number	A serial number that is generated by a StoreOnce System. The number is used for all replication jobs and does not change.
More settings	
Product Class	The product class of the StoreOnce System.
Replication Status	Status of replication: running or not.
System Supported Protocol Versions	Replication versions that are supported.
Capacity	Storage capacity of the StoreOnce System.
Free Space	The amount of free space on the StoreOnce System.
Software Version	Software version of the StoreOnce System.
System Time	The current time on the StoreOnce System.
Blackout Window Active	Indicates if a blackout window is active or not. When active, no replication can occur.

Adding replication target systems

Prerequisites

You know the IP address of the intended target StoreOnce system.

Procedure

1. Navigate to the **Replication Settings** screen.
   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Partner Systems** tab.
3. Expand the **Actions** menu and select **Add**.
   When the action is completed, the target StoreOnce System is added to the list of partner systems.

Editing and deleting replication target systems

Procedure

1. Navigate to the **Replication Settings** screen.
   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Partner Systems** tab.
3. Click the target system, and then expand the **Actions** menu and select **Edit** or **Delete**.

Locating replication serial numbers

Procedure

1. On the source StoreOnce System, navigate to the **Replication Settings** screen.
   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Partner Systems** tab.
3. The replication serial number for the StoreOnce System is shown in the top panel.

Pausing replication

Procedure

1. Navigate to the **Replication Settings** screen.
   If necessary, see **Viewing replication settings** on page 143.
2. On the **Replication Settings** screen, click the **Blackout Windows** tab.
3. Expand the **Actions** menu and select **Pause Replication**.

Permissions (replication)

The Permissions tab shows replication serial numbers of partner StoreOnce Systems.

See also:

- **Adding replication permissions for target systems** on page 153.
- **Removing replication permissions for target systems** on page 153.

Viewing replication event history

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.

2. On the **Replication Settings** screen, click the **Permissions** tab.

   The Permissions tab shows a list replication serial numbers for partner StoreOnce Systems.

Adding replication permissions for target systems

Adding replication permission on a target system is a one-time step that allows the target system to accept replication from the source system. Replication is not started between the systems.

TIP: If replication permission for **Public Access** appears on the target system permissions list, then any StoreOnce System has permission to replicate to the target system.

Prerequisites

- The replication target system must have been previously added to the **Partner Systems** list on the source system.
- In this procedure, you must have the replication serial number of the source system available. The best practice is to copy the replication serial number and have it available to paste in. Learn more: **Locating replication serial numbers** on page 152.

Procedure

1. On the target system, navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.

2. On the **Replication Settings** screen, click the **Permissions** tab.
3. Expand the **Actions** menu and select **Add Replication Serial Number**.

   When the action is complete, the replication serial number of the source system is added to the list of replication permissions.

Removing replication permissions for target systems

Removing a replication permission from a target system prevents the target system from accepting replication from the removed source system.

Prerequisites

In this procedure, you must know the replication serial number of the source StoreOnce System. Learn more: **Locating replication serial numbers** on page 152.

Procedure

1. On the target system, navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.

2. On the **Replication Settings** screen, click the **Permissions** tab.
3. In the list of replication serial numbers, click the replication serial number of the source system that you want to remove. Then expand the **Actions** menu and select **Remove Replication Serial Number**.

Resuming replication

Procedure

1. Navigate to the **Replication Settings** screen.

   If necessary, see **Viewing replication settings** on page 143.

2. On the **Replication Settings** screen, click the **Blackout Windows** tab.
3. Expand the **Actions** menu and select **Resume Replication**.

Reports

Reports overview

StoreOnce System reports are available as online reports.

Online reports. Online reports are interactive graphical reports. You can interactively select and filter report content. Online reports are viewed on the Reports screen. Learn more: **Viewing online reports** on page 156.

Online reports display information for a single StoreOnce system or a single device.

Report content categories

The following report content categories are displayed in tabs on the Reports screen.

Backup/Restore

- Backup/Restore Throughput graph:

  Catalyst Write, Catalyst Read | NAS Write, NAS Read | VTL Write, VTL Read
- Backup/Restore Sessions graph:

  Catalyst Sessions, NAS Sessions, VTL Sessions

Replication/Copy

- Replication/Copy Throughput graph:

  Catalyst Copy Target, Catalyst Copy Source | NAS Replication Target, NAS Replication Source | VTL Replication Target, VTL Replication Source
- Replication/Copy Sessions graph:

  Catalyst Target Sessions, Catalyst Source Sessions | NAS Target Sessions, NAS Source Sessions | VTL Target Sessions, VTL Source Sessions

Cloud Bank

- Cloud Bandwidth Utilization graph:

  Uploaded Bytes, Downloaded Bytes
- Cloud Requests graph:

  GET Requests, PUT Requests, POST Requests, HEAD Requests, LIST Requests, DELETE Requests

Capacity

- Capacity Usage graph:

  User Data Stored, Size on Disk, Size in Cloud
- Capacity Dedupe Ratio graph:

  Dedupe Ratio
- Pending Space Reclamation:

  Bytes Pending, Secure Erase Bytes Pending

Resources

- System Resources Utilization

  CPU, Memory, Data Disk, OS Disk
- Data Disks Throughput

  Write Throughput, Read Throughput
- OS Disks Throughput

  Write Throughput, Read Throughput

Interface

- **Ethernet Received** (for each Ethernet card speed and card)
- **Ethernet Transmit** (for each Ethernet card speed and card)
- **Fibre Channel Received** (for each Fibre Channel card speed and card)
- **Fibre Channel Transmit** (for each Fibre Channel card speed and card)

Viewing online reports

TIP: When you log in to a federation lead system, the Reports screen displays information for the lead system. The screen does not show aggregated information for the federation.

Procedure

1. On the main menu, select **Reports**.

   The **Reports** screen includes tabs for **Backup/Restore**, **Replication/Copy**, **Cloud Bank**, **Capacity**, **Resources**, **Interface**, **Custom**, and **Scheduled**.

2. To choose the **Devices** in the online reports, click the device selection icon ( ).

   You can choose from lists of Catalyst stores, NAS shares, and VT libraries. You can select **All Devices** or a single device.

3. To choose a time **Period** for the online reports, click the clock icon ( ).

   You can choose from defined time periods, or specify a custom time period.

Event log

Viewing event logs

Procedure

1. On the main menu, select **Event Log**.

   To filter and sort the list, or to include internal system events, click the filter icon ( ).

   The **Event Log** screen displays a list of events.

2. Some events include additional details. To view all the details for an event, click its information icon ( ).

Manually deleting events

You can manually delete events that were generated before a date and time that you specify.

See also: **Managing automatic event deletion** on page 157.

Procedure

1. On the main menu, select **Event Log**.
2. On the **Event Log** screen, expand the **Actions** menu and select **Clear Event Log**.

Managing automatic event deletion

You can specify the number of months that an event is retained in the log before it is automatically deleted.

See also: **Manually deleting events** on page 157.

Procedure

1. On the main menu, select **Event Log**.
2. On the **Event Log** screen, expand the **Actions** menu and select **Manage Retention**.

Restart, shutdown, and upgrade

Restarting and shutting down StoreOnce systems

Only a user with the Administrator role can restart or shut down a StoreOnce System.

IMPORTANT:

- If you restart or shut down a StoreOnce system, all users will be disconnected. Also, all running tasks will be interrupted.
- You can only restart or shut down a StoreOnce system that you are directly logged in to. You cannot restart or shut down a federation member system from the federation lead.
- If you shut down a StoreOnce System, you must use the hypervisor to start it again.

Procedure

1. On the main menu, select **Settings**.
2. On the **Settings** screen, expand the **Actions** menu and select **Restart** or **Shutdown**.

   The corresponding dialog is displayed.

   Read and carefully consider the warning messages. If you do not want to proceed, click the close icon (✕). Otherwise, click the confirmation check box and then click **Restart** or **Shutdown**.

Upgrade overview

The upgrade package contains new StoreOnce software, as well as firmware for the hardware components to be upgraded.

An upgrade is not an online process. Services will shut down to perform the updates. The whole StoreOnce System will be offline for a period.

Upgrade checks

As part of the upgrade, the upgrade package is validated. All the checks must pass before the upgrade is allowed to proceed. The following checks are performed:

- Signature check. Ensures that the package is a valid package and has been securely signed by HPE.
- Checksum check. Validates that the package is not corrupted.
- Image type check. Verifies that the image type is valid for this StoreOnce system.
- Version check. Verifies that the currently installed software version can be upgraded to the version in the upgrade package.
- System readiness check. Verifies that the hardware components and software services are in a healthy state. If any checks report an error, then you will need to fix the issue before the upgrade is allowed to proceed.

Upgrading StoreOnce Systems

Only a user with the Administrator role can upgrade a StoreOnce System.

IMPORTANT: You can only upgrade a StoreOnce system that you are directly logged in to. You cannot upgrade a federation member system from the federation lead system.

Prerequisites

You have obtained the StoreOnce upgrade package (.star file). The upgrade package file is located where it can be accessed from the StoreOnce System.

Procedure

1. On the main menu, select **Settings**.
2. On the **Settings** screen, expand the **Actions** menu and then select **Upgrade**.

   The **Upgrade** screen guides you through steps for:

   - Selecting and uploading an upgrade package.
   - Validating the upgrade package.
   - Upgrading the StoreOnce System.

System settings

Viewing the StoreOnce software version

Procedure

On the main menu, select **System Dashboard**.

To see the software version of a federation member, select **Federation Dashboard**, then select the system of interest.

The **System Information** section shows the software version.

Viewing warranty serial numbers

Each major component of a StoreOnce hardware model has its own warranty serial number. For example, the base system (server), expansion enclosures, and expansion disk packs have warranty serial numbers.

The warranty serial numbers are preconfigured on the hardware and cannot be changed.

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **Warranty Serial Number** panel.

   The **Warranty Serial Number** screen shows warranty information for the StoreOnce System.

StoreOnce VSA licensing

StoreOnce VSA systems can use either the Standalone licensing mode or Enterprise licensing mode. In both modes, all customer licenses are permanent and do not expire.

IMPORTANT: The two licensing modes use different license files that are not interchangeable. Once you select Standalone or Enterprise licensing mode, you cannot switch to the other mode.

NOTE: The term 'Enterprise licensing' describes the licensing mode where licenses are added to an AutoPass license server and then allocated to connect StoreOnce VSA instances.

- **Standalone licensing**: The StoreOnce system operates as a single unit. You use the StoreOnce Management Console to add (upload) Standalone license files directly to the StoreOnce system. Standalone licenses cannot be deleted from a system, or moved to another system.
- **Enterprise licensing**: The StoreOnce system is connected to a central HPE AutoPass License Server that has been loaded with Enterprise licenses. You use the StoreOnce Management Console to add Enterprise licenses to a StoreOnce System. The StoreOnce Management Console handles all the steps to check out Enterprise licenses from the license server.

  You can also use the StoreOnce Management Console to remove Enterprise licenses from a StoreOnce System. The StoreOnce Management Console handles all the steps to return Enterprise

licenses to the license server. Returned Enterprise licenses can be reused on the same StoreOnce System or on other StoreOnce Systems.

- **Cloud Detach licenses**. Cloud Detach licenses are an exception to the general Enterprise licensing. When a Catalyst Cloud Bank store is archived, a license is checked out automatically and is stored with the archived or detached Catalyst store. A local copy of that Cloud Detach license is held on the client for information only. Cloud Detach licenses cannot be returned to the server.

When you first deploy a StoreOnce VSA system, you can choose Standalone licensing, Enterprise licensing, or try it free for 90 days with the built-in instant-on license. After the 90-day trial period ends, you must license the StoreOnce VSA system to continue using it.

Licenses available

- **90 day instant-on license**: Activated automatically on first boot. Immediately enables operation for up to 90 days. While using the instant-on license, you can add up to 500 TB of storage. StoreOnce Catalyst and replication are enabled. Encryption is not available. The StoreOnce VSA system is not eligible for technical support.

  You can add a base license at any time during the 90 days. When you install a base license or connect to a license server, the instant-on license terminates. License any storage you have configured as appropriate for your chosen licensing mode. If you do not apply a base license within 90 days, the StoreOnce VSA system enters Unlicensed mode and storage becomes read-only.
- **Base license**: Activates the full potential of the StoreOnce VSA system. The base license also makes the StoreOnce VSA system eligible for technical support. The StoreOnce VSA system requires a base license before you can add capacity or security licenses. If you use Enterprise licensing, connecting to a license server automatically applies a base license to the StoreOnce VSA system.
  - In Standalone mode, the base license allows 4 TB of storage.
  - In Enterprise mode, the default capacity is set to 1 TB. Check out capacity licenses that equal or exceed the storage on the StoreOnce VSA system.
- **Capacity license**: Expands the capacity of the existing base license.
  - In Standalone mode, the capacity license provides capacity in 1 TB increments. The maximum is 500 TB total on the StoreOnce VSA system.
  - In Enterprise mode, the capacity license provides capacity in 100 TB increments added to the license server pool. The capacity is allocated to individual systems in 1 TB increments. The maximum is 500 TB total on the StoreOnce VSA system.
- **Cloud Storage license**: Enables connection to Cloud storage through a Cloud Service Provider.
  - In Standalone licensing mode, the cloud storage license provides cloud capacity in 1 TB increments. The maximum is twice the maximum local storage total in the cloud.
  - In Enterprise licensing mode, the cloud storage license provides cloud capacity in 100 TB increments added to the license server pool. The cloud capacity is allocated to individual systems in 1 TB increments. The maximum is twice the maximum local storage total in the cloud. Multiple StoreOnce VSA systems can access this storage.

- **Cloud Archive license**: Allows the StoreOnce VSA system to archive and disconnect from a cloud store and place it in archive mode.
- **Security license**: Enables the security features of Data at Rest Encryption and Data in Flight Encryption. In Enterprise licensing mode, the security license enables an unlimited number of connected StoreOnce VSA systems to use encryption.

Obtaining StoreOnce and AutoPass license server licenses

This topic applies to:

- StoreOnce VSA systems with standalone licensing.
- AutoPass license server

Use the HPE My License Portal to activate licenses for your StoreOnce System and your AutoPass license server.

Procedure

1. Go to the HPE My License Portal at **https://myenterpriselicense.hpe.com**.
2. Log in using your HPE Passport user ID and password.
3. After obtaining the license, do one of the following actions:
   - For the StoreOnce VSA, save the license to a .DAT file that can be accessed from the StoreOnce server.
   - For the AutoPass License server, save the license file to a location that can be accessed from the license server.

Viewing StoreOnce licenses

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **License Management** panel.
   - For StoreOnce VSA systems with Standalone licensing: The **License Management** screen shows tabs for **Overview** and **Licenses**.
   - For StoreOnce VSA systems with Enterprise licensing: The **License Management** screen shows tabs for **Overview**, **Licenses**, and **License Server**.
3. To view a license summary, click the **Overview** tab. To view a list of the installed licenses, click the **Licenses** tab.

License Management screen and properties

License Management screen, Overview tab

Property	Description
Licensing Mode	Standalone or Enterprise
Locking ID (Serial Number)	ID that locks the license to a specific StoreOnce System.
Licensed Features	
Name	Licensed feature name. For example, *Encryption*.
Licensed Capacity	
Capacity	The amount of capacity covered by the license.
Cloud Bank Storage Read/Write Capacity	Capacity covered by the Cloud Bank Read/Write license.
Cloud Bank Storage Detach Capacity	Capacity covered by the Cloud Bank Detach license.
Licensed Optional Hardware	
Name	Licensed optional hardware name. For example, *Fibre Channel Optional Hardware* or *Network Interface Optional Hardware*.

License Management screen, Licenses tab

TIP:

Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ().

Property	Description
Name	The license name. For example, *BB969A HPE StoreOnce 5250/5650 120TB Drawer*.
Category	The license category. For example, *Storage*.
License Type	The license type. For example, *Capacity* or *Encryption*.
Capacity	The amount of capacity covered by the license.

Table Continued

Property	Description
Expiration	Date and time that the license expires.
More properties	
Description	Full description of the license. For example, *BB969A HPE StoreOnce 5250/5650 120TB Drawer/Capacity Upgrade LTU*.
Valid From	Date and time that the license was first activated.
Status Information	License status. For example, *This license is valid and active*.

License Management screen, Optional Hardware tab

TIP:

- Columns for the most often viewed properties are shown by default. To add or remove columns, click the column selector icon ( ).
- To display the properties in a **Details** flyout, click the information icon ( ).

Property	Description
Slot	Slot identification. For example, *PCI-E Slot 1*.
Card Model	Hardware card model. For example, *561T*.
Name	Hardware option name. For example, *HPE StoreOnce Gen4 10GbE-T Network Card*.
License State	Licensed or Not Licensed.
Hardware State	State description. For example, *Valid hardware*.
More properties	
License Name	Full description of the license. For example, *BB985A HPE StoreOnce Gen4 10GbE-T Network Card*
License Status	Full description of the license status. For example, *PCI-E Slot 1 has a valid license*.
Hardware Status	Full description of the status. For example, *Valid hardware - good state*.

Adding StoreOnce Standalone licenses

This topic applies to:

StoreOnce VSA systems with Standalone licensing.

IMPORTANT:

- Once you add a Standalone license to a StoreOnce VSA System, you cannot change to Enterprise license mode.
- Once a Standalone license is added to a StoreOnce System, it cannot be deleted or moved to another StoreOnce System.

Prerequisites

You must have obtained the StoreOnce license file from HPE. The file must be in a location where it can be accessed from the Add License dialog. Learn more: **Obtaining StoreOnce and AutoPass license server licenses** on page 162.

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **License Management** panel.
3. On the **License Management** screen, click the + (add) icon. The **Add License** dialog opens.

After adding the license, the license is uploaded, validated, and installed on the StoreOnce System. After a few seconds, the status on the **Overview** tab is updated and the license is shown on the **Licenses** tab.

If the license is the first to be added to a StoreOnce VSA system, the license mode is set to Standalone.

Deleting StoreOnce Standalone licenses

This topic applies to:

StoreOnce VSA systems with Standalone licensing.

IMPORTANT: Once a Standalone license is added to a StoreOnce System, the license cannot be deleted by StoreOnce System users or administrators. If necessary, contact HPE Support regarding removal of Standalone licenses.

Adding Enterprise licenses

This topic applies to StoreOnce VSA systems with Enterprise licensing. Learn more: **StoreOnce VSA licensing** on page 160.

Prerequisites

- The StoreOnce System must be in the *connected* state with an active Enterprise license server.
- An Enterprise base license must exist on the StoreOnce System.

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **License Management** panel.
3. On the **License Management** screen, expand the **Actions** menu and select **Add license**.
4. On the **Add license** dialog, select the license to add.

Connecting Enterprise license servers

This topic applies to StoreOnce VSA systems with Enterprise licensing. Learn more: **StoreOnce VSA licensing** on page 160.

Prerequisites

An Enterprise License Server must have been previously added to the StoreOnce System licensing configuration.

TIP: A StoreOnce System typically remains connected to its Enterprise license server, unless it is explicitly disconnected by an administrator. The need to reconnect might be required in cases when the Enterprise license server was disconnected during maintenance of the server.

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **License Management** panel.
3. On the **License Management** screen, expand the **Actions** menu and select **Connect**.

Disconnecting Enterprise license servers

This topic applies to:

StoreOnce VSA systems with Enterprise licensing. Learn more: **StoreOnce VSA licensing** on page 160.

A StoreOnce System with Enterprise licensing typically remains connected to its Enterprise license server, unless it is explicitly disconnected by an administrator. For example, it might be disconnected when performing upgrades of the license server.

WARNING:

- Disconnecting the StoreOnce System from an Enterprise license server will remove all licenses from the StoreOnce System.
- All Catalyst stores, Cloud Bank stores, NAS shares, and VT libraries will become read-only.
- The StoreOnce System will enter an unlicensed state.
- When the StoreOnce System is reconnected later, a base license and a 1 TB capacity license will automatically be added. You will need to explicitly add more licenses to cover the full capacity of the StoreOnce System.

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **License Management** panel.
3. On the **License Management** screen, expand the **Actions** menu and select **Disconnect**.

Removing Enterprise licenses

This topic applies to StoreOnce VSA systems with Enterprise licensing. Learn more: **StoreOnce VSA licensing** on page 160

WARNING: If you remove the Enterprise *base license* for a StoreOnce System:

- All other installed Enterprise licenses will be removed from the StoreOnce System
- The StoreOnce System will disconnect from the Enterprise license server.
- The StoreOnce System will enter an *unlicensed* state.

Prerequisites

The StoreOnce System must be in the *connected* state with an active Enterprise license server.

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **License Management** panel.
3. On the **License Management** screen, expand the **Actions** menu and select **Remove**.
4. On the **Remove** (license) dialog, select the license to remove.

Unlicensed mode

This topic applies to:

- StoreOnce VSA systems with Standalone licensing.
- StoreOnce VSA systems with Enterprise licensing.

A StoreOnce VSA system can become unlicensed (and enter the Unlicensed mode) in one of the following ways:

- The 90 day instant-on license has expired.
- A StoreOnce VSA with Enterprise licensing has been intentionally disconnected from its Enterprise license server. Learn more: **Disconnecting Enterprise license servers**.
- A StoreOnce VSA with Enterprise licensing has unintentionally lost contact with its license server and has not reconnected within seven days.

When a StoreOnce VSA is unlicensed (in the Unlicensed mode):

- The StoreOnce VSA operates in read-only mode for 60 days.
- The StoreOnce VSA can be returned to a licensed state by adding a license before 60 days elapses.
- **WARNING:** If a license is not added within 60 days, the StoreOnce VSA deactivates and can only be reactivated by HPE Support.

Editing system date and time

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **System Date & Time** panel.

   The **System Date & Time** dialog enables you to change the date and time settings.

   NOTE: Setting the clock backward triggers the clock tampering detection. Repeated clock tamper events will cause the system to lock and requires HPE Support intervention to recover the system.

Editing system information

You can edit the system name. You can also view and edit optional information such as a contact name, phone number, and email address.

Procedure

1. Do one of the following:

   - On the main menu, select **System Dashboard**, and then click the edit icon ( ) on the **System Information** panel.
   - On the main menu, select **Settings**, and then click the **System Information** panel.

Editing user preferences

You can change your preferences for display formats. For example, you can choose units-of-measure for the system, drives, and volumes. You can also choose display formats for date, time, and WWNs.

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **User Preferences** panel.

   The **Preferences** dialog shows the preferences and allows you to change the settings.

Capacity units

Binary units:

1 KiB = 1024 bytes (2^{10})

1 MiB = 1,048,576 bytes (2^{20}), or 1024 KiB

1 GiB = 1,073,741,824 bytes (2^{30}), or 1024 MiB

1 TiB = 1,099,511,627,776 bytes (2^{40}), or 1024 GiB

1 PiB = 1,125,899,906,842,624 bytes (2^{50}), or 1024 TiB

Decimal units:

1 KB = 1,000 bytes (10^3)

1 MB = 1,000,000 bytes (10^6), or 1000 KB

1 GB = 1,000,000,000 bytes (10^9), or 1000 MB

1 TB = 1,000,000,000,000 bytes (10^{12}), or 1000 GB

1 PB = 1,000,000,000,000,000 bytes (10^{15}), or 1000 TB

Using the StoreOnce First Time Setup wizard

The StoreOnce First Time Setup wizard guides you through the steps to set up a recently installed StoreOnce System.

Procedure

1. Browse to the recently installed StoreOnce System. The First Time Setup wizard is automatically displayed.

   TIP: If a StoreOnce System has already been set up, its First Time Setup wizard is not displayed.

2. The setup steps include:

   - Setting the **Administrator Password**.
   - Setting the **Console Password**.
   - Setting basic **System Information** such as the system name (host name), location, and contact information.
   - Setting the **System Date & Time**. You can set the date and time manually, or synchronize the date and time with a network time server.
   - Configuring **Storage**. The wizard detects the factory installed storage. The wizard also enables you to configure additional storage capacity that you might have installed. The wizard also reports issues with additional storage, for example, when additional storage is not installed in the correct location.
   - Configuring **Remote Support**.

Updating StoreOnce system information

Procedure

1. On the main menu, select **Settings**.
2. In the **System** section, click the **System Information** panel.

   The **System Information** dialog allows you to change the system properties.

Hardware settings

Storage

Viewing storage

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Storage** panel.

   The **Storage** screen includes tabs for **Local Storage**, **Cloud Bank Storage**, and **Capacity Threshold**.

Configuring storage

After storage is added to a StoreOnce System, you must configure the storage to make it usable.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Storage** panel.
3. On the **Storage** screen, click the **Local Storage** tab, and then expand the **Actions** menu and select **Configure**.

Rescanning storage

Rescanning storage is not a required task but can be used to check if devices are visible.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Storage** panel.
3. On the **Storage** screen, click the **Local Storage** tab, and then expand the **Actions** menu and select **Rescan**.

   Newly detected storage is added to the storage list with a status of *Unconfigured*.

Unconfiguring storage

⚠ **WARNING:** If you unconfigure the storage:

- All your data will be lost
- Data services will stop running
- Running backup/restore jobs will fail

Unconfiguring storage can only be performed by a user with the Administrator role.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Storage** panel.
3. On the **Storage** screen, click the **Local Storage** tab, and then expand the **Actions** menu and select **Unconfigure**.

Editing storage capacity thresholds

You can edit user-defined thresholds for when a StoreOnce System generates storage capacity **Information**, **Warning**, and **Alert** events.

- **Info** thresholds must be less than **Warning**, and **Warning** must be less than **Alert**.
- User-defined thresholds cannot be set higher than system-defined thresholds.
- System-defined thresholds cannot be edited.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Storage** panel.
3. On the **Storage** screen, click the **Capacity Threshold** tab.
4. On the **Local Storage Threshold** panel, click the edit icon ( ).
5. On the **Capacity Threshold** dialog, you can specify **Info**, **Warning**, and **Alert** thresholds.

Networking

Network Configuration

The networking features in StoreOnce Systems allow you to support complex network environments. The following topics summarize the networking features and settings. The topics also include StoreOnce Management Console procedures for using the networking settings.

StoreOnce networking features overview

StoreOnce VSA network ports

Deployment of a StoreOnce VSA system creates one network port. More ports can be added using the hypervisor. Ports that are added with a hypervisor are automatically added to the StoreOnce network configuration. The maximum number of ports is set by the number of ports that the hypervisor allows.

The StoreOnce Management Console for StoreOnce VSA does not support the configuration of bonded ports. It is assumed that bonded ports will be created within the hypervisor infrastructure and a single port is presented to the StoreOnce VSA. The bonded port can be backed by many physical ports on the hypervisor host.

IPv4 and IPv6

StoreOnce Systems support IPv4 and IPv6 protocols on each network port. Static and DHCP configuration is supported for both protocols. IPv6 is not supported with IPsec.

Management and data interfaces

All network subnets can be configured to provide access to the network management interface or have this access disabled. This approach allows separation between data and management networks if required.

All network subnets can be configured to provide access to a mixture of the following data interfaces:

- RMC (iSCSI) (mutually exclusive with VTL)
- VTL (iSCSI) (mutually exclusive with RMC)
- NAS (CIFS and NFS)
- Catalyst and Replication

Additionally, each network subnet can be configured to allow SNMP trap delivery.

VLAN tagging

Subnets can have VLAN tagging enabled. Enabling VLAN allows:

- Network VLANs to be extended down to StoreOnce systems. Thus providing logically separate networks to be maintained.
- Multiple VLAN tagged subnets can be created on a single set of network ports.

Static routing

Each subnet can be configured with a set of static routes. The static routes can allow access through a specified gateway server to a particular IP address, or range of IP addresses which might not be accessible through the default gateway.

Data in Flight encryption (IPsec)

IPsec encryption can be configured on subnets to allow encrypted data transfer between specific devices. The encryption can be used for Replication, Catalyst copy, or backing up data from a host. IPsec is not supported on networks with IPv6 protocol.

Networking concepts

- **Port Sets**. A port set is a configuration containing one or more network ports. A port set can be configured with one or more network subnets.
- **Subnets**. A subnet is a logical configuration which contains the addressing and access information for the network. VLAN tagging, data-in-flight encryption (IPsec), and static routing are also configuration parameters of a subnet.
- **DNS**. DNS configuration applies to all port sets. However, DNS server details can be provided by DHCP networks within subnets.

Viewing the active network configuration

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel. The **Networking** screen opens.

   The active configuration is shown. Network settings are shown for **Port Sets** and **DNS Server**.

- The **Port Sets** panel shows the status, name, IP addresses of its subnets, and port type.
- The **DNS Server** panel shows the DNS server addresses (up to three) and a DNS search suffix.

Viewing port set details and subnet details

TIP: In the following steps, you can navigate back to a previous screen by clicking the arrow icon (←) that is near the screen name.

3. On the **Networking** screen, **Port Sets** panel, click the information icon (ⓘ) for the port set. The **Port Set** screen opens.
   - The port set **Configuration** panel shows the status, name, network ports, bond mode, frame size, and type.
   - The port set **Subnets** panel shows subnet IP address and VLAN tag.

     To view subnet details, click the information icon (ⓘ) for the subnet. The **Subnet** screen opens. Detailed subnet information is shown on the **Configuration**, **Routes**, and **Encryption Links** panels.

Editing the active network configuration

Editing the active network configuration allows you to modify the StoreOnce System settings for port sets, subnets, and DNS server.

As you use the various networking screens and dialogs, your changes are temporarily saved. However, no changes are made to the active configuration until you select **Activate** on the **Actions** menu of the **Edit Configuration** screen.

If you decide to not activate your changes, you can click the arrow icon (←) to the left of the **Edit Configuration** screen name. The active configuration screen will be redisplayed and your changes will be discarded.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel.
3. On the **Networking** screen, select **Edit Configuration** on the **Actions** menu.

   The **Edit Configuration** screen opens and displays settings for **Port Sets** and **DNS server**. You can perform the following actions:

   - Add, edit, and delete port sets.
   - Edit DNS servers.
   - Activate changes to the network configuration

Activating network configurations

Activation can take some time to complete. When completed, the **Active Configuration** on the **Networking** screen will reflect the new network configuration.

WARNING:

- If the new network settings are different from the previous settings, backup/restore, copy, and replication operations might fail.
- If the network management interface has changed, the connection to this management session might be lost.

Prerequisites

You have used the **Edit Configuration** action that will change the StoreOnce System network configuration.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel.

   The active configuration is shown.
3. Select **Edit configuration** on the **Actions** menu.
4. On the **Edit Configuration** screen, select **Activate** on the **Actions** menu. The **Activate** dialog opens.

   Read and carefully consider the warning messages. If you do not want to activate the new network configuration, click the close icon ( ). Otherwise, click **Activate**.

Adding, editing, and deleting port sets

- A port set can be edited, but it cannot be renamed. If you need a port set with a different name, you must add a new port set.
- Port sets can be deleted. When you activate the new configuration, the port set is deleted. Also, any associated subnets, routes, and encryption links are deleted.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel.
3. On the **Networking** screen, select **Edit configuration** on the **Actions** menu.
4. On the **Edit Configuration** screen, do one of the following:
   - **Add**. Click **Add port set** on the **Actions** menu. Use the **Add Port Set** dialog to add a port set.
   - **Edit**. Click its edit icon ( ) on the **Port Sets** panel. On the **Port Set** screen, click **Edit port set** on the **Actions** menu. Use the **Edit Port Set** dialog to change settings.
   - **Delete**. To delete a port set, click its delete icon ( ) on the **Port Sets** panel. Use the **Delete Port Set** dialog to delete the port set.
5. **Settings for adding and editing a port set**

- **Name**. Is a required text field that identifies the port set.
- **Ports**. A list of network ports on the StoreOnce System is shown with check boxes to add those ports to the port Set. Only ports of the same type and speed may be included in the same port set.

  (Hardware models) The StoreOnce products have three network port types. They are listed on the Port Set configuration page as:

  - **1 Gig TP**. 1 GbE LOM ports (included on all StoreOnce hardware)
  - **10 Gig FIBRE**. 10/25Gb SFP ports (optional expansion)
  - **10 Gig TP**. 10GbE-T ports (optional expansion)

  A port may only be a member of one port set. So any ports already configured in an existing port set are grayed out in the list and cannot be selected.

  Bond mode. When more than one port is selected, a further option appears in the configuration to configure the Bond Mode for the Port Set. All port parameters must match to be bondable.
  - **1 (Active Passive Bonding)**. This option provides basic port failover capability and does not require configuration of the network switch. However it does not result in improved aggregate network performance.
  - **4 (Link Aggregate Control (LACP) Bonding)**.This option aggregates the bandwidth of the network ports, and provides failover, however it does require network switch support and configuration.
  - **6 (Adaptive Load Balance Bonding)**. This option provides port failover capability and some level of bandwidth aggregation. The option does not need switch configuration but the aggregation is less effective than Mode 4.

- **Frame size**. Frame size defines the amount of data contained in an Ethernet frame, the default is 1500 bytes. Larger size frames, often referred to as jumbo frames, can improve performance of the port set. Use this property to increase or decrease the value, which must be an integer between 1280 and 9000.
- **IMPORTANT:** If you specify jumbo frames, other devices on the network (clients and switches) must also be configured to enable jumbo frames. The compatibility is necessary to avoid packets fragmenting or dropping.

6. When you are ready, click **OK**.

IMPORTANT: Your new settings will not become active until you activate the network configuration.

Adding, editing, and deleting subnets

- A subnet can be edited to change its configuration.
- However, you cannot change DHCP to static addressing, or from static to DHCP. To change the addressing, delete the subnet and then add a new subnet to replace it.
- Subnets can be deleted. When you activate the new configuration, the subnet is deleted. Also, any associated routes, and encryption links are deleted.
- Port sets can have one or more subnets, depending on the configuration:

- A maximum of 1 subnet, if configured with DHCP support IPv4 and IPv6 with no VLAN tagging.
- A maximum of 2 subnets, if configured with static addressing, a separate subnet can be created for IPv4 and IPv6.
- A maximum of 128 subnets per protocol (IPv4 and IPv6), if VLAN tagged subnets are created.

  However, there is a maximum of 128 subnets per protocol for a StoreOnce System. The subnets can be spread across multiple port sets or included in a single port set.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel.
3. On the **Networking** screen, select **Edit configuration** on the **Actions** menu.
4. On the **Edit Configuration** screen, click the edit icon ( ) for the port set.
5. On the **Port Set** screen, do one of the following:
   - **Add**. Click **Add subnet** on the **Actions** menu. Use the **Add Subnet** dialog to add a subnet.
   - **Edit**. Click its edit icon ( ) on the **Subnets** panel. On the **Subnet** screen, click **Edit subnet** on the **Actions** menu. Use the **Edit Subnet** dialog to change settings.
   - **Delete**. To delete a subnet, click its delete icon ( ) on the **Subnets** panel. Use the **Delete Subnet** dialog to delete the subnet.
6. **Settings for adding and editing a subnet**
   - **IP Assignment**. When adding a subnet, you must first select the IP assignment, **Manual** or **Automatic (DHCP)**. When editing a subnet, the IP assignment cannot be changed.

     If you select **Manual**, you can specify:
     - **IP address**. IPv4 or IPv6 format.
     - **Prefix**. Network prefix in CIDR format as a numeric value (without a / character).
     - **VLAN** (optional). VLAN tag numeric value.

       No entry implicitly indicates there is no tagging. An entry of zero (0) explicitly indicates there is no VLAN tagging. When tagged, the allowed values are 2 to 4094.
     - **Gateway address** (optional). Network gateway IP address in IPv4 or IPv6 format. The IP address must be in the same subnet range as the IP address.
   - If you select **Automatic (DHCP)**, you can specify:
     - **Protocol**. IPv4 or IPv6.
     - **VLAN** (optional). VLAN tag numeric value.

       No entry implicitly indicates there is no tagging. An entry of zero (0) explicitly indicates there is no VLAN tagging. When tagged, the allowed values are 2 to 4094.
     - **IPv4 Gateway address** (optional). This choice is displayed if IPv4 protocol is selected. Network gateway IP address in IPv4 or IPv6 format. The IP address must be in the same subnet range as the IP address.

TIP: Only provide this gateway if you want to override the gateway that is supplied by DHCP.

- **Allow management traffic**. All subnets can be enabled to allow access to the StoreOnce management interface and REST interface. The default is to enable. Disabling the setting prevents management administration from the subnet.
- **Services** (optional). All subnets can be configured to provide access to a mixture of data interface types. Select the protocols that are required to be accessible through this interface.
  - iSCSI protocol (RMC) (mutually exclusive with VTL)
  - iSCSI protocol (VTL) (mutually exclusive with RMC)
  - NAS (CIFS and NFS)
  - Catalyst and Replication
  - SNMP

7. When you are ready, click **OK**.

IMPORTANT: Your new settings will not become active until you activate the network configuration.

Adding, editing, deleting static routes

After a subnet has been created, static routes can be added. Static routes can be helpful for accessing a StoreOnce System through a gateway other than the one defined in the main subnet configuration.

To add a static route:

- The active network configuration must already include the subnet.
- The subnet IP assignment must be static.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel.
3. On the **Networking** screen, select **Edit configuration** on the **Actions** menu.
4. On the **Edit Configuration** screen, click the edit icon ( ) for the port set.
5. On the **Port Set** screen, click the edit icon ( ) for the subnet.
6. On the **Subnet** screen, do one of the following:

- **Add**. Select **Add route** on the **Actions** menu. Use the **Add Route** dialog to add a route.
- **Edit**. Click its edit icon ( ) on the **Routes** panel. Use the **Edit Route** dialog to change settings.
- **Delete**. To delete a route, click its delete icon ( ) on the **Routes** panel. Use the **Delete Route** dialog to delete the route.

7. **Settings for adding and editing a route**
   - **Target address**. The IP address of the target, which may be a specific IP address or the subnet on which it is located. The final values in the IP address indicate whether this address is a host (specific value) or a subnet (value = 0). For example:

     xxx.xxx.xxx.0 indicates any target on the specified IPv4 subnet.

     xxxx:xxxx:xxxx:xxxx:: indicates any target on the specified IPv6 subnet.
   - **Prefix**. Defines the range of IP addresses that are available in the subnet to which the route is being created.
   - **Gateway address**. The address of the gateway through which traffic will be routed to the target host or subnet, this address must be in the same range as the current address.
8. When you are ready, click **OK**.

IMPORTANT: Your new settings will not become active until you activate the network configuration.

Adding and deleting encryption links

After subnets are created, you can add point-to-point, data-in-flight encryption links (using IPsec) on a per subnet basis. Data-in-flight encryption can be used to secure network links between data centers for StoreOnce VT libraries, NAS replication, or low-bandwidth Catalyst Copy operations.

- **IMPORTANT:** Data-in-flight encryption is not supported for DHCP or IPv6 subnets.

  If you select an IPv6 subnet, encryption links actions are not displayed.
- Encryption links can be created and deleted, but cannot be edited.
- There are no limits to the number of encryption links per subnet.
- HPE recommends that the StoreOnce System and client computer equivalent data-in-flight configurations and use the same passphrase.

Prerequisites

- The encryption links feature requires a StoreOnce Security Pack license.
- The subnets must have already been created.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel.

3. On the **Networking** screen, select **Edit configuration** on the **Actions** menu.
4. On the **Edit Configuration** screen, click the edit icon ( ) for the port set.
5. On the **Port Set** screen, click the edit icon ( ) for the subnet.
6. On the **Subnet** screen, do one of the following:
   - **Add**. Select **Add encryption link** on the **Actions** menu. Use the **Add Encryption Link** dialog to add a link.
   - **Delete**. To delete a link, click its delete icon ( ) on the **Encryption Links** panel. Use the **Delete Encryption Link** dialog to delete the link.
7. **Settings for adding an encryption link**
   - **Target Address**. The IP address of the remote device. For example, a client or another StoreOnce System used for replication and StoreOnce Catalyst copy.
   - **Passphrase**. The passphrase to use for the link. The passphrase will be shown as dots. To display the passphrase in text, check **Show passphrase** check box.

     Ensure that the passphrase is also configured on the target device.
8. When you are ready, click **OK**.

IMPORTANT: Your new settings will not become active until you activate the network configuration.

Editing DNS servers

You can include up to three DNS servers, and one DNS Search Suffix, in a StoreOnce network configuration.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel.
3. On the **Networking** screen, select **Edit Configuration** on the **Actions** menu.
4. On the **Edit Configuration** screen, select **Edit DNS** on the **Actions** menu.
5. On the **DNS Configuration** dialog:
   - **DNS address**. IP address of the DNS server in IPv4 or IPv6 format.

     Up to three DNS addresses can be included. If you enter fewer than 3 static addresses, DHCP can add addresses. The static entries take precedence.
   - **DNS search domains**. Up to 6 are allowed statically. DHCP can extend it to a total of 8. The static entries take precedence.

Pinging systems

Pinging allows you to check the connectivity from the StoreOnce System to backup clients, servers, and other StoreOnce Systems.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel.
3. On the **Networking** screen, select **Ping** on the **Actions** menu.
4. On the **Ping** dialog, enter an IPv4 or IPv6 address. Click **Begin**.

   The results of the test are displayed.

Using traceroute

Traceroute allows you to check the network path from the StoreOnce System to backup clients, servers, and other StoreOnce Systems. You can use traceroute to help resolve performance issues.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Networking** panel.
3. On the **Networking** screen, select **Traceroute** on the **Actions** menu.
4. On the **Traceroute** dialog, enter an IPv4 or IPv6 address. Click **Begin**.

   The results of the test are displayed.

Fibre Channel

StoreOnce VSA and Fibre Channel support

When running on VMware, StoreOnce VSA systems support Fibre Channel (target mode) connectivity for StoreOnce Catalyst and VT library targets.

This StoreOnce VSA functionality is not supported on Hyper-V.

To enable Fibre Channel device support on a StoreOnce VSA, set up a VM-direct path I/O to the StoreOnce VSA from the ESXi host. The Fibre Channel HBA device is provided directly to the StoreOnce VSA through a physical device passthrough mechanism. Once the VM-direct path I/O is set up, the StoreOnce VSA can act as a Fibre Channel target over StoreOnce Catalyst and VT Library interfaces.

IMPORTANT: To support VT libraries over Fibre Channel, NPIV (N-port ID Virtualization) must be enabled on the Fibre Channel switch under the SAN fabric.

See the *VMware Compatibility Guide for Supported Server Models with FC VM-Direct Path Feature* and the VMware knowledge base for more information on configuring passthrough.

Viewing Fibre Channel port settings and properties

You can view the settings and properties of the Fibre Channel ports on StoreOnce Systems.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Fibre Channel** panel.
3. The **Fibre Channel** screen shows a list of the Fibre Channel ports on the StoreOnce System.

TIP: Columns for the most often viewed settings and properties are shown by default. To add or remove columns, click the column selector icon ( ).

Fibre Channel settings and properties

Fibre Channel screen

TIP: Columns for the most often viewed settings and properties are shown by default. To add or remove columns, click the column selector icon ( ).

Property	Description
Status	The status of each port. Can be Up, Down, Warning, Error, or Not Used. Warnings occur if the port is not available or is down, or if the system is unable to obtain speed information. Errors occur if there is a fault or the system cannot obtain the link status.
Port Location	The physical location of the Fibre Channel port, described by the PCIe card slot number that the card is in and the physical port number. For example, Slot 5 Port1.
Current Speed	The current speed of the port. Controlled by the Selected Speed.
Selected Speed	You can use the **Edit Port** dialog to control the speed. Choices are Auto, 1G, 2G, 4G, 8G, 16G, and 32G. When using auto-negotiate, the speed will be auto-negotiated between the switch and the StoreOnce System to select the highest supported speed.
Beacon	You can use the **Edit Port** dialog to enable and disable the beacon. The beacon toggles an LED on the physical HBA. The color of the button changes to show the status of the beacon. Grey is off, blue is on.
More properties	
Topology	You can use the **Edit Port** dialog to select the topology. Choices are N_Port, Loop, and Auto. Loop mode (private loop) is a direct connection between a host and the StoreOnce System without a switch. Private loop is supported up to 8 Gb speeds only (does not support 16 Gb and 32 Gb).
Status Information	Provides the reason if the port status is Error. A healthy port does not report any status information.

Editing Fibre Channel port settings

WARNING: Editing the Fibre Channel port settings resets the Fibre Channel link and can affect backup and restore jobs that are running.

TIP:

- Fibre Channel port settings apply to StoreOnce Catalyst target devices over Fibre Channel, and VT libraries.
- Changing the port speed causes the port status to be reported as Down.

Prerequisites

Only administrators can edit the Fibre Channel port settings.

Procedure

1. On the main menu, select **Settings**.
2. In the **Hardware** section, click the **Fibre Channel** panel.
3. On the **Fibre Channel** screen, select the port and then click the edit icon ( ).
4. On the **Edit Port** dialog, make your changes and click **Update**.

User management settings

User roles and types

TIP: To identify the current user, click the user icon ( ) in the lower left corner of the main menu.

User roles

The following roles can be associated users:

- **Administrator**: This role allows a user to create and edit management and StoreOnce functions in the StoreOnce Management Console. Any user with the Administrator role has the same permissions as the default Admin account.
- **Observer**: This role limits access to monitoring and viewing.
- **SecurityOfficer**: This role limits the user to creating, editing, and managing security features. For example, key managers, SSL certificates, user management, and directory management.
- **BackupAdmin**: This role limits the user to creating, editing, and managing data services features.
- **Backup Operator**: This role limits the user to monitoring and viewing the data services features.

User types

The following types of user accounts are available:

- Local User (with an Administrator or Observer role): Logs in locally and is authenticated using credentials on the StoreOnce System.
- Directory User (with any user role): Logs in as a domain user. External users are authenticated using their domain credentials by an external Microsoft Active Directory Server.
- Directory Group (with any user role): A Microsoft Active Directory group. Members of the group login as domain users.

TIP: To add directory users or groups, first add the HPE StoreOnce device to an Active Directory domain. Then configure the connection to the Active Directory domain. See **Adding directory servers** on page 184.

Default account

- When a StoreOnce System is installed, one default user account (Admin) is created with the Administrator role. You cannot delete the account.

  When you first access a StoreOnce System, you use the StoreOnce First Time Setup wizard to set the password for the Admin account.

  IMPORTANT: HPE strongly recommends that you change the default password. After the Admin account password has been changed, it cannot be changed back to the default password.

- If Admin credentials are lost, the Admin password can be reset through a locally attached Initialisation Console. HPE recommends changing the Initialisation Console password after installation and storing it in an offline password security tool.

Best practices

- After using the StoreOnce First Time Setup wizard, a user with the Administrator role can configure additional user accounts. HPE recommends assigning roles to user accounts that allow the minimum necessary privileges to prevent accidental or malicious data loss.
- If you create a group with the Observer role, HPE recommends setting up a user in the group with the Administrator role. (Roles set with the Add User action take precedence over roles set with the Add Group action).
- HPE recommends using Active Directory or LDAP users types, if possible.
- If you use the StoreOnce federations features, HPE recommends that you add users to all the StoreOnce Systems in the federation to enable remote management.

Adding, editing, and deleting users and groups

Procedure

1. On the main menu, select **Settings**.
2. In the **User Management** section, click the **Users and Groups** panel.
3. On the **Users and Groups** screen:
   - To add a user or group, Select **Add user or group** on the **Actions** menu.
   - To edit a user, click the user name.
   - To remove a user, click the user name, then click **Remove**.

Adding directory servers

Procedure

1. On the main menu, select **Settings**.
2. In the **User Management** section, click the **Directory** panel.
3. On the **Directory** panel, click the **Add** or the + icon.
4. On the **Connect to Directory Server** screen, complete the fields and click **Connect**.
5. On the **Add Directory Server** screen, click **Trust Certificate**.
6. Click **Trust** to accept the certificate from the directory server and proceed with the configuration process.
7. On the **Configure Directory Server** screen, complete the fields, and click **Ok** to finish.

Removing directory servers

Procedure

1. On the main menu, select **Settings**.
2. In the **User Management** section, click the **Directory** panel.
3. On the **Directory** panel, click the remove icon ( ).

Configuring password policies

Procedure

1. On the main menu, select **Settings**.
2. In the **User Management** section, click the **Users and Groups** panel.
3. On the **Users and Groups** screen, select **Configure password policy** on the **Actions** menu.

Security settings

Certificates

The StoreOnce Management Console is accessed through the HTTPS protocol. HTTPS requires the exchange of an SSL (Secure Sockets Layer) certificate to authenticate the connection between a web browser and the StoreOnce System.

By default, StoreOnce Systems return a generic certificate. The generic certificate is created when a StoreOnce System is deployed for the first time. The generic certificate cannot be verified up to a trusted certificate authority, therefore it is not considered to be secure by web browsers.

You can replace the generic security certificates with your own trusted certificates. Learn more: **Replacing default certificates - overview** on page 186.

Certificate Authority (CA)

A certificate authority (CA) is a trusted organization that issues digital certificates that verify the ownership of a public encryption key. Certificates that are signed by certificate authorities provide verification to devices, browsers, and websites that the certificate source has been validated and can be trusted.

Viewing security certificates

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Certificates** panel.

   The **Certificates** screen is displayed.

   - The top portion of the **Certificates** screen shows the details of the current CA-signed server certificate for the StoreOnce system.
   - The bottom portion of the screen shows the list of root and intermediate CA-signed certificates for the server certificate.

   Learn more: **Certificate Authority (CA)** on page 186.

3. To view the details of a root or intermediate CA-signed certificate, click its panel.

Replacing default certificates - overview

This overview describes how to replace the default security certificates on a StoreOnce System with certificates for your environment.

Procedure

Generate and submit a certificate signing request

1. On the StoreOnce Management Console for the StoreOnce System, generate a certificate signing request (CSR). For details, see **Generating certificate signing requests (CSR)** on page 187.

   TIP: If your certificate authority (CA) does not require a certificate signing request, this step is not required. For example, this step is not required if the certificate authority provides a private key.

2. In a separate application, submit the CSR to your certificate authority.

Receive and import the CA-signed certificates

3. In a separate application, receive the CA-signed certificates. Depending on the certificate authority, it might take several hours or longer to receive the signed certificates.
   - At a minimum, the certificate authority response will include a root CA certificate and a CA-signed server certificate.
   - In some cases, the certificate authority response might also include a private key, intermediate CA certificates, or both.
4. In a separate application, save the CA-signed certificate files to a location where you can copy them to your clipboard.
5. On the StoreOnce Management Console for the StoreOnce System, import the certificates. For details, see **Importing security certificates** on page 188.

Generating certificate signing requests (CSR)

TIP: If your certificate authority does not require a CSR, this step is not required. For example, this step is not required if the certificate authority provides a private key.

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Certificates** panel.
3. On the **Certificates** screen, select **Generate CSR** on the **Actions** menu.
4. On the **Generate CSR** dialog, click the edit icon ( ).
5. On the **Distinguished Name** dialog, replace the default properties that were provided with the StoreOnce System with the properties for your environment. Click **OK**. The screen returns to the **Generate CSR** dialog.

   IMPORTANT: In a security certificate, the Common Name, and Subject Alternative Name (if any), must match the host name of the system. Otherwise, browsers will report that the host is not trusted.
6. On the **Generate CSR** dialog, a message warns that changing the **Distinguished Name** will cause the screen to refresh. This message is expected behavior. To proceed to the **Certificate Signing Request** dialog, click **Change**.
7. On the **Certificate Signing Request** dialog, click **View Certificate Sign Request (CSR)**.
8. On the **Certificate Signing Request** dialog, follow the onscreen instructions to copy the CSR text to your clipboard. Click **OK**.

   TIP: Depending on your certificate authority, you might need to save the CSR text to a file. Or, you might paste it in to another application.
9. In a separate application, submit the CSR to your certificate authority. When you receive the certificates, continue with the process. See **Replacing default certificates - overview** on page 186.

Importing security certificates

Prerequisites

- You have generated and submitted a certificate signing request for the StoreOnce System to your certificate authority.
- You have received the CA-signed certificates for the StoreOnce System. They are located where you can copy the certificate text to your clipboard.

  If you received a private key, it is located where you can copy its text to your clipboard.

Procedure

1. On the main menu of the StoreOnce System, select **Settings**, and then click the **Certificates** panel.
2. In the **Security** section, click the **Certificates** panel.
3. On the **Certificates** screen, select **Import Certificates** on the **Actions** menu.
4. Click **Import Root and Intermediate Certificates**.

   a. In a separate application, locate the CA signed certificate. Copy its contents to your clipboard.

   b. In the StoreOnce Management Console, paste the contents of the CA signed certificate in the text box. Click **Import**.

   TIP: You can import only one certificate at a time. If you have more than one, repeat this step.

   The certificate is added to the StoreOnce System and the **Import Certificates** dialog is redisplayed.

   The **CA Certificates** panel on the **Import Certificates** dialog indicates that the number of certificates that have been imported. You can click the information icon (ⓘ) to see the list of imported certificates on the StoreOnce System.
5. If you received a private key from the certificate authority, click **Private Key** and then click **Add Private Key**.

   a. In a separate application, locate the CA private key. Copy its contents to your clipboard.

   b. In the StoreOnce Management Console, paste the contents of the CA private key in the text box.

   c. If the CA private key is encrypted, enter its encryption password.

   d. Click **Add**.

   The private key is added and the **Import Certificates** dialog is redisplayed.
6. Click **Import CA-signed Server Certificate**

   a. In a separate application, locate the CA-signed server certificate. Copy its contents to your clipboard.

   b. In the StoreOnce Management Console, paste the contents of the CA-signed server certificate in the text box. Click **Import**.

IMPORTANT: HPE recommends that you close the browser session after clicking **Import**. Then start a new browser session. Starting a new browser session is required for the new CA-signed server certificate to take effect with the browser.

Removing CA security certificates

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Certificates** panel.

   The **Certificates** screen shows the details of the security certificate for the StoreOnce system and a list of CA certificates.

   Learn more: **Certificate Authority (CA)** on page 186.
3. To remove a CA certificate, click its panel and then select **Remove** in the lower right corner of the dialog.

Key Manager

StoreOnce Systems can use the Local Key Manager (LKM) or External Key Manager (EKM) to manage keys for Data at Rest and Data in Flight encryption. The Local Key Manager is the default key manager and is used unless a StoreOnce System has been configured to use the External Key Manager.

StoreOnce Systems support the following external key manager products:

- Micro Focus Enterprise Secure Key Manager (ESKM)
- Gemalto SafeNet KeySecure

At any point in time, you can configure a StoreOnce System to use the Local Key Manager or the External Key Manager. However, the two key managers cannot be used at the same time.

Best practices

Local Key Manager. When using the Local Key Manager, the local key store contains the encryption keys used for Data at Rest Encryption or Data in Flight Encryption.

HPE recommends that you back up the local key store and save it securely off site in case the original key store becomes corrupted.

Keep only the latest version of the key store after you create or delete an encrypted VT library, NAS share, StoreOnce Catalyst store, or data in flight encryption link.

External Key Manager. When using the External Key Manager, the local key store contains only the credentials required to authenticate with an external key manager product.

HPE recommends that you back up the local key store after the StoreOnce System has been successfully configured to use an external key manager product.

All the encryption keys used for Data in Flight Encryption or Data at Rest Encryption are stored and managed by the external key manager product.

Viewing the Key Manager mode

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Key Manager** panel.

   The **Key Manager** screen is displayed.

   The **Overview** panel shows the name of the Key Manager mode that is enabled.

   If the **External Key Manager** mode is enabled:

   - The **Overview** panel displays the External Key Manager type and its IP address.
   - The **Certificates** panel lists the applicable security certificates for the External Key Manager.
3. To view the details of an External Key Manager certificate, click its panel.

Backing up Key Manager configurations

HPE strongly recommends making regular backups of the Key Manager on StoreOnce Systems.

Circumstances for making backups that deserve special attention include:

- When the Local Key Manager mode is active and you have just created an encrypted StoreOnce VT library, NAS share, Catalyst store, or Cloud Bank store.
- After enrolling a StoreOnce System with an external key manager product. You will be asked to create a backup of the local key manager. HPE strongly recommends that you retain a copy of the backup.

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Key Manager** panel.
3. On the **Key Manager** screen, select **Backup** on the **Actions** menu.
4. On the **Backup** dialog, enter and confirm the password that you want to use for the encrypted StoreOnce Key Manager file.

   IMPORTANT: The Key Manager backup file is encrypted with the password that you enter. The Key Manager backup can only be restored by providing that password.

Restoring Key Manager configurations

This procedure is intended for the rare circumstances in which the Key Manager on a StoreOnce System must be restored.

Prerequisites

You have access to the Key Manager backup file for the StoreOnce System and know its password.

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Key Manager** panel.
3. On the **Key Manager** screen, select **Restore** on the **Actions** menu.
4. On the **Restore** dialog, read the warning message. When ready, enter the password for the Key Manager configuration backup file.
5. Click the confirmation check box, and then click **OK**.

   The Key Manager configuration is restored.

Enrolling with an External Key Manager

This procedure describes how to enroll a StoreOnce System with an External Key Manager. Completing the procedure disables the StoreOnce Local Key Manager mode and enables the External Key Manager mode.

Once a StoreOnce System is enrolled with an external key manager product, the encryption keys are migrated from the Local Key Manager to the External Key Manager. The keys are no longer persisted on the StoreOnce System.

Prerequisites

You are familiar with your External Key Manager and know your External Key Manager login user name and password.

Procedure

Generate and submit an External Key Manager certificate signing request

1. On the StoreOnce Management Console for the StoreOnce System, generate an External Key Manager certificate signing request. For details, see **Generating External Key Manager certificate signing requests** on page 192.
2. In the External Key Manager application, paste the EKM certificate signing request text in the relevant application screen.

Receive the External Key Manager signed certificate

3. In a separate application, receive the External Key Manager signed certificate.

Using the Enroll dialog

4. On the StoreOnce Management Console for the StoreOnce System, click **Enroll**. The **Enroll** dialog opens.

   IMPORTANT: To complete the enrollment, you must make a backup copy of the Local Key Manager configuration. The backup is required in case you have to withdraw from the External Key Manager at a later date.

5. On the **Enroll** dialog, click **Backup the key manager configuration**. The **Backup** dialog opens.
6. On the **Backup** dialog, enter the password that you want to use to encrypt the backup copy of the Local Key Manager configuration. Click **Backup**. The **Enroll** dialog is redisplayed and shows that the backup action has been completed.
7. On the **Enroll** dialog, click **Configure External Key Manager Server**.

8. On the **Configure External Key Manager Server** dialog, provide the information for the External Key Manager. Click **OK**.
   - For **ESKM**, enter the IP addresses of the servers, the Certificate authority name, Port number, and ESKM EKM credentials.
   - For **SafeNet**, enter the IP addresses of the servers, the Port number, and the SafeNet EKM password.

   The **Enroll** dialog is redisplayed and shows that the External Key Manager information has been entered.
9. In the External Key Manager application, copy the root CA certificate text to your clipboard.
10. On the **Enroll** dialog, click **Import Root Certificate**.
11. On the **Import Root Certificate** dialog, paste the certificate text in the text box. Click **OK**.

    The **Enroll** dialog is redisplayed and shows that the root certificate has been staged for enrollment.
12. In the External Key Manager application, copy the signed certificate text to your clipboard.
13. On the **Enroll** dialog, click **Import Signed Certificate**.
14. On the **Import Signed Certificate** dialog, paste the certificate text in the text box. Click **OK**.

    The **Enroll** dialog is redisplayed and shows that the signed certificate has been staged for enrollment.
15. To start the enrollment, click **Enroll**.
    - The enrollment can take several seconds.
    - When enrollment is completed, the Key Manager mode for the StoreOnce System is changed from Local Key Manager to External Key Manager.

Generating External Key Manager certificate signing requests

Prerequisites

You are familiar with your External Key Manager and know your External Key Manager login user name and password.

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Key Manager** panel.
3. On the **Key Manager** screen, select **Generate CSR** on the **Actions** menu.
4. On the **Generate CSR** dialog, click **Provide External Key Manager Credentials**.
5. On the **External Key Manager Credentials** dialog, enter your External Key Manager login user name and password. Click **OK.**

   The **Generate CSR** dialog is redisplayed and your External Key Manager user name is shown.
6. Click **Generate**.

   The **Signing Request** dialog opens.

7. On the **Signing Request** dialog, follow the onscreen instructions to copy the External Key Manager signing request text to your clipboard. Click **OK**.
8. In a separate application, submit the External Key Manager certificate signing request to your certificate authority. When you receive the certificates, continue with the enrollment process. See **Enrolling with an External Key Manager** on page 191.

Renewing External Key Manager certificates

Prerequisites

- The External Key Manager mode is currently enabled.
- You are familiar with your External Key Manager and know your External Key Manager login password.
- You have received new certificates. The certificates are located where you can copy the certificate text to your clipboard.

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Key Manager** panel.
3. On the **Key Manager** screen, select **Renew Certificates** on the **Actions** menu.
4. On the **Renew** dialog, click **Configure Renew settings**.
5. On the **Renew Settings** dialog, enter your External Key Manager login password. Click **OK.**

   The **Renew** dialog is redisplayed and indicates that the settings are configured.

Import the root CA certificate

6. In a separate application, copy the root CA certificate text to your clipboard.
7. On the **Renew** dialog, click **Import Root Certificate**.
8. On the **Import Root Certificate** dialog, paste the certificate text in the text box. Click **OK**.

   The **Renew** dialog is redisplayed and shows that the root certificate has been provided.

Import the signed certificate

9. In a separate application, copy the certificate text to your clipboard.
10. On the **Renew** dialog, click **Import Signed Certificate**.
11. On the **Import Signed Certificate** dialog, paste the certificate contents in the text box. Click **OK**.

    The **Renew** dialog is redisplayed and shows that the signed certificate has been staged provided.
12. To proceed with the renewal, click **Renew**.

    The **Key Manager** screen is redisplayed. The new expiration dates for the certificates are shown on the **Certificates** panel.

Withdrawing from an External Key Manager

This procedure describes how to withdraw a StoreOnce System from an External Key Manager. Withdrawing from the External Key Manager will return the StoreOnce System to Local Key Manager mode.

⚠ **WARNING:** Withdrawing from the External Key Manager mode can result in total data loss on the StoreOnce System.

When you withdraw the keys that are on the external key manager product are no longer available to the StoreOnce System.

If you must withdraw, you can restore a copy of the local key manager that you backed up when enrolling with the external key manager product. However, the backup will not contain any new keys that were generated when the StoreOnce System was in External Key Manager mode.

Prerequisites

The External Key Manager mode is currently enabled.

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Key Manager** panel.
3. On the **Key Manager** screen, select **Withdraw** on the **Actions** menu.
4. On the **Withdraw** dialog, read warning message and carefully consider whether you want to proceed. To proceed, click the confirmation check box.
5. Enter your StoreOnce login password and then click **Withdraw**.

   Withdrawal is completed. The **Key Manager** screen indicates that the Local Key Manager mode is re-enabled.

EKM enrollment common errors

Overview

- Most errors during an EKM enrollment will require that you use the **Withdraw** action and restart the enrollment.
- When you withdraw from an external key manager, you must restore the Local Key Manager key store that you backed up when you started the enrollment.

Possible enrollment errors

- **Failed to communicate with the external key manager**. The user credentials are incorrect, or the wrong certificates were uploaded. This error is the most common type.
- **User or group already exists**. A user or group exists on the external key manager that is identical to the user and group for the enrollment.

  The duplicate user or group was created during a previous enrollment attempt. These accounts are not automatically deleted on the external key manager. Manually delete the accounts.

Data in Flight encryption guidelines

General

- The encryption is software-based and is a licensed feature of StoreOnce Systems.
- It is supported for low-bandwidth replication and low-bandwidth copy jobs.
- Is not recommended for backup up jobs due to performance.
- Is compatible with Gen3 StoreOnce Systems.
- StoreOnce Data Services have no visibility of Data in Flight encryption.
- Does not support certificate-based authentication.
- Is not applicable to Fibre Channel traffic.

Networking detail

You can set up multiple encrypted links for each subnet to allow connectivity to multiple client systems.

IMPORTANT: Data in Flight encryption is:

- Not supported for IPv6 subnets.
- Not supported for direct backup operations to StoreOnce Systems over a local network. This support consideration is due to the performance impacts of encryption.
- Intended to secure network links between data centers for StoreOnce VT library or NAS replication, or for low-bandwidth StoreOnce Catalyst copy operations.

A single encryption link allows a specific client IP address to have a secure connection with all nodes and IP addresses configured by the subnet. Each encryption link applies to:

- All IP addresses in the subnet of the specific network addressing mode (IPv4) including both VIF and physical address, if appropriate.
- All nodes in the cluster.

The following Data In Flight encryption guidelines apply:

- Configure the StoreOnce systems and client computer with an equivalent configuration and use the same passphrase.
- There is no limit to the number of encryption links per subnet.
- If using IPv4, configurations for encryption links are possible and auto detected based on the IP address format used for the client-side IP.
- You cannot configure encryption links on DHCP-enabled subnets.
- You cannot configure encryption links on IPv6 subnets.
- You can create and delete encryption links, but you cannot modify them. To change the passphrase used for a link, delete and recreate that link with the new passphrase.
- You must have an active security pack license on the StoreOnce System to create encryption links.

  If no license was applied or the license has expired, the encryption link section of the StoreOnce Management Console will show a warning. In this case, you cannot create encryption links. However, you can delete encryption links that were created before the security pack license expired.

Login Banner

Enabling and disabling StoreOnce login banners

Administrators can enable and disable an informational banner that is displayed on the StoreOnce Management Console login screen.

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Login Banner** panel.

Sessions

Viewing sessions

You can view a list of open user sessions. The user name, IP address, and date and time when the login was initiated are shown.

TIP: Users with the Administrator role can force close any of the open sessions in the list.

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Sessions** panel.

   The **Sessions** screen shows a list of active sessions.

Configuring session timeout policy

You can configure the user session timeout policy for the StoreOnce System. Open sessions are automatically logged out after the timeout period is reached.

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Sessions** panel.
3. On the **Sessions** screen, click the tools icon ( ).

Initialisation Console credentials

Initialisation Console user name and password

The StoreOnce Initialisation Console user name and password are used to log in to a StoreOnce Initialisation Console through a login prompt.

Typical Initialisation Console user login methods are:

- For StoreOnce VSA:
  - Using a hypervisor console to access a StoreOnce VSA System.

For more information about the Initialisation Console, see the *HPE StoreOnce VSA Deployment and Configuration Guide*.

Depending on the login connection method, a StoreOnce Initialisation Console user can:

- Reset the StoreOnce administrator user (*Admin*) password.
- Generate a StoreOnce support login challenge for support access.
- View or change the StoreOnce System IP address.
- Change the StoreOnce Initialisation Console user password.

Initial setting

The StoreOnce Initialisation Console user name is *console*. The Initialisation Console user name cannot be changed.

The Initialisation Console default password is *changeme*. During the first login to a StoreOnce System, an administrator must change the Initialisation Console user password. The change is required on first login when using a login prompt, or using the First Time Setup wizard.

The Initialisation Console user password can be also changed after the first login. Learn more: **Changing the Initialisation Console user password** on page 197.

Changing the Initialisation Console user password

You can change the Initialisation Console user password for a StoreOnce System. Learn more: **Initialisation Console user name and password** on page 196.

You can change the password from within the Initialisation Console or from the StoreOnce Management Console. The following procedure is for the StoreOnce Management Console.

Procedure

1. On the main menu, select **Settings**.
2. In the **Security** section, click the **Console Password** panel.

Data at Rest encryption guidelines

Data at Rest encryption ensures that data cannot be accessed on stolen, discarded, or replaced disks. It is not intended to protect a running StoreOnce System from being attacked.

General

- The encryption is software-based and is a licensed feature of StoreOnce Systems.
- Data at Rest encryption can be applied to VT libraries, NAS shares, and StoreOnce Catalyst stores. You must enable Data at Rest encryption when creating the VT library, NAS share, or StoreOnce Catalyst store. The encryption cannot be enabled after creation of the device.
- Data is encrypted post-deduplication. Encryption has no impact on the deduplication ratio.
- Data is unencrypted as it is read from disk for restore, replication, and copy jobs.

Detail

- The encryption algorithm is AES-256.
- A key obtained from the StoreOnce Key Manager is used for key wrapping keys (KEK) and data encryption keys (DEK).
- The wrapped DEK is persisted on the StoreOnce System.
- If a StoreOnce system is configured to use an external key manager, the KEK is not persisted within the StoreOnce system.

Support settings

Remote Support

If Remote Support is enabled, your StoreOnce System automatically contacts Hewlett Packard Enterprise if issues arise, such as a hardware component failure.

Also, Remote Support sends telemetry information to Hewlett Packard Enterprise. You can view this information on the HPE InfoSight website at **https://infosight.hpe.com**.

Configuring remote support

The Remote Support screen allows you to view the level of remote support with HPE.

Remote support can be enabled and disabled. Remote support is disabled by default. You can configure the remote support level, proxy server, site information, and customer information.

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Remote Support** panel.

   The **Remote Support** screen opens. A status bar near the top of the screen indicates whether remote support is enabled or disabled. Remote support is disabled by default.
3. To enable or disable remote support, click **Configure remote support** on the **Actions** menu. The **Configure Remote Support** dialog opens.

   a. To enable or disable remote support, click the edit icon () on the **General** panel. The **Remote Support Options** dialog opens.

   b. To enable remote support, click **Send support data to HPE**. To disable remote support, click **No support**.

   c. If you chose to enable remote support, HPE recommends that you also select **Allow HPE and partners to contact me**.

   d. You can also click **Advanced options** to see the URL of the **Enterprise server** that receives event messages. You do not need to change the URL.

   e. When you have completed your choices, click **OK**. The dialog closes and the **Configure Remote Support** dialog is redisplayed. Your choice for remote support level is shown. If you have chosen to enable remote support, the **Proxy** panel is displayed.
4. On the **Proxy** panel, click **Configure Remote Support Proxy**. The **Proxy** dialog opens.

   a. To specify a proxy server, click the **Proxy Required** toggle and enter:

- **IP address**. The IP address of the proxy server that connects to the Internet.
- **Port**. The port used by the proxy server.

b. To specify authentication (if required), click the **Proxy server authentication** toggle, and then enter **Username** and **Password** to log in to the proxy server.

c. Click **OK**. The dialog closes and the **Configure Remote Support** dialog is redisplayed. Your entries for the proxy are shown.

5. Click **Enter Site Information**. The **Site Information** dialog opens. Enter your site information. Click **OK**. The dialog closes and the **Configure Remote Support** dialog is redisplayed. Your entries for site information are shown.
6. Click **Enter Customer Information**. The **Customer Information** dialog opens. Enter your customer information. Click **OK**. The dialog closes and the **Configure Remote Support** dialog is redisplayed. Your entries for site information are shown.
7. Click **Update**. The **Remote Support** screen is redisplayed with the new Remote Support Configuration.

Viewing the temporary support password mode

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Temporary Support Password** panel.
3. The **Temporary Support Password** screen indicates the temporary support password mode, *time*, or *ciphertext*.

Sending test events

You can send a test event to verify Remote Support connectivity to HPE.

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Support** panel.
3. On the **Support** screen, click **Send test event** on the **Actions** menu.

Log Collection

Hewlett Packard Enterprise support will ask customers to upload support tickets to an FTP site to aid diagnosis of issues a customer may be experiencing. Information about support tickets that have been generated is displayed on the Log Collection page.

There are two types of Log Collections that can be generated:

Comprehensive - This Log Collection type contains all the logs from the system, as well as the output of certain commands that are required for debugging.

Slim - This Log Collection type contains a subset of the logs from the Comprehensive ticket. It is typically used by Hewlett Packard Enterprise support to obtain an overview of all the components in the system

Viewing log collections

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Log Collection** panel.

   The **Log Collection** screen shows a list of log collections.
3. To view an individual log collection, click its panel.

Generating, downloading, and removing log collections

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Log Collection** panel.
3. On the **Log Collection** screen, do one of the following:
   - To generate a log collection, click the plus icon (+).
   - To download or remove a log collection, click its download () or remove () icon.

Temporary support passwords

The industry-wide use of static vendor-only support user passwords is not advised in security- and compliance-aware sites. Temporary support passwords functionality replaces those types of passwords in StoreOnce systems.

There are two types of temporary support passwords:

- Time-based passwords
- Encrypted ciphertext passwords

Time-based passwords

Time-based passwords are unique to each support user account and StoreOnce system.

The passwords change each hour and can only be generated in the HPE support center to authorized HPE employees and contractors.

While operating in time-based mode, passwords cannot be changed since they change automatically each hour. If you chose time-based passwords, you do not need to change your HPE support processes. Service personnel from HPE can acquire the password when needed without customer interaction.

Encrypted ciphertext passwords

Encrypted ciphertext passwords are randomly created on the StoreOnce system for each support user account.

You can change these passwords any time. However, the passwords are not known to you or to HPE. Recovery is only possible by exporting the ciphertext for transmission to HPE. An HPE authorized support center user can decrypt the ciphertext to provide the password to onsite HPE service personnel or contractors.

If you choose encrypted ciphertext passwords, you must export the ciphertext and provide it to the HPE personnel working with you. The ciphertext is pasted into a tool at HPE that can unwrap and decrypt the ciphertext to recover the password.

After the support activity is complete, you can change the password so that the recovered password is no longer valid.

Viewing the temporary support password mode

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Temporary Support Password** panel.
3. The **Temporary Support Password** screen indicates the temporary support password mode, *time*, or *ciphertext*.

Changing the temporary support password mode

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Temporary Support Password** panel.
3. On the **Temporary Support Password** screen, click **Set mode**.The **Set mode** dialog opens.
4. Select the mode (*time* or *ciphertext*) and click **OK**.

Exporting temporary support password ciphertext

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Temporary Support Password** panel.
3. On the **Temporary Support Password** screen, select **Display ciphertext** on the **Actions** menu. The **Display Ciphertext** dialog opens.
4. Select the **Username** for which the ciphertext is required (*hpeadmin* or *hpesupport*). Click **OK**.

Changing temporary support password ciphertext

Procedure

1. On the main menu, select **Settings**.
2. In the **Support** section, click the **Temporary Support Password** panel.
3. On the **Temporary Support Password** screen, select **Display ciphertext** on the **Actions** menu. The **Display Ciphertext** dialog opens.
4. Select the **Username** for which the changed ciphertext is required (*hpeadmin* or *hpesupport*). Click **Regenerate**.

Notification settings

Notifications

The Notifications screen displays the configuration for sending out event notifications through email.

The configuration includes information for routing email (SMTP server), as well as associating events with destination email addresses.

A single event can generate a notification to multiple email addresses. Also, different sets of events can generate notifications to different email addresses.

Viewing email alerts

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **Notifications** panel.

   The **Notifications** screen **Subscriptions** panel shows the configured email alerts.

Editing SMTP settings

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **Notifications** panel.
3. On the **Notifications** screen, click **Edit SMTP settings** on the **Actions** menu.

Adding SMTP subscriptions

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **Notifications** panel.
3. On the **Notifications** screen, select **Add subscription** on the **Actions** menu.

   NOTE: Each severity alert requires a separate subscription.

Editing and deleting SMTP subscriptions

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **Notifications** panel.
3. On the**Notifications** screen, click its edit icon ( ) or delete icon ( ).

Sending test email

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **Notifications** panel.
3. On the **Notifications** screen, click **Send test email** on the **Actions** menu.

SNMP

Viewing and configuring SNMP

The SNMP (Simple Network Management Protocol) screen allows you to.

- View and edit the SNMP Agent setup.
- Add and manage SNMP users.
- Add and manage SNMP trapsinks.

When the SNMP feature is enabled, it reports the overall StoreOnce System status through SNMP traps. It also reports software status messages and hardware status messages as reported in the event log, email alerts, or the StoreOnce Management Console.

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **SNMP** panel.
3. The **SNMP** screen includes tabs for **Overview**, **Agent Setup**, **Trapsinks**, and **Users**.
   - To view summaries of the SNMP configuration, click the **Overview** tab. To view lists of the items in the summaries, click the graphic segments and legends.
   - To configure SNMP, select the tabs for **Agent Setup**, **Trapsinks**, and **Users**.

Editing SNMP agent setups

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **SNMP** panel.
3. On the **SNMP** screen, click the **Agent Setup** tab.
4. On the **Agent Setup** tab, expand the **Actions** menu and select **Edit Agent Setup**.

Adding SNMP trapsinks

Prerequisites

To add an SNMP trapsink:

- At least one SNMP user has been added. Learn more: **Adding SNMP users** on page 205.
- You know the destination IP address and port number of the trapsink.

Procedure

1. On the main menu, select **Settings**.
2. In the **Notifications** section, click the **SNMP** panel.
3. On the **SNMP** screen, click the **Trapsinks** tab.
4. On the**Trapsinks** tab, expand the **Actions** menu and select **Add**.

Editing and deleting SNMP trapsinks

Prerequisites

Before adding a trapsink, you must have at least one SNMP user already added.

Procedure

1. On the main menu, select **Settings**.
2. In the **Notifications** section, click the **SNMP** panel.
3. On the **SNMP** screen, click the **Trapsinks** tab.
4. On the**Trapsinks** tab, select the trapsink. Then, expand the **Actions** menu and select **Edit** or **Delete**.

Adding SNMP users

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **SNMP** panel.
3. On the **SNMP** screen, click the **Users** tab.
4. On the**Users** tab, expand the **Actions** menu and select **Add**.

Editing and deleting SNMP users

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **SNMP** panel.
3. On the **SNMP** screen, click the **Users** tab.
4. On the**Users** tab, select the user, and then expand the **Actions** menu and select **Edit** or **Delete**

- To add a user, expand the **Actions** menu and select **Add**.
- To edit or delete a user, .

Testing SNMP agents

Once SNMP is configured, you can test that it is set up correctly. Testing also confirms that traps can make it to the trapsinks.

Procedure

1. On the main menu, select **Settings**.
2. In the **Notification** section, click the **SNMP** panel.
3. On the **SNMP** screen, click the **Agent Setup** tab.
4. On the **Agent Setup** tab, expand the **Actions** menu and select **Test SNMP Agent**.

Remote Logging Server

Adding remote logging servers

Prerequisites
To add a remote logging server, you must know:

- IP address (or FQDN) and the port number of the remote logging server
- The logging server type: Audit or Syslog
- The connection protocol: TCP or UDP

Procedure

1. On the main menu, select **Settings**.
2. In the **Notifications** section, click the **Remote Logging Server** panel.
3. On the **Remote Logging Server** screen, expand the **Actions** menu and select **Add**.

Editing and deleting remote logging servers

Procedure

1. On the main menu, select **Settings**.
2. In the **Notifications** section, click the **Remote Logging Server** panel.
3. On the **Remote Logging Server** screen, select the server. Then, expand the **Actions** menu and select **Edit** or **Delete**.

Best practices

Data services best practices

- Target similar data types to dedicated VT libraries, NAS shares, and StoreOnce Catalyst stores, and avoid mixing data types within a library, share, and store. Backups of differing data types, such as two different database types, will not deduplicate well against each other. Separating different data types into separate libraries/shares/stores reduces the complexity leading to optimum long-term performance.
- Where possible, split a backup session into multiple backup streams. Allowing StoreOnce to process multiple backups streams in parallel increases backup performance.
- Do not delete backup items (StoreOnce Catalyst items, VT library cartridges, or files from NAS shares) directly from the StoreOnce Management Console. Instead, use the backup application to expire the backup items to ensure application consistency.
- Secure Erase on libraries/shares/stores will have a system performance impact due to increased disk I/O. Enable Secure Erase when it is needed, and disabled it when no longer needed.
- Do not enable backup application level compression, encryption, or deduplication. These processes will severely impact StoreOnce deduplication.

StoreOnce Catalyst best practices

- Wherever possible, use low-bandwidth StoreOnce Catalyst for optimal backup performance and network usage.
- When performing low-bandwidth StoreOnce Catalyst backups, spread the number of backup sessions across multiple media servers to reduce the possibility of a media server becoming a performance bottleneck.
- When using ProLiant media servers and database servers for low-bandwidth StoreOnce Catalyst, enable “HPE Static High-Performance Mode” through the ProLiant “Power Management” settings for the best backup performance. This setting is not the default.
- For optimum performance, set StoreOnce Catalyst client log levels to the default ERROR log level.
- When performing backups over Fibre Channel or Ethernet, StoreOnce Catalyst compression and checksums can be set to DISABLED through the backup application configuration file. When performing StoreOnce Catalyst Ethernet backups over WAN, StoreOnce Catalyst compression and checksums must be ENABLED (default) through the backup application (plug-in) configuration file.
- When configuring a backup application to use a Fully Qualified Domain Name (FQDN) address for a StoreOnce System, be sure that the FQDN is fully registered with a Domain Name Server. Do not use local host file entries. This step is important when using StoreOnce Catalyst Copy jobs because the source StoreOnce System will use the FQDN to communicate directly with the target StoreOnce System. Using local client host file entries will result in the source StoreOnce System not being able to resolve the target FQDN address.
- To reduce the chance of connection failures on busy Windows clients when using Catalyst over Ethernet, decrease the TIMED_WAIT Windows TCP parameter.

  And if needed, also increase the ephemeral port range. Ephemeral ports are range of ports that Windows Server uses for outbound communications over TCP/IP. When an outbound connection is finished, the port associated to the connection is temporarily put into a TIMED_WAIT state in which time it is temporarily unavailable for reuse.

Decrease the TIMED_WAIT parameter from 120 seconds to 30 seconds by creating the TcpTimedWaitDelay parameter in the following Windows registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters with value 30 and type REG_DWORD.

StoreOnce Catalyst over Fibre Channel best practices

- Be sure the “Number of Devices per Login” is set appropriately for StoreOnce Catalyst Copy, Windows, Linux, HP-UX, AIX, and Solaris media and database servers.
- If running the backup application as a nonroot or nonadministrator, be sure that the correct access permissions have been set on the StoreOnce Catalyst over Fibre Channel client device files.
- Zone every backup/media server to a minimum of two Fibre Channel ports with at least two StoreOnce node Fibre Channel ports across different Fibre Channel cards, ideally across different SANs. Multiple connections allow for higher availability.

StoreOnce Catalyst via Micro Focus Data Protector best practices

When protecting Microsoft SQL databases, the dedupe ratio and performance can be improved as follows. Increase the SQL MAXTRANSFERSIZE and SQL BLOCKSIZE in the Data Protector omnirc configuration file.

In omnirc, set the following parameters:

- OB2SQLMAXTRANSFERSIZE=4194304
- OB2SQLBLOCKSIZE=65536

For further details of how to modify omnirc, refer to the Micro Focus *Data Protector user guide*.

Troubleshooting

All member systems in a federation are unreachable

Symptom

When you are logged in to the lead system in a federation, the status of all member systems in the federation shows as *unreachable*.

Cause

This issue can occur when the IP address of the lead system in a federation has changed since the federation was created. A change in the IP address of the lead system breaks the trust relationship between the lead system and the member systems.

Action

1. For each member system in the federation:
   a. Remove the member system from the federation.
   b. Add the member system back in the federation.

Backup application connection issues

When having issues connecting to a StoreOnce System from a backup application, perform the following checks:

- Make sure that you have the latest version or software patches for the backup application. For supported applications, see the *HPE StoreOnce Support Matrix* **https://www.hpe.com/Storage/StoreOnceSupportMatrix**.
- Stop and restart the backup application services after the backup device has been discovered. If you still cannot access the device, check the Device Manager to make sure it is accessible from the host.
- **iSCSI devices**

  Make sure that the iSCSI initiator is connected to the devices and log on to them. If the devices are not connected, configure them on the targets tab of the iSCSI Initiator.
- **Fibre Channel devices**
  - Models with an 8Gb Fibre Channel card have a theoretical limit of 255 devices per Fibre Channel port on a host or switch.
  - Models with 4Gb Fibre Channel card have a theoretical limit of 127 devices per Fibre Channel port on a host or switch.
- **Practical limitations**

  There are practical limitations on the number of devices that each host or HBA can access. It is possible to configure more drive and library devices than a host can access.

- The limit for Windows or Linux hosts using the iSCSI interface is 64.
- For Fibre Channel, HPE recommends that no more than 64 devices be configured for use by a single host. (Even though Fibre Channel connection supports a greater theoretical number of devices per Fibre Channel port on a host or switch.)

NAS CIFS timeout issues

By default, the Windows CIFS timeout is set low for NAS backup implementations.

A low timeout setting can lead to various error messages related to lost connection to the share, unrecoverable write errors or timeout issues. The timeouts can result in backup job failures.

HPE recommends that you add or increase the *SessTimeout* value from the default of 45 seconds to 300 seconds (five minutes).

Increasing the timeout ensures that the Windows CIFS timeout does not cause your backup application to prematurely timeout the running job.

NOTE: Increasing the timeout setting can resolve issues resulting from timeouts. However, it is not exclusively the only reason for such failures.

Many out-of-sequence writes causing slow response times within the product often can be the root cause. If increasing the timeout is not successful, further analysis may be required.

Procedure

1. On the client machine. From the Windows **Start** menu, click **Run**.
2. In the **Open:** box, type **regedit** and click **OK**.
3. Expand and locate the registry subtree:

   HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \LanmanWorkstation \Parameters
4. Add a REG_DWORD key with the name of SessTimeout.
5. Set the timeout value. HPE recommends to initially set the timeout value at 300 and then change the value according to the situation of your machine.
6. Reboot the client machine.

NAS NFS stale handle error

The following process can cause problems when connecting to a NAS NFS share:

1. A NAS NFS share is created on a StoreOnce System and then is mounted on a host Linux machine.
2. The NAS NFS share is deleted on the StoreOnce System without first unmounting it on the host Linux machine.
3. The NAS NFS share is created again on the StoreOnce System with the same name.

In this process, the Linux client will assign a new set of inodes to the new share. But when trying to access the old mount point it will use the previous set of inodes and will therefore not connect.

To resolve the stale handle issue, and restore the connection, reboot the host Linux machine.

Obtaining log collections

A log collection is a snapshot in time of the StoreOnce System. The log collection shows the configuration, status, and health of the product, as well as historical events for use with troubleshooting the product.

The support ticket also contains lower-level trace logs for the use of Hewlett Packard Enterprise engineers.

If a kernel or process crash occurs, an automatic ticket is generated.

To manually generate a log collection, see **Generating, downloading, and removing log collections** on page 201.

Password issues

If the Admin password is lost, you can reset the password using the StoreOnce Initialisation Console.

The reset Admin password functionality in th Initialisation Console is available only when you are logged in locally to the StoreOnce System or iLO. Or from the hypervisor console for a StoreOnce VSA system.

This procedure applies to local authentication only. If you are using LDAP or Active Directory, this feature has no effect.

Procedure

1. Log in to the **Initialisation Console**. Use the username **console** and the password that was set during the first configuration of the StoreOnce system.
2. Select **Reset admin password**. The password is reset to the default *admin*.
3. After the reset is applied, navigate to the web interface on a new tab. On the password dialog, change the default password.

Reported capacity shows an unexpected drop

Symptom

The reported capacity for a StoreOnce system is less than expected. The low reported capacity can last for several minutes and involves the capacities of Cloud Bank stores or VT libraries.

On a Capacity Usage graph, the unexpected drop can appear as a dip (white area) in the total capacity of the StoreOnce System.



Cause

This issue can occur after a StoreOnce System is rebooted, or the data services on the StoreOnce System are restarted.

After a reboot or restart, the capacities of Cloud Bank stores and VT libraries are first reported as zero. It can take up to several minutes for the actual capacities to be reported.

Action

1. Review a Capacity report graph.

- If the drop occurred in the past, and the reported capacity has returned to expected levels, no action is required.
- If the drop is being reported now, allow several minutes to verify that the reported capacity returns to expected levels.

Restarting data services

The **Restart data services** action is only available if you are logged as a user with the role of administrator. It is intended for use in limited circumstances. For example, when the status of the data services reports a critical fault and recommends restarting the data services.

⚠ **WARNING:** Restarting data services will cause running *backups*, *restores*, and *copies* to be canceled. Ongoing *replications* will be interrupted but will attempt to resume after the restart is complete.

Procedure

1. On the main menu, select **Data Services**.
2. On the **Data Services** screen, expand the **Actions** and select **Restart data services**.

StoreOnce websites

Hewlett Packard Enterprise Information Library for StoreOnce products

www.hpe.com/info/storeonce/docs

HPE StoreOnce Support Matrix

www.hpe.com/storage/StoreOnceSupportMatrix

HPE StoreOnce Systems QuickSpecs

www.hpe.com/support/StoreOnceQuickSpecs

HPE StoreOnce Data Protection Backup Appliances information page

www.hpe.com/storage/storeonce

General websites

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

Enter "StoreOnce" into the keyword search box.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.