Storage Manager 2020 R1

Administrator's Guide

Part Number: 680-017-029
May 2021
Rev. B

DELL EMC

Preface

This guide describes how to use Storage Manager to manage and monitor your storage infrastructure.

For information about installing and configuring required Storage Manager components, see the *Storage Manager Installation Guide*.

How to Find Information

To Find	Action
A description of a field or option in the user interface	In Storage Manager, click **Help**. In Unisphere, select **Help** from the **?** drop-down menu.
Tasks that can be performed from a particular area of the user interface	1. In Storage Manager, click **Help**. In Unisphere, select **Help** from the **?** drop-down menu. 2. See the Related Tasks section at the bottom of the topic.
A term in a .pdf file	Using Adobe Acrobat or Adobe Reader: ● To find a matching term, press Control+F, type the search term, then press Enter. ● To find all matching terms, press Control+Shift+F, type the term in the search field, then click **Search**.

Contacting Dell

Go to https://www.dell.com/support.

Revision History

Table 1. Document Revision History

Revision	Date	Description
A	November 2020	Initial release
B	May 2021	Updated for the release of Storage Center 7.5.1

Audience

Storage administrators make up the target audience for this document. The intended reader has a working knowledge of storage and networking concepts.

Related Publications

The following documentation is available for storage components managed using Storage Manager.

Storage Manager Documents

- *Storage Manager Installation Guide*

Contains installation and setup information.

- *Storage Manager Administrator's Guide*

  Contains in-depth feature configuration and usage information.

- *Unisphere and Unisphere Central for SC Series Administrator's Guide*

  Contains instructions and information for managing storage devices using Unisphere and Unisphere Central for SC Series.

- *Storage Manager Release Notes*

  Provides information about Storage Manager releases, including new features and enhancements, open issues, and resolved issues.

- *Storage Manager Online Help*

  Provides context-sensitive help for the Client, Data Collector, and Server Agent.

- *Unisphere and Unisphere Central for SC Series Online Help*

  Provides context-sensitive help for Unisphere and Unisphere Central for SC Series.

- *Dell Storage REST API Release Notes*

  Contains a list of known issues and workarounds for the Dell Storage REST API.

- *Dell Storage API PowerShell SDK Release Notes*

  Contains a list of known issues and workarounds for the Dell Storage API for PowerShell.

Storage Center Documents

- *Storage Center Release Notes*

  Contains information about features and open and resolved issues for a particular product version.

- *Storage Center Deployment Guides*

  Provides cabling instructions for Storage Center controllers, switches, and enclosures and provides instructions for configuring a new Storage Center.

- *Storage Center Software Update Guide*

  Describes how to update Storage Center software from an earlier version to the current version.

- *Storage Center Update Utility Administrator's Guide*

  Describes how to update the Storage Center software on storage systems. Updating the Storage Center software using the Storage Center Update Utility is intended for storage systems that cannot be updated using the standard Storage Center update methods.

- *Storage Center Command Utility Reference Guide*

  Provides instructions for using the Storage Center Command Utility. The Command Utility provides a command-line interface (CLI) to enable management of Storage Center functionality on Windows, Linux, Solaris, and AIX platforms.

- *Storage Center Command Set for Windows PowerShell*

  Provides instructions for getting started with Windows PowerShell cmdlets and scripting objects that interact with the Storage Center via the PowerShell interactive shell, scripts, and hosting applications. Help for individual cmdlets is available online.

FluidFS Cluster Documents

- *FluidFS FS8600 Appliance Pre-Deployment Requirements*

  Provides a checklist that assists in preparing to deploy an FS8600 appliance prior to a Dell installer or certified business partner arriving on site to perform an FS8600 appliance installation. The target audience for this document is Dell installers and certified business partners who perform FS8600 appliance installations.

- *FluidFSFS8600 Appliance Deployment Guide*

Provides information about deploying an FS8600 appliance, including cabling the appliance to the Storage Center(s) and the network, and deploying the appliance using the Storage Manager software. The target audience for this document is Dell installers and certified business partners who perform FS8600 appliance installations.

- *FluidFS FS8600 Appliance CLI Reference Guide*

  Provides information about the FS8600 appliance command-line interface. The target audience for this document is customers.

- *FluidFSFS8600 Appliance Firmware Update Guide*

  Provides information about upgrading the FluidFS software. The target audience for this document is customers.

- *FluidFS Release Notes*

  Provides information about FluidFS releases, including new features and enhancements, open issues, and resolved issues. The target audience for this document is customers.

- *Dell FS8600 Appliance Service Guide*

  Provides information about FS8600 appliance hardware, system component replacement, and system troubleshooting. The target audience for this document is Dell installers and certified business partners who perform FS8600 appliance hardware service.

Dell Support

- Knowledge Base
- Servers, Storage, and Networking
- Storage technical documents and videos

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2020 - 2021 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Chapter 1: Storage Manager Overview....24
Environmental and System Requirements....24
Storage Manager Components....24
Default Ports Used by Storage Manager....25
Data Collector Ports....25
Client Ports....26
Server Agent Ports....26
IPv6 Support....26
Storage Manager Features....27
Storage Management Features....27
Disaster Recovery Features....28
Monitoring and Reporting Features....29
Storage Manager Client Overview....30

Chapter 2: Getting Started....32
Use the Client to Connect to the Data Collector....32
Next Steps....33
Add Storage Manager Users....33
Add Storage Centers to Storage Manager....34
Configure Storage Center Volumes....34
Add Servers to the Storage Centers....34
Add PS Groups to Storage Manager....34
Add FluidFS Clusters to Storage Manager....34
Configure Email Notifications....34
Set up Remote Storage Centers and Relication QoS....35
Configure Replications and Live Volumes....35
Prepare for Disaster Recovery....35

Chapter 3: Storage Center Overview....36
How Storage Virtualization Works....36
Storage Center Hardware Components....36
Disk Management....37
Drive Spares....38
Volumes....38
Storage Types....38
Data Progression....40
Low Space Modes....40
Storage Center Operation Modes....42
Storage Profiles....42
User Interface for Storage Center Management....45
Summary Tab....45
Storage Tab....46
Hardware Tab....47
IO Usage Tab....48

Charting Tab....48
Alerts Tab....49
Logs Tab....49

Chapter 4: Storage Center Deployment....50
Discover and Configure Uninitialized SCv2000 Series Storage Systems....50
Open the **Discover and Configure Uninitialized Storage Centers** Wizard From the Storage Manager Client Welcome Screen....50
Open the **Discover and Configure Uninitialized Storage Centers** Wizard from the Storage Manager Client....50
Select a Storage Center to Initialize....51
Set System Information....51
Set Administrator Information....52
Configure iSCSI Fault Domains (iSCSI Front-End Only)....52
Confirm the Storage Center Configuration....52
Deploy the Storage Center....53
Review Redundant Paths (FC or SAS Front-End Only)....53
Inherit Settings....53
Configure Time Settings....53
Configure SMTP Server Settings....54
Set Up SupportAssist....54
Accept the SupportAssist Collection Agreement....54
Provide Contact Information....55
Provide Site Contact Information....55
Validate the SupportAssist Connection....55
Update Storage Center....55
Set Default Storage Profile (SCv2000 Series Controllers Only)....56
Complete Configuration and Perform Next Steps....56
Discover and Configure Uninitialized SCv3000 Series Storage Systems....57
Open the **Discover and Configure Uninitialized Storage Centers** Wizard From the Storage Manager Client Welcome Screen....57
Open the **Discover and Configure Uninitialized Storage Centers** Wizard from the Storage Manager Client....58
Select a Storage Center to Initialize....58
Welcome Page....59
Customer Installation Authorization....59
Set System Information....59
Set Administrator Information....60
Confirm the Storage Center Configuration....60
Deploy the Storage Center....60
Enter Key Management Server Settings....60
Create a Storage Type....61
Fault Tolerance....61
Inherit Settings....63
Configure Time Settings....63
Configure SMTP Server Settings....63
Set Up SupportAssist....64
Accept the SupportAssist Collection Agreement....64
Provide Contact Information....64
Provide Site Contact Information....64

Validate the SupportAssist Connection....65
Update Storage Center....65
Complete Configuration and Perform Next Steps....65
Discover and Configure Uninitialized SC5020 and SC7020 Storage Systems....66
Open the **Discover and Configure Uninitialized Storage Centers** Wizard From the Storage Manager Client Welcome Screen....66
Open the **Discover and Configure Uninitialized Storage Centers** Wizard from the Storage Manager Client....66
Introduction to Storage Center Initial Configuration....67
Select a Storage Center to Initialize....67
Welcome Page....68
Customer Installation Authorization....68
Set System Information....68
Set Administrator Information....69
Confirm the Storage Center Configuration....69
Deploy the Storage Center....69
Enter Key Management Server Settings....69
Create a Storage Type....70
Fault Tolerance....70
Inherit Settings....72
Configure Time Settings....72
Configure SMTP Server Settings....73
Set Up SupportAssist....73
Accept the SupportAssist Collection Agreement....73
Provide Contact Information....74
Provide Site Contact Information....74
Validate the SupportAssist Connection....74
Complete Configuration and Perform Next Steps....74
Configuring SC4020 and SC8000 Storage Centers....75
Welcome Page....75
Submit the Storage Center License....76
Create a Disk Folder....76
Add a Controller (Configure Storage Center Wizard)....76
Set System Information....77
Enter Key Management Server Settings....77
Configure Ports....77
Inherit Settings....79
Configure Time Settings....80
Configure SMTP Server Settings....80
Accept the SupportAssist Collection Agreement....80
Provide Contact Information....80
Provide Site Contact Information....81
Validate the SupportAssist Connection....81
Complete Configuration and Perform Next Steps....81
Configuring SC9000 Storage Centers....82
Welcome Page....83
Set System Information....83
Submit the Storage Center License....83
Create a Disk Folder....84
Deploy the Storage Center – Add a Controller....84

Deploy the Storage Center....84
Enter Key Management Server Settings....84
Create a Storage Type....85
Configure Ports....85
Inherit Settings....87
Configure Time Settings....87
Configure SMTP Server Settings....87
Set Up SupportAssist....88
Accept the SupportAssist Collection Agreement....88
Provide Contact Information....88
Provide Site Contact Information....88
Validate the SupportAssist Connection....89
Complete Configuration and Perform Next Steps....89
Set Up a localhost or VMware Host....89
Set Up a localhost from Initial Setup....89
Set Up a VMware Host from Initial Setup....90
Set Up a VMware vCenter Host from Initial Setup....91

Chapter 5: Storage Center Administration....92
Adding and Organizing Storage Centers....92
Storage Center User Privileges and User Groups....92
User Privilege Levels....93
Adding and Removing Storage Centers....93
Organizing Storage Centers....95
Managing Volumes....97
Attributes That Determine Volume Behavior....97
Volume Icons....97
Creating Volumes....98
Modifying Volumes....102
Copying Volumes....107
Migrating Volumes With Live Migrate....110
Creating and Managing Volume Folders....117
Creating and Managing Volume Snapshots....118
Mapping Volumes to Servers....121
Deleting Volumes and Volume Folders....125
Managing Data Reduction....126
Data Eligible for Data Reduction....126
Supported Hardware Platforms....127
Compression....127
Deduplication....128
View Amount of Space Saved by Data Reduction....128
Change the Default Data Reduction Profile....129
Pause or Resume Data Reduction....129
Disable Data Reduction for a Volume....130
Managing Snapshot Profiles....130
Default Snapshot Profiles....131
Consistent and Non-Consistent Snapshot Profiles....131
Creating and Applying Snapshot Profiles....131
Modifying Snapshot Profiles....133
Managing Expiration Rules for Remote Snapshots....134

Managing Storage Profiles....135
Create a Storage Profile (Storage Center 7.2.1 and Earlier)....135
Create a Storage Profile (Storage Center 7.2.10 and Later)....136
Apply a Storage Profile to One or More Volumes....136
Apply a Storage Profile to a Server....137
Delete a Storage Profile....137
Managing QoS Profiles....137
Create a QoS Profile....138
Edit a QoS Profile....138
Delete a QoS Volume Profile....138
Apply a QoS Profile to a Volume....139
Remove a Group QoS Profile From a Volume....139
Importing Volumes from an External Storage Array....139
Connect to an External Storage Array (iSCSI)....139
PS Series Storage Array Import Requirements....140
Storage Center Import Requirements....140
MD Series Import Requirements....140
Supported Server Operating Systems for Online Import....140
Import Data from an External Device (Offline)....141
Import Data from an External Device (Online)....141

Chapter 6: Storage Center Server Administration....143
Server Management Options....143
Managing Storage Center Server Objects....143
Managing Servers Centrally Using Storage Manager....144
Managing Servers on a Storage Center....144
Creating Servers....144
Modifying Servers....149
Mapping Volumes to Servers....152
Creating and Managing Server Folders....155
Deleting Servers and Server Folders....156
Managing Servers Centrally on the Servers View....156
Server Types That Can Be Centrally Managed....156
Storage Manager Server Agent for Windows Servers....157
IPMI Support for NAS Appliances....157
Registering Servers with Storage Manager....157
Organizing and Removing Registered Servers....159
Updating Server Information....161
Managing Server Data Collection and Reporting Settings....162
Creating Server Volumes and Datastores....163
Assigning/Creating Virtual Servers on Storage Centers....166
Manually Mapping a Windows Server to a Storage Center Server....167
Managing NAS Appliances Powered by Windows Storage Server....167
Installing and Using the Server Agent on a Windows Server....169
Download the Server Agent....169
Install and Register the Server Agent....170
Manage the Server Agent with Server Agent Manager....172
Uninstalling the Server Agent....173

Chapter 7: Managing Virtual Volumes With Storage Manager 174
Configuring VVols in Storage Manager 174
Safeguarding VVols Data 174
VMware Virtual Volume Concepts 175
Setting Up VVols Operations on Storage Manager 176
Virtual Volumes Restrictions 176
VASA Provider 177
Register the VASA Provider 177
Unregister a VASA Provider 177
Using Storage Manager Certificates With VASA Provider 178
Managing Storage Containers 179
Data Reduction Options for VVols 180
Create a Storage Container Using the Storage View 183
Edit a Storage Container Using the Storage View 184
Delete a Storage Container 184
View Storage Container Information 184
Creating VVol Datastores 184
Create a Datastore and Map it to VMware ESX Server 184
View VVol and Datastore Information 185
Protocol Endpoint Monitoring 186

Chapter 8: PS Series Storage Array Administration 188
About Groups 188
Adding PS Series Groups 189
Organizing PS Series Groups 191
Remove a PS Series Group 192
Launch Group Manager 192
About Volumes 192
Create a Volume 194
Modify a Volume 195
Create a Volume Folder 195
Edit a Volume Folder 196
Delete a Volume Folder 196
Move a Volume to a Folder 196
Move Multiple Volumes to a Folder 197
Rename a Volume 197
Clone a Volume 197
Modify Volume Access Settings 198
Set a Volume Online or Offline 198
Add Access Policy Groups to a Volume 198
Add Access Policies to a Volume 199
Create a Basic Access Point 199
Delete a Volume 199
Restore a Volume from the Recycle Bin 200
Empty the Recycle Bin 200
Permanently Delete a Volume in the Recycle Bin 200
About Snapshots 201
Create a Snapshot 201

Create a Snapshot Schedule....201
Modify Snapshot Properties....202
Control Snapshot Space Borrowing....202
Set a Snapshot Online or Offline....202
Restore a Volume from a Snapshot....203
Delete a Snapshot....203
Managing Replication Schedules....203
Create an Hourly Replication Schedule....203
Create a Daily Replication Schedule....204
Schedule a Replication to Run Once....204
Edit a Replication Schedule....205
Enable or Disable a Replication Schedule....205
Delete a Replication Schedule....205
About Access Policies....206
Create a Local CHAP Account....206
Edit a Local CHAP Account....206
Modify Target Authentication....207
Set the iSCSI Discovery Filter....207
Create an Access Policy Group....207
Edit an Access Policy Group....208
Delete an Access Policy Group....208
Create an Access Policy....209
Edit an Access Policy....209
Delete an Access Policy....211
Monitoring a PS Series Group....211
View Logs....211
View Event Logs....212
View Audit Logs....212
View Outbound Replications....212
View Inbound Replications....212
View Replication History....213
View Alerts....213

Chapter 9: Storage Center Maintenance....214
Managing Storage Center Settings....214
Viewing and Modifying Storage Center Information....214
Modifying Storage Center Network Settings....216
Configuring Storage Center User Preferences....218
Configuring Storage Center Data Settings....221
Configuring Storage Center Secure Console Settings....223
Configuring Storage Center SMTP Settings....224
Configuring Storage Center SNMP Settings....225
Configuring Storage Center Time Settings....226
Configuring Filters to Restrict Administrative Access....227
Configuring a Storage Center to Inherit Settings....229
Managing Storage Center Users and Groups....230
User Privilege Levels....230
User Groups....230
User Account Management and Authentication....230
Managing Local Storage Center Users....230

Managing Local Storage Center User Groups 236
Enabling Directory Services Authentication 238
Managing Directory Service Users 241
Managing Directory User Groups 245
Managing Local Storage Center User Password Requirements 247
Managing Front-End I/O Ports 249
Front-End Connectivity Modes 249
About Fault Domains and Ports 250
Failover Behavior 251
Rebalance Front-End Ports 252
Managing Front-End I/O Port Hardware 252
Converting Front-End Ports to Virtual Port Mode 256
Managing Back-End I/O Port Hardware 257
Configure Back-End Ports 257
Configure Individual Back-End I/O Ports 257
Rename a Back-End I/O Port 257
Grouping Fibre Channel I/O Ports Using Fault Domains 258
Create a Fibre Channel Fault Domain 258
Rename a Fibre Channel Fault Domain 258
Remove Ports from an Fibre Channel Fault Domain 259
Delete a Fibre Channel Fault Domain 259
Grouping iSCSI I/O Ports Using Fault Domains 260
iSCSI VLAN Tagging Support 260
Creating iSCSI Fault Domains 261
Modifying iSCSI Fault Domains 263
Configuring NAT Port Forwarding for iSCSI Fault Domains 267
Configuring CHAP for iSCSI Fault Domains 269
Grouping SAS I/O Ports Using Fault Domains 271
Create a SAS Fault Domain 271
Delete a SAS Fault Domain 272
Managing Disks and Disk Folders 272
Storage Center Disk Management 272
Scan for New Disks 273
Create a Disk Folder 273
Delete Disk Folder 273
Modify a Disk Folder 274
Manage Unassigned Disks 274
Enable or Disable the Disk Indicator Light 275
Release a Disk 275
Cancel Releasing a Disk 275
Delete a Disk 276
Restore a Disk 276
Replace a Failed Disk 276
Managing Secure Data 277
How Secure Data Works 277
Configure Key Server 277
Configure Rekey Interval for Disk Folder 278
Rekey a Disk Folder 279
Rekey a Disk 279
Copy Volumes to Disk Folder 279

Create Secure Data Disk Folder....280
Managing Data Redundancy....280
Redundancy Requirements....280
Managing RAID....281
Managing Storage Types....282
Managing Disk Enclosures....284
Add an Enclosure....284
Remove an Enclosure....284
Replace an Enclosure....285
Rename a Disk Enclosure....286
Set an Asset Tag for a Disk Enclosure....286
Delete an Enclosure....286
Mute an Enclosure Alarm....287
Unmute an Enclosure Alarm....287
Clear the Swap Status for an Enclosure Cooling Fan....287
Clear the Swap Status for an Enclosure I/O Module....287
Clear the Swap Status for an Enclosure Power Supply....288
Replace a Failed Power Supply....288
Clear the Under Voltage Status for a Power Supply....288
Clear the Swap Status for a Temperature Sensor....289
Clear the Minimum and Maximum Recorded Values for Temperature Sensor....289
Replace a Failed Cooling Fan Sensor....289
Enable or Disable the Disk Indicator Light....290
Clear the Swap Status for a Disk....290
Managing Storage Center Controllers....290
Add a Controller....290
Replace a Failed Controller....291
Enable or Disable a Controller Indicator Light....291
Replace a Failed Cooling Fan Sensor....292
Managing I/O Card Changes....292
Add a UPS to a Storage Center....294
Updating Storage Center....294
Update Storage Center Software....294
Using the Storage Center Update Utility....295
Shutting Down and Restarting a Storage Center....295
Shut Down All Controllers in Storage Center....295
Restart All Controllers in a Storage Center....296
Shut Down a Controller....296
Restart a Controller....296
Reset a Controller to Factory Default....297
Managing Field Replaceable Units (FRU)....297
Managing FRU Tickets....297

Chapter 10: Viewing Storage Center Information....299
Viewing Summary Information....299
Storage Center Summary Plugins....299
Viewing Summary Information for a Storage Center....299
Viewing Summary Information for Multiple Storage Centers....301
Using the Status Plugin....302
Using the Storage Summary Plugin....304

Using the Front End IO Summary Plugin....306
Using the Current Alerts Plugin....307
Using the Replication Validation Plugin....307
Using the Top 10 Fastest Growing Volumes Plugin....308
Using the Current Threshold Alerts Plugin....308
Viewing Detailed Storage Usage Information....309
View Storage Usage by Tier and RAID Type....309
View Storage Usage by Volumes....309
View Historical Storage Usage....310
View a Data Progression Pressure Report....311
Viewing Historical IO Performance....312
Using the IO Usage Tab....312
Viewing Current IO Performance....314
Using the Charting Tab....314
Configuring Chart Options....316
Configuring User Settings for Charts....316
Configuring Chart Settings....317
Configure the Storage Center Data Gathering Schedule....318
Exporting Usage Data....319
Export Storage Usage Data....319
Export I/O Usage Data....320
Monitoring Storage Center Hardware....321
Monitoring a Storage Center Controller....321
Monitoring a Storage Center Disk Enclosure....324
Monitoring SSD Endurance....327
Viewing UPS Status....328

Chapter 11: SMI-S....330
SMI-S Provider....330
Supported Management Solutions....330
Supported SMI-S 1.6 Profiles....330
SMI-S Namespace....331
Setting Up SMI-S....331
SMI-S Prerequisites....331
Enable SMI-S for the Data Collector....331
Using the Dell SMI-S Provider with Microsoft SCVMM....332
SCVMM Prerequisites....332
Limitations for SCVMM 2012....333
Modify the SCVMM 2012 Management Server Registry to Allow HTTPS....333
Prepare the SCVMM 2012 Server for Indications....334
Use SCVMM to Discover the SMI-S Provider....334

Chapter 12: FluidFS Administration....336
How FS8600 Scale-Out NAS Works....336
FS8600 Scale-Out NAS Terminology....337
Key Features of the Scale-Out NAS....338
Overview of the FS8600 Hardware....339
Overview of the FS8600 Architecture....339
Data Caching and Redundancy....341

File Metadata Protection ... 341
Load Balancing and High Availability ... 341
Ports Used by the FluidFS Cluster ... 342
FluidFS System Management for FS Series Appliances ... 342
Seamless Session Failover ... 342
Using the Storage Manager Client or CLI to Connect to the FluidFS Cluster ... 343
Managing Secured Management ... 344
Managing the FluidFS Cluster Name ... 348
Accept the End-User License Agreement ... 348
Managing the System Time ... 349
Managing the FTP Server ... 349
Managing SNMP ... 350
Managing the Health Scan Throttling Mode ... 352
Managing the Operation Mode ... 352
Managing Client Connections ... 353
Shutting Down and Restarting NAS Controllers ... 355
Managing NAS Appliance and NAS Controller Blinking ... 356
FluidFS Networking ... 357
Managing the Default Gateway ... 357
Managing DNS Servers and Suffixes ... 357
Managing Static Routes ... 359
Managing the Client Networks ... 360
Viewing the Fibre Channel WWNs ... 364
Managing iSCSI SAN Connectivity ... 365
Add or Remove an iSCSI Port ... 365
Add or Remove an iSCSI Fabric ... 365
Change the VLAN Tag for an iSCSI Fabric ... 366
Change the NAS Controller IP Addresses for an iSCSI Fabric ... 366
FluidFS Account Management and Authentication ... 366
Account Management and Authentication ... 366
Default Administrative Accounts ... 367
Default Local User and Local Group Accounts ... 369
Managing Administrator Accounts ... 369
Managing Local Users and Groups Using MMC ... 372
Managing Local Users ... 372
Managing Local Groups ... 375
Managing Active Directory ... 378
Managing LDAP ... 380
Managing NIS ... 384
Managing User Mappings Between Windows and UNIX/Linux Users ... 385
FluidFS NAS Volumes, Shares, and Exports ... 388
Managing the NAS Pool ... 388
View Internal Storage Reservations ... 388
View the Size of the NAS Pool ... 388
Expand the Size of the NAS Pool ... 388
Set the Metadata Tier ... 389
Enable or Disable the NAS Pool Used Space Alert ... 389
Enable or Disable the NAS Pool Unused Space Alert ... 390
About Multitenancy ... 390
Create a New Tenant ... 393

Moving a NAS Volume Between Tenants....394
Managing NAS Volumes....395
Managing SMB Shares....406
Managing NFS Exports....418
Global Namespace....422
Using FTP....423
Using Symbolic Links....424
Managing Quota Rules....424
About Data Reduction....424
FluidFS Data Protection....428
Managing Antivirus....428
Managing Snapshots....429
Managing NDMP....434
Managing Replication....442
File Access Notification....456
FluidFS Monitoring....456
Monitoring NAS Appliance Hardware....456
FluidFS Maintenance....460
Connecting Multiple Data Collectors to the Same Cluster....460
Adding and Removing FluidFS Clusters in Storage Manager....460
Organizing FluidFS Clusters Using Folders....461
Adding a Storage Center to a FluidFS Cluster....462
Adding and Deleting NAS Appliances in a FluidFS Cluster....463
Detaching, Attaching, and Replacing a NAS Controller....465
Managing Service Packs....467
Managing Firmware Updates....469
Update Firmware Using FTP....469
Restoring the NAS Volume Configuration....469
Restoring Local Users....470
Restoring Local Groups....471
Reinstalling FluidFS from the Internal Storage Device....472
FS Series VAAI Plugin....473
Enable or Disable the FS Series VAAI Plugin....473
Installation Instructions....473
Plugin Verification....474
Removal Instructions....474
FluidFS Troubleshooting....475
Viewing the Event Log....475
Running Diagnostics....476
Configuring the BMC Network....478
Launching the iBMC Virtual KVM....478
Troubleshooting Common Issues....479

Chapter 13: Remote Storage Centers and Replication QoS....495
Connecting to Remote Storage Centers....495
Connecting Storage Centers Using Fibre Channel....495
Connecting Storage Centers Using iSCSI....495
Creating and Managing Replication QoS Definitions....497
Create a QoS Definition....497
Rename a QoS Definition....498

Change the Link Speed for a QoS Definition..... 498
Enable or Disable Bandwidth Limiting for a QoS Definition..... 498
Modify the Bandwidth Limit Schedule for a QoS Definition..... 498
Delete a QoS Definition..... 499

Chapter 14: Storage Center Replications and Live Volumes..... 500
Storage Center Replications..... 500
Replication Types..... 501
Replication Requirements..... 502
Replication Behavior When a Destination Volume Fails..... 502
Replicating a Single Volume to Multiple Destinations..... 502
Replication on SCv2000 Series Storage Systems..... 503
Replication Icons..... 503
Simulating Replications..... 503
Replicating Volumes..... 505
Migrating Volumes to Another Storage Center..... 506
Modifying Replications..... 507
Monitoring Replications..... 510
Managing Cross-Platform Replication..... 512
Cross-Platform Replication Requirements..... 512
Managing Replications Between PS Series Groups and Storage Centers..... 513
Managing Replication Schedules..... 515
Storage Center Live Volumes..... 518
Live Volume Requirements..... 518
Live Volume Types..... 518
Live Volume Icon..... 519
Live Volume Roles..... 519
Automatic Failover for Live Volumes..... 521
Managed Replications for Live Volumes..... 524
Creating Live Volumes..... 525
Modifying Live Volumes..... 527
Modifying Live Volumes with Automatic Failover..... 533
Live Volume ALUA..... 533
Monitoring Live Volumes..... 535

Chapter 15: Storage Center DR Preparation and Activation..... 538
How Disaster Recovery Works..... 538
Step 1: A Volume is Replicated to a DR Site..... 538
Step 2: The Source Site Goes Down..... 539
Step 3: An Administrator Activates Disaster Recovery..... 539
Step 4: Connectivity is Restored to the Source Site..... 540
Step 5: An Administrator Restores the Source Volume..... 540
Disaster Recovery Administration Options..... 542
Preparing for Disaster Recovery..... 542
Saving and Validating Restore Points..... 542
Predefining Disaster Recovery Settings for Replications..... 543
Test Activating Disaster Recovery..... 544
Activating Disaster Recovery..... 546
Types of Disaster Recovery Activation for Live Volumes..... 546

Disaster Recovery Activation Limitations....547
Planned vs Unplanned Disaster Recovery Activation....547
Disaster Recovery Activation Procedures....547
Activating Disaster Recovery for PS Series Group Replications....550
Restarting Failed Replications....551
Restart Replication for Multiple Restore Points....551
Restart a Replication for a Single Restore Point....551
Restoring Replications and Live Volumes....552
Volume Restore Options....552
Volume Restore Limitations....552
Restoring a Live Volume and a Managed Replication....552
Volume Restore Procedures....553
Deleting Restore Points....554

Chapter 16: Remote Data Collector....555
Remote Data Collector Management....555
Remote Data Collector Requirements....555
Virtual Appliance Requirements....556
Installing and Configuring a Remote Data Collector....556
Install a Remote Data Collector....556
Installing and Configuring the Storage Manager Virtual Appliance as a Remote Data Collector....557
Disconnecting and Reconnecting a Remote Data Collector....560
Temporarily Disconnect a Remote Data Collector....560
Reconnect a Remote Data Collector to a Storage Center....560
Remove a Remote Data Collector....560
Using a Remote Data Collector to Activate Disaster Recovery....561
Log in to the Remote Data Collector....561
Create a User....563
Use a Remote Data Collector to Prepare for Disaster Recovery....563
Use a Remote Data Collector to Test Activate Disaster Recovery....564
Use a Remote Data Collector to Activate Disaster Recovery....564
Enabling Email Notifications for the Remote Data Collector....564

Chapter 17: Storage Replication Adapter for VMware SRM....565
Where to Find Dell SRA Deployment Instructions....565
Dell SRA for Windows Limitations....565
Dell SRA Requirements for VMware SRM....565
VMware SRM and Storage Manager Prerequisites....566
Dell SRA with Stretched Storage and vMotion....567
Storage Manager SRA Configurations....567

Chapter 18: Threshold Alerts....569
Configuring Threshold Definitions....569
Setting Up Threshold Definitions....569
Assigning Storage Objects to Threshold Definitions....572
Assigning Threshold Definitions to Storage Objects....573
Viewing Threshold Alerts for Threshold Definitions....574
Viewing and Deleting Threshold Alerts....575
View Current and Historical Threshold Alerts....575

Filter Threshold Alerts by Storage Center....575
Filter Threshold Alerts by Threshold Definition Properties....575
View the Threshold Definition that Generated an Alert....576
Delete Historical Threshold Alerts....576
Configuring Volume Advisor Movement Recommendations....576
Threshold Definitions That Support Volume Advisor....576
General Volume Advisor Requirements....577
Additional Requirements for the Volume Latency Threshold Definition....577
Types of Volume Movement Recommendations....577
Creating Threshold Definitions to Recommend Volume Movement....579
Moving a Volume Based on a Recommendation....581
Export Threshold Alerts....583
Configuring Email Notifications for Threshold Alerts....583
Configure SMTP Server Settings....584
Configure an Email Address for Your User Account....585
Configure Email Notification Settings for Your User Account....585
Performing Threshold Queries....585
View Saved Queries....586
Create a Threshold Query....586
Run a Saved Threshold Query....586
Export the Results of a Threshold Query....587
Edit a Saved Threshold Query....587

Chapter 19: Storage Center Reports....588
Chargeback Reports....588
Storage Center Automated Reports....588
Displaying Reports....589
View a Storage Center Automated Report....589
View a Chargeback Report....589
Working with Reports....590
Update the List of Reports....590
Navigate Through the Pages of a Report....590
Print a Report....591
Save a Report....591
Delete a Report....591
Configuring Automated Report Generation....591
Set Up Automated Reports for All Storage Centers....592
Set Up Automated Reports for an Individual Storage Center....592
Testing Automated Reports Settings....593
Configure Storage Manager to Email Reports....594
Configure SMTP Server Settings....594
Configure an Email Address for Your User Account....594
Configure Email Notification Settings for Your User Account....595

Chapter 20: Storage Center Chargeback....596
Configure Chargeback or Modify Chargeback Settings....596
Assign Storage Costs for Global Disk Classes....597
Assign Storage Costs for Storage Center Disk Tiers....598
Configuring Chargeback Departments....599

Setting Up Departments 599
Managing Department Line Items 600
Assigning Volumes to Chargeback Departments 601
Perform a Manual Chargeback Run 604
Viewing Chargeback Runs 605
View a Chart of Department Costs for a Chargeback Run 605
View the Results of the Chargeback Run in Table Format 605
View Cost and Storage Savings Realized by Dynamic Capacity for a Chargeback Run 605
View Cost and Storage Savings Realized by Using Data Instant Snapshots for a Chargeback Run 606
View Cost Savings Realized by Using Data Progression for a Chargeback Run 606
Working with Charts 606
Zoom in on an Area of the Chart 606
Return to the Normal Zoom Level of the Chart 606
Save the Chart as a PNG Image 607
Print the Chart 607
Exporting Chargeback Data 607
Export Chargeback Run Data 607
Export Chargeback Run Data for a Single Department 607

Chapter 21: Storage Center Monitoring 609
Storage Alerts 609
Status Levels for Alerts and Indications 609
Viewing Storage System Alerts 610
Send Storage Center Alerts and Indications to the Data Collector Immediately 612
Events 612
Storage Manager Event Types 612
Viewing Data Collector Events 614
Configuring Email Alerts for Storage Manager Events 616
Storage Logs 618
Viewing Storage Logs 618
Audit Logs 621
Viewing Audit Logs 621
Export Monitoring Data 623
Configure Data Collection Schedules 623

Chapter 22: Data Collector Management 625
Access the Data Collector View 625
Configuring Data Collector Settings 626
Configuring General Settings 626
Configuring Environment Settings 633
Configuring Monitoring Settings 635
Configuring Virtual Appliance Settings 640
Managing Available Storage Centers 642
Delete an Available Storage Center 642
Clear All Data for a Storage Center 642
Remove a Storage Center from a Data Collector User Account 643
Managing Available PS Series Groups 643
Delete an Available PS Series Group 643
Remove a PS Series Group from a Data Collector User 644

Managing Available FluidFS Clusters....644
Delete an Available FluidFS Cluster....644
Remove a FluidFS Cluster from a Data Collector User Account....645
Managing the Storage Manager Virtual Appliance....645
Log in to the Storage Manager Virtual Appliance CLI....645
Configure Virtual Appliance Settings....646
View Diagnostic Information for the Virtual Appliance....648
Migrate a Microsoft SQL Server Database....649
Uninstalling the Data Collector....650
Deleting Old Data Collector Databases....650

Chapter 23: Storage Manager User Management....651
Storage Manager User Privileges....651
Reporter Privileges....651
Volume Manager Privileges....651
Administrator Privileges....651
Authenticating Users with an External Directory Service....652
Configuring an External Directory Service....652
Grant Access to Directory Service Users and Groups....655
Revoke Access for Directory Service Users and Groups....656
Managing Local Users Through the Data Collector....658
Update the Information Displayed on the Users & System Tab....658
Create a User....658
Configure or Modify the Email Address of a User....659
Change the Privileges Assigned to a User....659
Change the Preferred Language for a Storage Manager User....660
Force the User to Change the Password....660
Change the Password for a User....661
Set Storage Center Mappings for a Reporter User....661
Delete a User....662
Delete a Storage Center Mapping for a User....662
Unlock a Local User Account....663
Managing Local User Password Requirements....663
Configure Local Storage Manager User Password Requirements....663
Apply Password Requirements to Storage Center Users....664
Reset Password Aging Clock....665
Require Users to Change Passwords....665
Managing User Settings with the Storage Manager Client....666
Change User Password....666
Configure Email Settings....666
Change the Preferred Language....666
Configure Charting Options....667
Configure Client Options....667

Chapter 24: SupportAssist Management....669
Data Types that Can Be Sent Using SupportAssist....669
Configure SupportAssist Settings for the Data Collector....670
Configure SupportAssist Settings for a Single Storage Center....670
Manually Sending Diagnostic Data Using SupportAssist....671

Manually Send Diagnostic Data for Multiple Storage Centers....671
Send Diagnostic Data for a Single Storage Center 671
Save SupportAssist Data to a File....672
Saving SupportAssist Data to a USB Flash Drive 673
USB Flash Drive Requirements....673
Prepare the USB Flash Drive....673
Save SupportAssist Data to the USB Flash Drive....673
Troubleshooting SupportAssist USB Issues....674
Managing SupportAssist Settings....674
Edit SupportAssist Contact Information....674
Configure SupportAssist to Automatically Download Updates....675
Configure a Proxy Server for SupportAssist....675
CloudIQ....675
Controlling Data Sent to CloudIQ....676

1

Storage Manager Overview

Storage Manager allows you to monitor, manage, and analyze Storage Centers, FluidFS clusters, and PS Series Groups from a centralized management console.

- The Storage Manager Data Collector stores data and alerts it gathers from Storage Centers in an external database or an embedded database. Some functions of the Data Collector are managed by the web application Unisphere Central.
- Storage Manager Client connects to the Data Collector to perform monitoring and administrative tasks.

Topics:

- Environmental and System Requirements
- Storage Manager Components
- Default Ports Used by Storage Manager
- IPv6 Support
- Storage Manager Features
- Storage Manager Client Overview

Environmental and System Requirements

To view the latest environmental and system requirements for Storage Manager 2020 R1, see the *Storage Manager 2020 R1 Release Notes* on https://www.dell.com/support.

Storage Manager Components

Storage Manager consists of the following components:.

Table 2. Storage Manager Components

Component	Description	Setup Documentation
Primary Storage Manager Data Collector	Service that gathers reporting data and alerts from managed storage systems.	*Storage Manager Installation Guide*
Storage Manager Client	Windows or Linux application that connects to a single Storage Center or connects to a Storage Manager Data Collector to provide a centralized management interface for one or more storage system.	*Storage Manager Installation Guide*
Remote Storage Manager Data Collector	A secondary Storage Manager Data Collector that is connected to the primary Storage Manager Data Collector. The remote Storage Manager Data Collector can be used to activate a disaster recovery site if the primary Storage Manager Data Collector becomes unavailable.	*Storage Manager Installation Guide* and *Storage Manager Administrator's Guide*
Storage Manager Server Agent	Software installed on a Windows server that enables the Storage Manager Data Collector to gather information about storage objects on a Windows server.	*Storage Manager Administrator's Guide*

Default Ports Used by Storage Manager

The Storage Manager components use network connections to communicate with each other and with other network resources. The following tables list the default network ports used by the Storage Manager Data Collector, Storage Manager Client, and Storage Manager Server Agent. Many of the ports are configurable.

NOTE: Some ports might not be needed for your configuration. For details, see the Purpose column in each table.

Data Collector Ports

The following tables list the default ports that are used by the Storage Manager Data Collector:

Inbound Data Collector Ports

NOTE: Configure the firewall rules on the server that the Data Collector is installed to enable inbound connections on the inbound Data Collector ports.

The Data Collector accepts connections on the following ports:

Port	Protocol	Name	Purpose
3033	TCP	Web Server Port	• Communication from clients, including the Storage Manager Client, Unisphere Central, and Dell Storage Replication Adapter (SRA) • Communication with tiebreaker for Automatic Failover • Alerts from FluidFS clusters
3034	TCP	Web Server Port	Receiving vCenter/ESXi communication for VASA and VVol provisioning and administration
8080	TCP	Legacy Web Services Port	Receiving: • Storage Manager Server Agent communication • Alerts forwarded from Storage Center SANs
5989	TCP	SMI-S over HTTPS	Receiving encrypted SMI-S communication

Outbound Data Collector Ports

The Data Collector initiates connections to the following ports:

Port	Protocol	Name	Purpose
25	TCP	SMTP	Sending email notifications
443	TCP	SSL	• Communicating with the Storage Manager Data Collector • Sending diagnostic data with SupportAssist
1199	TCP	SIMS RMI	Communicating with managed PS Series groups
1433	TCP	Microsoft SQL Server	Connecting to an external Microsoft SQL Server database
3033	TCP	SSL	Communicating with managed Storage Centers
3306	TCP	MySQL	Connecting to an external MySQL database
8080	TCP	VMware SDK	Communicating with VMware servers
27355	TCP	Server Agent Socket Listening Port	Storage Manager Server Agent communication
35451	TCP	FluidFS	Communicating with managed FluidFS clusters
44421	TCP	FluidFS diagnostics	Retrieving diagnostics from managed FluidFS clusters

Client Ports

Storage Manager clients use the following ports:

Inbound Ports

The Storage Manager Client and Unisphere Central do not use any inbound ports.

Outbound Ports

The Storage Manager Client and Unisphere Central initiate connections to the following port:

Port	Protocol	Name	Purpose
3033	TCP	Web Server Port	Communicating with the Storage Manager Data Collector

Server Agent Ports

The following tables list the ports used by the Storage Manager Server Agent.

Inbound Server Agent Port

The Server Agent accepts connections on the following port.

Port	Protocol	Name	Purpose
27355	TCP	Server Agent Socket Listening Port	Receiving communication from the Data Collector

Outbound Server Agent Port

The Server Agent initiates connections to the following port.

Port	Protocol	Name	Purpose
8080	TCP	Legacy Web Services Port	Communicating with the Data Collector

IPv6 Support

The Storage Manager Data Collector can use IPv6 to accept connections from Storage Manager Client and to communicate with managed Storage Center SANs.

To use IPv6, assign IPv6 addresses as described in the following table.

IPv6 Connection	Requirements
Storage Manager Client to Data Collector	• Storage Manager Client computer must have an IPv6 address. • Data Collector server must have both an IPv4 address and an IPv6 address.
Data Collector to Storage Center	• Data Collector server must have both an IPv4 address and an IPv6 address. • Storage Center SAN must have both an IPv4 address and an IPv6 address on the management interface.

Storage Manager Features

Storage Manager provides the following features.

Storage Management Features

Storage Manager provides the following storage management features.

Storage Center Management

Storage Manager allows you to centrally manage multiple Storage Centers. For each Storage Center, you can configure volumes, snapshot profiles, and storage profiles. You can also present configured storage to servers by defining server objects and mapping volumes to them.

Related concepts

Storage Center Administration on page 92

PS Group Management

Storage Manager allows you to centrally manage your PS Groups. For each PS Group, you can configure volumes, snapshots, and replications between a PS Group and Storage Center. You can also configure access policies to grant volume access to hosts.

FluidFS Cluster Management

Storage Manager allows you to centrally manage your FluidFS clusters and monitor FluidFS cluster status and performance. A FluidFS cluster is a scale-out NAS solution consisting of FS8600 NAS appliances, the Fluid File System (FluidFS), and Storage Center. FluidFS, a scale-out file system, provides high performance, highly scalable, and efficient file storage for Windows, UNIX, and Linux clients. Combined with Storage Center, FluidFS provides a unified block and file storage solution.

Servers

Storage Manager allows you to manage the storage that is allocated servers and provides Storage Center integration with Windows and VMware servers.

There are two ways to manage servers in Storage Manager:

- Add the servers to a Storage Center
- Register Windows and VMware servers with the Storage Manager Data Collector.

Related concepts

Storage Center Server Administration on page 143

SMI-S

Storage Manager supports the Storage Management Initiative Specification (SMI-S), a standard interface specification developed by the Storage Networking Industry Association (SNIA). SMI-S allows Storage Manager to interoperate with storage management software and hardware from other vendors.

NOTE: The Storage Manager Data Collector must be installed in a Microsoft Windows environment. SMI-S is not supported on a Virtual Appliance.

Related concepts

SMI-S on page 330

VVols

Storage Manager supports the VMware virtual volumes (VVols) framework. VMware administrators use vCenter to create virtual machines and VVols. You must be connected to a Data Collector Managerto use VVols.

When properly configured, you can use Storage Manager to manage and view VVols, storage containers, datastores, and other aspects of VMware infrastructure.

Related concepts

Managing Virtual Volumes With Storage Manager on page 174

Disaster Recovery Features

Storage Manager allows you to plan and implement a disaster recovery strategy for your Storage Center volumes.

Remote Storage Centers and Quality of Service

Storage Centers can be connected to each other by Fibre Channel or iSCSI to allow data to be copied between them. Storage Manager allows you to coordinate connected Storage Centers to distribute copies of your data to remote sites, ensuring that your data is protected and available even if one site goes down.

Replication Quality of Service (QoS) definitions allow you to control when and how much bandwidth is used for communication between Storage Centers.

Related concepts

Remote Storage Centers and Replication QoS on page 495

Replications and Live Volumes

As part of an overall Disaster Recovery Plan, replication copies volume data from one managed storage system to another managed storage system to safeguard data against local or regional data threats. If the source storage system or source site becomes unavailable, you can activate the destination volume to regain access to your data.

A Live Volume is a pair of replicating volumes that can be mapped and active at the same time. Similar to a conventional replication, the primary (source) volume on a primary storage system replicates to a secondary (destination) volume on a secondary storage system. However, both the primary volume and secondary volume can accept writes.

Related concepts

Storage Center Replications and Live Volumes on page 500

Disaster Recovery Activation

If you configure replications, Live Volumes, or both, you can use Storage Manager to prepare for and perform disaster recovery. Storage Manager allows you to predefine your disaster recovery plans, including which servers the recovery volumes will be mapped to. In the event of a real disaster, you can use Storage Manager to activate your disaster recovery plans, making your data available to the resources that need it as soon as possible.

Related concepts

Storage Center DR Preparation and Activation on page 538

Remote Data Collector

A remote Data Collector is installed at a remote site and connected to the primary Data Collector to provide access to disaster recovery options when the primary Data Collector is unavailable. In the event that the primary Data Collector is down, you can connect to the remote Data Collector at another site to perform Disaster Recovery.

Related concepts

Remote Data Collector on page 555

Dell Storage Replication Adapter for VMware SRM

Storage Manager includes the DellStorage Replication Adapter (SRA), which allows sites to manage disaster recovery for VMware infrastructure using the VMware vCenter Site Recovery Manager.

Related concepts

Storage Replication Adapter for VMware SRM on page 565

Monitoring and Reporting Features

Storage Manager provides the following reporting and monitoring features.

Threshold Alerts

The Threshold Alerts feature provides centralized administration and monitoring of threshold alert definitions. The types of usage metrics that can be monitored are I/O, storage, and replication usage. The Storage Manager Data Collector collects the usage data from the managed Storage Centers. Storage objects on the Storage Centers are assigned to threshold definitions and each threshold definition contains one or more threshold values. When the value of a monitored metric reaches a threshold value, an alert occurs.

Related concepts

Threshold Alerts on page 569

Reports

The Reports feature allows a user to view Storage Center and Chargeback reports generated by Storage Manager. Storage Manager can be configured to generate the reports on a scheduled basis.

Related concepts

Storage Center Reports on page 588

Chargeback

The Chargeback feature monitors storage consumption and calculates data storage operating costs. Chargeback can be configured to charge for storage based on the amount of allocated space or the amount of configured space. When cost is based on allocated space, Chargeback can be configured to charge based on storage usage, which is the amount of space used, or storage consumption, which is the difference in the amount of space used since the last Chargeback run.

Related concepts

Storage Center Chargeback on page 596

Log Monitoring

The Log Monitoring feature provides a centralized location to view Storage Center alerts, indications, and logs collected by the Storage Manager Data Collector and system events logged by Storage Manager.

Related concepts

Storage Center Monitoring on page 609

Performance Monitoring

The Performance Monitoring feature provides access to summary information about the managed Storage Centers and historical/current I/O performance information. Use this information to monitor the health and status of Storage Centers.

Related concepts

Viewing Storage Center Information on page 299

Storage Manager Client Overview

The Storage Manager Client is a Windows-based program that allows you to connect to the Storage Manager Data Collector and centrally manage your Storage Centers, PS Groups, and FluidFS clusters.

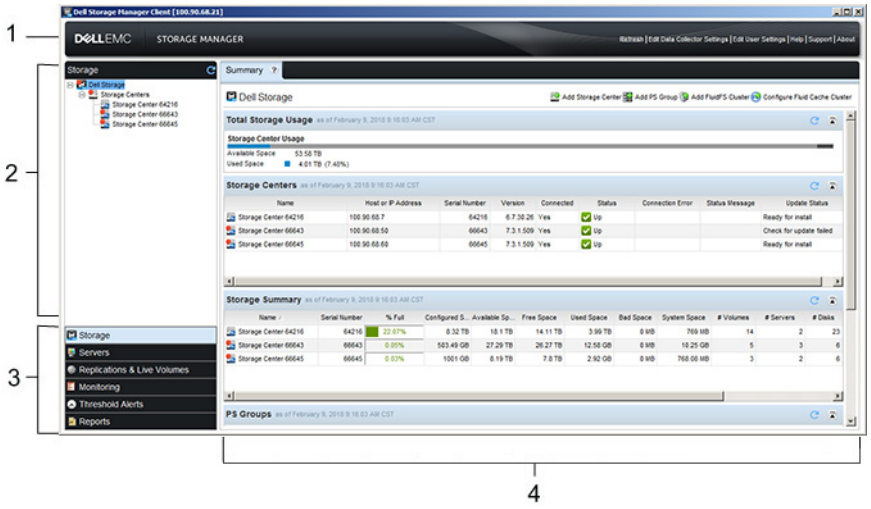


Figure 1. Storage Manager Client Window

The left pane, which is comprised of the *View* pane and Views, can be resized by dragging the right border to the left or right.

The following table describes the primary elements of the Storage Manager Client.

Callout	Client Elements	Description
1	Top pane	Contains the following options: • **Refresh** – When clicked, updates the information displayed in the Storage Manager Client. • **Edit Data Collector Settings** – When clicked, opens a dialog box that allows you to view and modify Data Collector settings. • **Edit User Settings** – When clicked, opens a dialog box that allows you to view and modify your account settings. • **Help** – When clicked, displays the Storage Manager Online Help in a web browser. • **Support** – When clicked, displays the Dell Support Site in a web browser.

Callout	Client Elements	Description
		• **About** – When clicked, opens a dialog box that displays the software version of the Storage Manager Client.
2	Navigation pane	Displays options specific to the view that is currently selected. For example, when the **Storage** view is selected, the view pane displays the Storage Centers, PS Groups, and FluidFS clusters that have been added to Storage Manager.
3	Views	Displays the view buttons. The views are: • **Storage** – When selected, allows you to view, monitor, and configure managed Storage Centers, PS Groups, and FluidFS clusters. • **Servers** – When selected, allows you to register servers to the Data Collector and perform server actions. • **Replications & Live Volumes** – When selected, allows you to configure replications, Live Volumes, Quality of Service definitions, and manage disaster recovery. • **Monitoring** – When selected, allows you to view and acknowledge alerts, indications, and logs. • **Threshold Alerts** – When selected, allows you to run threshold queries and define threshold alerts. • **Chargeback** – When selected, allows you to configure and run Chargeback in order to bill organizations based on storage usage. • **Reports** – When selected, allows you to view automated reports and Chargeback reports.
4	Right pane	Displays management and monitoring options for the view that is selected in the views pane.

2

Getting Started

Start the Storage Manager Client and connect to the Data Collector. When you are finished, review the next steps for suggestions on how to proceed.

For instructions on setting up a new Storage Center, see Storage Center Deployment on page 50.

Topics:

- Use the Client to Connect to the Data Collector
- Next Steps

Use the Client to Connect to the Data Collector

Start the Storage Manager Client and use it to connect to the Data Collector. By default, you can log on as a local Storage Manager user. If the Data Collector is configured to use an external directory service, you can log on as an Active Directory or OpenLDAP user. If Kerberos authentication is configured, you can log on automatically using your Windows session credentials without typing them manually. You can also connect directly to a Storage Center with the Storage Manager Client.

Prerequisites

- The Storage Manager Client must be installed on the computer you are using. For installation instructions, see the *Storage Manager Installation Guide*.
- If the Data Collector is not configured to use an external Active Directory or OpenLDAP directory service, you must know the user name and password for a local Storage Manager user account.
- If you want to log on as an Active Directory or OpenLDAP user, the Data Collector must be configured to use an external Active Directory or OpenLDAP directory service, and your directory user account or directory user group must be added to a Storage Manager user group.
- If you want to log on automatically using your Windows session credentials, the Data Collector must be configured to use Kerberos authentication with an external Active Directory or OpenLDAP directory service.

Steps

1. Start the **Storage Manager Client** application. The Storage Manager Client appears.
2. If the Storage Manager Client welcome screen displays, select a language from the **Display Language** drop-down menu then click **Log in to a Storage Center or Data Collector**.
   The Storage Manager Client login page appears.

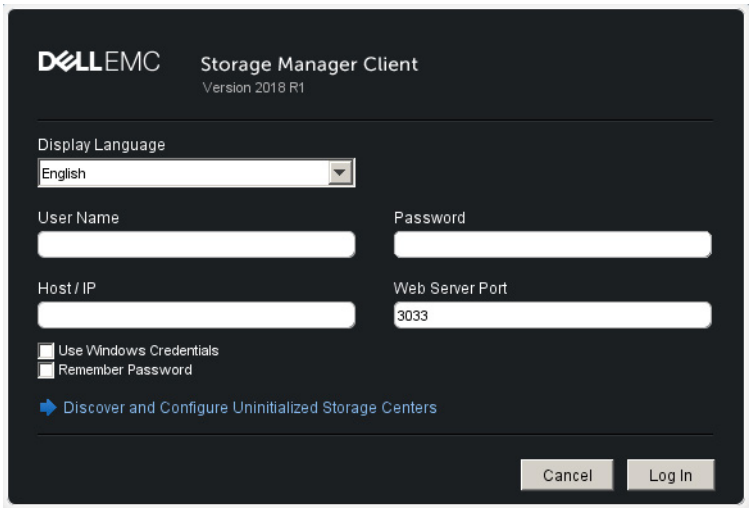


Figure 2. Storage Manager Client Login

3. To change the language displayed in the Storage Manager Client, select a language from the **Display Language** drop-down menu.
4. Type the user name and password in the **User Name** and **Password** fields.
5. Specify your credentials.
   - If you want to log on as a local Storage Manager user, Active Directory user, or OpenLDAP user, type the user name and password in the **User Name** and **Password** fields.
     - For OpenLDAP, the user name format is supported (example: *user*).
     - For Active Directory, the user name (example: *user*), User Principal Name (example: *user*@*domain*), and NetBIOS ID (example: *domain**user*) user name formats are supported.
   - If you want to log on automatically using your Windows session credentials, select the **Use Windows Credentials** check box.
6. In the **Host/IP** field, type the host name or IP address of the server that hosts the Data Collector. If the Data Collector and Client are installed on the same system, you can type `localhost` instead.
7. If you changed the Web Server Port during installation, type the updated port in the **Web Server Port** field.
8. Click **Log In**. The Client connects to the Data Collector and displays the **Storage** view.

NOTE: If the **Display Language** does not match the preferred language of the user, a warning message appears.

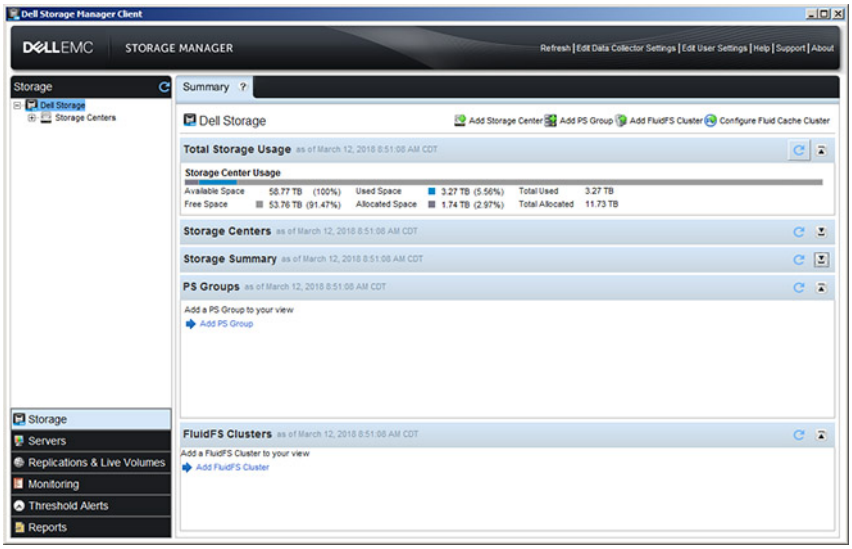


Figure 3. Storage Manager Client Storage View

Related concepts

Authenticating Users with an External Directory Service on page 652
Managing Local Users Through the Data Collector on page 658

Next Steps

This section describes some basic tasks that you may want to perform after your first log on to Storage Manager. These tasks are configuration dependent and not all tasks are required at all sites.

Add Storage Manager Users

The Data Collector controls user access to Storage Manager functions and associated Storage Centers based on the privileges assigned to users: Reporter, Volume Manager, or Administrator. New users, as well as the associated Storage Centers, are created and managed only by the Data Collector. If you want to allow other members of your organization to use Storage Manager, use the Data Collector to grant them access. You can grant access using either of the following methods:

- Create local Storage Manager users.
- Configure the Data Collector to authenticate users using an external Active Directory or OpenLDAP directory service, and then grant access to specific directory users and/or user groups.

Related concepts

Storage Manager User Management on page 651

Add Storage Centers to Storage Manager

Use the Storage Manager Client to add Storage Centers to Storage Manager.

Related concepts

Adding and Organizing Storage Centers on page 92

Configure Storage Center Volumes

After you have added Storage Centers to the Data Collector or connected directly to a single Storage Center, you can create and manage volumes on the Storage Centers.

You can also manage snapshot profiles and storage profiles on the Storage Centers.

Related concepts

Managing Volumes on page 97
Managing Snapshot Profiles on page 130
Managing Storage Profiles on page 135

Add Servers to the Storage Centers

Use Storage Manager to add servers that use Storage Center volumes to the associated Storage Centers. To enable additional functionality, such as the ability to display operating system and connectivity information, and to manage the volumes or datastores mapped to the servers, register these servers to the Storage Manager Data Collector. Before you register Windows servers, you must first install the Storage Manager Server Agent.

Related concepts

Storage Center Server Administration on page 143

Add PS Groups to Storage Manager

Use the Storage Manager Client to add PS Groups to Storage Manager.

Add FluidFS Clusters to Storage Manager

If you have one or more FluidFS clusters, add them to Storage Manager during the FluidFS cluster deployment process.

Related concepts

Adding and Removing FluidFS Clusters in Storage Manager on page 460

Configure Email Notifications

The Data Collector can send emails to notify you when alerts occur and automated reports are ready. To enable email notifications, configure the SMTP settings on the Data Collector and add an email address to your user account on the Data Collector.

Related concepts

Configuring Email Alerts for Storage Manager Events on page 616

Configuring Email Notifications for Threshold Alerts on page 583
Configure Storage Manager to Email Reports on page 594

Set up Remote Storage Centers and Relication QoS

If you want to protect your data by replicating volumes from one Storage Center to another, set up connectivity between your Storage Centers. Create Replication Quality of Service (QoS) definitions on each Storage Center to control how much bandwidth is used to transmit data to remote Storage Centers.

Related concepts

Remote Storage Centers and Replication QoS on page 495

Configure Replications and Live Volumes

To make sure that your data is protected even if one site goes down, configure replications and Live Volumes to mirror volumes to remote Storage Centers.

Related concepts

Storage Center Replications and Live Volumes on page 500

Prepare for Disaster Recovery

If you configure replications or Live Volumes, you can predefine disaster recovery settings to simplify the disaster recovery process. You can also install a remote Data Collector at another site to allow access to Storage Manager disaster recovery options when the primary Data Collector is unavailable.

Related concepts

Preparing for Disaster Recovery on page 542
Remote Data Collector on page 555

3

Storage Center Overview

Storage Center is a storage area network (SAN) that provides centralized, block-level storage that can be accessed by Fibre Channel, iSCSI, or Serial Attached SCSI (SAS).

Topics:

- How Storage Virtualization Works
- User Interface for Storage Center Management

How Storage Virtualization Works

Storage Center virtualizes storage by grouping disks into pools of storage called Storage Types, which hold small chunks (pages) of data. Block-level storage is allocated for use by defining volumes and mapping them to servers. The storage type and storage profile associated with the volume determines how a volume uses storage.

Storage Center combines the following features to provide virtualized storage.

- Disk Management – Sorts disks into disk folders and assigns a storage type based on the disk types.
- Volumes – Allocate storage for use.
- Storage Types – Define a datapage size and redundancy levels for the disk folder.
- Data Progression – Moves pages between tiers and drive types, as well as among multiple RAID levels within the same tier.
- Storage Profiles – Define how data progression moves pages between tiers.

Storage Center Hardware Components

Storage Center consists of one or two controllers, switches, and might include one or more disk enclosures.

Controllers

A Storage Center controller provides the central processing capability for the Storage Center Operating System and managing RAID storage. A Storage Center is typically configured with a pair of controllers. In a dual-controller Storage Center configuration, the two controllers must be the same model.

I/O cards in the controller provide communication with disk enclosures and servers that use the storage. Controllers provide two types of I/O ports:

- **Front-end ports** – Hosts, servers, or Network Attached Storage (NAS) appliances access storage by connecting to controller Fibre Channel I/O cards, FCoE I/O cards, or iSCSI I/O through one or more network switches. Some storage systems contain SAS ports that are designated as front-end ports, which can be connected directly to a server. Ports for front-end connections are located on the back of the controller, but are configured as front-end ports.
- **Back-end ports** – Enclosures, which hold the physical drives that provide back-end storage, connect directly to the controller. Fibre Channel and SAS transports are supported through ports designated as back-end ports. Back-end ports are in their own private network between the controllers and the drive enclosures.

Switches

Switches provide robust connectivity to servers, allowing for the use of multiple controllers and redundant transport paths. Cabling between controller I/O cards, switches, and servers is referred to as front-end connectivity.

Enclosures

Enclosures house and control drives that provide storage. Enclosures are connected directly to controller I/O cards. These connections are referred to as back-end connectivity.

Fibre Channel Switched Bunch of Disks (SBOD) and Serial Advanced Technology Attachment (SATA) enclosures are supported for existing Storage Centers and for controller migrations only.

Disk Management

Storage Center manages both physical disks and the data movement within the virtual disk pool. Disks are organized physically, logically, and virtually.

- **Physically** – Disks are grouped by the enclosure in which they reside, as shown in the **Enclosures** folder.
- **Logically** – Disks are grouped by class in disk folders. Storage Center enclosures may contain any combination of disk classes.
- **Virtually** – All disk space is allocated into tiers. The fastest disks reside in Tier 1 and slower drives with lower performance reside in Tier 3. Data that is accessed frequently remains in Tier 1, and data that has not been accessed for the last 12 progression cycles is gradually migrated to Tiers 2 and 3. Data is promoted to a higher tier after three days of consistent activity. Disk tiering is shown when you select a Storage Type.

For SCv3000, SC5020, and SC7020 storage systems, Storage Center uses the Automatic Drive Placement function to manage drives automatically. When configuring a storage system, Storage Center manages the disks into folders based on function of the disk. FIPS-certified Self-Encrypting Drives (SEDs) are managed into a separate folder than other disks. When Storage Center detects new disks, it manages the disk into the appropriate folder.

In Storage Center version 7.3 and later, the Automatic Drive Placement function can be turned on or off for all Storage Centers (except SCv2000 series storage systems) using the Storage Center Storage settings.

Disk Management on SCv2000 series Storage Systems

Storage Centers with SCv2000 series storage systems manage disks automatically, limiting the disk management options. After adding disks, Storage Center recognizes the new disks, creates a new disk folder if necessary, then manages the disks in the disk folder. If a disk is intentionally down for testing purposes, then is deleted, you can restore the disk to manage the disk again in a disk folder.

The following disk management options are not available for SCv2000 series storage systems:

- Creating disk folders
- Adding disks to disk folders
- Managing disk spares

Disk Folders

A disk folder contains both managed drives and spare disk space. Managed drives are used for data storage. Spare disk space is held in reserve to automatically replace a drive if a drive fails. By default, the **Assigned** disk folder is the parent disk folder for all drives. Drives are further grouped by class in subordinate folders.

Disk Classes

Disks are classified based on their performance characteristics. Each class is shown in a separate folder within the **Assigned** disk folder.

- **Hard Disk Drives (HDDs)** – For HDDs, the disk classification describes its spindle speed and can be any of three disk types.

- 7K (RPM)
- 10K (RPM)
- 15K (RPM)

- **Solid State Drives (SSDs)** – SSDs are differentiated by read or write optimization.
  - Write-intensive (SLC SSD)
  - Read-intensive (MLC SSD)

Drive Spares

Drive spares are drives or drive space reserved by the Storage Center to compensate for a failed drive. When a drive fails, Storage Center restripes the data across the remaining drives.

Distributed Sparing

When updating to Storage Center version 7.3, a banner message prompts you to optimize disks. Clicking the link guides you through the process of optimizing disks for Distributed Sparing. During disk optimization, a meter displays the progress in the **Disks** view. When disks are optimized, spare disk space is distributed across all drives in a drive folder and is designated as Spare Space. This allows the system to use all disks in a balanced and optimized manner, and ensures the fastest recovery time following a disk failure. Distributed Sparing is the default for systems shipping with Storage Center version 7.3 or later.

Reserved Spare Drive

Prior to Storage Center version 7.3, a spare drive is used as a replacement for the failed drive. Storage Center designates at least one drive spare for each disk class. Storage Center groups drives into groups of no more than 21 drives, with one drive in each group designated as a spare drive. For example, a disk class containing 21 drives will have 20 managed drives and one spare drive. A disk class with 22 drives will have 20 managed drives and two spare drives. Storage Center designates the one additional drive as a spare drive. Storage Center designates the largest drives in the disk class as spare drives.

When Storage Center consumes a spare drive, a feature called Drive Spare Rightsizing allows Storage Center to modify the size of a larger capacity spare drive to match the capacity of the drive being replaced in the tier. After modifying the size of the drive in this manner, it cannot be modified to its original size. Drive Spare Rightsizing is enabled by default for all controllers running Storage Center version 7.2 beginning with version 7.2.11. It allows Technical Support to dispatch larger capacity drives of the same disk class when the same size drive is not available, providing faster delivery times.

Volumes

A Storage Center volume is a logical unit of storage that can represent more logical space than is physically available on the Storage Center. Before data can be written to a volume, it must be mapped to a server, then formatted as a drive. Depending on the configuration of the server, data can be written to the volume over iSCSI, Fibre Channel, or SAS.

The storage type and storage profile selected when the volume is created determines how a volume behaves. The storage type sets the datapage size and redundancy levels. The storage profile determines how data progression moves pages on the volume between tiers and RAID levels.

Storage Types

A Storage Type is a pool of storage with a single datapage size and specified redundancy levels. Storage Center assesses the disks available in a disk folder and presents the applicable storage type options. Once the selection is made, it cannot be changed without assistance from technical support, even when disk types change.

NOTE: SCv2000 series storage systems manage storage types automatically by assigning each disk class to a new storage type. SSD storage types have a 512 K datapage size and HDD storage types have a 2 MB datapage size. These Storage Types cannot be modified and non-redundant storage types are not allowed.

Disk Types

The type of disks present in a Storage Center determines how Data Progression moves data between tiers. Storage Center supports write-intensive SSDs, and 7K, 10K, and 15K HDDs. A minimum number of disks are required, which may be installed in the controller or in an expansion enclosure:

- An all-flash array requires a minimum of four SSDs of the same disk class, for example four write-intensive SSDs.
- A hybrid array requires a minimum of seven HDDs or four SSDs of the same disk class, for example seven 10K HDDs.

Datapage Size

By default, data is migrated between tiers and RAID levels in 2 MB blocks. Data can be moved in smaller or larger blocks to meet specific application requirements. These blocks are referred to as datapages.

- **2 MB** – Default datapage size, this selection is appropriate for most applications.
- **512 KB** – Appropriate for applications with high performance needs, or in environments in which snapshots are taken frequently under heavy I/O. Selecting this size increases overhead and reduces the maximum available space in the storage type. All-flash storage systems use 512 KB by default.
- **4 MB** – Appropriate for systems that use a large amount of disk space with infrequent snapshots.

  CAUTION: Before changing the datapage setting, contact technical support to discuss the impact on performance and for advice about how to ensure that system resources remain balanced.

Redundancy

Redundancy provides fault tolerance for a drive failure. Two redundancy options are available.

- **Redundant**: Protects against the loss of any one drive (if single redundant) or any two drives (if dual redundant).
- **Non-Redundant**: Uses RAID 0 in all classes, in all tiers. Data is striped but provides no redundancy. If one drive fails, all data is lost.

  NOTE: Non-Redundant is not recommended because data is not protected against a drive failure. Do not use non-redundant storage for a volume unless the data has been backed up elsewhere.

Redundancy levels per tier include single or dual redundant. The options may be restricted depending on the disk size.

- **Single Redundant**: Single-redundant tiers can contain any of the following types of RAID storage:
  - RAID 10 (each drive is mirrored)
  - RAID 5-5 (striped across 5 drives)
  - RAID 5-9 (striped across 9 drives)
- **Dual redundant**: Dual redundant is the recommended redundancy level for all tiers. It is enforced for 3 TB HDDs and higher and for 18 TB SSDs and higher. Dual-redundant tiers can contain any of the following types of RAID storage:
  - RAID 10 Dual-Mirror (data is written simultaneously to three separate drives)
  - RAID 6-6 (4 data segments, 2 parity segments for each stripe)
  - RAID 6-10 (8 data segments, 2 parity segments for each stripe.)

Redundancy Requirements

Drive size is used to determine the redundancy level to apply to a tier of drives. If any drive in a tier surpasses a threshold size, a specific redundancy level can be applied to the tier containing that drive. If a redundancy level is required, the Storage Center operating system sets the level and it cannot be changed.

Table 3. HDD Redundancy Recommendations and Requirements

Disk Size	Level of Redundancy Recommended or Enforced
Up to 3 TB	Dual redundant is the recommended level **NOTE:** Non-redundant storage is not an option for SCv2000 Series storage systems.
3 TB and higher	Dual redundant is required and enforced

Table 4. SSD Redundancy Recommendations and Requirements

Disk Size	Level of Redundancy Recommended or Enforced
Up to 18 TB	Dual redundant is the recommended level **NOTE:** Non-redundant storage is not an option for SCv2000 Series storage systems.
18 TB and higher	Dual redundant is required and enforced

Data Progression

Storage Center uses Data Progression to move data within a virtualized storage environment. Data Progression moves data between tiers and drive types, as well as among multiple RAID levels within the same tier, for a constant balance of performance and cost.

How Data Progression Works

Once every 24 hours, Storage Center assesses disk use and moves data to disk space that is more efficient for the data usage. By default, Data Progression runs each day at 7 PM system time, but the timing of the run can be changed in the Storage Center settings. Data Progression behavior is determined by the storage profile applied to each volume. Data progression runs until it completes or reaches the maximum run time.

NOTE: On SCv2000 series storage systems, Data Progression moves data between RAID 10 and RAID 5/6 and restripes RAID, but it does not move data between storage tiers.

Data Progression and Snapshots

Storage Center also uses Data Progression to move snapshots. When a snapshot is created, either as scheduled or manually, the data is frozen and moved to the tier specified by the storage profile to hold snapshots.

Snapshots can occur as a scheduled event according to the snapshot profile, manually by creating a snapshot, or on demand by Storage Center to move data off of Tier 1 in a flash-optimized storage type.

Low Space Modes

A Storage Center enters Conservation mode when free space becomes critically low, and enters Emergency mode when the system can no longer write to the disks because there is not enough free space.

Prior to entering Conservation mode, the Storage Center displays alerts indicating that disk space is running low. The alert reflects the amount of space left, beginning with 10%, before the system stops operating. The alert updates each time the remaining space decreases by 1%.

Conservation Mode

A Storage Center enters Conservation mode when free space becomes critically low. Immediate action is necessary to avoid entering Emergency mode.

NOTE: Because of Conservation mode's proximity to the emergency threshold, do not use it as a tool to manage storage or to plan adding disks to the Storage Center.

In Conservation mode, Storage Manager Client responds with the following actions:

- Generates a Conservation mode alert.
- Prevents new volume creation.
- Expires snapshots at a faster rate than normal (Storage Center version 7.2 and earlier).

Emergency Mode

Storage Center enters Emergency mode when the system can no longer operate because it does not have enough free space.

In Emergency mode, Storage Center responds with the following actions:

- Generates an Emergency Mode alert.
- Expires snapshots at a faster rate than normal (Storage Center version 7.2 and earlier)
- Prevents new volume creation.
- Volumes become either inaccessible or read-only.
- Prevents restart or shutdown operation

CAUTION: Do not turn off the storage controllers in emergency mode. Contact technical support for assistance in recovering from Emergency mode.

CAUTION: Because Emergency mode prevents all server I/O, Emergency mode is service affecting. Administrators must take special care to continually monitor free space on the Storage Center and add or free up space as needed to avoid reaching the Emergency mode threshold.

Troubleshoot Conservation or Emergency Mode

To resolve Conservation or Emergency mode, reclaim consumed disk space.

About this task

Perform each step, then wait a few minutes and check available disk space.

Steps

1. Delete any unnecessary volumes and then empty the recycle bin.
2. Expire unnecessary snapshots.

Next steps

If these steps do not resolve Conservation or Emergency mode, contact technical support.

Preventing Low Space Modes

Manage disk space to prevent a Storage Center from entering Conservation or Emergency mode.

Prevent low space issues using these tips:

- Empty the recycle bin regularly.
- Lower the frequency of snapshots or set snapshots to expire earlier.
- Change the storage profile to a more space-efficient profile. Available profiles might include Low Priority (Tier 3) and Maximize Efficiency.
- Configure a threshold definition to create an alert when space starts to get low.
- Migrate volumes from a pagepool with a full tier to a different pagepool with more free space.
- Delete unnecessary volumes.
- If Data Reduction is licensed, enable Compression or Deduplication with Compression on some volumes.

Related concepts

Configuring Threshold Definitions on page 569

Related tasks

Empty the Recycle Bin on page 125
Apply a Storage Profile to One or More Volumes on page 136

Storage Center Operation Modes

Storage Center operates in four modes: Installation, Pre-production, Production, and Maintenance.

Name	Description
Install	Storage Center is in Install mode before completing the setup wizard for the Storage Center. Once setup is complete, Storage Center switches to Pre-Production mode.
Pre-Production	During Pre-production mode, Storage Center suppresses alerts sent to support so that support is not alerted to expected test scenarios caused by testing. Use the Pre-production mode to perform tests on the Storage Center before placing it into a production environment. After passing tests, manually change the operational mode from Pre-production to Production mode.
Production	Production mode is the operation mode used when the Storage Center is in a production environment. Storage Center does not suppress alerts in this mode.
Maintenance	When Storage Center is in Maintenance mode, it suppresses alerts sent to support in the same way when it is in Pre-production mode. Switch to Maintenance mode before performing maintenance on the Storage Center that may trigger alerts to support.

Related concepts

Change the Operation Mode of a Storage Center on page 215

Storage Profiles

Storage profiles control how Storage Center manages volume data. For a given volume, the selected storage profile dictates which disk tier accepts initial writes, as well as how data progression moves data between tiers to balance performance and cost. Predefined storage profiles are the most effective way to manage data in Storage Center. The storage profiles available are determined by the storage type.

The ability to select storage profiles is controlled by user settings. Storage profiles might not be visible to all users. If your user volume defaults allow you to select a storage profile, the **Storage** tab displays them under the **Storage Profiles** node.

Storage Profiles for Standard Storage Types

The table below summarizes the storage profiles available for standard storage types. Each profile is described in more detail following the table.

Name	Initial Write Tier	Tier (T) and RAID Levels	Progression
Recommended (All Tiers)	1	Writes: T1 RAID 10 Snapshots: RAID 5/RAID 6	Yes - to all Tiers
High Priority (Tier 1)	1	Writes: T1 RAID 10 Snapshots: T1 RAID 5/RAID 6	No
Medium Priority (Tier 2)	2	Writes: T2 RAID 10 Snapshots: T2 RAID 5/RAID 6	No
Low Priority (Tier 3)	3	Writes: T3 RAID 10 Snapshots: T3 RAID 5/RAID 6	No

NOTE: The Recommended, High Priority, and Medium Priority profiles are not available for the Flash Optimized storage type.

Recommended (All Tiers)

The Recommended storage profile is available only when data progression is licensed. Cost and performance are optimized when all volumes use the Recommended storage profile. The Recommended profile allows automatic data progression between and across all storage tiers based on data type and usage.

When a volume uses the Recommended profile, all new data is written to Tier 1 RAID level 10 storage. Data progression moves less active data to Tier 1 RAID 5/ RAID 6 or a slower tier based on how frequently the data is accessed. In this way, the most active blocks of data remain on high-performance drives, while less active blocks automatically move to lower-cost, high-capacity SAS drives.

Because SSDs are automatically assigned to Storage Tier 1, profiles that include Storage Tier 1 allow volumes to use SSD storage. If you have volumes that contain data that is not accessed frequently, and do not require the performance of Tier 1 SSDs, use a Medium or Low Priority profile or create and apply a new profile that does not include Storage Tier 1.

High Priority (Tier 1)

The High Priority storage profile provides the highest performance by storing data on Tier 1. It is efficient in terms of using RAID 5 or 6, but it uses more expensive media to store the data. A volume created using the High Priority profile stores written data on Tier 1 RAID 10. Snapshot data is stored on Tier 1 RAID 5/RAID 6. Storage Center does not migrate data to lower storage tiers unless Tier 1 storage becomes full.

If data progression is not licensed, the default storage profile is High Priority. Without data progression, you must configure volumes to use a specific tier of storage, because data will not migrate between tiers.

Medium Priority (Tier 2)

The Medium Priority storage profile provides a balance between performance and cost efficiency. A volume created using the Medium Priority profile stores written data on Tier 2 RAID 10. Snapshot data is stored on Tier 2 RAID 5/RAID 6. Storage Center does not migrate data to other storage tiers unless Tier 2 storage becomes full.

Low Priority (Tier 3)

The Low Priority profile provides the most cost efficient storage. Creating a volume using the Low Priority profile stores written data on Tier 3 RAID 10. Snapshot data is stored on Tier 3 RAID 5/6. Storage Center does not migrate data to higher tiers of storage unless Tier 3 storage becomes full.

Storage Profiles for Flash-Optimized Storage

The table below summarizes storage profiles available for flash-optimized storage types. Each profile is described in more detail following the table.

Name	Initial Write Tier	Tier (T) and RAID Levels	Progression
Low Priority (Tier 3)	3	Writes: T3 RAID 10 snapshots: T3 RAID 5/6	No
Flash Optimized with Progression (Tier 1 to All Tiers)	1	Writes: T1 RAID 10 snapshots: T2/T3 RAID 5/6	Yes to all tiers
Write Intensive (Tier 1)	1	Writes: T1 RAID 10 snapshots: T1 RAID 10	No
Flash Only with Progression (Tier 1 to Tier 2)	1	Writes: T1 RAID 10 snapshots: T2 RAID 5	Yes to Tier 2 only
Low Priority with Progression (Tier 3 to Tier 2)	3	Writes: T3 RAID 10 snapshots: T3 RAID 5/6 or T2 RAID 5	Yes to Tier 2 only

Low Priority (Tier 3)

The Low Priority profile provides the most cost efficient storage. Creating a volume using the Low Priority profile stores written data on Tier 3 RAID 10. Snapshot data is stored on Tier 3 RAID 5/6. Storage Center does not migrate data to higher tiers of storage unless Tier 3 storage becomes full.

Flash-Optimized with Progression (Tier 1 to All Tiers)

The Flash Optimized with Progression storage profile provides the most efficient storage for an enclosure containing both read-intensive and write-intensive SSDs. When a storage type uses this profile, all new data is written to write-intensive Tier 1 drives. Snapshot data is moved to Tier 2, and less-active data progresses to Tier 3.

If Tier 1 fills to within 95% of capacity, Storage Center creates a space-management snapshot and moves it immediately to Tier 2 to free up space on Tier 1. The space-management snapshot is moved immediately and does not wait for a scheduled data progression. Space-management snapshots are marked as `Created On Demand` and cannot be modified manually or used to create View volumes. Space-management snapshots coalesce into the next scheduled or manual snapshot. Storage Center creates only one on demand snapshot per volume at a time.

Write-Intensive (Tier 1)

The Write-Intensive storage profile directs all initial writes to write-intensive SSDs on Tier 1 (RAID 10). The data does not progress to any other tier. This profile is useful for storing transaction logs and temporary database files.

Flash Only with Progression (Tier 1 to Tier 2)

The Flash Only with Progression storage profile performs initial writes on high-performance Tier 1 drives. Less active data progresses to Tier 2, but remains on SSDs. This profile is useful for storing volumes with data that requires optimal read performance, such as golden images, linked clones, and some databases.

Low Priority with Progression (Tier 3 to Tier 2)

The Low Priority with Progression storage profile directs initial writes to less expensive Tier 3 (RAID 10) drives, and then allows frequently accessed data to progress to Tier 2. This profile is useful for migrating large amounts of data to Storage Center without overloading Tier 1 SSDs.

Storage Profiles for SCv2000 Series Storage Systems

The following table summarizes the storage profiles available to SCv2000 series storage systems:

Name	Initial Write Tier	Tier (T) and RAID Levels	RAID Tiering
Balanced	1	Writes: T1 RAID 10 Snapshots: T1 RAID 5/6	Between RAID types only
Maximize Performance	1	Writes: T1 RAID 10 Snapshots: T1 RAID 10	No
Maximize Efficiency	1	Writes: T1 RAID 5/6 Snapshots: T1 RAID 5/6	No

Balanced

The Balanced storage profile balances efficiency and performance for any volume using that storage profile.

When a volume uses the Balanced storage profile, all new data is written to RAID 10. When Storage Center creates a snapshot, Data Progression moves snapshot data from RAID 10 to RAID 5/6.

Maximize Performance

Maximize Performance keeps new data and snapshot data on RAID 10 to increase performance. Maximize Performance is useful for volumes with important and frequently used data.

Maximize Efficiency

Maximize Efficiency writes new data to RAID 5/6 and keeps snapshot data on RAID 5/6. Use Maximize Efficiency for volumes with less-important data and infrequently used data.

User Interface for Storage Center Management

Most storage configuration and management for an individual Storage Center is performed from the **Storage** view in the Storage Manager Client. Select a Storage Center in the **Storage** navigation pane to view and manage it.

The following tabs appear in the display pane when a Storage Center is selected:

- Summary Tab
- Storage Tab
- Hardware Tab
- IO Usage Tab
- Charting Tab

Summary Tab

The **Summary** tab displays a customizable dashboard that summarizes Storage Center information. The Summary tab is displayed by default when a Storage Center is selected from the Storage navigation tree.

NOTE: Disk Space details and graphs are displayed in Storage Center version 7.4.10 and later.

System RAID Overhead Ratio and Estimated Usable Space are displayed in Storage Center version 7.5.1 and later.

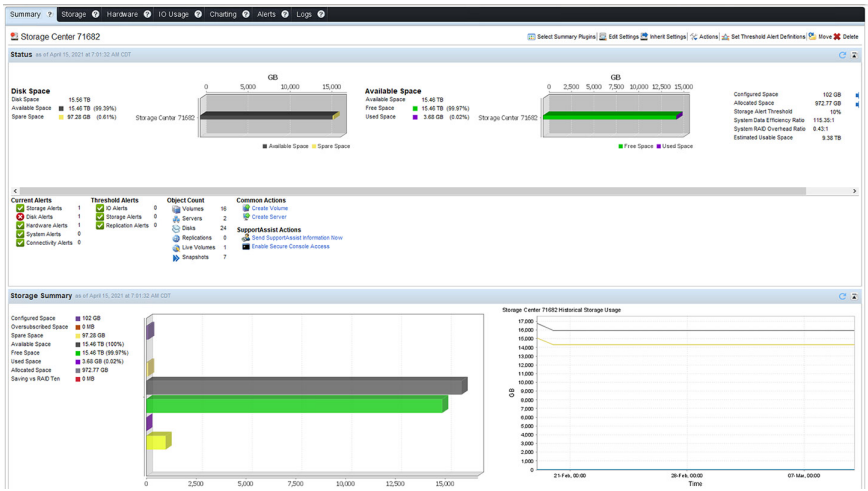


Figure 4. Summary Tab

Related concepts

Managing Storage Center Settings on page 214
Viewing Summary Information on page 299

Storage Tab

The **Storage** tab of the **Storage** view allows you to view and manage storage on the Storage Center. This tab is made up of two elements: the navigation pane and the right pane.

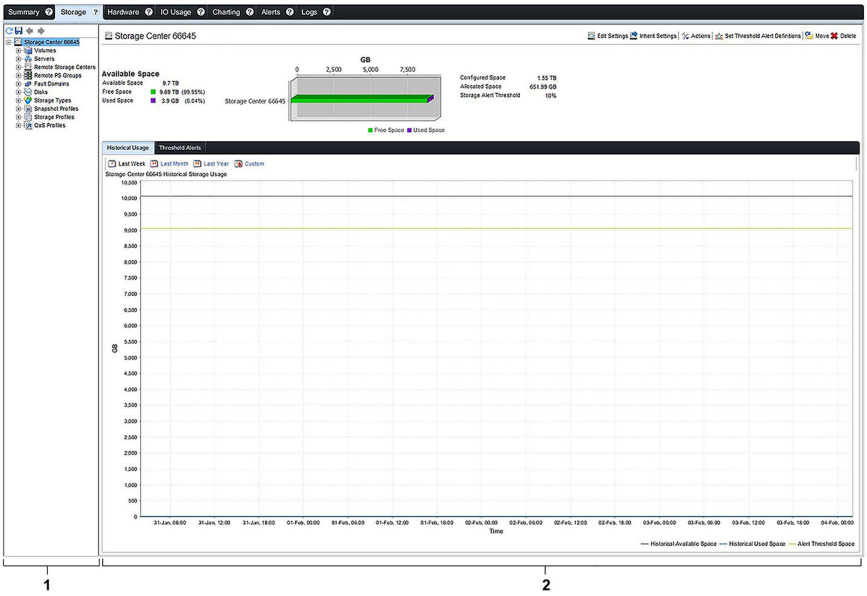


Figure 5. Storage Tab

Call Out	Name
1	Navigation pane
2	Right pane

Navigation Pane

The **Storage** tab navigation pane shows the following nodes:

- **Storage Center**: Shows a summary of current and historical storage usage on the selected Storage Center.
- **Volumes**: Allows you to create and manage volumes and volume folders on the selected Storage Center, as well as create a local recovery from a volume snapshot. You can also create storage containers, which are used with virtual volumes.
- **Servers**: Allows you to create and manage physical and virtual servers, server clusters, and server folders on the selected Storage Center.
- **Remote Storage Centers**: Allows you to create and view iSCSI connections to remote Storage Centers for which you have access.
- **Disks**: Allows you to view and manage disks and disk folders on the selected Storage Center.
- **Portable Volumes**: Allows you to view and manage portable volumes, which are used to transport initial replication data to remote Storage Centers. This option is useful when transferring the initial replication data over the network would be too slow.

  NOTE: Portable Volumes are not supported in Storage Center version 7.3 and later.
- **Storage Types**: Allows you to view the Storage Types prepared on the selected Storage Center.
- **Snapshot Profiles**: Allows you to view, modify, and create Snapshot Profiles for the selected Storage Center, and apply Snapshot Profiles to one or more volumes.
- **Storage Profiles**: Allows you to view and create Storage profiles defined on the selected Storage Center. This node appears only if **Allow Storage Profile Selection** is enabled in the Storage Center user preferences.
- **QoS Profiles**: Allows you to define Quality of Service Profiles for volumes or groups of volumes on the selected Storage Center. This node appears only if **Allow QoS Profile Selection** is enabled in the Storage Center user preferences.

Right Pane

The right pane shows information and configuration options for the node or object selected in the navigation pane. The information and configuration options displayed for each node is described in the online help.

Related concepts

Adding and Organizing Storage Centers on page 92
Managing Storage Center Settings on page 214
Managing Volumes on page 97
Managing Snapshot Profiles on page 130
Managing Servers on a Storage Center on page 144
Managing Storage Profiles on page 135
Managing QoS Profiles on page 137

Hardware Tab

The **Hardware** tab of the **Storage** view displays status information for the Storage Center hardware and allows you to perform hardware-related tasks.

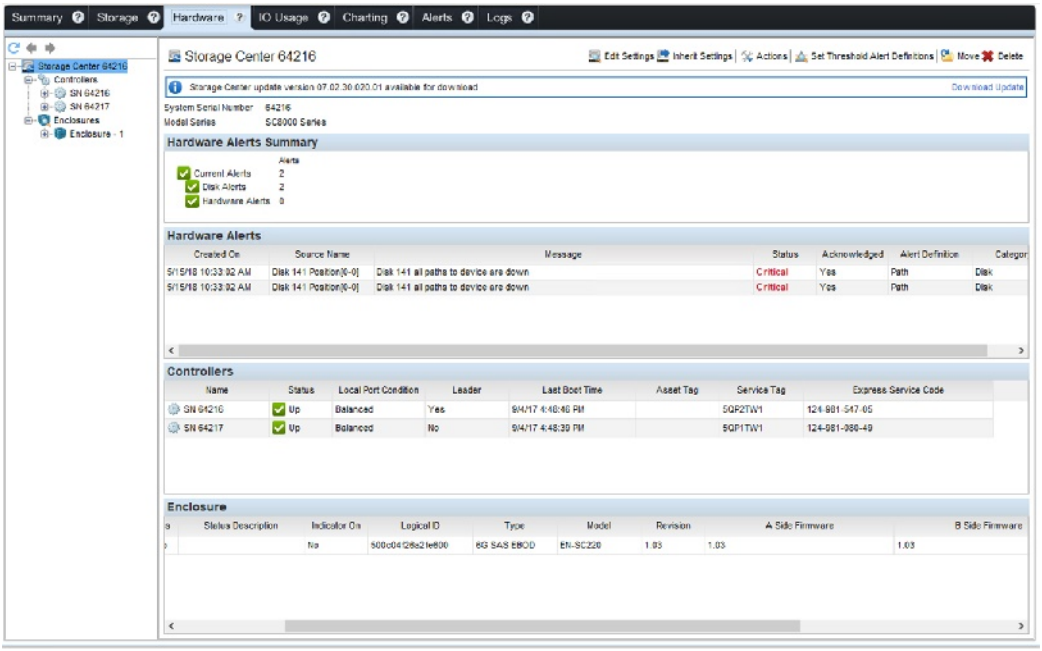


Figure 6. Hardware Tab

Related concepts

Monitoring Storage Center Hardware on page 321
Managing Disk Enclosures on page 284
Shutting Down and Restarting a Storage Center on page 295

IO Usage Tab

The **IO Usage** tab of the **Storage** view displays historical performance statistics for the selected Storage Center and associated storage objects. This tab is visible only when connected to the Storage Center through the Data Collector.

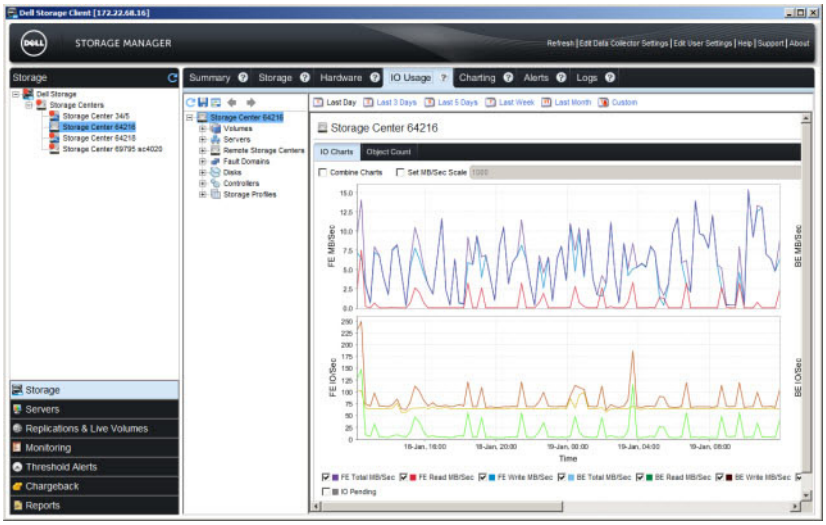


Figure 7. Storage View IO Usage Tab

Related concepts

Viewing Historical IO Performance on page 312

Charting Tab

The **Charting** tab of the **Storage** view displays real-time IO performance statistics for the selected storage object.

Figure 8. Charting Tab

Related concepts

Viewing Current IO Performance on page 314

Alerts Tab

The Alerts tab displays alerts for the Storage Center.

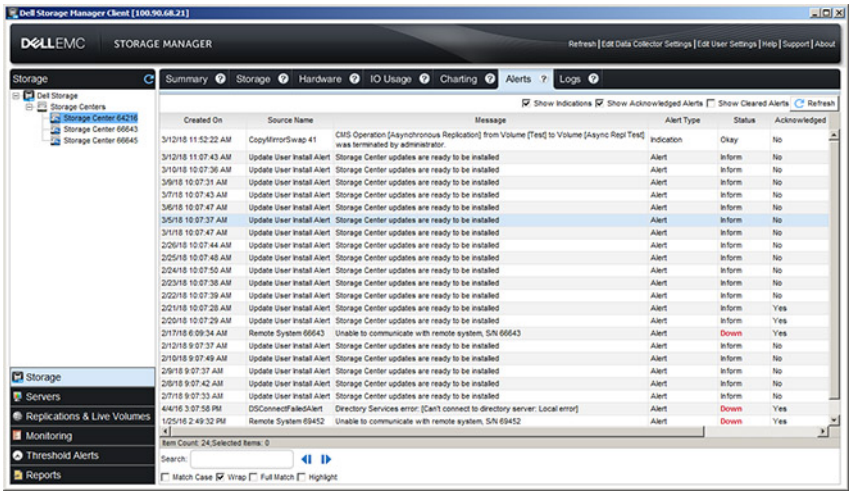


Figure 9. Alerts Tab

Logs Tab

The Logs tab displays logs from the Storage Center.

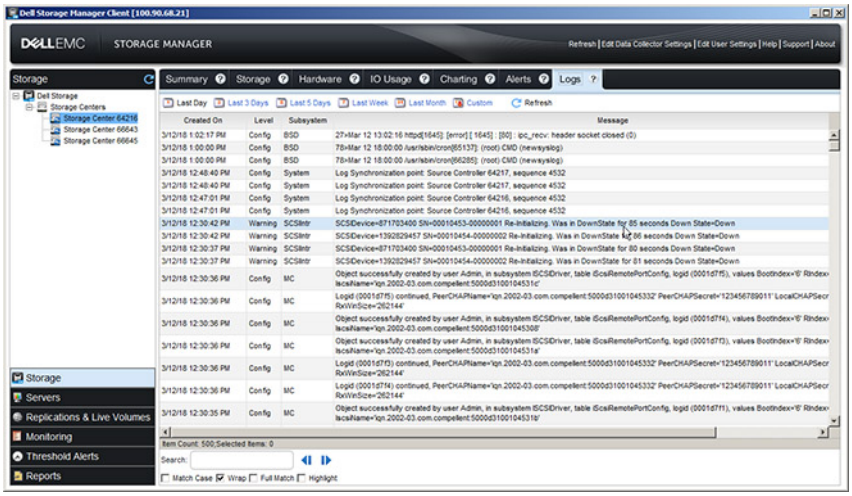


Figure 10. Logs Tab

4

Storage Center Deployment

Use the Discover and Configure Uninitialized Storage Centers or Configure Storage Center wizard to set up a Storage Center to make it ready for volume creation and storage management. After configuring a Storage Center, you can set up a localhost, or a VMware vSphere or vCenter host.

Topics:

- Discover and Configure Uninitialized SCv2000 Series Storage Systems
- Discover and Configure Uninitialized SCv3000 Series Storage Systems
- Discover and Configure Uninitialized SC5020 and SC7020 Storage Systems
- Configuring SC4020 and SC8000 Storage Centers
- Configuring SC9000 Storage Centers
- Set Up a localhost or VMware Host

Discover and Configure Uninitialized SCv2000 Series Storage Systems

When setting up the system, use the Discover and Configure Uninitialized Storage Centers wizard to find and configure new SCv2000 series storage systems. The wizard helps set up a Storage Center to make it ready for volume creation.

NOTE: Make sure that you are running the latest version of the Dell Storage Manager Client.

Open the Discover and Configure Uninitialized Storage Centers Wizard From the Storage Manager Client Welcome Screen

Open the wizard directly from the welcome screen to discover and configure a Storage Center.

Prerequisites

- Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run using Windows Administrator privileges.

Steps

1. Open the Storage Manager Client welcome screen.
2. Click **Discover and Configure Uninitialized Storage Centers**.
   The **Discover and Configure Uninitialized Storage Centers** wizard opens.

Open the Discover and Configure Uninitialized Storage Centers Wizard from the Storage Manager Client

Open the wizard from the Storage Manager Client to discover and configure a Storage Center.

Prerequisites

- The Storage Manager Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run using Windows Administrator privileges.
- The client must be connected to a Storage Manager Data Collector.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, click **Storage Centers**.
3. In the **Summary** tab, click **Discover and Configure Uninitialized Storage Centers** .
   The **Discover and Configure Uninitialized Storage Centers** wizard opens.

Select a Storage Center to Initialize

The next page of the Discover and Configure Uninitialized Storage Centers wizard provides a list of uninitialized Storage Centers discovered by the wizard.

Steps

1. Select the Storage Center to initialize.
2. (Optional) To blink the indicator light for the selected Storage Center, click **Enable Storage Center Indicator**. You can use the indicator light to verify that you have selected the correct Storage Center.
3. Click **Next**.
4. If the Storage Center is partially configured, the Storage Center login pane is displayed. Type the management IPv4 address and the password for the Storage Center Admin user, then click **Next** to continue.

Deploy the Storage Center Using the Direct Connect Method

Use the direct connect method to manually deploy the Storage Center when it is not discoverable.

Steps

1. Use an Ethernet cable to connect the computer running the Storage Manager Client to the management port of the top controller.
2. Cable the bottom controller to the management network switch.
3. Click **Discover and Configure Uninitialized Storage Centers**. The **Discover and Configure Uninitialized Storage Centers** wizard opens.
4. Fill out the information on the initial configuration pages and stop when the **Confirm Configuration** page is displayed.
5. At this point, recable the management port of the top controller to the management network.
6. Connect the computer to the same subnet or VLAN as the Storage Center.
   a. Click **Next**.
   b. If the cable is not properly connected or the host cannot access the controller, an **Error setting up connection** message is displayed. Correct the connection, and click **OK**.
   c. If the deployment wizard is closed, click **Discover and Configure Uninitialized Storage Centers** to relaunch the deployment wizard.
   d. Type **`Admin`** in the **User Name** field, type the password entered on the **Set Administrator Information** page in the **Password** field, and click **Next**.

Set System Information

The **Set System Information** page allows you to enter Storage Center and storage controller configuration information to use when connecting to the Storage Center using Storage Manager.

Steps

1. Type a descriptive name for the Storage Center in the **Storage Center Name** field.
2. Type the system management IPv4 address for the Storage Center in the **Virtual Management IPv4 Address** field.
   The management IPv4 address is the IP address used to manage the Storage Center and is different from a storage controller IPv4 address.
3. Type an IPv4 address for the management port of each storage controller.

   NOTE: The storage controller IPv4 addresses and management IPv4 address must be within the same subnet.

4. Type the subnet mask of the management network in the **Subnet Mask** field.
5. Type the gateway address of the management network in the **Gateway IPv4 Address** field.
6. Type the domain name of the management network in the **Domain Name** field.
7. Type the DNS server addresses of the management network in the **DNS Server** and **Secondary DNS Server** fields.
8. Click **Next**.

Set Administrator Information

The Set Administrator Information page allows you to set a new password and an email address for the Admin user.

Steps

1. Enter a new password for the default Storage Center administrator user in the **New Admin Password** and **Confirm Password** fields.
2. Enter the email address of the default Storage Center administrator user in the **Admin Email Address** field.
3. Click **Next**.
   - For a Fibre Channel or SAS storage system, the **Confirm Configuration** page appears.
   - For an iSCSI storage system, the **Configure iSCSI Fault Domains** page appears.

Configure iSCSI Fault Domains (iSCSI Front-End Only)

For a Storage Center with iSCSI front-end ports, use the Configure Fault Tolerance page and the Fault Domain pages to enter network information for the fault domains and ports.

Steps

1. (Optional) On the **Configure Fault Tolerance** page, click **More information about fault domains** or **How to set up an iSCSI network** to learn more about these topics.
2. Click **Next**.

   NOTE: If any iSCSI ports are down, a dialog box appears that allows you to unconfigure these ports. Unconfiguring the down iSCSI ports will prevent unnecessary alerts.

3. On the **Configure iSCSI HBA Fault Domain 1** page, enter network information for the fault domain and its ports.

   NOTE: Make sure that all the IP addresses for iSCSI Fault Domain 1 are in the same subnet.

4. Click **Next**.
5. On the **Configure iSCSI HBA Fault Domain 2** page, enter network information for the fault domain and its ports. Then click **Next**.

   NOTE: Make sure that all the IP addresses for iSCSI Fault Domain 2 are in the same subnet.

6. Click **Next**.

Confirm the Storage Center Configuration

Make sure that the configuration information shown on the Confirm Configuration page is correct before continuing. If you selected DHCP IPv4 as the network configuration source, the dynamically assigned IP addresses are displayed on this page.

Steps

1. Verify that the Storage Center settings are correct.
2. If the configuration information is correct, click **Apply Configuration**.

   If the configuration information is incorrect, click **Back** and provide the correct information.

   NOTE: After you click the **Apply Configuration** button, the configuration cannot be changed until after the Storage Center is fully deployed.

Deploy the Storage Center

The Storage Center sets up the controller using the information provided on the previous pages.

Steps

1. The Storage Center performs system setup tasks. The **Deploy Storage Center** page displays the status of these tasks.
   To learn more about the initialization process, click **More information about Initialization**.
   - If one or more of the system setup tasks fails, click **Troubleshoot Initialization Error** to learn how to resolve the issue.
   - If the Configuring Disks task fails, click **View Disks** to see the status of the drives detected by the Storage Center.
   - If any of the Storage Center front-end ports are down, the **Storage Center Front-End Ports Down** dialog box opens. Select the ports that are not connected to the storage network, then click **OK**.
2. When all of the Storage Center setup tasks are complete, click **Next**.

Review Redundant Paths (FC or SAS Front-End Only)

For a Storage Center with Fibre Channel or SAS front-end ports, the Fault Tolerance page displays an example fault domain topology based on the number of controllers and type of front-end ports. The Review Redundant Paths page displays information about the fault domains created by the Storage Center.

Steps

1. (Optional) On the **Fault Tolerance** page, click **More information about fault domains** to learn more about fault domains.
2. Click **Next**.

   NOTE: If there are down SAS or Fibre Channel HBA ports, a dialog box appears that allows you to unconfigure down ports. Unconfiguring the down SAS or Fibre Channel HBA ports will prevent unnecessary alerts.

3. On the **Review Redundant Paths** page, make sure that all the information about the fault domains is correct.
4. Click **Next**.

Inherit Settings

Use the Inherit Settings page to copy settings from a Storage Center that is already configured.

Prerequisites

You must be connected through a Data Collector.

Steps

1. Select the Storage Center from which to copy settings.
2. Place a check next to each setting that you want to inherit, or click **Select All** to inherit all settings.
3. Click **Next**.
   If you chose to inherit time and SMTP settings from another Storage Center, the **Time Settings** and **SMTP Server Settings** pages are skipped in the wizard.

Configure Time Settings

Configure an NTP server to set the time automatically, or set the time and date manually.

Steps

1. From the **Region** and **Time Zone** drop-down menus, select the region and time zone used to set the time.
2. Select **Use NTP Server** and type the host name or IPv4 address of the NTP server, or select **Set Current Time** and set the time and date manually.
3. Click **Next**.

Configure SMTP Server Settings

If you have an SMTP server, configure the SMTP email settings to receive information from the Storage Center about errors, warnings, and events.

Steps

1. By default, the **Enable SMTP Email** checkbox is selected and enabled. If you do not have an SMTP server you can disable SMTP email by clearing the **Enable SMTP Email** checkbox.
2. Alternatively, if you have an SMTP server, configure the SMTP server settings.
   a. In the **Recipient Email Address** field, enter the email address where the information will be sent.
   b. In the **SMTP Mail Server** field, enter the IP address or fully qualified domain name of the SMTP mail server.
   c. (Optional) In the **Backup SMTP Mail Server** field, enter the IP address or fully qualified domain name of a backup SMTP mail server and click **OK**.
   d. Click **Test Server** to verify connectivity to the SMTP server.
   e. If the SMTP server requires emails to contain a MAIL FROM address, specify an email address in the **Sender Email Address** field.
   f. (Optional) In the **Common Subject Line** field, enter a subject line to use for all emails sent by the Storage Center.
3. Click **Next**.

Set Up SupportAssist

If the storage system is running Storage Center 7.3 or later, the **Set Up SupportAssist** page opens.

About this task

Use the **Set Up SupportAssist** page to enable SupportAssist.

Steps

1. To allow SupportAssist to collect diagnostic data and send this information to technical support, select the **Receive proactive notifications, notices, and other predictive support** checkbox.
2. Click **Next**.
   If you chose to clear the **Receive proactive notifications, notices, and other predictive support** checkbox and click **Next**, a **SupportAssist Recommended** dialog box opens.
   - To return to the **Set Up SupportAssist** page, click **No**.
   - To disable SupportAssist and proceed to the **Update Storage Center** page, click **Yes**.

Accept the SupportAssist Collection Agreement

Use the Accept SupportAssist Collection Agreement page to accept to the terms of the agreement and enable SupportAssist.

Steps

1. To allow SupportAssist to collect diagnostic data and send this information to technical support, select the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox.
2. Click **Next**.

   NOTE: If you chose to clear the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox, a **SupportAssist Recommended** dialog box opens.
   - To return to the **Accept SupportAssist Collection Agreement** page, click **No**.
   - To opt out of SupportAssist, click **Yes**.

Provide Contact Information

Specify contact information for technical support to use when sending support-related communications from SupportAssist.

Steps

1. Specify the contact information.
2. (Storage Center 7.2 or earlier) To receive SupportAssist email messages, select the **Send me emails from SupportAssist when issues arise, including hardware failure notifications** check box.
3. Select the preferred contact method, language, and available times.
4. (Storage Center 7.2 or earlier) Type a shipping address where replacement Storage Center components can be sent.
5. (Storage Center 7.2 or earlier) Click **Finish**.
6. (Storage Center 7.3 or later) Click **Next**.

Provide Site Contact Information

If the storage system is running Storage Center 7.3 or later, specify the site contact information.

Steps

1. Select the **Enable Onsite Address** checkbox.
2. Type a shipping address where replacement Storage Center components can be sent.
3. Click **Next**.
   The **Confirm Enable SupportAssist** dialog box opens.
4. Click **Yes**.

Validate the SupportAssist Connection

If the storage system is running Storage Center 7.3 or later, the **Validate SupportAssist Connection** page opens.

About this task

The **Validate SupportAssist Connection** page displays a summary of the SupportAssist contact information and confirms that the Storage Center is connected to SupportAssist.

Steps

- To complete the SupportAssist setup, click **Finish**.

Update Storage Center

The Storage Center attempts to contact the SupportAssist Update Server to check for updates. If you are not using SupportAssist, you must use the Storage Center Update Utility to update the Storage Center operating system before continuing.

Steps

- If no update is available, the **Storage Center Up to Date** page appears. Click **Next**.
- If an update is available, the current and available Storage Center versions are listed.
  1. Click **Install** to update to the latest version.
  2. If the update fails, click **Retry Update** to try to update again.
  3. When the update is complete, click **Next**.
- If the SupportAssist Data Collection and Storage Agreement was not accepted, the Storage Center cannot check for updates.
  - To proceed without checking for an update, click **Next**.
  - To accept the agreement and check for an update:

1. Click **Accept SupportAssist Data Collection and Storage Agreement** to review the agreement.
2. Select **By checking this box you accept the above terms**.
3. Click **Next**. The Storage Center attempts to contact the SupportAssist Update Server to check for updates.

- The **Setup SupportAssist Proxy Settings** dialog box appears if the Storage Center cannot connect to the SupportAssist Update Server. If the site does not have direct access to the Internet but uses a web proxy, configure the proxy settings:
  1. Select **Enabled**.
  2. Enter the proxy settings.
  3. Click **OK**. The Storage Center attempts to contact the SupportAssist Update Server to check for updates.

Configure the Storage Center Update Utility

The Storage Center Update Utility is used to update Storage Centers that are not connected to the SupportAssist update server. Configure Storage Center to use the Storage Center Update Utility if SupportAssist is not enabled.

Prerequisites

SupportAssist must be disabled.

About this task

If Storage Center is unable to check for an update, the **Unable to Check for Update** page appears.

Steps

1. Click **Use Update Utility server and setup configuration**.
   The **Configure Update Utility** dialog box appears.
2. In the **Update Utility Host or IP Address** field, type the host name or IP address of the Storage Center Update Utility.
3. In the **Update Utility Port** field, type the port of the Storage Center Update Utility.
   Storage Center checks for an update on the Storage Center Update Utility then applies the update if necessary.
   NOTE: If Storage Center failed to connect to the Update Utility, the **Edit Update Utility Configuration** dialog box appears.

Set Default Storage Profile (SCv2000 Series Controllers Only)

The storage profile determines the RAID types used when creating a volume.

Steps

1. Select a profile from the **Default Storage Profile** drop-down menu.
   NOTE: It is recommended to use the **Maximize Efficiency** storage profile if you plan to import data to this Storage Center.
2. (Optional) To allow a different storage profile to be selected when creating a volume, place a check next to **Allow Storage Profile selection when creating a volume**.
3. Click **Next**.

Complete Configuration and Perform Next Steps

The Storage Center is now configured. The Configuration Complete page provides links to a Storage Manager Client tutorial and wizards to perform the next setup tasks.

Steps

1. (Optional) Click one of the **Next Steps** to configure a localhost, configure a VMware host, or create a volume.
   When you have completed the step, you are returned to the **Configuration Complete** page. After you finish the Next Steps, continue to Step 2.
2. Click **Finish** to exit the wizard.

Related concepts

Creating Volumes on page 98

Related tasks

Create a Server from the localhost on page 147
Create a Server from a VMware vSphere Host on page 148
Create a Server from a VMware vCenter Host on page 148

Configure Embedded iSCSI Ports

Configure the embedded Ethernet ports on the Storage Center for use as iSCSI ports.

Prerequisites

The storage system must be one of the following:

- SCv2000
- SCv2020
- SCv2080
- SC4020

Steps

1. Configure the fault domain and ports (**embedded fault domain 1** or **Flex Port Domain 1**).

   NOTE: The Flex Port feature allows both Storage Center system management traffic and iSCSI traffic to use the same physical network ports. However, for environments where the Storage Center system management ports are mixed with network traffic from other devices, separate the iSCSI traffic from management traffic using VLANs.

   a. Enter the target IPv4 address, subnet mask, and gateway for the fault domain.
   b. Enter an IPv4 address for each port in the fault domain.

   NOTE: Make sure that all the IP addresses for the fault domain are in the same subnet.

2. Configure the fault domain and ports (**embedded fault domain 2** or **Flex Port Domain 2**).
   a. Enter the target IPv4 address, subnet mask, and gateway for the fault domain.
   b. Enter an IPv4 address for each port in the fault domain.

   NOTE: Make sure that all the IP addresses for the fault domain are in the same subnet.

3. Click **OK**.

Discover and Configure Uninitialized SCv3000 Series Storage Systems

Use the Discover and Configure Uninitialized Storage Centers wizard to find and configure new SCv3000 Series storage systems. The wizard helps set up a Storage Center to make it ready for volume creation.

NOTE: Make sure that you are running the latest version of the Dell Storage Manager Client.

Open the Discover and Configure Uninitialized Storage Centers Wizard From the Storage Manager Client Welcome Screen

Open the wizard directly from the welcome screen to discover and configure a Storage Center.

Prerequisites

- Client must be running on a system with a 64-bit operating system.

- The Storage Manager Client must be run using Windows Administrator privileges.

Steps

1. Open the Storage Manager Client welcome screen.
2. Click **Discover and Configure Uninitialized Storage Centers**.
   The **Discover and Configure Uninitialized Storage Centers** wizard opens.

Open the Discover and Configure Uninitialized Storage Centers Wizard from the Storage Manager Client

Open the wizard from the Storage Manager Client to discover and configure a Storage Center.

Prerequisites

- The Storage Manager Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run using Windows Administrator privileges.
- The client must be connected to a Storage Manager Data Collector.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, click **Storage Centers**.
3. In the **Summary** tab, click **Discover and Configure Uninitialized Storage Centers** .
   The **Discover and Configure Uninitialized Storage Centers** wizard opens.

Select a Storage Center to Initialize

The next page of the Discover and Configure Uninitialized Storage Centers wizard provides a list of uninitialized Storage Centers discovered by the wizard.

Steps

1. Select the Storage Center to initialize.
2. (Optional) To blink the indicator light for the selected Storage Center, click **Enable Storage Center Indicator**. You can use the indicator light to verify that you have selected the correct Storage Center.
3. Click **Next**.
4. If the Storage Center is partially configured, the Storage Center login pane is displayed. Type the management IPv4 address and the password for the Storage Center Admin user, then click **Next** to continue.

Deploy the Storage Center Using the Direct Connect Method

Use the direct connect method to manually deploy the Storage Center when it is not discoverable.

Steps

1. Use an Ethernet cable to connect the computer running the Storage Manager Client to the management port of the top controller.
2. Cable the bottom controller to the management network switch.
3. Click **Discover and Configure Uninitialized Storage Centers**. The **Discover and Configure Uninitialized Storage Centers** wizard opens.
4. Fill out the information on the initial configuration pages and stop when the **Confirm Configuration** page is displayed.
5. At this point, recable the management port of the top controller to the management network.
6. Connect the computer to the same subnet or VLAN as the Storage Center.
   a. Click **Next**.

b. If the cable is not properly connected or the host cannot access the controller, an **Error setting up connection** message is displayed. Correct the connection, and click **OK**.
c. If the deployment wizard is closed, click **Discover and Configure Uninitialized Storage Centers** to relaunch the deployment wizard.
d. Type **Admin** in the **User Name** field, type the password entered on the **Set Administrator Information** page in the **Password** field, and click **Next**.

Welcome Page

Use the Welcome page to verify the Storage Center information, and optionally change the name of the Storage Center.

Steps

1. Verify that the Service Tag and serial number match the Storage Center to set up.
2. (Optional) Type a name for the Storage Center.
3. Click **Next**.

Customer Installation Authorization

If the storage system is running Storage Center 7.3 or later, customer authorization is required.

Steps

1. Type the customer name and title.
2. Click **Next**.

Set System Information

The **Set System Information** page allows you to enter Storage Center and storage controller configuration information to use when connecting to the Storage Center using Storage Manager.

Steps

1. Type a descriptive name for the Storage Center in the **Storage Center Name** field.
2. If the storage system is running Storage Center 7.3 or later, select the network configuration option from the **Network Configuration Source** drop-down menu.
   - **DHCP IPv4** – Selected by default. IP addresses will be discovered and assigned.
   - **Static** – Enter static IP addresses manually.
3. If the network configuration source is set to Static:
   a. Type the system management IPv4 address for the Storage Center in the **Virtual Management IPv4 Address** field.
      The management IPv4 address is the IP address used to manage the Storage Center and is different than a storage controller IPv4 address.
   b. Type an IPv4 address for the management port of each storage controller.
      NOTE: The storage controller IPv4 addresses and management IPv4 address must be within the same subnet.
   c. Type the subnet mask of the management network in the **Subnet Mask** field.
   d. Type the gateway address of the management network in the **Gateway IPv4 Address** field.
   e. Type the domain name of the management network in the **Domain Name** field.
   f. Type the DNS server addresses of the management network in the **DNS Server** and **Secondary DNS Server** fields.
4. Click **Next**.

Set Administrator Information

The Set Administrator Information page allows you to set a new password and an email address for the Admin user.

Steps

1. Enter a new password for the default Storage Center administrator user in the **New Admin Password** and **Confirm Password** fields.
2. Enter the email address of the default Storage Center administrator user in the **Admin Email Address** field.
3. Click **Next**.
   - For a Fibre Channel or SAS storage system, the **Confirm Configuration** page appears.
   - For an iSCSI storage system, the **Configure iSCSI Fault Domains** page appears.

Confirm the Storage Center Configuration

Make sure that the configuration information shown on the Confirm Configuration page is correct before continuing. If you selected DHCP IPv4 as the network configuration source, the dynamically assigned IP addresses are displayed on this page.

Steps

1. Verify that the Storage Center settings are correct.
2. If the configuration information is correct, click **Apply Configuration**.

   If the configuration information is incorrect, click **Back** and provide the correct information.

   NOTE: After you click the **Apply Configuration** button, the configuration cannot be changed until after the Storage Center is fully deployed.

Deploy the Storage Center

The Storage Center sets up the controller using the information provided on the previous pages.

Steps

1. The Storage Center performs system setup tasks. The **Deploy Storage Center** page displays the status of these tasks.

   To learn more about the initialization process, click **More information about Initialization**.
   - If one or more of the system setup tasks fails, click **Troubleshoot Initialization Error** to learn how to resolve the issue.
   - If the Configuring Disks task fails, click **View Disks** to see the status of the drives detected by the Storage Center.
   - If any of the Storage Center front-end ports are down, the **Storage Center Front-End Ports Down** dialog box opens. Select the ports that are not connected to the storage network, then click **OK**.
2. When all of the Storage Center setup tasks are complete, click **Next**.

Enter Key Management Server Settings

Specify key management server settings, such as hostname and port.

Steps

1. In the **Hostname** field, type the host name or IP address of the key management server.
2. In the **Port** field, type the number of a port with open communication with the key management server.
3. In the **Timeout** field, type the amount of time in seconds after which the Storage Center should stop attempting to reconnect to the key management server after a failure.
4. To add alternate key management servers, type the host name or IP address of another key management server in the **Alternate Hostnames** area, and then click **Add**.
5. If the key management server requires a user name to validate the Storage Center certificate, enter the name in the **Username** field.

6. If the key management server requires a password to validate the Storage Center certificate, enter the password in the **Password** field.
7. Click **Browse** next to the **Root CA Certificate**. Navigate to the location of the root CA certificate on your computer and select it.
8. Click **Browse** next to the certificate fields for the controllers. Navigate to the location of the controller certificates on your computer and select them.
9. Click **Next**.

Create a Storage Type

Select the datapage size and redundancy level for the Storage Center.

Steps

1. Select a datapage size.
   - **Standard (2 MB Datapage Size)**: Default datapage size, this selection is appropriate for most applications.
   - **High Performance (512 KB Datapage Size)**: Appropriate for applications with high performance needs, or in environments in which snapshots are taken frequently under heavy I/O. Selecting this size increases overhead and reduces the maximum available space in the Storage Type. All-flash storage systems use 512 KB by default.
   - **High Density (4 MB Datapage Size)**: Appropriate for systems that use a large amount of disk space and take snapshots infrequently.
2. Select a redundancy type.
   - **Redundant**: Protects against the loss of any one drive (if single redundant) or any two drives (if dual redundant).
   - **Non-Redundant**: Uses RAID 0 in all classes, in all tiers. Data is striped but provides no redundancy. If one drive fails, all data is lost.

     NOTE: Non-Redundant is not recommended because data is not protected against a drive failure. Do not use non-redundant storage for a volume unless the data has been backed up elsewhere.
3. For Redundant Storage Types, you must select a redundancy level for each tier unless the drive type or size requires a specific redundancy level
   - **Single Redundant**: Single-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 (each drive is mirrored)
     - RAID 5-5 (striped across 5 drives)
     - RAID 5-9 (striped across 9 drives)
   - **Dual redundant**: Dual redundant is the recommended redundancy level for all tiers. It is enforced for 3 TB HDDs and higher and for 18 TB SSDs and higher. Dual-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 Dual-Mirror (data is written simultaneously to three separate drives)
     - RAID 6-6 (4 data segments, 2 parity segments for each stripe)
     - RAID 6-10 (8 data segments, 2 parity segments for each stripe.)
4. **Drive Addition** is selected by default. Leave this option selected.
5. Click **Next**.

Fault Tolerance

Set up Fibre Channel, iSCSI and SAS ports with redundant paths for fault tolerance.

Steps

1. Select the checkbox of each type of port you want to configure. You must select at least one type to continue.

   NOTE: If a port type is grayed out, no ports of that type have been detected.
2. Click **Next**.

Configure Fibre Channel Ports

For a Storage Center with Fibre Channel front-end ports, the Review Fault Domains page displays information about the fault domains that were created by the Storage Center.

Prerequisites

One port from each controller within the same fault domain must be cabled.

NOTE: If the Storage Center is not cabled correctly to create fault domains, the **Cable Ports** page opens and explains the issue. Click **Refresh** after cabling more ports.

Steps

1. Review the fault domains that have been created.
2. (Optional) Click **Copy to clipboard** to copy the fault domain information.
3. (Optional) Review the information on the **Zoning**, **Hardware**, and **Cabling Diagram** tabs.

   NOTE: The ports must already be zoned.

4. Click **Next**.

Configure iSCSI Ports

For a Storage Center with iSCSI front-end ports, verify iSCSI cabling and then enter network information for the fault domains and ports.

Prerequisites

One port from each controller within the same fault domain must be cabled.

Steps

1. Review the information on the **iSCSI - Cable Ports** page. If the Storage Center is not cabled correctly to create fault domains, fix the cabling and click **Refresh**
2. Click **Next**.
   The**Set IPv4 Addresses for iSCSI Fault Domain 1** page opens.
3. Enter network information for the fault domain and its ports.

   NOTE: Make sure that all the IP addresses for iSCSI Fault Domain 1 are in the same subnet.

4. Click **Next**.
5. On the **Set IPv4 Addresses for iSCSI Fault Domain 2** page, enter network information for the fault domain and its ports. Then click **Next**.

   NOTE: Make sure that all the IP addresses for iSCSI Fault Domain 2 are in the same subnet.

6. Click **Next**.
7. Review the fault domain information.
8. (Optional) Click **Copy to clipboard** to copy the fault domain information.
9. (Optional) Review the information on the **Hardware** and **Cabling Diagram** tabs.
10. Click **Next**.

Configure SAS Ports

For a Storage Center with SAS front-end ports, the Review Fault Domains page displays information about the fault domains that were created by the Storage Center.

Prerequisites

- One port from each controller within the same fault domain must be cabled.

- The ports for each fault domain must be cabled to the same server.

Steps

1. Review the information on the **SAS - Cable Ports** page. If the Storage Center is not cabled correctly to create fault domains, fix the cabling and click **Refresh**.
2. Click **Next**.
   The **SAS – Review Fault Domains** page opens.
3. Review the fault domains that have been created.
4. (Optional) Click **Copy to clipboard** to copy the fault domain information.
5. (Optional) Review the information on the **Hardware** and **Cabling Diagram** tabs.
6. Click **Next**.

Inherit Settings

Use the Inherit Settings page to copy settings from a Storage Center that is already configured.

Prerequisites

You must be connected through a Data Collector.

Steps

1. Select the Storage Center from which to copy settings.
2. Place a check next to each setting that you want to inherit, or click **Select All** to inherit all settings.
3. Click **Next**.
   If you chose to inherit time and SMTP settings from another Storage Center, the **Time Settings** and **SMTP Server Settings** pages are skipped in the wizard.

Configure Time Settings

Configure an NTP server to set the time automatically, or set the time and date manually.

Steps

1. From the **Region** and **Time Zone** drop-down menus, select the region and time zone used to set the time.
2. Select **Use NTP Server** and type the host name or IPv4 address of the NTP server, or select **Set Current Time** and set the time and date manually.
3. Click **Next**.

Configure SMTP Server Settings

If you have an SMTP server, configure the SMTP email settings to receive information from the Storage Center about errors, warnings, and events.

Steps

1. By default, the **Enable SMTP Email** checkbox is selected and enabled. If you do not have an SMTP server you can disable SMTP email by clearing the **Enable SMTP Email** checkbox.
2. Alternatively, if you have an SMTP server, configure the SMTP server settings.
   a. In the **Recipient Email Address** field, enter the email address where the information will be sent.
   b. In the **SMTP Mail Server** field, enter the IP address or fully qualified domain name of the SMTP mail server.
   c. (Optional) In the **Backup SMTP Mail Server** field, enter the IP address or fully qualified domain name of a backup SMTP mail server and click **OK**.
   d. Click **Test Server** to verify connectivity to the SMTP server.
   e. If the SMTP server requires emails to contain a MAIL FROM address, specify an email address in the **Sender Email Address** field.

f. (Optional) In the **Common Subject Line** field, enter a subject line to use for all emails sent by the Storage Center.

3. Click **Next**.

Set Up SupportAssist

If the storage system is running Storage Center 7.3 or later, the **Set Up SupportAssist** page opens.

About this task

Use the **Set Up SupportAssist** page to enable SupportAssist.

Steps

1. To allow SupportAssist to collect diagnostic data and send this information to technical support, select the **Receive proactive notifications, notices, and other predictive support** checkbox.
2. Click **Next**.
   If you chose to clear the **Receive proactive notifications, notices, and other predictive support** checkbox and click **Next**, a **SupportAssist Recommended** dialog box opens.
   - To return to the **Set Up SupportAssist** page, click **No**.
   - To disable SupportAssist and proceed to the **Update Storage Center** page, click **Yes**.

Accept the SupportAssist Collection Agreement

Use the Accept SupportAssist Collection Agreement page to accept to the terms of the agreement and enable SupportAssist.

Steps

1. To allow SupportAssist to collect diagnostic data and send this information to technical support, select the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox.
2. Click **Next**.

   NOTE: If you chose to clear the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox, a **SupportAssist Recommended** dialog box opens.
   - To return to the **Accept SupportAssist Collection Agreement** page, click **No**.
   - To opt out of SupportAssist, click **Yes**.

Provide Contact Information

Specify contact information for technical support to use when sending support-related communications from SupportAssist.

Steps

1. Specify the contact information.
2. (Storage Center 7.2 or earlier) To receive SupportAssist email messages, select the **Send me emails from SupportAssist when issues arise, including hardware failure notifications** check box.
3. Select the preferred contact method, language, and available times.
4. (Storage Center 7.2 or earlier) Type a shipping address where replacement Storage Center components can be sent.
5. (Storage Center 7.2 or earlier) Click **Finish**.
6. (Storage Center 7.3 or later) Click **Next**.

Provide Site Contact Information

If the storage system is running Storage Center 7.3 or later, specify the site contact information.

Steps

1. Select the **Enable Onsite Address** checkbox.

2. Type a shipping address where replacement Storage Center components can be sent.
3. Click **Next**.
   The **Confirm Enable SupportAssist** dialog box opens.
4. Click **Yes**.

Validate the SupportAssist Connection

If the storage system is running Storage Center 7.3 or later, the **Validate SupportAssist Connection** page opens.

About this task

The **Validate SupportAssist Connection** page displays a summary of the SupportAssist contact information and confirms that the Storage Center is connected to SupportAssist.

Steps

- To complete the SupportAssist setup, click **Finish**.

Update Storage Center

The Storage Center attempts to contact the SupportAssist Update Server to check for updates. If you are not using SupportAssist, you must use the Storage Center Update Utility to update the Storage Center operating system before continuing.

Steps

- If no update is available, the **Storage Center Up to Date** page appears. Click **Next**.
- If an update is available, the current and available Storage Center versions are listed.
  1. Click **Install** to update to the latest version.
  2. If the update fails, click **Retry Update** to try to update again.
  3. When the update is complete, click **Next**.
- If the SupportAssist Data Collection and Storage Agreement was not accepted, the Storage Center cannot check for updates.
  - To proceed without checking for an update, click **Next**.
  - To accept the agreement and check for an update:
  1. Click **Accept SupportAssist Data Collection and Storage Agreement** to review the agreement.
  2. Select **By checking this box you accept the above terms**.
  3. Click **Next**. The Storage Center attempts to contact the SupportAssist Update Server to check for updates.
- The **Setup SupportAssist Proxy Settings** dialog box appears if the Storage Center cannot connect to the SupportAssist Update Server. If the site does not have direct access to the Internet but uses a web proxy, configure the proxy settings:
  1. Select **Enabled**.
  2. Enter the proxy settings.
  3. Click **OK**. The Storage Center attempts to contact the SupportAssist Update Server to check for updates.

Complete Configuration and Perform Next Steps

The Storage Center is now configured. The Configuration Complete page provides links to a Storage Manager Client tutorial and wizards to perform the next setup tasks.

Steps

1. (Optional) Click one of the **Next Steps** to configure a localhost, configure a VMware host, or create a volume.
   When you have completed the step, you are returned to the **Configuration Complete** page. After you finish the Next Steps, continue to Step 2.
2. Click **Finish** to exit the wizard.

Related concepts

Creating Volumes on page 98

Related tasks

Create a Server from the localhost on page 147
Create a Server from a VMware vSphere Host on page 148
Create a Server from a VMware vCenter Host on page 148

Discover and Configure Uninitialized SC5020 and SC7020 Storage Systems

Use the Discover and Configure Uninitialized Storage Centers wizard to find and configure new SC5020, SC5020F, SC7020, or SC7020F storage systems. The wizard helps set up a Storage Center to make it ready for volume creation.

NOTE: Make sure that you are running the latest version of the Dell Storage Manager Client.

Open the Discover and Configure Uninitialized Storage Centers Wizard From the Storage Manager Client Welcome Screen

Open the wizard directly from the welcome screen to discover and configure a Storage Center.

Prerequisites

- Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run using Windows Administrator privileges.

Steps

1. Open the Storage Manager Client welcome screen.
2. Click **Discover and Configure Uninitialized Storage Centers**.
   The **Discover and Configure Uninitialized Storage Centers** wizard opens.

Open the Discover and Configure Uninitialized Storage Centers Wizard from the Storage Manager Client

Open the wizard from the Storage Manager Client to discover and configure a Storage Center.

Prerequisites

- The Storage Manager Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run using Windows Administrator privileges.
- The client must be connected to a Storage Manager Data Collector.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, click **Storage Centers**.
3. In the **Summary** tab, click **Discover and Configure Uninitialized Storage Centers** .
   The **Discover and Configure Uninitialized Storage Centers** wizard opens.

Introduction to Storage Center Initial Configuration

The Storage Center Initial Configuration page provides a list of prerequisite actions that must be performed and information that is required to initialize a Storage Center.

Prerequisites

- The host server, on which the Storage Manager software is installed, must be on the same subnet or VLAN as the Storage Center.
- Layer 2 multicast must be allowed on the network.
- Make sure that IGMP snooping is disabled on the switch ports connected to the Storage Center.

Steps

1. Make sure the prerequisites that are listed on the Storage Center Initial Configuration page are met.
2. Make sure the information that is required to initialize the Storage Center is gathered.
3. Click **Next**. The **Select a Storage Center to Initialize** page is displayed and it lists the uninitialized Storage Centers discovered by the wizard.

   NOTE: If the wizard does not discover the Storage Center that you want to initialize, perform the following actions:
   - Make sure that the Storage Center hardware is physically attached to all necessary networks.
   - Temporarily disable any firewall on the host server that is running the Storage Manager software.
   - Click **Rediscover** to rediscover the uninitialized Storage Centers.
   - Follow the steps in *Deploy the Storage Center Using the Direct Connect Method*.

Select a Storage Center to Initialize

The next page of the Discover and Configure Uninitialized Storage Centers wizard provides a list of uninitialized Storage Centers discovered by the wizard.

Steps

1. Select the Storage Center to initialize.
2. (Optional) To blink the indicator light for the selected Storage Center, click **Enable Storage Center Indicator**. You can use the indicator light to verify that you have selected the correct Storage Center.
3. Click **Next**.
4. If the Storage Center is partially configured, the Storage Center login pane is displayed. Type the management IPv4 address and the password for the Storage Center Admin user, then click **Next** to continue.

Deploy the Storage Center Using the Direct Connect Method

Use the direct connect method to manually deploy the Storage Center when it is not discoverable.

Steps

1. Use an Ethernet cable to connect the computer running the Storage Manager Client to the management port of the top controller.
2. Cable the bottom controller to the management network switch.
3. Click **Discover and Configure Uninitialized Storage Centers**. The **Discover and Configure Uninitialized Storage Centers** wizard opens.
4. Fill out the information on the initial configuration pages and stop when the **Confirm Configuration** page is displayed.
5. At this point, recable the management port of the top controller to the management network.
6. Connect the computer to the same subnet or VLAN as the Storage Center.
   a. Click **Next**.
   b. If the cable is not properly connected or the host cannot access the controller, an **Error setting up connection** message is displayed. Correct the connection, and click **OK**.

c. If the deployment wizard is closed, click **Discover and Configure Uninitialized Storage Centers** to relaunch the deployment wizard.
d. Type **Admin** in the **User Name** field, type the password entered on the **Set Administrator Information** page in the **Password** field, and click **Next**.

Welcome Page

Use the Welcome page to verify the Storage Center information, and optionally change the name of the Storage Center.

Steps

1. Verify that the Service Tag and serial number match the Storage Center to set up.
2. (Optional) Type a name for the Storage Center.
3. Click **Next**.

Customer Installation Authorization

If the storage system is running Storage Center 7.3 or later, customer authorization is required.

Steps

1. Type the customer name and title.
2. Click **Next**.

Set System Information

The **Set System Information** page allows you to enter Storage Center and storage controller configuration information to use when connecting to the Storage Center using Storage Manager.

Steps

1. Type a descriptive name for the Storage Center in the **Storage Center Name** field.
2. If the storage system is running Storage Center 7.3 or later, select the network configuration option from the **Network Configuration Source** drop-down menu.
   - **DHCP IPv4** – Selected by default. IP addresses will be discovered and assigned.
   - **Static** – Enter static IP addresses manually.
3. If the network configuration source is set to Static:
   a. Type the system management IPv4 address for the Storage Center in the **Virtual Management IPv4 Address** field.
   The management IPv4 address is the IP address used to manage the Storage Center and is different than a storage controller IPv4 address.
   b. Type an IPv4 address for the management port of each storage controller.
   NOTE: The storage controller IPv4 addresses and management IPv4 address must be within the same subnet.
   c. Type the subnet mask of the management network in the **Subnet Mask** field.
   d. Type the gateway address of the management network in the **Gateway IPv4 Address** field.
   e. Type the domain name of the management network in the **Domain Name** field.
   f. Type the DNS server addresses of the management network in the **DNS Server** and **Secondary DNS Server** fields.
4. Click **Next**.

Set Administrator Information

The Set Administrator Information page allows you to set a new password and an email address for the Admin user.

Steps

1. Enter a new password for the default Storage Center administrator user in the **New Admin Password** and **Confirm Password** fields.
2. Enter the email address of the default Storage Center administrator user in the **Admin Email Address** field.
3. Click **Next**.
   - For a Fibre Channel or SAS storage system, the **Confirm Configuration** page appears.
   - For an iSCSI storage system, the **Configure iSCSI Fault Domains** page appears.

Confirm the Storage Center Configuration

Make sure that the configuration information shown on the Confirm Configuration page is correct before continuing. If you selected DHCP IPv4 as the network configuration source, the dynamically assigned IP addresses are displayed on this page.

Steps

1. Verify that the Storage Center settings are correct.
2. If the configuration information is correct, click **Apply Configuration**.

   If the configuration information is incorrect, click **Back** and provide the correct information.

   NOTE: After you click the **Apply Configuration** button, the configuration cannot be changed until after the Storage Center is fully deployed.

Deploy the Storage Center

The Storage Center sets up the controller using the information provided on the previous pages.

Steps

1. The Storage Center performs system setup tasks. The **Deploy Storage Center** page displays the status of these tasks.

   To learn more about the initialization process, click **More information about Initialization**.
   - If one or more of the system setup tasks fails, click **Troubleshoot Initialization Error** to learn how to resolve the issue.
   - If the Configuring Disks task fails, click **View Disks** to see the status of the drives detected by the Storage Center.
   - If any of the Storage Center front-end ports are down, the **Storage Center Front-End Ports Down** dialog box opens. Select the ports that are not connected to the storage network, then click **OK**.
2. When all of the Storage Center setup tasks are complete, click **Next**.

Enter Key Management Server Settings

Specify key management server settings, such as hostname and port.

Steps

1. In the **Hostname** field, type the host name or IP address of the key management server.
2. In the **Port** field, type the number of a port with open communication with the key management server.
3. In the **Timeout** field, type the amount of time in seconds after which the Storage Center should stop attempting to reconnect to the key management server after a failure.
4. To add alternate key management servers, type the host name or IP address of another key management server in the **Alternate Hostnames** area, and then click **Add**.
5. If the key management server requires a user name to validate the Storage Center certificate, enter the name in the **Username** field.

6. If the key management server requires a password to validate the Storage Center certificate, enter the password in the **Password** field.
7. Click **Browse** next to the **Root CA Certificate**. Navigate to the location of the root CA certificate on your computer and select it.
8. Click **Browse** next to the certificate fields for the controllers. Navigate to the location of the controller certificates on your computer and select them.
9. Click **Next**.

Create a Storage Type

Select the datapage size and redundancy level for the Storage Center.

Steps

1. Select a datapage size.
   - **Standard (2 MB Datapage Size)**: Default datapage size, this selection is appropriate for most applications.
   - **High Performance (512 KB Datapage Size)**: Appropriate for applications with high performance needs, or in environments in which snapshots are taken frequently under heavy I/O. Selecting this size increases overhead and reduces the maximum available space in the Storage Type. All-flash storage systems use 512 KB by default.
   - **High Density (4 MB Datapage Size)**: Appropriate for systems that use a large amount of disk space and take snapshots infrequently.
2. Select a redundancy type.
   - **Redundant**: Protects against the loss of any one drive (if single redundant) or any two drives (if dual redundant).
   - **Non-Redundant**: Uses RAID 0 in all classes, in all tiers. Data is striped but provides no redundancy. If one drive fails, all data is lost.

     NOTE: Non-Redundant is not recommended because data is not protected against a drive failure. Do not use non-redundant storage for a volume unless the data has been backed up elsewhere.
3. For Redundant Storage Types, you must select a redundancy level for each tier unless the drive type or size requires a specific redundancy level
   - **Single Redundant**: Single-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 (each drive is mirrored)
     - RAID 5-5 (striped across 5 drives)
     - RAID 5-9 (striped across 9 drives)
   - **Dual redundant**: Dual redundant is the recommended redundancy level for all tiers. It is enforced for 3 TB HDDs and higher and for 18 TB SSDs and higher. Dual-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 Dual-Mirror (data is written simultaneously to three separate drives)
     - RAID 6-6 (4 data segments, 2 parity segments for each stripe)
     - RAID 6-10 (8 data segments, 2 parity segments for each stripe.)
4. **Drive Addition** is selected by default. Leave this option selected.
5. Click **Next**.

Fault Tolerance

Set up Fibre Channel, iSCSI and SAS ports with redundant paths for fault tolerance.

Steps

1. Select the checkbox of each type of port you want to configure. You must select at least one type to continue.

   NOTE: If a port type is grayed out, no ports of that type have been detected.
2. Click **Next**.

Configure Fibre Channel Ports

Create a Fibre Channel fault domain to group FC ports for failover purposes.

Steps

1. On the first **Configure Fibre Channel Fault Tolerance** page, select a transport mode: **Virtual Port** or **Legacy**.
2. Select the method for creating fault domains:
   - **Generate Fault Domain Configuration** – One of the following fault domains is created, depending on system configuration and mode selected:

Transport Mode	One Controller	Two Controllers
Virtual Port	Two controller ports	Two controller ports, one on each controller
Legacy	One controller port	Four controller ports, two on each controller

   - **Specify Number of Fault Domains** – Set the number of fault domains to create.
3. Click **Next**.

   NOTE: If you selected **Generate Fault Domain Configuration**, proceed to step 5.

4. If you selected **Specify Number of Fault Domains**, configure each fault domain.
   a. In the **Name** field, type a name for the fault domain.
   b. (Optional) In the **Notes** field, type notes for the fault domain.
   c. In the **Ports** table, select the Fibre Channel ports to add to the fault domain. All FC ports in the fault domain should be connected to the same FC fabric.
   d. Click **Next**. If you are configuring more than one fault domain, repeat these steps for each domain.
5. On the final **Configure Fibre Channel Fault Tolerance** page, review the fault domain setup.
6. (Optional) To change the fault domain setup, select from the following options:
   - Click **Create Fault Domain** to create a new fault domain.
   - Click **Edit Fault Domain** to edit the current fault domain.
   - Click **Remove** to delete a fault domain.
7. Click **Next**.
   - If you are setting up iSCSI fault domains, the **Configure iSCSI Fault Domain** page opens.
   - If you are setting up SAS back-end ports but not iSCSI fault domains, the **Configure Back-End Ports** page opens.
   - If you are not setting up iSCSI fault domains or SAS back-end ports, the **Inherit Settings** or **Time Settings** page opens.

Configure iSCSI Ports

Create an iSCSI fault domain to group ports for failover purposes.

Steps

1. On the first **Configure iSCSI Fault Tolerance** page, select the number of fault domains to create, and then click **Next**.
2. On the next **Configure iSCSI Fault Tolerance** page, configure the first fault domain:
   a. In the **Name** field, type a name for the fault domain.
   b. (Optional) In the **Notes** field, type notes for the fault domain.
   c. In the **Target IPv4 Address** field, type an IP address to assign to the iSCSI control port.
   d. In the **Subnet Mask** field, type the subnet mask for the IP address.
   e. In the **Gateway IPv4 Address** field, type the IP address for the iSCSI network default gateway.
   f. In the **Ports** table, select the iSCSI ports to add to the fault domain. All iSCSI ports in the fault domain should be connected to the same Ethernet network.
   g. Click **Next**. If you are configuring more than one fault domain, repeat these steps for each fault domain.
3. On the final **Configure iSCSI Fault Tolerance** page, review the fault domain setup.
4. (Optional) To change the fault domain setup, select from the following options:
   - Click **Create Fault Domain** to create a new fault domain.
   - Click **Edit Fault Domain** to edit the current fault domain.
   - Click **Remove** to delete a fault domain.

5. Click **Next**.
   - If you are setting up SAS back-end ports, the **Configure Back-End Ports** page opens.
   - If you are not setting up SAS back-end ports, the **Inherit Settings** or **Time Settings** page opens.

Configure SAS Ports

For a Storage Center with SAS front-end ports, the Review Fault Domains page displays information about the fault domains that were created by the Storage Center.

Prerequisites

- One port from each controller within the same fault domain must be cabled.
- The ports for each fault domain must be cabled to the same server.

Steps

1. Review the information on the **SAS - Cable Ports** page. If the Storage Center is not cabled correctly to create fault domains, fix the cabling and click **Refresh**.
2. Click **Next**.
   The **SAS – Review Fault Domains** page opens.
3. Review the fault domains that have been created.
4. (Optional) Click **Copy to clipboard** to copy the fault domain information.
5. (Optional) Review the information on the **Hardware** and **Cabling Diagram** tabs.
6. Click **Next**.

Inherit Settings

Use the Inherit Settings page to copy settings from a Storage Center that is already configured.

Prerequisites

You must be connected through a Data Collector.

Steps

1. Select the Storage Center from which to copy settings.
2. Place a check next to each setting that you want to inherit, or click **Select All** to inherit all settings.
3. Click **Next**.
   If you chose to inherit time and SMTP settings from another Storage Center, the **Time Settings** and **SMTP Server Settings** pages are skipped in the wizard.

Configure Time Settings

Configure an NTP server to set the time automatically, or set the time and date manually.

Steps

1. From the **Region** and **Time Zone** drop-down menus, select the region and time zone used to set the time.
2. Select **Use NTP Server** and type the host name or IPv4 address of the NTP server, or select **Set Current Time** and set the time and date manually.
3. Click **Next**.

Configure SMTP Server Settings

If you have an SMTP server, configure the SMTP email settings to receive information from the Storage Center about errors, warnings, and events.

Steps

1. By default, the **Enable SMTP Email** checkbox is selected and enabled. If you do not have an SMTP server you can disable SMTP email by clearing the **Enable SMTP Email** checkbox.
2. Alternatively, if you have an SMTP server, configure the SMTP server settings.
   a. In the **Recipient Email Address** field, enter the email address where the information will be sent.
   b. In the **SMTP Mail Server** field, enter the IP address or fully qualified domain name of the SMTP mail server.
   c. (Optional) In the **Backup SMTP Mail Server** field, enter the IP address or fully qualified domain name of a backup SMTP mail server and click **OK**.
   d. Click **Test Server** to verify connectivity to the SMTP server.
   e. If the SMTP server requires emails to contain a MAIL FROM address, specify an email address in the **Sender Email Address** field.
   f. (Optional) In the **Common Subject Line** field, enter a subject line to use for all emails sent by the Storage Center.
3. Click **Next**.

Set Up SupportAssist

If the storage system is running Storage Center 7.3 or later, the **Set Up SupportAssist** page opens.

About this task

Use the **Set Up SupportAssist** page to enable SupportAssist.

Steps

1. To allow SupportAssist to collect diagnostic data and send this information to technical support, select the **Receive proactive notifications, notices, and other predictive support** checkbox.
2. Click **Next**.
   If you chose to clear the **Receive proactive notifications, notices, and other predictive support** checkbox and click **Next**, a **SupportAssist Recommended** dialog box opens.
   - To return to the **Set Up SupportAssist** page, click **No**.
   - To disable SupportAssist and proceed to the **Update Storage Center** page, click **Yes**.

Accept the SupportAssist Collection Agreement

Use the Accept SupportAssist Collection Agreement page to accept to the terms of the agreement and enable SupportAssist.

Steps

1. To allow SupportAssist to collect diagnostic data and send this information to technical support, select the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox.
2. Click **Next**.

   NOTE: If you chose to clear the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox, a **SupportAssist Recommended** dialog box opens.
   - To return to the **Accept SupportAssist Collection Agreement** page, click **No**.
   - To opt out of SupportAssist, click **Yes**.

Provide Contact Information

Specify contact information for technical support to use when sending support-related communications from SupportAssist.

Steps

1. Specify the contact information.
2. (Storage Center 7.2 or earlier) To receive SupportAssist email messages, select the **Send me emails from SupportAssist when issues arise, including hardware failure notifications** check box.
3. Select the preferred contact method, language, and available times.
4. (Storage Center 7.2 or earlier) Type a shipping address where replacement Storage Center components can be sent.
5. (Storage Center 7.2 or earlier) Click **Finish**.
6. (Storage Center 7.3 or later) Click **Next**.

Provide Site Contact Information

If the storage system is running Storage Center 7.3 or later, specify the site contact information.

Steps

1. Select the **Enable Onsite Address** checkbox.
2. Type a shipping address where replacement Storage Center components can be sent.
3. Click **Next**.
   The **Confirm Enable SupportAssist** dialog box opens.
4. Click **Yes**.

Validate the SupportAssist Connection

If the storage system is running Storage Center 7.3 or later, the **Validate SupportAssist Connection** page opens.

About this task

The **Validate SupportAssist Connection** page displays a summary of the SupportAssist contact information and confirms that the Storage Center is connected to SupportAssist.

Steps

- To complete the SupportAssist setup, click **Finish**.

Complete Configuration and Perform Next Steps

The Storage Center is now configured. The Configuration Complete page provides links to a Storage Manager Client tutorial and wizards to perform the next setup tasks.

Steps

1. (Optional) Click one of the **Next Steps** to configure a localhost, configure a VMware host, or create a volume.
   When you have completed the step, you are returned to the **Configuration Complete** page. After you finish the Next Steps, continue to Step 2.
2. Click **Finish** to exit the wizard.

Related concepts

Creating Volumes on page 98

Related tasks

Create a Server from the localhost on page 147

Create a Server from a VMware vSphere Host on page 148
Create a Server from a VMware vCenter Host on page 148

Configuring SC4020 and SC8000 Storage Centers

Use the Configure Storage Center wizard to set up a new SC4020 or SC8000 Storage Center. The wizard helps configure the Storage Center to make it ready for volume creation.

Prerequisites

- The Storage Manager Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run by a Storage Manager Client user with the Administrator privilege.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select **Dell Storage** or **Storage Centers**.
3. In the **Summary** tab, click **Add Storage Center**. The **Add Storage Center** wizard opens.
4. Select **Add a new Storage Center to the Data Collector**, then click **Next**.
5. Specify Storage Center login information.
   - **Hostname or IP Address** – Type the host name or IP address of a Storage Center controller. For a dual-controller Storage Center, enter the IP address or host name of the management controller.
   - **User Name** and **Password** – Type the user name and password for a Storage Center user.
     NOTE: If you specify a Storage Center user with the Reporter or Volume Manager privilege, access to the Storage Center from Storage Manager is restricted based on the privilege and user groups that were assigned to the Storage Center user.
   - **Folder** – Select the parent folder for the Storage Center.
6. Click **Finish**. The **Change Password** dialog box opens.
7. a. In the **User Name** field, type the Storage Center user name.
   b. In the **Password** field, type the Storage Center user password.
   c. In the **Host/IP** field, type the host name or IP address of the Storage Center.
   d. If you changed the web server port during installation, type the updated port in the **Web Server Port** field.
8. Click **Log In**. The Client connects to the Storage Center and indicates that initial configuration is necessary.
9. Type a new password in the **New Password** and **Confirm Password** fields.
10. Click **OK**. The **Configure Storage Center** wizard opens.
11. Make sure that you have the required information that is listed on the first page of the wizard. This information is needed to configure the Storage Center.
12. Click **Next**. The **Submit Storage Center License** page opens.

Welcome Page

Use the Welcome page to verify the Storage Center information, and optionally change the name of the Storage Center.

Steps

1. Verify that the Service Tag and serial number match the Storage Center to set up.
2. (Optional) Type a name for the Storage Center.
3. Click **Next**.

Submit the Storage Center License

Use the Submit Storage Center License page to type the name and title of the approving customer and to select the Storage Center license file.

Steps

1. Click **Browse**.
   The **Select License File** window opens.
2. Browse to the location of the license file, select the file, and then click **Select**.
3. Verify the approving customer information and license file path, then click **Next**.
   The **Create Disk Folder** page opens.

Create a Disk Folder

Create a disk folder to manage unassigned disks.

Steps

1. Type a name for the disk folder.
2. (Optional) To create a secure disk folder, select the **Create as a Secure Data Folder** checkbox.

   NOTE: This option is available only if all drives support Secure Data.

3. Click **Change** to open a dialog box for selecting the disks to assign to the folder.
4. Click **Next**.
   The **Create Storage Type** page opens.
5. Select the redundancy level from the drop-down menu for each disk tier.
6. (Optional) Select the datapage size from the **Datapage Size** drop-down menu.
7. Click **Next**.
   The **Add Controller** page opens.

Add a Controller (Configure Storage Center Wizard)

Configure the second controller for systems with two controllers. The Configure Storage Center Wizard automatically adds the second controller for SC4020 Storage Centers with two controllers. You must manually configure the SC8000 Storage Center.

About this task

- If the system has only one controller, click **Next** to proceed to the **Set System Information** page.
- For SC4020 Storage Centers with two controllers, click **Next** to add the second controller automatically.
- For SC8000 Storage Centers with two controllers, proceed with the following steps.

Steps

1. Type a serial number for the second controller.
2. Type the IPv4 address and eth1 IPv4 address of the second controller.
3. If the first controller has an IPv6 address set and the Storage Center supports IPv6, type the IPv6 address and IPv6 subnet prefix of the second controller.
4. Click **Next**. The **Set System Information** page opens.

Set System Information

The **Set System Information** page allows you to enter Storage Center and storage controller configuration information to use when connecting to the Storage Center using Storage Manager.

Steps

1. Type a descriptive name for the Storage Center in the **Storage Center Name** field.
2. If the storage system is running Storage Center 7.3 or later, select the network configuration option from the **Network Configuration Source** drop-down menu.
   - **DHCP IPv4** – Selected by default. IP addresses will be discovered and assigned.
   - **Static** – Enter static IP addresses manually.
3. If the network configuration source is set to Static:
   a. Type the system management IPv4 address for the Storage Center in the **Virtual Management IPv4 Address** field.
      The management IPv4 address is the IP address used to manage the Storage Center and is different than a storage controller IPv4 address.
   b. Type an IPv4 address for the management port of each storage controller.
      NOTE: The storage controller IPv4 addresses and management IPv4 address must be within the same subnet.
   c. Type the subnet mask of the management network in the **Subnet Mask** field.
   d. Type the gateway address of the management network in the **Gateway IPv4 Address** field.
   e. Type the domain name of the management network in the **Domain Name** field.
   f. Type the DNS server addresses of the management network in the **DNS Server** and **Secondary DNS Server** fields.
4. Click **Next**.

Enter Key Management Server Settings

Specify key management server settings, such as hostname and port.

Steps

1. In the **Hostname** field, type the host name or IP address of the key management server.
2. In the **Port** field, type the number of a port with open communication with the key management server.
3. In the **Timeout** field, type the amount of time in seconds after which the Storage Center should stop attempting to reconnect to the key management server after a failure.
4. To add alternate key management servers, type the host name or IP address of another key management server in the **Alternate Hostnames** area, and then click **Add**.
5. If the key management server requires a user name to validate the Storage Center certificate, enter the name in the **Username** field.
6. If the key management server requires a password to validate the Storage Center certificate, enter the password in the **Password** field.
7. Click **Browse** next to the **Root CA Certificate**. Navigate to the location of the root CA certificate on your computer and select it.
8. Click **Browse** next to the certificate fields for the controllers. Navigate to the location of the controller certificates on your computer and select them.
9. Click **Next**.

Configure Ports

Use the Configure Fault Tolerance pages to configure the front-end and back-end ports of the system.

Steps

1. Select **Configure Fault Domains** next to **Fibre Channel** or **iSCSI** to set up fault domains for those ports. If the system has both Fibre Channel and iSCSI ports, select **Configure Fault Domains** next to both port types.
2. Select **Configure Back-End Ports** next to **SAS (Back-End)** to set up SAS ports to connect to the enclosures.

3. Select **Configure Fault Domains** next to **SAS (Front-End)** to set up front-end SAS ports to connect directly to hosts.
4. Click **Next**.

Configure Fibre Channel Ports

Create a Fibre Channel fault domain to group FC ports for failover purposes.

Steps

1. On the first **Configure Fibre Channel Fault Tolerance** page, select a transport mode: **Virtual Port** or **Legacy**.
2. Select the method for creating fault domains:
   - **Generate Fault Domain Configuration** – One of the following fault domains is created, depending on system configuration and mode selected:

Transport Mode	One Controller	Two Controllers
Virtual Port	Two controller ports	Two controller ports, one on each controller
Legacy	One controller port	Four controller ports, two on each controller

   - **Specify Number of Fault Domains** – Set the number of fault domains to create.
3. Click **Next**.

   NOTE: If you selected **Generate Fault Domain Configuration**, proceed to step 5.

4. If you selected **Specify Number of Fault Domains**, configure each fault domain.
   a. In the **Name** field, type a name for the fault domain.
   b. (Optional) In the **Notes** field, type notes for the fault domain.
   c. In the **Ports** table, select the Fibre Channel ports to add to the fault domain. All FC ports in the fault domain should be connected to the same FC fabric.
   d. Click **Next**. If you are configuring more than one fault domain, repeat these steps for each domain.
5. On the final **Configure Fibre Channel Fault Tolerance** page, review the fault domain setup.
6. (Optional) To change the fault domain setup, select from the following options:
   - Click **Create Fault Domain** to create a new fault domain.
   - Click **Edit Fault Domain** to edit the current fault domain.
   - Click **Remove** to delete a fault domain.
7. Click **Next**.
   - If you are setting up iSCSI fault domains, the **Configure iSCSI Fault Domain** page opens.
   - If you are setting up SAS back-end ports but not iSCSI fault domains, the **Configure Back-End Ports** page opens.
   - If you are not setting up iSCSI fault domains or SAS back-end ports, the **Inherit Settings** or **Time Settings** page opens.

Configure iSCSI Ports

Create an iSCSI fault domain to group ports for failover purposes.

Steps

1. On the first **Configure iSCSI Fault Tolerance** page, select the number of fault domains to create, and then click **Next**.
2. On the next **Configure iSCSI Fault Tolerance** page, configure the first fault domain:
   a. In the **Name** field, type a name for the fault domain.
   b. (Optional) In the **Notes** field, type notes for the fault domain.
   c. In the **Target IPv4 Address** field, type an IP address to assign to the iSCSI control port.
   d. In the **Subnet Mask** field, type the subnet mask for the IP address.
   e. In the **Gateway IPv4 Address** field, type the IP address for the iSCSI network default gateway.
   f. In the **Ports** table, select the iSCSI ports to add to the fault domain. All iSCSI ports in the fault domain should be connected to the same Ethernet network.
   g. Click **Next**. If you are configuring more than one fault domain, repeat these steps for each fault domain.
3. On the final **Configure iSCSI Fault Tolerance** page, review the fault domain setup.
4. (Optional) To change the fault domain setup, select from the following options:

- Click **Create Fault Domain** to create a new fault domain.
- Click **Edit Fault Domain** to edit the current fault domain.
- Click **Remove** to delete a fault domain.

5. Click **Next**.
   - If you are setting up SAS back-end ports, the **Configure Back-End Ports** page opens.
   - If you are not setting up SAS back-end ports, the **Inherit Settings** or **Time Settings** page opens.

Configure SAS Fault Domains

Specify the number of fault domains to create for front-end SAS ports on SC4020 controllers.

Steps

1. On the **Configure Front End SAS Fault Tolerance** page, select the number of fault domains to be created.
2. Click **Next**. Storage Manager selects un-used, front-end SAS ports and groups them into the preferred port pairs for the fault domains.
   The **Configure Front End SAS Fault Tolerance** page opens.
3. Review the information on the page and verify that the fault domains contain only one port from each controller.
4. Click **Next**.
   Storage Center creates the fault domains.

Configure Back-End Ports (Configure Storage Center Wizard)

Select SAS ports to configure for connecting to enclosures.

Steps

1. On the **Configure Back-End Ports** page, select the SAS ports to configure.
2. Click **Next**. The **Inherit Settings** or **Time Settings** page opens.

Configure Back-End Ports (Configure Storage Center Wizard)

Select SAS ports to configure for connecting to enclosures.

Steps

1. On the **Configure Back-End Ports** page, select the SAS ports to configure.
2. Click **Next**. The **Inherit Settings** or **Time Settings** page opens.

Inherit Settings

Use the Inherit Settings page to copy settings from a Storage Center that is already configured.

Prerequisites

You must be connected through a Data Collector.

Steps

1. Select the Storage Center from which to copy settings.
2. Place a check next to each setting that you want to inherit, or click **Select All** to inherit all settings.
3. Click **Next**.
   If you chose to inherit time and SMTP settings from another Storage Center, the **Time Settings** and **SMTP Server Settings** pages are skipped in the wizard.

Configure Time Settings

Configure an NTP server to set the time automatically, or set the time and date manually.

Steps

1. From the **Region** and **Time Zone** drop-down menus, select the region and time zone used to set the time.
2. Select **Use NTP Server** and type the host name or IPv4 address of the NTP server, or select **Set Current Time** and set the time and date manually.
3. Click **Next**.

Configure SMTP Server Settings

If you have an SMTP server, configure the SMTP email settings to receive information from the Storage Center about errors, warnings, and events.

Steps

1. By default, the **Enable SMTP Email** checkbox is selected and enabled. If you do not have an SMTP server you can disable SMTP email by clearing the **Enable SMTP Email** checkbox.
2. Alternatively, if you have an SMTP server, configure the SMTP server settings.
   a. In the **Recipient Email Address** field, enter the email address where the information will be sent.
   b. In the **SMTP Mail Server** field, enter the IP address or fully qualified domain name of the SMTP mail server.
   c. (Optional) In the **Backup SMTP Mail Server** field, enter the IP address or fully qualified domain name of a backup SMTP mail server and click **OK**.
   d. Click **Test Server** to verify connectivity to the SMTP server.
   e. If the SMTP server requires emails to contain a MAIL FROM address, specify an email address in the **Sender Email Address** field.
   f. (Optional) In the **Common Subject Line** field, enter a subject line to use for all emails sent by the Storage Center.
3. Click **Next**.

Accept the SupportAssist Collection Agreement

Use the Accept SupportAssist Collection Agreement page to accept to the terms of the agreement and enable SupportAssist.

Steps

1. To allow SupportAssist to collect diagnostic data and send this information to technical support, select the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox.
2. Click **Next**.

   NOTE: If you chose to clear the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox, a **SupportAssist Recommended** dialog box opens.

   - To return to the **Accept SupportAssist Collection Agreement** page, click **No**.
   - To opt out of SupportAssist, click **Yes**.

Provide Contact Information

Specify contact information for technical support to use when sending support-related communications from SupportAssist.

Steps

1. Specify the contact information.
2. (Storage Center 7.2 or earlier) To receive SupportAssist email messages, select the **Send me emails from SupportAssist when issues arise, including hardware failure notifications** check box.
3. Select the preferred contact method, language, and available times.
4. (Storage Center 7.2 or earlier) Type a shipping address where replacement Storage Center components can be sent.

5. (Storage Center 7.2 or earlier) Click **Finish**.
6. (Storage Center 7.3 or later) Click **Next**.

Provide Site Contact Information

If the storage system is running Storage Center 7.3 or later, specify the site contact information.

Steps

1. Select the **Enable Onsite Address** checkbox.
2. Type a shipping address where replacement Storage Center components can be sent.
3. Click **Next**.
   The **Confirm Enable SupportAssist** dialog box opens.
4. Click **Yes**.

Validate the SupportAssist Connection

If the storage system is running Storage Center 7.3 or later, the **Validate SupportAssist Connection** page opens.

About this task

The **Validate SupportAssist Connection** page displays a summary of the SupportAssist contact information and confirms that the Storage Center is connected to SupportAssist.

Steps

- To complete the SupportAssist setup, click **Finish**.

Complete Configuration and Perform Next Steps

The Storage Center is now configured. The Configuration Complete page provides links to a Storage Manager Client tutorial and wizards to perform the next setup tasks.

Steps

1. (Optional) Click one of the **Next Steps** to configure a localhost, configure a VMware host, or create a volume.
   When you have completed the step, you are returned to the **Configuration Complete** page. After you finish the Next Steps, continue to Step 2.
2. Click **Finish** to exit the wizard.

Related concepts

Creating Volumes on page 98

Related tasks

Create a Server from the localhost on page 147
Create a Server from a VMware vSphere Host on page 148
Create a Server from a VMware vCenter Host on page 148

Configure Embedded iSCSI Ports

Configure the embedded Ethernet ports on the Storage Center for use as iSCSI ports.

Prerequisites

The storage system must be one of the following:

- SCv2000

- SCv2020
- SCv2080
- SC4020

Steps

1. Configure the fault domain and ports (**embedded fault domain 1** or **Flex Port Domain 1**).

   NOTE: The Flex Port feature allows both Storage Center system management traffic and iSCSI traffic to use the same physical network ports. However, for environments where the Storage Center system management ports are mixed with network traffic from other devices, separate the iSCSI traffic from management traffic using VLANs.

   a. Enter the target IPv4 address, subnet mask, and gateway for the fault domain.
   b. Enter an IPv4 address for each port in the fault domain.

   NOTE: Make sure that all the IP addresses for the fault domain are in the same subnet.

2. Configure the fault domain and ports (**embedded fault domain 2** or **Flex Port Domain 2**).
   a. Enter the target IPv4 address, subnet mask, and gateway for the fault domain.
   b. Enter an IPv4 address for each port in the fault domain.

   NOTE: Make sure that all the IP addresses for the fault domain are in the same subnet.

3. Click **OK**.

Configuring SC9000 Storage Centers

Use the Configure Storage Center wizard to set up a new SC9000 Storage Center. The wizard helps configure the Storage Center to make it ready for volume creation.

Prerequisites

- The Storage Manager Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run by a Storage Manager Client user with the Administrator privilege.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select **Dell Storage** or **Storage Centers**.
3. In the **Summary** tab, click **Add Storage Center**. The **Add Storage Center** wizard opens.
4. Select **Add a new Storage Center to the Data Collector**, then click **Next**.
5. Specify Storage Center login information.
   - **Hostname or IP Address** – Type the host name or IP address of a Storage Center controller. For a dual-controller Storage Center, enter the IP address or host name of the management controller.
   - **User Name** and **Password** – Type the user name and password for a Storage Center user.

     NOTE: If you specify a Storage Center user with the Reporter or Volume Manager privilege, access to the Storage Center from Storage Manager is restricted based on the privilege and user groups that were assigned to the Storage Center user.
   - **Folder** – Select the parent folder for the Storage Center.
6. Click **Finish**. The **Change Password** dialog box opens.
7. a. In the **User Name** field, type the Storage Center user name.
   b. In the **Password** field, type the Storage Center user password.
   c. In the **Host/IP** field, type the host name or IP address of the Storage Center.
   d. If you changed the web server port during installation, type the updated port in the **Web Server Port** field.
8. Click **Log In**. The Client connects to the Storage Center and indicates that initial configuration is necessary.
9. Type a new password in the **New Password** and **Confirm Password** fields.
10. Click **OK**. The **Configure Storage Center** wizard opens.

11. Make sure that you have the required information that is listed on the first page of the wizard. This information is needed to configure the Storage Center.
12. Click **Next**. The **Submit Storage Center License** page opens.

Welcome Page

Use the Welcome page to verify the Storage Center information, and optionally change the name of the Storage Center.

Steps

1. Verify that the Service Tag and serial number match the Storage Center to set up.
2. (Optional) Type a name for the Storage Center.
3. Click **Next**.

Set System Information

The **Set System Information** page allows you to enter Storage Center and storage controller configuration information to use when connecting to the Storage Center using Storage Manager.

Steps

1. Type a descriptive name for the Storage Center in the **Storage Center Name** field.
2. If the storage system is running Storage Center 7.3 or later, select the network configuration option from the **Network Configuration Source** drop-down menu.
   - **DHCP IPv4** – Selected by default. IP addresses will be discovered and assigned.
   - **Static** – Enter static IP addresses manually.
3. If the network configuration source is set to Static:
   a. Type the system management IPv4 address for the Storage Center in the **Virtual Management IPv4 Address** field.

      The management IPv4 address is the IP address used to manage the Storage Center and is different than a storage controller IPv4 address.
   b. Type an IPv4 address for the management port of each storage controller.

      NOTE: The storage controller IPv4 addresses and management IPv4 address must be within the same subnet.

   c. Type the subnet mask of the management network in the **Subnet Mask** field.
   d. Type the gateway address of the management network in the **Gateway IPv4 Address** field.
   e. Type the domain name of the management network in the **Domain Name** field.
   f. Type the DNS server addresses of the management network in the **DNS Server** and **Secondary DNS Server** fields.
4. Click **Next**.

Submit the Storage Center License

Use the Submit Storage Center License page to type the name and title of the approving customer and to select the Storage Center license file.

Steps

1. Click **Browse**.
   The **Select License File** window opens.
2. Browse to the location of the license file, select the file, and then click **Select**.
3. Verify the approving customer information and license file path, then click **Next**.
   The **Create Disk Folder** page opens.

Create a Disk Folder

Create a disk folder to manage unassigned disks.

Steps

1. Type a name for the disk folder.
2. (Optional) To create a secure disk folder, select the **Create as a Secure Data Folder** checkbox.

   NOTE: This option is available only if all drives support Secure Data.

3. Click **Change** to open a dialog box for selecting the disks to assign to the folder.
4. Click **Next**.
   The **Create Storage Type** page opens.
5. Select the redundancy level from the drop-down menu for each disk tier.
6. (Optional) Select the datapage size from the **Datapage Size** drop-down menu.
7. Click **Next**.
   The **Add Controller** page opens.

Deploy the Storage Center – Add a Controller

In a dual-controller storage system, the wizard prompts you to add the second controller.

Steps

1. Select **Add Second Controller**.
2. Type a serial number for the second controller.
3. Type the IPv4 address and eth1 IPv4 address of the second controller.
4. If the first controller has an IPv6 address set and the Storage Center supports IPv6, type the IPv6 address and IPv6 subnet prefix of the second controller.
5. Click **Next**. The **Set System Information** page opens.

Deploy the Storage Center

The Storage Center sets up the controller using the information provided on the previous pages.

Steps

1. The Storage Center performs system setup tasks. The **Deploy Storage Center** page displays the status of these tasks.
   To learn more about the initialization process, click **More information about Initialization**.
   - If one or more of the system setup tasks fails, click **Troubleshoot Initialization Error** to learn how to resolve the issue.
   - If the Configuring Disks task fails, click **View Disks** to see the status of the drives detected by the Storage Center.
   - If any of the Storage Center front-end ports are down, the **Storage Center Front-End Ports Down** dialog box opens. Select the ports that are not connected to the storage network, then click **OK**.
2. When all of the Storage Center setup tasks are complete, click **Next**.

Enter Key Management Server Settings

Specify key management server settings, such as hostname and port.

Steps

1. In the **Hostname** field, type the host name or IP address of the key management server.
2. In the **Port** field, type the number of a port with open communication with the key management server.
3. In the **Timeout** field, type the amount of time in seconds after which the Storage Center should stop attempting to reconnect to the key management server after a failure.

4. To add alternate key management servers, type the host name or IP address of another key management server in the **Alternate Hostnames** area, and then click **Add**.
5. If the key management server requires a user name to validate the Storage Center certificate, enter the name in the **Username** field.
6. If the key management server requires a password to validate the Storage Center certificate, enter the password in the **Password** field.
7. Click **Browse** next to the **Root CA Certificate**. Navigate to the location of the root CA certificate on your computer and select it.
8. Click **Browse** next to the certificate fields for the controllers. Navigate to the location of the controller certificates on your computer and select them.
9. Click **Next**.

Create a Storage Type

Select the datapage size and redundancy level for the Storage Center.

Steps

1. Select a datapage size.
   - **Standard (2 MB Datapage Size)**: Default datapage size, this selection is appropriate for most applications.
   - **High Performance (512 KB Datapage Size)**: Appropriate for applications with high performance needs, or in environments in which snapshots are taken frequently under heavy I/O. Selecting this size increases overhead and reduces the maximum available space in the Storage Type. All-flash storage systems use 512 KB by default.
   - **High Density (4 MB Datapage Size)**: Appropriate for systems that use a large amount of disk space and take snapshots infrequently.
2. Select a redundancy type.
   - **Redundant**: Protects against the loss of any one drive (if single redundant) or any two drives (if dual redundant).
   - **Non-Redundant**: Uses RAID 0 in all classes, in all tiers. Data is striped but provides no redundancy. If one drive fails, all data is lost.

     NOTE: Non-Redundant is not recommended because data is not protected against a drive failure. Do not use non-redundant storage for a volume unless the data has been backed up elsewhere.
3. For Redundant Storage Types, you must select a redundancy level for each tier unless the drive type or size requires a specific redundancy level
   - **Single Redundant**: Single-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 (each drive is mirrored)
     - RAID 5-5 (striped across 5 drives)
     - RAID 5-9 (striped across 9 drives)
   - **Dual redundant**: Dual redundant is the recommended redundancy level for all tiers. It is enforced for 3 TB HDDs and higher and for 18 TB SSDs and higher. Dual-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 Dual-Mirror (data is written simultaneously to three separate drives)
     - RAID 6-6 (4 data segments, 2 parity segments for each stripe)
     - RAID 6-10 (8 data segments, 2 parity segments for each stripe.)
4. **Drive Addition** is selected by default. Leave this option selected.
5. Click **Next**.

Configure Ports

Use the Configure Fault Tolerance pages to configure the front-end and back-end ports of the system.

Steps

1. Select **Configure Fault Domains** next to **Fibre Channel** or **iSCSI** to set up fault domains for those ports. If the system has both Fibre Channel and iSCSI ports, select **Configure Fault Domains** next to both port types.
2. Select **Configure Back-End Ports** next to **SAS (Back-End)** to set up SAS ports to connect to the enclosures.
3. Select **Configure Fault Domains** next to **SAS (Front-End)** to set up front-end SAS ports to connect directly to hosts.

4. Click **Next**.

Configure Fibre Channel Ports

Create a Fibre Channel fault domain to group FC ports for failover purposes.

Steps

1. On the first **Configure Fibre Channel Fault Tolerance** page, select a transport mode: **Virtual Port** or **Legacy**.
2. Select the method for creating fault domains:
   - **Generate Fault Domain Configuration** – One of the following fault domains is created, depending on system configuration and mode selected:

Transport Mode	One Controller	Two Controllers
Virtual Port	Two controller ports	Two controller ports, one on each controller
Legacy	One controller port	Four controller ports, two on each controller

   - **Specify Number of Fault Domains** – Set the number of fault domains to create.
3. Click **Next**.

   NOTE: If you selected **Generate Fault Domain Configuration**, proceed to step 5.

4. If you selected **Specify Number of Fault Domains**, configure each fault domain.
   a. In the **Name** field, type a name for the fault domain.
   b. (Optional) In the **Notes** field, type notes for the fault domain.
   c. In the **Ports** table, select the Fibre Channel ports to add to the fault domain. All FC ports in the fault domain should be connected to the same FC fabric.
   d. Click **Next**. If you are configuring more than one fault domain, repeat these steps for each domain.
5. On the final **Configure Fibre Channel Fault Tolerance** page, review the fault domain setup.
6. (Optional) To change the fault domain setup, select from the following options:
   - Click **Create Fault Domain** to create a new fault domain.
   - Click **Edit Fault Domain** to edit the current fault domain.
   - Click **Remove** to delete a fault domain.
7. Click **Next**.
   - If you are setting up iSCSI fault domains, the **Configure iSCSI Fault Domain** page opens.
   - If you are setting up SAS back-end ports but not iSCSI fault domains, the **Configure Back-End Ports** page opens.
   - If you are not setting up iSCSI fault domains or SAS back-end ports, the **Inherit Settings** or **Time Settings** page opens.

Configure iSCSI Ports

Create an iSCSI fault domain to group ports for failover purposes.

Steps

1. On the first **Configure iSCSI Fault Tolerance** page, select the number of fault domains to create, and then click **Next**.
2. On the next **Configure iSCSI Fault Tolerance** page, configure the first fault domain:
   a. In the **Name** field, type a name for the fault domain.
   b. (Optional) In the **Notes** field, type notes for the fault domain.
   c. In the **Target IPv4 Address** field, type an IP address to assign to the iSCSI control port.
   d. In the **Subnet Mask** field, type the subnet mask for the IP address.
   e. In the **Gateway IPv4 Address** field, type the IP address for the iSCSI network default gateway.
   f. In the **Ports** table, select the iSCSI ports to add to the fault domain. All iSCSI ports in the fault domain should be connected to the same Ethernet network.
   g. Click **Next**. If you are configuring more than one fault domain, repeat these steps for each fault domain.
3. On the final **Configure iSCSI Fault Tolerance** page, review the fault domain setup.
4. (Optional) To change the fault domain setup, select from the following options:
   - Click **Create Fault Domain** to create a new fault domain.

- Click **Edit Fault Domain** to edit the current fault domain.
- Click **Remove** to delete a fault domain.

5. Click **Next**.
   - If you are setting up SAS back-end ports, the **Configure Back-End Ports** page opens.
   - If you are not setting up SAS back-end ports, the **Inherit Settings** or **Time Settings** page opens.

Inherit Settings

Use the Inherit Settings page to copy settings from a Storage Center that is already configured.

Prerequisites

You must be connected through a Data Collector.

Steps

1. Select the Storage Center from which to copy settings.
2. Place a check next to each setting that you want to inherit, or click **Select All** to inherit all settings.
3. Click **Next**.
   If you chose to inherit time and SMTP settings from another Storage Center, the **Time Settings** and **SMTP Server Settings** pages are skipped in the wizard.

Configure Time Settings

Configure an NTP server to set the time automatically, or set the time and date manually.

Steps

1. From the **Region** and **Time Zone** drop-down menus, select the region and time zone used to set the time.
2. Select **Use NTP Server** and type the host name or IPv4 address of the NTP server, or select **Set Current Time** and set the time and date manually.
3. Click **Next**.

Configure SMTP Server Settings

If you have an SMTP server, configure the SMTP email settings to receive information from the Storage Center about errors, warnings, and events.

Steps

1. By default, the **Enable SMTP Email** checkbox is selected and enabled. If you do not have an SMTP server you can disable SMTP email by clearing the **Enable SMTP Email** checkbox.
2. Alternatively, if you have an SMTP server, configure the SMTP server settings.
   a. In the **Recipient Email Address** field, enter the email address where the information will be sent.
   b. In the **SMTP Mail Server** field, enter the IP address or fully qualified domain name of the SMTP mail server.
   c. (Optional) In the **Backup SMTP Mail Server** field, enter the IP address or fully qualified domain name of a backup SMTP mail server and click **OK**.
   d. Click **Test Server** to verify connectivity to the SMTP server.
   e. If the SMTP server requires emails to contain a MAIL FROM address, specify an email address in the **Sender Email Address** field.
   f. (Optional) In the **Common Subject Line** field, enter a subject line to use for all emails sent by the Storage Center.
3. Click **Next**.

Set Up SupportAssist

If the storage system is running Storage Center 7.3 or later, the **Set Up SupportAssist** page opens.

About this task

Use the **Set Up SupportAssist** page to enable SupportAssist.

Steps

1. To allow SupportAssist to collect diagnostic data and send this information to technical support, select the **Receive proactive notifications, notices, and other predictive support** checkbox.
2. Click **Next**.
   If you chose to clear the **Receive proactive notifications, notices, and other predictive support** checkbox and click **Next**, a **SupportAssist Recommended** dialog box opens.
   - To return to the **Set Up SupportAssist** page, click **No**.
   - To disable SupportAssist and proceed to the **Update Storage Center** page, click **Yes**.

Accept the SupportAssist Collection Agreement

Use the Accept SupportAssist Collection Agreement page to accept to the terms of the agreement and enable SupportAssist.

Steps

1. To allow SupportAssist to collect diagnostic data and send this information to technical support, select the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox.
2. Click **Next**.

   NOTE: If you chose to clear the **By checking this box, you accept the above terms and turn on SupportAssist** checkbox, a **SupportAssist Recommended** dialog box opens.
   - To return to the **Accept SupportAssist Collection Agreement** page, click **No**.
   - To opt out of SupportAssist, click **Yes**.

Provide Contact Information

Specify contact information for technical support to use when sending support-related communications from SupportAssist.

Steps

1. Specify the contact information.
2. (Storage Center 7.2 or earlier) To receive SupportAssist email messages, select the **Send me emails from SupportAssist when issues arise, including hardware failure notifications** check box.
3. Select the preferred contact method, language, and available times.
4. (Storage Center 7.2 or earlier) Type a shipping address where replacement Storage Center components can be sent.
5. (Storage Center 7.2 or earlier) Click **Finish**.
6. (Storage Center 7.3 or later) Click **Next**.

Provide Site Contact Information

If the storage system is running Storage Center 7.3 or later, specify the site contact information.

Steps

1. Select the **Enable Onsite Address** checkbox.
2. Type a shipping address where replacement Storage Center components can be sent.
3. Click **Next**.
   The **Confirm Enable SupportAssist** dialog box opens.

4. Click **Yes**.

Validate the SupportAssist Connection

If the storage system is running Storage Center 7.3 or later, the **Validate SupportAssist Connection** page opens.

About this task

The **Validate SupportAssist Connection** page displays a summary of the SupportAssist contact information and confirms that the Storage Center is connected to SupportAssist.

Steps

- To complete the SupportAssist setup, click **Finish**.

Complete Configuration and Perform Next Steps

The Storage Center is now configured. The Configuration Complete page provides links to a Storage Manager Client tutorial and wizards to perform the next setup tasks.

Steps

1. (Optional) Click one of the **Next Steps** to configure a localhost, configure a VMware host, or create a volume.
   When you have completed the step, you are returned to the **Configuration Complete** page. After you finish the Next Steps, continue to Step 2.
2. Click **Finish** to exit the wizard.

Related concepts

Creating Volumes on page 98

Related tasks

Create a Server from the localhost on page 147
Create a Server from a VMware vSphere Host on page 148
Create a Server from a VMware vCenter Host on page 148

Set Up a localhost or VMware Host

After configuring a Storage Center, you can set up block-level storage for a localhost, VMware vSphere host, or VMware vCenter.

Set Up a localhost from Initial Setup

Configure a localhost to access block-level storage on the Storage Center. It is recommended that you perform this procedure for each host that is connected to the Storage Center.

Prerequisites

- Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run by a Storage Manager Client user with the Administrator privilege.
- The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator or Volume Manager privilege.
- On a Storage Center with Fibre Channel IO ports, configure the Fibre Channel zoning.

Steps

1. On the **Configuration Complete** page of the **Discover and Configure Storage Center** wizard, click **Configure this host to access a Storage Center**.
   The **Set up localhost on Storage Center** wizard appears.
2. Click **Next**.
   - If the Storage Center has iSCSI ports and the host is not connected to an iSCSI interface, the **Log into Storage Center via iSCSI** page appears. Select the target fault domains, and then click **Next**.
   - In all other cases, the **Verify localhost Information** page appears.
3. Select an available port, and then click **Next**. The server definition is created on the Storage Center.
   The **Host Setup Successful** page displays the best practices that were set by the wizard and best practices that were not set. Make a note of any best practices that were not set. It is recommended that these updates be applied manually before starting I/O to the Storage Center.
4. (Optional) To create a volume after finishing host setup, select the **Launch wizard to create a volume for this host** checkbox.
5. Click **Finish**.

Set Up a VMware Host from Initial Setup

Configure a VMware vSphere host to access block-level storage on the Storage Center.

Prerequisites

- Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run by a Storage Manager Client user with the Administrator privilege.
- The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator or Volume Manager privilege.
- On a Storage Center with Fibre Channel IO ports, configure the Fibre Channel zoning before starting this procedure.
- To configure a host to access block-level storage on a Storage Center with SAS HBAs, you must connect to the Storage Center through a Dell Storage Manager Data Collector.
- To download the correct SAS HBA driver for an ESXi host, go to www.vmware.com/resources/compatibility and search for **`Dell mpt3sas 04.00.00.00.1`**. Click the **Dell 12GB/s HBA external** link, and download the `mpt3sas version 04.00.00.00.1vmw` driver.
- To update the SAS HBA driver on an ESXi host, see www.dell.com/Support/Article/us/en/19/HOW11081.
- Configure only one ESXi host at a time.

Steps

1. On the **Configuration Complete** page of the **Discover and Configure Storage Center** wizard, click **Configure VMware vSphere to access a Storage Center**.
   The **Set up VMware Host on Storage Center** wizard appears.
2. Enter the IP address or host name, the user name, and password of the VMware host.
3. Click **Next**.
   - If the Storage Center has iSCSI ports and the host is not connected to any interface, the **Log into Storage Center via iSCSI** page appears. Select the target fault domains, and then click **Log In**.
   - In all other cases, the **Verify vCenter Information** page appears.
4. Select an available port, and then click **Next**. The server definition is created on the Storage Center.
   The **Host Setup Successful** page displays the best practices that were set by the wizard and best practices that were not set. Make a note of any best practices that were not set by the wizard. It is recommended that these updates be applied manually before starting I/O to the Storage Center.
5. (Optional) To create a volume after finishing host setup, select the **Launch wizard to create a volume for this host** check box.
6. Click **Finish**.

Set Up a VMware vCenter Host from Initial Setup

Configure a VMware vCenter host to access block-level storage on the Storage Center.

Prerequisites

- Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run by a Storage Manager Client user with the Administrator privilege.
- The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator or Volume Manager privilege.
- On a Storage Center with Fibre Channel IO ports, configure the Fibre Channel zoning before starting this procedure.
- To configure a host to access block-level storage on a Storage Center with SAS HBAs, you must connect to the Storage Center through a Dell Storage Manager Data Collector.
- To download the correct SAS HBA driver for an ESXi host, go to www.vmware.com/resources/compatibility and search for **`Dell mpt3sas 04.00.00.00.1`**. Click the **Dell 12GB/s HBA external** link, and download the `mpt3sas version 04.00.00.00.1vmw` driver.
- To update the SAS HBA driver on an ESXi host, see www.dell.com/Support/Article/us/en/19/HOW11081.
- Configure only one ESXi host or server object at a time.

Steps

1. On the **Configuration Complete** page of the **Discover and Configure Storage Center** wizard, click **Configure VMware vSphere to access a Storage Center**.
   The **Set up VMware Host on Storage Center** wizard appears.
2. Enter the IP address or host name, the user name, and password of the vCenter Server.
3. Click **Next**.
   The **Verify vCenter Information** page appears and displays the VMware hosts that are connected or partially connected.
4. Click **Next**.
5. Enter the IP address or host name, the user name, and password of a VMware host.
6. Select an available port, and then click **Next**. The server definition is created on the Storage Center.
   The **Host Setup Successful** page displays the best practices that were set by the wizard and best practices that were not set. Make a note of any best practices that were not set by the wizard. It is recommended that these updates be applied manually before starting I/O to the Storage Center.
7. (Optional) To create a volume after finishing host setup, select the **Launch wizard to create a volume for this host** check box.
8. Click **Finish**.

5

Storage Center Administration

Storage Center provides centralized, block-level storage that can be accessed by Fibre Channel, iSCSI, or SAS connections.

Topics:

- Adding and Organizing Storage Centers
- Managing Volumes
- Managing Data Reduction
- Managing Snapshot Profiles
- Managing Storage Profiles
- Managing QoS Profiles
- Importing Volumes from an External Storage Array

Adding and Organizing Storage Centers

Adding and organizing Storage Centers can only be done using Storage Manager connected to a Data Collector.

Note the following restrictions about Storage Manager user accounts:

- An individual Storage Manager user can view and manage only the Storage Centers that have been mapped to his or her account. In other words, the Storage Centers that are visible to one Storage Manager user are not necessarily visible to another user.
- When a Storage Manager user adds a Storage Center, he or she must provide credentials for a Storage Center user. The privilege level and user groups assigned to the Storage Center user determine the access that is allowed on the Data Collector.
- The first time you add a Storage Center to the Data Collector, you must specify a Storage Center user account that has the Administrator privilege. When you subsequently add the Storage Center for other Storage Manager users, you can specify Storage Center user accounts of any privilege level.
- If yourStorage Manager user account has the Reporter privilege, you must specify a Storage Center user account that has the Reporter privilege.

  NOTE: A Storage Manager Administrator can also use the Data Collector to grant Storage Center access to a Storage Manager user with the Reporter privilege.
- Manage a Storage Center using one Data Collector only. Issues can occur if a Storage Center is managed by multiple Data Collectors.

Storage Center User Privileges and User Groups

Storage Center groups determine which storage objects can be viewed by the Storage Center user, and the privilege level defines what the user can do.

NOTE: Storage Center user privileges and Storage Manager user privileges share the same names, but they are not the same. Storage Center user privileges control access to Storage Center functionality, and Storage Manager user privileges control access to Storage Manager functionality. A user may have a different role in Storage Manager than in Storage Center. This role difference affects small details of that user's access.

Related concepts

Storage Manager User Privileges on page 651

User Privilege Levels

Each user is assigned a single privilege level. Storage Center has three levels of user privilege.

Table 5. Storage Center User Privilege Levels

Privilege Level	Allowed Access
Administrator	Read and write access to the entire Storage Center (no restrictions). All Administrators have the same predefined privileges. Only Administrators can manage users and user groups.
Volume Manager	Read and write access to the folders associated with the assigned user groups. Users with this privilege level can create volumes in the allowed volume folders and map them to existing servers in the allowed server folders.
Reporter	Read-only access to the folders associated with the assigned user groups.

Adding and Removing Storage Centers

You must be connected to a Data Collector to add or remove Storage Centers.

NOTE: For user interface reference information, click **Help**.

Add a Storage Center

Add a Storage Center to Storage Manager to manage and monitor the Storage Center from the Storage Manager Client.

Prerequisites

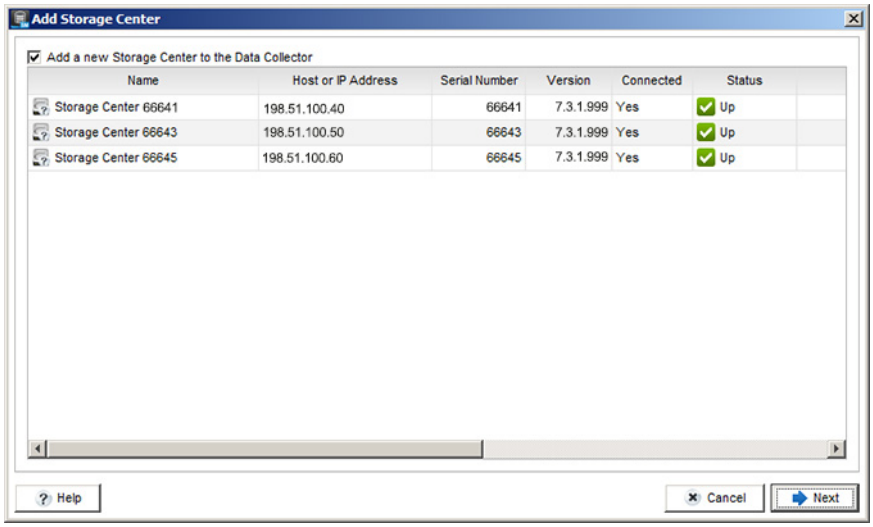
- You must have the username and password for a Storage Center user account.
  - The first time a Storage Center is added to Storage Manager, you must specify a Storage Center user account that has the Administrator privilege. When the Storage Center is then added for other Storage Manager users, you can specify Storage Center user accounts of any privilege level.
  - If your Storage Manager user account has the Reporter privilege, you must specify a Storage Center user account that has the Reporter privilege.

    NOTE: Storage Manager users with Reporter level privileges have limited access to Storage Manager. To grant a Reporter Storage Manager user more privileges, add Storage Center mappings to that user in the Storage Manager Data Collector. Only Administrator level Storage Manager users can set mapping for users.
- The Storage Manager Data Collector must have connectivity to the Storage Center management interface.
- The Storage Center certificate must contain the hostname or management IP address that is used to add the Storage Center to Storage Manager.

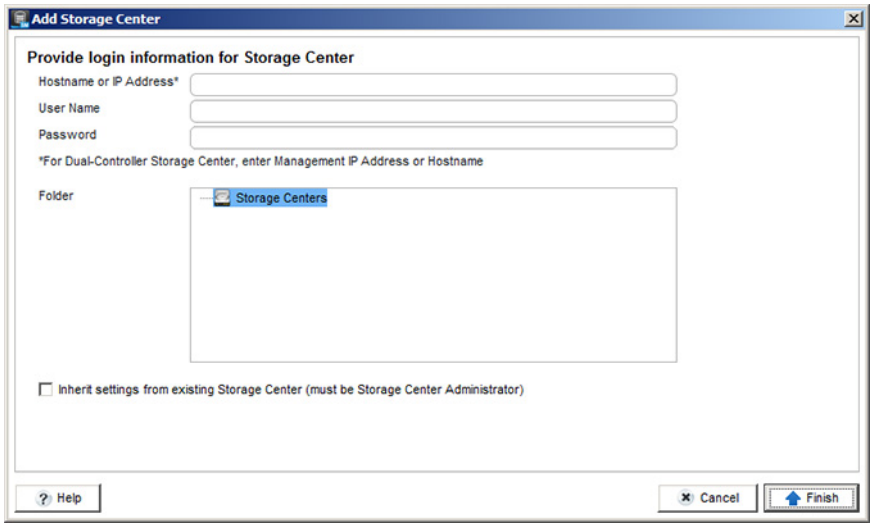
Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select **Storage Centers**.
3. In the **Summary** tab, click **Add Storage Center**. The **Add Storage Center** wizard opens.

- If one or more Storage Centers are mapped to another user, the dialog box displays a list of available Storage Centers.



- If no Storage Centers are mapped to another user, the dialog box allows you to enter a new Storage Center.



4. (Conditional) If the dialog box is displaying a list of Storage Centers, select a Storage Center from the list or add a new one.
   - To add a Storage Center that does not appear in the list, ensure that the **Add a new Storage Center to the Data Collector** check box is selected, then click **Next**.
   - To add a Storage Center that appears in the list, clear the **Add a new Storage Center to the Data Collector** check box, select the appropriate Storage Center, then click **Next**.
5. Enter Storage Center login information.
   - **Hostname or IP Address:** (New Storage Center only) Enter the hostname or IP address of a Storage Center controller. For a dual-controller Storage Center, enter the IP address or hostname of the management controller.
   - **User Name** and **Password:** Enter the username and password for a Storage Center user.

     NOTE: If you specify a Storage Center user with the Reporter or Volume Manager privilege, access to the Storage Center from Storage Manager is restricted based on the privilege and user groups that are assigned to the Storage Center user.
   - **Folder**: Select the parent folder for the Storage Center.
6. (Optional) Configure the Storage Center to use settings applied to another Storage Center by selecting the **Inherit settings from existing Storage Center** check box. If this check box is selected, after the wizard closes the Inherit Settings wizard appears.
7. Click **Finish**.
   - If the **Inherit settings from existing Storage Center** check box was not selected, the Storage Center is added to Storage Manager.
   - If the **Inherit settings from existing Storage Center** check box was selected, the Inherit Settings dialog box appears.
8. (Inherit settings only) Choose the Storage Center settings to inherit.

a. Select the Storage Center from which you want to inherit settings, then click **Next**. The wizard advances to the next page.
b. Select the check box for each category of settings that you want to inherit. For user interface reference information, click **Help**.
c. When you are done, click **Finish**.
   - If passwords are not configured for the SupportAssist proxy, Secure Console proxy, or SMTP server, the dialog box closes.
   - If a password for the SupportAssist proxy, Secure Console proxy, or SMTP server is configured, you are prompted to enter the required passwords.
d. Enter the required passwords to complete the wizard.

Related tasks

Set Storage Center Mappings for a Reporter User on page 661

Reconnect to a Storage Center

If Storage Manager cannot communicate with or log in to a Storage Center, Storage Manager marks the Storage Center as down. Reconnect to the Storage Center to provide the updated connectivity information or credentials.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center.
3. In the **Summary** tab, click **Reconnect to Storage Center**. The Reconnect to Storage Center dialog box appears.
4. Enter Storage Center logon information.
   - **Hostname or IP Address:** Enter the host name or IP address of a Storage Center controller. For a dual-controller Storage Center, enter the IP address or host name of the management controller.
   - **User Name** and **Password:** Enter the user name and password for a Storage Center user.
     NOTE: If you specify a Storage Center user with the Reporter or Volume Manager privilege, access to the Storage Center from Storage Manager is restricted based on the privilege and user group(s) assigned to the Storage Center user.
5. Click **OK**.

Remove a Storage Center

Remove a Storage Center when you no longer want to manage it from Storage Manager.

About this task

NOTE: When a Storage Center is removed from all Storage Manager users with the Administrator or Volume Manager privilege, it is automatically removed from Storage Manager users with the Reporter privilege.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center you want to remove.
3. In the **Summary** tab, click **Delete**. The **Delete Objects** dialog box appears.
4. Click **OK**.

Organizing Storage Centers

Use folders to group Storage Centers in Storage Manager.

NOTE: For user interface reference information, click **Help**.

Create a Storage Center Folder

Use folders to group and organize Storage Centers.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select **Storage Centers**.
3. In the **Summary** tab, click **Create Folder**.
   The **Create Folder** dialog box opens.
4. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
5. In the **Name** field, type a name for the folder.
6. In the **Parent** field, select a parent folder.
7. Click **OK**.

Move a Storage Center Into a Folder

Storage Centers can be organized into folders.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center that you want to move to a folder.
3. In the **Summary** tab, click **Move**.
   The **Select Folder** dialog box opens.
4. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
5. Select the folder to which to move the Storage Center.
6. Click **OK**.

Rename a Storage Center Folder

Use the **Edit Settings** dialog box to change the name of a Storage Center folder.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center folder you want to modify.
3. In the **Summary** tab, click **Edit Settings**.
   The **Edit Settings** dialog box opens.
4. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
5. In the **Name** field, type a name for the folder.
6. Click **OK**.

Move a Storage Center Folder

Use the **Edit Settings** dialog box to move a Storage Center folder.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center folder you want to modify.
3. In the **Summary** tab, click **Edit Settings**. The **Edit Settings** dialog box opens.

4. In the Parent area, select the Storage Centers node or a parent folder.
5. Click **OK**.

Delete a Storage Center Folder

Delete a Storage Center folder if it is no longer needed.

Prerequisites

The Storage Center folder must be empty.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center folder to delete.
3. In the **Summary** tab, click **Delete**.
   The **Delete** dialog box opens.
4. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
5. Click **OK**.

Managing Volumes

A Storage Center volume is a logical unit of storage that servers can access over a network. You can allocate more logical space to a volume than is physically available on the Storage Center.

Attributes That Determine Volume Behavior

When a volume is created, attributes are associated with the volume to control its behavior.

Attribute	Description
Storage Type	Specifies the disk folder, tier redundancy, and data page size of the storage used by the volume.
Storage Profile	Controls the RAID type, storage tiers, and data progression behavior for pages used by the volume.
Snapshot Profile	Describes when to take periodic snapshots (also known as point-in-time copies) for one or more volumes and the time at which snapshots are deleted (expired).
QoS Profile	Specifies a profile to apply to volumes, to potentially limit I/Os that the volumes can perform, and also defines their relative priority during times of congestion.

Related concepts

Managing Storage Profiles on page 135
Managing Snapshot Profiles on page 130
Managing QoS Profiles on page 137

Volume Icons

The following table describes the volume icons that appear in the **Storage** tab navigation pane:

Icon	Description
	The volume is not mapped to any servers.
	The volume is mapped to one or more servers.

Icon	Description
	The volume is the source for a replication to a remote Storage Center. **NOTE:** This icon is also displayed for volumes that have been configured to Copy, Mirror, or Migrate in the Storage Center Manager. These operations are not available in the Storage Manager Client.
	The volume is the destination for a replication from a remote Storage Center.
	The volume is the primary or secondary volume in a Live Volume.
	The volume is the source or destination of Live Migration.
	The volume was created from a Secure Data Storage Type.

Creating Volumes

Create volumes to present servers a logical unit of storage on a Storage Center.

NOTE: For user interface reference information, click **Help**.

Create a Volume Using Single-Step Dialog

If you need a small number of volumes, you can create them one at a time.

Prerequisites

The options for Volume QoS Profile and Group QoS Profile appear on the dialog box only if **Allow QoS Profile Selection** has been selected on the Storage Center Preferences.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Volumes**.
4. In the right pane, click **Create Volume**. The **Create Volume** dialog box opens.
5. In the **Name** field, type a name for the volume.
6. In the **Size** field, type a size for the volume in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).

   NOTE: A volume with a configured size greater than half the supported maximum volume size, as defined in the Storage Center Release Notes, does not support view volumes.

7. In the **Volume Folder** pane, select the parent folder for the volume.
8. (Optional) Configure the remaining volume attributes as needed.
   - To schedule snapshot creation and expiration for the volume, apply one or more Snapshot Profiles by clicking **Change** across from **Snapshot Profiles**.
   - To map the volume to a server, click **Change** across from **Server**.
   - If Chargeback is enabled, select the department to charge for storage costs associated with the volume by clicking **Change** across from **Chargeback Department**.
   - If Data Reduction is enabled on the Storage Center, select **Compression** or **Deduplication with Compression** to enable Data Reduction on the volume.
   - To use specific disk tiers and RAID levels for volume data, select the appropriate Storage Profile from the **Storage Profile** drop-down menu. Using the **Recommended** Storage Profile allows the volume to take full advantage of data progression.
   - If more than one Storage Type is defined on the Storage Center, select the **Storage Type** to provide storage from the **Storage Type** drop-down menu.
   - To set a Volume QoS Profile, either accept the default QoS Profile or click **Change** across from **Volume QoS Profile**. Then select a Volume QoS profile from the resulting list, and click **OK**.
   - To set a Group QoS Profile, click **Change** across from **Group QoS Profile**. Then select a Group QoS profile from the resulting list, and click **OK**.

- To adjust the Read/Write Cache, enter the desired size of the cache.
- To configure Replications and Live Volumes if they are licensed, select **Replications and Live Volumes**.

9. Click **OK**.

Create a Volume Using the Multiple-step Wizard

The multiple-step wizard is the default method of creating volumes for SCv2000 series controllers.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Volumes**.
4. In the right pane, click **Create Volume**.
   The **Create Volume** wizard opens.
5. In the **Volume Identification** page, specify the name, notes, and folder for the volume being created.
   a. In the name field, type the desired name of the volume.
   b. (Optional) In the notes field, type any notes associated with the volume.
   c. In the volume folder pane, specify the desired location of the volume.
   d. (Optional) To create a new folder, click **Create Folder**.
      The **Create Volume Folder** dialog box opens.
6. Click **Next**.
   The **Specify Capacity** page opens.
7. In the **Specify Capacity** page, specify the size of the volume and optionally set threshold definitions.
   a. In the **size** field, type the desired size of the volume.

      NOTE: A volume with a configured size greater than half the supported maximum volume size, as defined in the Storage Center Release Notes, does not support view volumes.

   b. (Optional) To select threshold definitions, click **Select Threshold Definition**. This option is not available on SCv2000 series controllers.
      The **Set Threshold Alert Definitions** dialog box opens.
8. Click **Next**.
   (Optional) The **Storage Options** page appears. If no options are available, the wizard will not display this page.
9. In the **Storage Options** page, specify the options for the volume.
   Storage options vary based on the features the Storage Center supports.
   - If more than one Storage Type is defined on the Storage Center, select the **Storage Type** to provide storage from the **Storage Type** drop-down menu.
   - To set a Volume QoS Profile, either accept the default QoS Profile or click **Change** across from **Volume QoS Profile**. Then select a Volume QoS profile from the resulting list, and click **OK**.
   - To set a Group QoS Profile, click **Change** across from **Group QoS Profile**. Then select a Group QoS profile from the resulting list, and click **OK**.
   - If Data Reduction is enabled on the Storage Center, select **Compression** or **Deduplication with Compression** to enable Data Reduction on the volume.
   - To enable the Read/Write Cache, select or clear the option. Read and write caching generally improves performance, however to improve performance for SSDs, disable write caching on volumes that use SSD storage.
10. Click **Next**.
    The **Set Snapshot Profiles** page opens.
11. Select a Snapshot Profile.
    - (Optional) To create a new Snapshot Profile, click **Create New Snapshot Profile**.
12. Click **Next**.
    The **Map to Server** page opens.
13. Select a server. Click **Create Server** to create a new server and map it to the new volume. You can also create the volume without mapping a server if you choose. To select this option, click **Yes** to the No Server Specified dialog. To select from a more detailed list of options, click **Advanced Mapping**.
14. Click **Next**.

The **Replication Tasks** page appears. This step appears only if Replication is licensed.

15. Set the Replication options for the new volume.
    - To create the volume without setting up a replication, select **No Replication or Live Volume**.
    - To create a volume as a replication, select **Replication Volume to Another Storage Center**.
    - To create the volume as a Live Volume, select **Create as Live Volume**.
16. Click **Next**.
    The **Volume Summary** page opens.
17. Click **Finish**.

Create Multiple Volumes Simultaneously Using Single-Step Dialog

If you need to create many volumes, you can streamline the process by creating multiple volumes at a time.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Volumes**.
4. In the right pane, click **Create Multiple Volumes**. The **Create Volume** dialog box opens.
5. Use the **Create Volume** dialog box to configure the base volume parameters.
   a. In the **Volume Count** field, type the number of volumes to create.
   b. In the **Base Volume Name** field, type a base name for the volumes. Each volume is named with a combination of the base name and the volume number.
   c. In the **Size** field, type a size for the volumes in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).

      NOTE: A volume with a configured size greater than half the supported maximum volume size, as defined in the Storage Center Release Notes, does not support view volumes.

   d. In the **Volume Folder** pane, select the parent folder for the volumes.
   e. In the **Notes** field, type any notes you want to associate with these volumes.
   f. (Optional) Configure the remaining volume attributes as needed.
      - To schedule snapshot creation and expiration for the volume, apply one or more Snapshot Profiles by clicking **Change** across from **Snapshot Profiles**.
      - To map the volume to a server, click **Change** across from **Server**.
      - If Chargeback is enabled, select the department to charge for storage costs associated with the volume by clicking **Change** across from **Chargeback Department**.
      - If Data Reduction is enabled on the Storage Center, select **Compression** or **Deduplication with Compression** to enable Data Reduction on the volume.
      - To use specific disk tiers and RAID levels for volume data, select the appropriate Storage Profile from the **Storage Profile** drop-down menu. Using the **Recommended** Storage Profile allows the volume to take full advantage of data progression.
      - If more than one Storage Type is defined on the Storage Center, select the **Storage Type** to provide storage from the **Storage Type** drop-down menu.
      - To set a Volume QoS Profile, either accept the default QoS Profile or click **Change** across from **Volume QoS Profile**. Then select a Volume QoS profile from the resulting list, and click **OK**.
      - To set a Group QoS Profile, click **Change** across from **Group QoS Profile**. Then select a Group QoS profile from the resulting list, and click **OK**.
      - To adjust the Read/Write Cache, enter the desired size of the cache.
      - To configure Replications and Live Volumes if they are licensed, select **Replications and Live Volumes**.
   g. Click **OK**. The **Create Multiple Volumes** dialog box opens and displays the volume you created in the previous step.
6. Use the **Create Multiple Volumes** dialog box to create additional volumes.
   - To add a volume based on a previous volume, select the volume from the list, then click **Clone Selected Volume**.
   - To manually define another volume, click **Add Volume**.
   - To modify an individual volume, select the volume from the list, then click **Edit Volume**.
   - To remove an individual volume, select the volume from the list, then click **Remove Volume**.

7. When you are finished, click **OK**.

Create Multiple Volumes Simultaneously Using the Multiple-Step Wizard

If you need to create many volumes, you can streamline the process by creating multiple volumes at a time. The multiple-step wizard is the default way to create volumes for the SCv2000 series controllers, and the only method available for direct connect SCv2000 series controllers to create multiple volumes simultaneously.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Volumes**.
4. In the right pane, click **Create Multiple Volumes**.
   The **Create Multiple Volumes** wizard opens.
5. In the **Volume Identification** page, specify the number of volumes to create, a base name, and notes, and select a folder for the volumes.
   a. In the volume count field, type the number of volumes.
   b. In the base volume name field, type the base name for the volumes. Each volume is named with a combination of the base name and the volume number.
   c. (Optional) In the notes field, type any notes associated with the volumes.
   d. In the volume folder pane, specify the desired location of the volumes. All volumes created will by default be placed in this folder. You can change this setting in the summary page before the wizard actually creates the volumes.
   e. (Optional) To create a new folder, click **Create New Folder**.
      The **Create Volume Folder** dialog box opens.
6. Click **Next**.
   The **Specify Capacity** page opens.
7. In the **Specify Capacity** page, specify the size of the volumes and optionally set threshold definitions.
   a. In the **size** field, type the desired size of the volumes in bytes, kilobytes (KB), gigabytes (GB), or terabytes (TB).

      NOTE: A volume with a configured size greater than half the supported maximum volume size, as defined in the Storage Center Release Notes, does not support view volumes.

   b. (Optional) To select threshold definitions, click **Select Threshold Definition**. This option is not available for SCv2000 or SCv3000 series controllers.
      The **Set Threshold Alert Definitions** dialog box opens.
8. Click **Next**.
   The **Storage Options** pane opens.
9. In the **Storage Options** page, specify the storage options for the volumes.
   - To schedule snapshot creation and expiration for the volume, apply one or more Snapshot Profiles by clicking **Change** across from **Snapshot Profiles**.
   - To map the volume to a server, click **Change** across from **Server**.
   - If Chargeback is enabled, select the department to charge for storage costs associated with the volume by clicking **Change** across from **Chargeback Department**.
   - If Data Reduction is enabled on the Storage Center, select **Compression** or **Deduplication with Compression** to enable Data Reduction on the volume.
   - To use specific disk tiers and RAID levels for volume data, select the appropriate Storage Profile from the **Storage Profile** drop-down menu. Using the **Recommended** Storage Profile allows the volume to take full advantage of data progression.
   - If more than one Storage Type is defined on the Storage Center, select the **Storage Type** to provide storage from the **Storage Type** drop-down menu.
   - To set a Volume QoS Profile, either accept the default QoS Profile or click **Change** across from **Volume QoS Profile**. Then select a Volume QoS profile from the resulting list, and click **OK**.
   - To set a Group QoS Profile, click **Change** across from **Group QoS Profile**. Then select a Group QoS profile from the resulting list, and click **OK**.
   - To adjust the Read/Write Cache, enter the desired size of the cache.
   - To configure Replications and Live Volumes if they are licensed, select **Replications and Live Volumes**.

NOTE: The storage options vary based on the features the Storage Center supports.

10. Click **Next**.
    The **Set Snapshot Profiles** page opens.
11. Select a Snapshot Profile.
    - (Optional) To create a new Snapshot Profile, click **Create New Snapshot Profile**.
12. Click **Next**.
    The **Map to Server** page opens.
13. Select a server. For more detailed options, click **Advanced Mapping**. To create a volume without selecting a server, click **Yes** to the No Server Specified dialog. To create a new server, click **New Server**.
14. Click **Next**. The **Replication Tasks** page opens. This step appears only if Replication is licensed. If Live Volume is licensed, those options are visible as well. These features are not available for all controllers. For clarification, see the replication licensing requirements for your system.
    - To create the volumes without setting up a replication, select **No Replication or Live Volume**.
    - To create a volume as a replication, select **Replicate Volume to Another Storage Center**.
    - To create the volume as a Live Volume, select **Create as Live Volume** .
15. Click **Next**.
    The **Volume Summary** pane opens.
16. Review the table of new volume settings.
    - To manually define another volume, click **Add Volume**.
    - To modify a previous volume, select the volume from the list, then click **Edit Volume**.
    - To add a volume based on a previous volume, select the volume from the list, then click **Clone Volume**.
    - To remove a previous volume, select the volume from the list, then click **Remove Volume**.
17. When you are finished, click **Finish**.

Modifying Volumes

You can rename, move, or expand a volume after it has been created. You can also modify advanced volume attributes if needed.

NOTE: For user interface reference information, click **Help**.

Edit Multiple Volumes

The Edit Multiple Volume dialog box allows you to edit the settings for multiple volumes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the right pane, click the **Volumes** node.
4. Click **Edit Multiple Volumes**.
   The **Edit Multiple Volumes** wizard opens.
5. Select the volume you want to edit.
6. Click **Next**.
7. Modify the volume settings as needed.
   For more information on the volume settings, click **Help**.
8. Click **Next**.
9. Review the changes.
10. Click **Finish**.
    The **Edit Multiple Volumes** wizard modifies the volumes then displays a results page.
11. Click **Finish**.

Rename a Volume

A volume can be renamed without affecting its availability.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to modify.
4. In the right pane, click **Edit Settings**.
   The **Edit Volume** dialog box opens.
5. In the **Name** field, type a new name for the volume.
6. Click **OK**.

Move a Volume to a Different Volume Folder

Volumes can be organized by placing them in folders.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to modify.
4. In the right pane, click **Move to Folder**.
   The **Move to Folder** dialog box opens.
5. In the navigation pane, select a new parent volume folder.
6. Click **OK**.

Move Multiple Volumes to a Different Volume Folder

Right-click a selection of volumes to move them to a different folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the **Volumes** node or the volume folder that contains the volumes.
4. In the right pane, select the volumes that you want to move.
   - To select contiguous volumes, select the first volume, then hold down Shift and select the last volume.
   - To select individual volumes, hold down Control while selecting them.
5. In the navigation pane, select a new parent volume folder.
6. Click **OK**.

Expand a Volume

Expand the size of a volume if more space is needed.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to expand.
4. In the right pane, click **Expand Volume**.
   The **Expand Volume** dialog box opens.
5. Type a new size for the volume, then click **OK**.

NOTE: Expanding a volume to a configured size greater than half the supported maximum volume size, as defined in the *Storage Center Release Notes*, will no longer support view volumes

Enable or Disable Read/Write Caching for a Volume

Read and write caching generally improves performance. To improve performance, disable write caching on volumes that use SSD storage.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Make sure **Allow Cache Selection** is enabled for volumes in the Storage Center user preferences.
   a. In the **Summary** tab, click Edit Settings.
   The **Edit Settings** dialog box opens.
   b. Click the **Preferences** tab.
   c. Make sure the **Allow Cache Selection** checkbox is selected.
   d. Click **OK**.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the volume you want to modify.
5. In the right pane, click **Edit Settings**. The **Edit Volume** dialog box opens.
6. Enable or disable the cache options as needed. These options are described in the online help.
   - Select or clear the **Read Cache** check box.

     For volumes using SSD storage, test applications before enabling or disabling read cache.
   - Select or clear the **Write Cache** check box.

     To improve performance, disable write caching on volumes that use SSD storage for most applications.
7. Click **OK**.

Assign Snapshot Profiles to a Volume

Assign one or more snapshot profiles to a volume if you want snapshots to be created on an automated schedule.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. From the **Storage** tab navigation pane, select the volume you want to modify.
4. From the right pane, click **Edit Settings**.
   The **Edit Volume** dialog box opens.
5. Select the appropriate snapshot profiles.
   a. Next to **Snapshot Profiles**, click **Change**. The **Select Snapshot Profiles** dialog box opens.
   b. From the top pane of the dialog box, select the snapshot profiles to assign to the volume.
   c. Click **OK** to close the **Select Snapshot Profiles** dialog box.
6. Click **OK** to close the **Edit Volume** dialog box.

Assign Snapshot Profiles to Multiple Volumes

Snapshot Profiles can be assigned to multiple volumes in one operation.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to modify.

4. In the right pane, select the volumes that you want to modify.
   - To select contiguous volumes, select the first volume, then hold down Shift and select the last volume.
   - To select individual volumes, hold down Control while selecting them.
5. Right-click the selection, then select **Set Snapshot Profiles**. The **Set Snapshot Profiles** dialog box opens.
6. In the upper table, select the check box for each Snapshot Profile you want to assign to the volume.
7. To remove the Snapshot Profiles that were previously assigned to the volume, select the **Replace Existing Snapshot Profiles** check box.
8. When you are finished, click **OK**.

Assign a Different Storage Profile to a Volume

The storage profile determines the RAID type and storage tiers used by the volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the right pane, click **Storage Profile**.
   The **Set Storage Profile** dialog box opens.
3. From the **Storage Profile** drop-down menu, select a storage profile.
4. Click **OK**.

Assign a Different Storage Profile to Multiple Volumes

The Storage Profile determines the RAID type and storage tiers used by the volume. A Storage Profile can be assigned to multiple volumes in one operation.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the **Volumes** node or the volume folder that contains the volumes.
4. In the right pane, select the volumes that you want to modify.
   - To select contiguous volumes, select the first volume, then hold down Shift and select the last volume.
   - To select individual volumes, hold down Control while selecting them.
5. Right-click the selection, then select **Set Storage Profile**. The **Set Storage Profile** dialog box opens.
6. From the **Storage Profile** drop-down menu, select a Storage Profile.
7. When you are finished, click **OK**.

Force Writes to the Lowest Storage Tier for a Volume

The **Import to lowest tier** option forces all data written to the volume to the lowest storage tier configured for the volume. This option is typically used when importing data to a new volume from an external source.

Prerequisites

The volume must use a standard storage type. The **Import to lowest tier** option is not available for flash-optimized storage types.

About this task

When the **Import To Lowest Tier** check box is selected, snapshots are no longer automatically created, snapshot profiles cannot be edited, and the volume does not adhere to storage profiles. After the import is complete, clear the **Import To Lowest Tier** check box to avoid potential performance degradation caused by writing to the lowest tier of drives. New writes from a host to the volume will follow the Storage Profile for the volume after the **Import To Lowest Tier** check box is cleared.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume to modify.
4. In the right pane, click **Edit Settings**.
   The **Edit Volume Settings** dialog box appears.
5. Click **Edit Advanced Volume Settings**.
   The **Edit Advanced Volume Settings** dialog box appears.
6. Select the **Import to lowest tier** checkbox.
7. Click **OK**.

Associate a Chargeback Department with a Volume

If Chargeback is enabled, you can assign a Chargeback Department to the volume to make sure the department is charged for the storage used by the volume.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the volume you want to modify.
5. In the right pane, click **Edit Settings**. The **Edit Volume** dialog box appears.
6. Next to **Chargeback Department**, click **Change**. The Add Chargeback Department dialog box appears.
7. Select the appropriate department, then click **OK**.
8. Click **OK** to close the **Edit Volume** dialog box.

Configure a Space Consumption Limit for a Volume

Set a space consumption limit to specify the maximum space that can be used on the volume. This option is not available for SCv2000 or SCv3000 series storage systems.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the right pane, click **Edit Settings**. The **Edit Volume** dialog box appears.
3. Configure the **Space Consumption Limit** options.
   a. Select **Enabled**.
   b. In the field, type the maximum space that can be used on the volume in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).
4. Click **OK** to close the **Edit Advanced Volume Settings** dialog box, then click **OK** to close the **Edit Volume** dialog box.

Configure an OpenVMS Unique Disk ID for a Volume

Configure an OpenVMS Unique Disk ID to identify the volume to servers running the OpenVMS operating system. You may need to reset this value when recovering a volume from a snapshot. For example, if you map a volume to a server, create a snapshot, and then mount a new view volume to the server, the new view volume has a new disk ID. To allow the server to recognize it as the same volume, you must modify the disk ID to match the original value.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to modify.
4. In the right pane, click **Edit Settings**. The **Edit Volume** dialog box appears.

5. Click **Edit Advanced Volume Settings**. The **Edit Advanced Volume Settings** dialog box appears.
6. In the **OpenVMS Unique Disk ID** field, type a new disk ID.
7. Click **OK** to close the **Edit Advanced Volume Settings** dialog box, then click **OK** to close the **Edit Volume** dialog box.

Configure Related View Volume Maximums for a Volume

For a given volume, you can configure the maximum number of view volumes, including the original volume, that can be created for volumes that share the same snapshot. You can also configure the maximum combined size for these volumes.

Prerequisites

Consult with technical support before changing these limits.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to modify.
4. In the right pane, click **Edit Settings**. The **Edit Volume** dialog box appears.
5. Click **Edit Advanced Volume Settings**. The **Edit Advanced Volume Settings** dialog box appears.
6. In the **Maximum Volume Count** field, type the maximum number of view volumes, including the original volume, that can be created for volumes that share the same snapshot history as this volume.
7. Click **OK** to close the **Edit Advanced Volume Settings** dialog box, then click **OK** to close the **Edit Volume** dialog box.

Copying Volumes

Copy a volume to create an identical volume for back-up or reuse of the data.

The destination volume of a copy, mirror, or migrate must meet the following requirements:

- Must not be mapped to a server.
- Must be the same size or larger than the source volume.
- Cannot be active on another controller.

Copy a Volume

Copying a volume copies the data from a source volume to a destination volume. Changes made to the source volume during the copy process are also made to the destination volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select a volume.
4. In the right pane, select **Local Copy** > **Copy Volume**. The **Copy Volume** dialog box opens.
5. Select an existing volume or create a new volume for the destination volume.
   - To select an existing volume, select a volume from the **Destination Volume** table.
   - To create a new volume for the destination volume, click **Create Volume**.
6. (Optional) Select **Copy Snapshots**.
7. From the **Priority** drop-down menu, select a priority level for the copy operation.
8. (Optional) Select **Schedule Start Time** to set a time for the copy to be created.
9. Click **OK**.

Related tasks

Create a Volume Using Single-Step Dialog on page 98
Creating Volumes on page 98

Create a Mirroring Volume

A mirroring volume is a copy of a volume that also dynamically changes to match the source volume. The source and destination volumes are continuously synchronized.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select a volume.
4. In the right pane, select **Local Copy** > **Mirror Volume**.
   The **Mirror Volume** dialog box opens.
5. Select an existing volume or create a new volume for the destination volume.
   - To select an existing volume, select a volume from the **Destination Volume** table.
   - To create a new volume for the destination volume, click **Create Volume**.
6. (Optional) Select **Copy Snapshots**.
7. From the **Priority** drop-down menu, select a priority level for the copy operation.
8. (Optional) Select **Schedule Start Time** to set a time for the copy to be created.
9. Click **OK**.

Related tasks

Create a Volume Using Single-Step Dialog on page 98
Creating Volumes on page 98

Migrate a Volume

Migrating a volume copies a source volume with its server–to–volume mappings to a destination volume. After migrating the volume, the destination volume is mapped to all servers previously mapped to the source volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select a volume.
4. In the right pane, select **Local Copy** > **Migrate Volume**.
   The **Migrate Volume** dialog box opens.
5. Select an existing volume or create a new volume for the destination volume.
   - To select an existing volume, select a volume from the **Destination Volume** table.
   - To create a new volume for the destination volume, click **Create Volume**.
6. (Optional) Click **Copy Snapshots** to also copy the snapshots from the source volume.
7. From the **Priority** drop-down menu, select a priority level for the copy operation.
8. (Optional) Select a post-migrate action.
   - **Do Nothing** – Migrates the volume without any post-migration actions
   - **Delete Source** – Deletes the source volume after migrating
   - **Reverse Mirror** – Mirrors the destination volume to the source volume
9. (Optional) Select **Schedule Start Time** to set a time for the copy to be created.
10. Click **OK**.

Related tasks

Create a Volume Using Single-Step Dialog on page 98
Creating Volumes on page 98

View Copy/Mirror/Migrate Information

The Summary tab displays information for any copy, mirror, or migrate relationship involving the selected volume. Copy and migrate information is displayed in the Summary tab only during the copy or migrate operation.

Prerequisites

The volume must be in a copy, mirror, or migrate relationship.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation pane, select a volume.
   The **Copy/Mirror/Migrate** area in the Volume **Summary** tab displays information for any copy, mirror, or migrate relationship involving the selected volume.

Change the Priority of a Copy, Mirror, or Migrate Operation

The priority of a copy, mirror, or migrate operation determines the importance of the operation and determines when the operation will take place in relation to other copy, mirror, or migrate operations.

Prerequisites

The volume must be a source volume in a copy, mirror, or migrate operation.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select a source volume currently in a copy, mirror, or migrate relationship.
4. In the **Copy/Mirror/Migrate** area, right-click a copy, mirror, or migrate relationship.
5. Click **Set Priority**.
   The **Set Priority** dialog box appears.
6. From the **Priority** drop-down menu, select a priority.
7. Click **OK**.

Delete a Copy, Mirror or Migrate Relationship

Delete a copy, mirror, or migrate relationship to prevent the source volume from copying to the destination volume. Deleting a relationship deletes the relationship from the source and destination volumes.

Prerequisites

The volume must be involved in a copy, mirror, or migrate relationship.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select a volume.
4. From the **Copy/Mirror/Migrate** table, select a copy, mirror, or migrate relationship.
5. Click **Delete Copy/Mirror/Migrate**.
   The **Delete** confirmation dialog box appears.
6. Click **OK**.

Migrating Volumes With Live Migrate

Live Migration moves a volume from one Storage Center to another Storage Center with no down time.

Live Migration Requirements

To create Live Migrations, the requirements listed in the following table must be met:

Requirement	Description
Storage Center version	The source and destination Storage Centers must be running version 7.1 or later. **NOTE:** Dell recommends that both Storage Centers run the same version of Storage Center software.
Storage Center license	No additional license is necessary.
Storage Manager configuration	The source and destination Storage Centers must be added to Storage Manager.
Storage Center communication	The source and destination Storage Centers must be connected using Fibre Channel or iSCSI, and each Storage Center must be defined on the other Storage Center. • On the source Storage Center, the destination Storage Center must be defined as a remote Storage Center. • On the destination Storage Center, the source Storage Center must be defined as a remote Storage Center.
Replication QoS definitions	Replication Quality of Service (QoS) definitions must be defined on the source Storage Center.
Server	• The source and destination Storage Centers must be mapped to a server. • MPIO must be enabled on the destination server to prevent I/O interruption during a Live Migration.

Live Migration Roles

Live Migrations have two roles: source and destination. These roles determine the active volume that is servicing I/O. The roles can be swapped one time, either automatically or manually.

In the following examples, the server sends an I/O request that modifies the source volume. The changes to the source volume are replicated to the destination Storage Center over Fibre Channel or iSCSI.

Before Live Migration

Before a Live Migration, the server sends I/O requests only to the volume to be migrated.

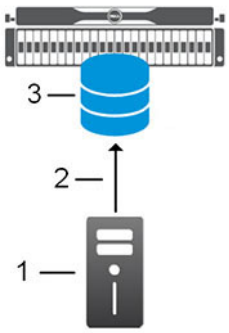


Figure 11. Example of Configuration Before Live Migration

1. Server
2. Server I/O request to volume over Fibre Channel or iSCSI
3. Volume to be migrated

Live Migration Before Swap Role

In the following diagram, the source Storage Center is on the left and the destination Storage Center is on the right.

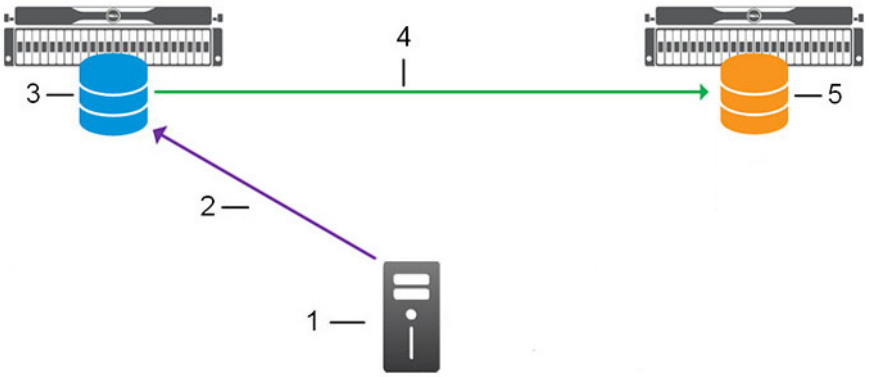


Figure 12. Example of Live Migration Configuration Before Swap Role

1. Server
2. Server I/O request to destination volume (forwarded to source Storage Center by destination Storage Center)
3. Source volume
4. Replication over Fibre Channel or iSCSI
5. Destination volume

Live Migration After Swap Role

In the following diagram, a role swap has occurred. The destination Storage Center is on the left and the new source Storage Center is on the right.

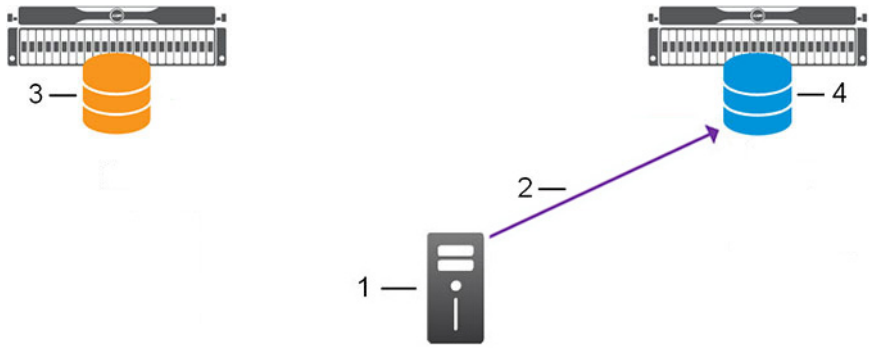


Figure 13. Example of Live Migration Configuration After Swap Role

1. Server
2. Server I/O request to destination volume (forwarded to source Storage Center by destination Storage Center)
3. Destination volume
4. New source volume

Live Migration After Complete

In the following diagram, the Live Migration is complete. The server sends I/O requests only to the migrated volume.

Figure 14. Example of Live Migration Configuration After Complete

1. Server
2. Old destination volume
3. Migrated volume
4. Server I/O request to migrated volume over Fibre Channel or iSCSI

Creating a Live Migration

Create a Live Migration to move a volume to another Storage Center without any down time.

NOTE: For user interface reference information, click **Help**.

Create a Live Migration for a Single Volume

Use Live Migration to move a volume from one Storage Center to another Storage Center with limited or no downtime.

Prerequisites

- The volume to be migrated must be mapped to a server.
- The volume cannot be part of a replication, Live Volume, or Live Migration.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation tree, select the volume.
4. In the right pane, click **Live Migrate Volume**.
   - If one or more Replication Quality of Service (QoS) definitions exist on the source Storage Center, the **Create Live Migration** wizard opens.
   - If a Replication QoS definition has not been created, the **Create Replication QoS** wizard opens. Use this wizard to create a QoS definition before you create a live migration for the volume.
5. Select a destination Storage Center for the live migration, then click **Next**.

   NOTE: If Fibre Channel or iSCSI connectivity is not configured between the local and remote Storage Centers, a dialog box opens. Click **Yes** to configure iSCSI connectivity between the Storage Centers.

6. (Optional) Modify Live Migration default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volume and map the destination volume to a server.
   - In the **Live Migration Attributes** area, enable or disable automatic role swap. When automatic role swap is enabled, Live Migrate swaps the roles immediately after the volume is synced. When it is disabled, you may swap the roles manually any time after the volume is synced.
7. Click **Create**.
   Live Migration begins to migrate the volume to the destination Storage Center.

Create a Live Migration for Multiple Volumes

Use Live Migration to move multiple volumes from one Storage Center to another Storage Center with limited or no downtime.

Prerequisites

- The volumes to be migrated must be mapped to a server.
- The volumes cannot be part of a replication, Live Volume, or Live Migration.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the **Volumes** node or the volume folder that contains the volumes.
4. In the right pane, select the volumes that you want to migrate.
5. Right-click the volumes, and then select **Live Migrate Volume**.
   - If one or more Replication Quality of Service (QoS) definitions exist on the source Storage Center, the **Create Live Migration** wizard opens.
   - If a Replication QoS definition has not been created, the **Create Replication QoS** wizard opens. Use this wizard to create a QoS definition before you create a live migration for the volume.
6. Select a destination Storage Center for the live migration, then click **Next**.

   NOTE: If Fibre Channel or iSCSI connectivity is not configured between the local and remote Storage Centers, a dialog box opens. Click **Yes** to configure iSCSI connectivity between the Storage Centers.

7. (Optional) Modify Live Migration default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volume and map the destination volume to a server.
   - In the **Live Migration Attributes** area, enable or disable automatic role swap. When automatic role swap is enabled, Live Migrate swaps the roles immediately after the volume is synced. When it is disabled, you may swap the roles manually any time after the volume is synced.
8. Click **Next**.
9. Verify the volumes and attributes for the Live Migration. To change any of the attributes, select a volume and then click **Edit Settings**.
10. Click **Create**.
    Live Migration begins to migrate the volumes to the destination Storage Center.

Modifying Live Migrations

Modify a Live Migration if you want to swap the source Storage Center, change Live Migration properties, or delete the Live Migration.

Swap the Source Storage Center for a Live Migration

If you did not elect to swap roles automatically, you must swap roles before completing a Live Migration.

Prerequisites

The Live Migration must be in the Ready to Be Swapped state.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Migrations** tab, select the Live Migration you want to modify, and then click **Swap Source Storage Center**.
   The **Swap Source Storage Center** dialog box opens.
3. Click **OK** to swap the source Storage Center for the Live Migration.

Cancel a Live Migration Source Storage Center Swap

Cancel a swap of the source Storage Center to keep the current source and destination Storage Center.

Prerequisites

The Live Migration must be in the Swapping state.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Migrations** tab, select the Live Migration whose swap you want to cancel, and then click **Cancel Swap of Source Storage Center**.
   The **Cancel Swap of Source Storage Center** dialog box opens.
3. Click **OK**.
   The swap is cancelled.
   NOTE: If the swap has completed, an error message displays. Click **OK**.

Allow a Live Migration to Automatically Swap Roles

Live Migrations can be configured to swap source and destination volumes automatically when the volumes are in sync.

Prerequisites

The Live Migration must be in the Syncing or Ready to Be Swapped state.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Migrations** tab, select the Live Migration you want to modify, and then click **Edit Settings**.
   The **Edit Live Migration** dialog box opens.
3. Select the **Automatically Swap Roles After In Sync** checkbox, and then click **OK**.

Complete a Live Migration

Complete a Live Migration to stop server I/O requests to the old source Storage Center and send all I/O requests only to the destination Storage Center. The old destination Storage Center is now the new source Storage Center. You can complete a single Live Migration or multiple Live Migrations at one time.

Prerequisites

- Swap roles must be complete for the Live Migration.
- The Live Migration must be in the Ready to be Completed state.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Migrations** tab, select the Live Migrations you want to complete.
3. Click **Complete**.
   The **Complete Live Migration** dialog box opens.
4. Verify the Live Migrations to complete, and then click **Finish**.
   The Live Migration completes. The server stops sending I/O requests to the volume on the old source Storage Center and the Live Migration is removed from the **Live Migrations** tab. The old source volume receives a new device ID and all mappings are removed.

Enable or Disable Deduplication for a Live Migration

Deduplication reduces the amount of data transferred and enhances the storage efficiency of the remote Storage Center. Deduplication copies only the changed portions of the snapshot history on the source volume, rather than all data captured in each snapshot.

Prerequisites

The Live Migration must be in either the Syncing or the Ready to be Swapped state.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Migrations** tab, select the Live Migration you want to modify, and then click **Edit Settings**.
   The **Edit Live Migration** dialog box opens.
3. Select or clear the **Deduplication** checkbox, then click **OK**.

Change the Source Replication QoS Node for a Live Migration

Select a different QoS node to change how the Live Migration uses bandwidth.

Prerequisites

The Live Migration must be in either the Syncing or the Ready to be Swapped state.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Migrations** tab, select the Live Migration you want to modify, and then click **Edit Settings**.
   The **Edit Live Migration** dialog box opens.

3. From the **Source Replication QoS Node** drop-down menu, select the QoS definition that will be used to control bandwidth usage between the local and remote Storage Centers.
4. Click **OK**.

Delete a Live Migration

Use the Live Migrations tab to delete a Live Migration whose source and destination Storage Center have not been swapped.

Prerequisites

The Live Migration must be in one of the following states:

- Syncing
- Ready to be Swapped
- Error

About this task

NOTE: It is recommended to delete a Live Migration only when both the source and destination Storage Centers show their status as Up and are connected to Dell Storage Manager.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Migrations** tab, select the Live Migration you want to delete.
3. Click **Delete**.
   The **Delete** dialog box opens.
4. Click **OK** to delete the Live Migration.

Viewing Live Migration Volumes

View the source or destination volume of a Live Migration in the Storage tab or IO Usage tab to see more information about the volume.

View the Source Volume of a Live Migration

View more information about the source volume of a Live Migration in the Storage tab or IO Usage tab.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Migrations** tab, select the Live Migration whose source volume you want to view.
3. Click **Source Volume**, then select one of the following options:
   - **Show In Storage Tab** - Displays the source volume in the **Storage** tab.
   - **Show In IO Usage Tab** - Displays the source volume in the **IO Usage** tab.

View the Destination Volume of a Live Migration

View more information about the destination volume of a Live Migration in the Storage tab or IO Usage tab.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Migrations** tab, select the Live Migration whose destination volume you want to view.
3. Click **Destination Volume**, then select one of the following options:
   - **Show In Storage Tab** - Displays the source volume in the **Storage** tab.
   - **Show In IO Usage Tab** - Displays the source volume in the **IO Usage** tab.

Creating and Managing Volume Folders

Use volume folders to organize volumes or to restrict access to volumes.

NOTE: For user interface reference information, click **Help**.

Create a Volume Folder

Create a volume folder either to organize volumes or to restrict access to volumes.

About this task

NOTE:

Members of a user group can only access volume folders that have been assigned to their user group, regardless of how the folders are organized. For example, a sub-folder created with Administrator privileges in a Volume Manager folder will not be visible to a user in the Volume Manager user group.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation pane, select **Volumes**.
3. In the right pane, click **Create Volume Folder**. The **Create Volume Folder** dialog box opens.
4. In the **Name** field, type a name for the folder.
5. In the **Parent** field, select a parent folder.
6. Click **OK**.

Rename a Volume Folder

Use the **Edit Settings** dialog box to rename a volume folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume folder you want to rename.
4. In the right pane, click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. In the **Name** field, type a new name for the volume folder.
6. Click **OK**.

Move a Volume Folder

Use the **Edit Settings** dialog box to move a volume folder. Folders can be nested in other folders.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the right pane, click **Edit Settings**.
   The **Edit Settings** dialog box opens.
4. In the **Parent** field, select the appropriate parent folder.
5. Click **OK**.

Associate a Chargeback Department with a Volume Folder

If Chargeback is enabled, you can assign a Chargeback Department to a folder to make sure the department is charged for the storage used by all volumes in the folder.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the volume folder you want to modify.
5. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
6. Next to **Chargeback Department**, click **Change**. The **Add Chargeback Department** dialog box appears.
7. Select the appropriate department, then click **OK**.
8. Click **OK** to close the **Edit Settings** dialog box.

Creating and Managing Volume Snapshots

Use snapshots to create a point-in-time copy (PITC) of one or more volumes. Creating volumesnapshots allows the volume to take full advantage of data progression.

NOTE: For user interface reference information, click **Help**.

Manually Create a Snapshot for a Volume

Create a manual snapshot to copy data for a point in time if you do not want to create a snapshot schedule.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume.
4. In the right pane, click **Create Snapshot**.
   - The **Create Snapshot** dialog box opens.
   - If the volume is associated with one or more consistent snapshot profiles, a confirmation dialog box opens.
5. If a confirmation dialog box opens:
   - Click **Yes** to create snapshots for all volumes associated with the consistent Snapshot Profile.
   - Click **No** to create a snapshot for the selected volume only.
6. In the **Expire Time** field, type the number of minutes, hours, days, or weeks to keep the snapshot before deleting it. If you do not want the snapshot to expire, select **Do Not Expire**.
7. (Optional) In the **Description** field, type a description of the snapshot. The default descriptive text is "Manually Created."
8. Click **OK**.

View Snapshots on a Volume

Click the **Snapshots** tab to see information about snapshots, such as freeze time, expiration time, size, and description. You can also view the snapshots on a volume in a tree view.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume.
4. In the right pane, click the **Snapshots** tab.
5. Click **Select View** to choose **Table View** or **Tree View**.

- Table View displays all of the information for a snapshot on one screen. This information includes Freeze Time, Expire Time, Size, Create Volume, and Snapshot Profile.
- Tree View displays a single field for each snapshot: Freeze Time, Expire Time, Size, or Description. To change the field displayed, click **Select Display Field** and then select a new field.

Assign Snapshot Profiles to a Volume

Assign one or more snapshot profiles to a volume if you want snapshots to be created on an automated schedule.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. From the **Storage** tab navigation pane, select the volume you want to modify.
4. From the right pane, click **Edit Settings**.
   The **Edit Volume** dialog box opens.
5. Select the appropriate snapshot profiles.
   a. Next to **Snapshot Profiles**, click **Change**. The **Select Snapshot Profiles** dialog box opens.
   b. From the top pane of the dialog box, select the snapshot profiles to assign to the volume.
   c. Click **OK** to close the **Select Snapshot Profiles** dialog box.
6. Click **OK** to close the **Edit Volume** dialog box.

Create a Local Recovery Volume (View Volume) from a Snapshot

Create a recovery volume (view volume) from a snapshot to access data that is contained in the snapshot. A volume created from a snapshot accesses the same data and consumes the same amount of space as the original volume. It will consume more space when new data is written to the new volume.

Prerequisites

QoS Profile options are shown only if **Allow QoS Profile Selection** has been enabled on the Storage Center **Preferences** dialog box.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume.
4. In the right pane, click the **Snapshots** tab.
5. Right-click the snapshot from which you want to create a local recovery volume, then select **Create Volume from Snapshot**. The **Create Volume from Snapshot** dialog box opens.
6. Select the snapshot from which you want to create a local recovery volume, then click **Create Volume from Snapshot**.
   The **Create Volume from Snapshot** dialog box opens.
7. (Optional) Modify default settings for the recovery volume as needed.
   - **Name**—Type a new name for the volume.
   - **Volume Folder**—Select a parent folder for the volume.
   - **Snapshot Profile**—Click **Change** to select snapshot profiles for the volume.
   - **Server**—Click **Change** to select a server to which to map the volume.
   - **Advanced Mapping**—When a server is selected, click **Advanced Mapping** to configure LUN settings, restrict mapping paths, or present the volume as read-only.
   - **Volume QoS Profile**—Click **Change** to select the volume QoS profile to assign to the volume.
8. Click **OK** to create the local recovery volume.

Pause Snapshot Creation for a Volume

Pause snapshot creation for a volume to temporarily prevent snapshot profiles from creating automatic snapshots for the volume. When snapshot creation is paused, the **Create Snapshot** option is not available when you right-click any volume on the Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the Snapshot Profile you want to pause.
4. In the bottom right pane, select the **Volumes** tab.
5. Right-click the volume for which you want to pause snapshot creation. Select **Edit Settings**. The **Edit Volume Settings** dialog box appears.
6. In the **Snapshot Profiles** area, select the **Snapshot Creation Paused** check box.
7. Click **OK**.

Pause Snapshot Expiration for a Volume

Pause snapshot expiration for a volume to temporarily prevent Snapshot Profiles from expiring snapshots for the volume. When snapshot expiration is paused, the **Create Snapshot** and **Delete** options are not available when you right-click any volume on the Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation pane, select the Snapshot Profile you want to pause.
3. In the bottom right pane, select the **Volumes** tab.
4. Right-click the volume for which you want to pause snapshot expiration.
   Select **Edit Settings**. The **Edit Volume Settings** dialog box opens.
5. In the **Snapshot Profiles** area, select the **Snapshot Expiration Paused** check box.
6. Click **OK**.

Allow the Most Recent Snapshot for a Volume to be Expired

If you do not need to keep at least one snapshot for a given volume at all times, you can allow the most recent volume snapshot to be expired by a Snapshot Profile.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation pane, select the volume.
3. In the right pane, click **Edit Settings**.
   The **Edit Volume** dialog box opens.
4. Click **Edit Advanced Volume Settings**.
   The **Edit Advanced Volume Settings** dialog box opens.
5. Select the **Allow Snapshots to coalesce into active Snapshot** checkbox.
6. Click **OK** to close the **Edit Advanced Volume Settings** dialog box.
7. Click **OK** to close the **Edit Volume** dialog box.

Expire a Snapshot Manually

If you no longer need a snapshot and you do not want to wait for it to be expired based on the snapshot profile, you can expire it manually.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to modify.
4. Click the **Storage** tab.
5. In the **Storage** tab navigation pane, select the volume for which you want to expire a snapshot.
6. In the right pane, click the **Snapshots** tab.
7. Right-click the snapshot you want to expire, then select **Expire**. The **Expire** dialog box opens.

   NOTE: To expire multiple snapshots simultaneously, hold down Shift while you select the snapshots, then right-click a selected snapshot and select **Expire**.

8. Select the snapshot you want to expire, then click **Expire**.
   The **Expire** dialog box opens.
9. Click **OK** to expire the selected snapshot.

Related concepts

Managing Snapshot Profiles on page 130

Mapping Volumes to Servers

Mapping a volume to a server allows the server to access the volume.

NOTE: For user interface reference information, click **Help**.

Map a Volume to a Server

Map a volume to a server to allow the server to use the volume for storage.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to map to a server.
4. In the right pane, click **Map Volume to Server**. The **Map Volume to Server** wizard opens.
5. Select the server to which you want to map the volume, then click **Next**. The wizard advances to the next page.
6. (Optional) Click **Advanced Mapping** to configure LUN settings, restrict mapping paths, or present the volume as read-only.
7. Click **Finish**.

Map Multiple Volumes to a Server

Multiple volumes can be mapped to a server in a single operation.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the **Volumes** node or the folder that contains the volumes.
4. In the right pane, select the volumes that you want to map.
   - To select contiguous volumes, select the first volume, then hold down Shift and select the last volume.

- To select individual volumes, hold down Control while selecting them.

5. In the right pane, click **Map Volume to Server**. The **Map Volume to Server** wizard opens.
6. Select the server to which you want to map the volumes, then click **Next**. The wizard advances to the next page.
7. (Optional) Click **Advanced Mapping** to configure LUN settings, restrict mapping paths, or present the volume as read-only.
8. Click **Finish**.

Unmap a Volume from a Server

Unmap a volume from a server if the server no longer needs to access the volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to unmap from a server.
4. In the right pane, click **Remove Mappings**.
   The **Remove Mappings** dialog box opens.
5. Select the server(s) to unmap from the volume, then click **OK**. If the volume is the destination of a replication and you selected the mapping to the source Storage Center, a confirmation dialog box appears.
6. If a confirmation dialog box appears:
   - Click **OK** to remove the mapping to the source Storage Center, which might interfere with the replication.
   - Click **Cancel** to keep the mapping to the source Storage Center.

Unmap Multiple Volumes from Servers

Multiple volumes can be unmapped from servers in a single operation.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the **Volumes** node or the folder that contains the volumes.
4. In the right pane, use shift+click and/or control+click to select multiple volumes.
5. Right-click the selection, then select **Remove Mappings**. The **Remove Mappings** dialog box appears.
6. Select the volume/server mappings to remove, then click **OK**. If a volume is the destination of a replication and you selected the mapping to the source Storage Center, a confirmation dialog box appears.
7. If a confirmation dialog box appears:
   - Click **OK** to remove the mapping to the source Storage Center, which might interfere with the replication.
   - Click **Cancel** to keep the mapping to the source Storage Center.

Promote a Volume Mapping from a Server to a Server Cluster

If a volume is mapped to a server that belongs to a server cluster, you can promote the mapping to the server cluster so that it is mapped on all servers in the cluster.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume.
4. In the right pane, click the **Mappings** tab.
5. In the right pane, select the server for which you want to promote the mapping, then click **Promote to Cluster**.
   The **Promote to Cluster** dialog box appears.
6. Click **OK**.

Demote a Mapping from a Server Cluster to an Individual Server

If a volume is mapped to a server cluster, you can demote the mapping so that it is mapped to one of the servers that belongs to the cluster.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume.
4. In the right pane, click the **Mappings** tab.
5. In the right pane, select the server for which you want to demote the mapping, then click **Demote from Cluster**.
   The **Demote from Cluster** dialog box opens.
6. Click **OK**.

Deploy a Bootable Volume Image to a New Server

Copy a bootable volume image and map it to a new server to streamline the server deployment process.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to copy.
4. In the right pane, click **Create Boot from SAN Copy**.
   The **Create Boot from SAN Copy** dialog box opens.
5. (Optional) Modify default settings for the volume copy as needed.
   - To change the volume name, modify the **Name** field.
   - To change the parent folder for the volume, select a folder in the **Volume Folder** pane.
   - To schedule snapshot creation and expiration for the volume, apply one or more snapshot profiles by clicking **Change** across from **Snapshot Profiles**.
6. Map the recovery volume to the server that will boot from it.
   a. Click **Change** across from **Server**. The **Select Server** dialog box appears.
   b. Select the server, then click **OK**. The **Select Server** dialog box closes.
   c. (Optional) Click **Advanced Mapping** to configure LUN settings, restrict mapping paths, or present the volume as read-only.
7. Click **OK**.

Change the LUN Used by a Volume/Server Mapping

The logical unit number identifies the volume to the server operating system.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume.
4. In the right pane, click the **Mappings** tab.
5. In the right pane, select the server for which you want to modify mapping settings, then click **Edit Settings**.
   The **Edit Settings** wizard opens.
6. Click **Continue**. The wizard advances to the next page.
7. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane of Unisphere Central.
8. From the **STORAGE** menu, click **Volumes**.
   The **Volumes** view is displayed.

9. Configure the LUN settings:
   - To specify a specific LUN number, clear the **Use next available LUN** checkbox, then type the LUN in the **LUN to use when mapping to Volume** field.
   - To assign the next unused LUN for the server, select the **Use next available LUN** checkbox.
   - To make the volume bootable, select the **Map volume using LUN 0** checkbox.
10. Click **OK**.

Specify Which Controller Processes IO for a Volume/Server Mapping

For dual-controller Storage Centers, you can manually specify which controller processes IO for a volume/server mapping. By default, the Storage Center automatically chooses a controller.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume.
4. In the right pane, click the **Mappings** tab.
5. In the right pane, select the server for which you want to modify mapping settings, then click **Edit Settings**. The **Edit Settings** wizard appears.
6. Click **Continue**. The wizard advances to the next page.
7. Clear the **Allow the Storage Center to automatically determine the best Controller to activate Volume on** check box.
8. From the **Activate Volume on Controller** drop-down menu, select the controller that should process IO for the volume/server mapping.
9. When you are finished, click **OK**.

Limit the Number of Paths That Can Be Used for a Volume/Server Mapping

You can specify the maximum number of paths used by servers that support multipath I/O.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation pane, select the volume.
3. In the right pane, click the **Mappings** tab.
4. In the right pane, select the server for which you want to modify mapping settings, then click **Edit Settings**. The **Edit Settings** wizard opens.
5. Click **Continue**. The wizard advances to the next page.
6. Use the arrows next to the **Maximum number of paths per Server** field to increase or decrease the path limit.
7. Click **OK**.

Change a Volume/Server Mapping to Read-Only

To prevent a server from writing to a volume, change the volume/server mapping to read-only.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation pane, select the volume.
3. In the right pane, click the **Mappings** tab.
4. In the right pane, select the server for which you want to modify mapping settings, then click **Edit Settings**. The **Edit Settings** wizard opens.
5. Click **Continue**. The wizard advances to the next page.
6. Select the **The volume should be presented as read-only to the server** checkbox.

7. Click **OK**.

Deleting Volumes and Volume Folders

Delete volumes and volume folders when they are no longer needed.

NOTE: For user interface reference information, click **Help**.

Delete a Volume

A deleted volume is moved to the Recycle Bin by default.

Prerequisites

Delete all associated replications, Live Volumes, or Live Migrations before deleting a volume.

CAUTION: You can recover a deleted volume that has been moved to the Recycle Bin. However, a deleted volume cannot be recovered after the Recycle Bin is emptied.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation pane, select the volume you want to delete.
3. In the right pane, click **Delete**.
   The **Delete** dialog box opens.
   CAUTION: Do not select Skip Recycle Bin and permanently delete volumes unless you want to immediately delete the volume without saving the metadata in the Recycle Bin. This option permanently deletes the volume, preventing you from recovering the data.
4. Click **OK** to delete the volume.
   The volume is marked for deletion and moved to the Recycle Bin.

Restore a Volume from the Recycle Bin

Restore a volume from the Recycle Bin if you need to retain the volume instead of deleting it.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation pane, select the volume in the Recycle Bin that you want to restore.
3. In the right pane, click **Restore Volume**. The volume is moved from the Recycle Bin to its previous location.

Empty the Recycle Bin

Empty the Recycle Bin if you are sure you want to delete the recycled volumes.

About this task

CAUTION: After the Recycle Bin is emptied, data in recycled volumes cannot be recovered.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Volumes** view, expand the **Recycle Bin**.
3. In the right pane, click **Empty Recycle Bin**.
   The **Empty Recycle Bin** dialog box opens.
4. Click **OK** to confirm that you want to permanently delete all volumes in the Recycle Bin.

Delete a Volume Folder

A volume folder must be empty before it can be deleted. If the deleted volumes from the folder are in the Recycle Bin, the volume folder is not considered empty and cannot be deleted.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the volume folder you want to delete.
5. In the right pane, click **Delete**. .
   The **Delete** dialog box opens
6. Click **OK** to delete the folder.

Managing Data Reduction

Data Reduction uses compression and deduplication to decrease the amount of disk space used by volume data.

Compression reduces the amount of space used by a volume by encoding data. Deduplication finds duplicate pages and removes them, conserving the disk space that would be used by additional copies. When deduplication is used, compression is also applied to a volume.

Data Eligible for Data Reduction

To reduce the impact of data reduction on read and write operations, a limited amount of data is eligible for compression and deduplication. Data Reduction Input limits the type of data that is eligible for data reduction. The following options are available for Data Reduction Input:

- **Inaccessible Snapshot Pages** – Allows Data Reduction to process data frozen by a snapshot and made inaccessible by new data written over the original data in the snapshot.
- **All Snapshot Pages** – Allows Data Reduction to process data frozen by a snapshot.

Change the Data Reduction Input

Change the type of data that compression and deduplication reduces.

Prerequisites

Data Reduction must be applied to the volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select a volume.
4. In the right pane, click **Edit Settings**. The **Edit Volume** dialog box opens.
5. Click **Edit Advanced Volume Settings**.
   The **Edit Advanced Volume Settings** dialog box opens.
6. In the **Volumes** view, select the volume you want to modify.
7. From the **Data Reduction Input** drop-down menu, select a Data Reduction input.
   - **Inaccessible Snapshot Pages** – Data frozen by a snapshot that has become inaccessible because other data has been written over it
   - **All Snapshot Pages** – Data frozen by a snapshot
8. Click **OK** to close the **Edit Advanced Volume Settings** dialog box.
9. Click **OK**.

Supported Hardware Platforms

The following controller series support Data Reduction:

- SCv3000 Series (Supports Compression only)
- SC4020
- SC5020
- SC5020F
- SC7020
- SC7020F
- SC8000
- SC9000

Compression

Compression reduces the amount of space used by a volume by encoding data. Compression runs daily with Data Progression. To change the time at which compression runs, reschedule Data Progression. Compression does not run with an on-demand Data Progression.

When compressed data is read, it is temporarily uncompressed in memory until the read is complete. When compression is disabled, pages are permanently uncompressed during the next compression cycle, and the original compressed page is deleted as time and resources permit. When a volume is deleted or a snapshot is coalesced, the related compressed data is also deleted.

Deleted data might create gaps in the compressed page, which can be filled with new compressed data. In addition, compressed pages are defragmented during Data Progression to remove gaps and use space more efficiently.

The Compression Savings amount is determined by comparing the total amount of space saved from all compressed pages to the total amount of used space that is eligible for compression. For example, if compression saves 1 GB on a volume with 10 GB of used space that is eligible for compression, the amount saved is 10 percent.

Apply Data Compression to a Volume

Apply Data Compression to a volume to reduce disk space usage for that volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the right pane, click **Edit Settings**.
   The **Edit Volume** dialog box opens.
4. From the **Data Reduction Profile** drop-down list, select **Compression**.
5. Click **OK**.

Related tasks

Creating Volumes on page 98
Modifying Volumes on page 102

Deduplication

Deduplication reduces the space used by a volume by identifying and deleting duplicate pages. Deduplication requires SSD drives.

Apply Deduplication With Compression to a Volume

Apply Deduplication with Compression to reduce the size of the volume. Deduplication and compression run during daily Data Progression.

Prerequisites

Allow Data Reduction Selection must be enabled in the **Preferences** tab of the **Edit Storage Center Settings** dialog box.

About this task

NOTE: The amount of space saved by Data Reduction is determined by the amount of data eligible for Data Reduction on the volume compared to the total amount of space used by that data on disk after Data Reduction.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select a volume.
4. In the right pane, click **Edit Settings**. .
   The **Edit Volume** dialog box opens
5. From the **Data Reduction Profile** drop-down menu, select **Deduplication with Compression**.

View Amount of Space Saved by Data Reduction

The total amount of space saved by Data Reduction depends on the amount of data eligible for data reduction and the type of data being processed. Certain types of data will be reduced more effectively than others. The amount of volume data eligible for data reduction is determined by the size of the data frozen by snapshots, and the Data Reduction Input setting.

Data Savings Ratios

System Data Reduction Ratio and System Data Efficiency Ratio show the data savings on the Storage Center using the available disk space-saving features.

System Data Reduction Ratio – Ratio that compares the amount of space that would be used by pages that are eligible for compression and deduplication to the amount of space actually used by those pages after Storage Center applies Data Reduction.

System Data Efficiency Ratio – Ratio that indicates the efficiency of compression, deduplication, RAID, and Thin Provisioning

View Amount of Space Saved for a Storage Type

Storage Center determines the total percentage of space saved for all volumes in a storage type by comparing the amount of space processed by Data Reduction to the amount of space used after data reduction.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the Storage tab navigation pane, expand **Storage Types**.
4. Select a Storage Type. The space saved by Data Reduction is displayed at the bottom of the **Summary** tab.
5. Select a storage type.
   The space saved by data reduction is displayed in the **Data Reduction Savings** section.

View Amount of Space Saved by Data Reduction on a Volume

The percentage of space saved by data reduction for a volume is an estimate found by comparing the total amount of space saved by compression and deduplication with the total amount of space processed by data reduction in the volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select a volume.
4. In the right pane, click the **Statistics** tab. The space saved by data reduction on that volume is displayed at the bottom of the **Statistics** tab.

Change the Default Data Reduction Profile

The default Data Reduction profile determines the type of data reduction that is applied to new volumes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**. The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. From the **Data Reduction Profile** drop-down list, select the default profile for new volumes.
   - Select **Compression** to apply compression to new volumes.
   - Select **Deduplication with Compression** to apply deduplication and compression to new volumes.

   NOTE: Selecting the **Allow Data Reduction Selection** checkbox enables users to select the data reduction option to apply to a volume.

Pause or Resume Data Reduction

Pause Data Reduction on a volume to prevent deduplication and/or compression from running during data progression. Pausing Data Reduction on a volume pauses deduplication and/or compression on all view volumes created from the original volume. After pausing Data Reduction, compression and deduplication stop running on new data but the existing data is not uncompressed.

Pause or Resume Data Reduction for a Volume

Pausing Data Reduction for a volume prevents compression and deduplication from happening until Data Reduction is resumed.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand Volumes.
4. Select a volume.
5. In the right pane, click **Edit Settings**.
   The **Edit Volume** dialog box opens.
6. Pause or resume Data Reduction on the volume.
   - To pause Data Reduction, select the **Data Reduction Paused** checkbox.
   - To resume Data Reduction, clear the **Data Reduction Paused** checkbox.
7. Click **OK**.

Pause or Resume Data Reduction for all Volumes

Pausing Data Reduction from the Storage Center Edit Settings dialog box pauses compression and deduplication for all volumes in that Storage Center.

About this task

NOTE: **Pause Data Reduction** cannot be applied to other Storage Centers from the Storage Center **Edit Settings** dialog box using inherit settings.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Storage** tab.
4. Pause or resume Data Reduction.
   - To pause Data Reduction, select the **Pause Data Reduction** checkbox.
   - To resume Data Reduction, clear the **Pause Data Reduction** checkbox.
5. Click **OK**.

Disable Data Reduction for a Volume

Disabling Data Reduction on a volume permanently uncompresses the reduced data starting the next data progression cycle.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the volume you want to modify.
4. In the right pane, click **Edit Settings**.
   The **Edit Volume** dialog box opens.
5. In the **Volumes** view, select the volume you want to modify.
6. From the **Data Reduction Profile** drop-down menu, select **None**.
7. Click **OK**.

Managing Snapshot Profiles

A Snapshot Profile is a collection of rules describing when to take periodic snapshots for one or more volumes and the time at which snapshots are deleted (expired).

A snapshot is a point-in-time copy (PITC) of one or more volumes. Storage Center snapshots differ from traditional snapshots/PITCs because blocks of data or pages are frozen and not copied. No user data is moved, making the process efficient in both time taken to complete the snapshot, and space used by snapshots.

NOTE: If two or more snapshots are scheduled to be created at the same time for a given volume, the Storage Center creates only one snapshot. The snapshot that has the longest expiration time is created, and the other scheduled snapshots are ignored.

Related concepts

Managing Storage Profiles on page 135
Managing QoS Profiles on page 137

Default Snapshot Profiles

By default, Storage Center provides two standard snapshot profiles that cannot be deleted.

- **Daily** – Creates a snapshot every day at 12:01 AM, and expires the snapshot in one week.
- **Sample** – Applies three schedule rules:
  - Creates a snapshot every 12 hours between 12:05 AM and 6 PM, expiring in five days.
  - Creates a snapshot on the first day of every month at 11:30 PM, expiring in 26 weeks.
  - Creates a snapshot every Saturday at 11:30 PM, expiring in 5 weeks.

Consistent and Non-Consistent Snapshot Profiles

When a snapshot is taken for a volume, I/O is halted to allow the operation to take place. A consistent snapshot profile halts I/O to all associated volumes until a snapshot is taken for each volume, ensuring that the snapshots contain data for the same time period. A non-consistent snapshot profile creates snapshots for associated volumes without guaranteeing that the snapshots will finish at the same time, which is less resource intensive.

Consistent Snapshot Profile	Non-Consistent Snapshot Profile
Halts I/O across all volumes as a group	Halts I/O for each volume independently of other volumes.
Resource intensive	Less resource intensive — depends on the amount of data written since the previous snapshot
Number of volumes limited based on storage controller. ● SC8000, SC9000, SC7020, and SC7020F: 100 ● SC5020 and SC5020F: 50 ● SC4020: 40 ● SCv2000 and SCv3000 series: 25	No limit to the number of volumes to which the snapshot profile is attached
Snapshots are taken of all volumes simultaneously	Choose between standard (one volume at a time) or parallel (all volumes simultaneously)
Can set an alert if snapshots cannot be completed within a defined time. Snapshots not completed before alert is generated are not taken. (This suspension can lead to incomplete groups of snapshots across volumes.)	All snapshots are taken
Can delete incomplete group of snapshots	All snapshots are taken
Can be converted to Non-Consistent snapshot profile	Can be converted to Consistent snapshot profile

Creating and Applying Snapshot Profiles

To create and expire snapshots automatically, create a snapshot profile and apply it to one or more volumes or servers.

NOTE: For user interface reference information, click **Help**.

Create a Snapshot Profile

Create a Snapshot Profile to define automated snapshot creation and expiration schedules that can be applied to volumes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Snapshot Profiles**.
4. In the right pane, click **Create Snapshot Profile**.
   The **Create Snapshot Profile** dialog box opens.
5. In the **Name** field, type a name for the snapshot profile.

6. Add a rule to the Snapshot Profile.
   a. Click **Add Rule**. The **Add Rule** dialog box opens.
   b. From the drop-down menu, select the frequency at which the rule runs.
   c. Configure the dates and times at which you want snapshots to be created.
   d. In the **Expiration** field, type the length of time to keep snapshots before deleting them.
   e. Click **OK**. The **Add Rule** dialog box closes.
7. (Optional) Create additional rules as necessary.
8. From the **Snapshot Creation Method** drop-down menu, select an option to control how snapshots triggered by the snapshot profile are created.
   - **Standard** – When selected, takes snapshots in series for all volumes associated with the snapshot.
   - **Parallel** – When selected, takes snapshots simultaneously for all volumes associated with the snapshot.
   - **Consistent** – When selected, halts I/O and takes snapshots for all volumes associated with the snapshot. Provides options for timing out snapshot creation and expiring incomplete snapshots.
9. Click **OK**.

Apply a Snapshot Profile to One or More Volumes

To add snapshot creation and expiration schedules to a volume, associate a snapshot profile with the volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the Snapshot Profile.
4. In the right pane, click **Apply to Volumes**. The **Apply to Volumes** dialog box opens.
5. Select the volumes to which you want to apply the snapshot profile. To select individual volumes in a volume folder, expand the folder and select each volume individually.
6. (Optional) To remove existing snapshot profiles from the selected volumes, select **Replace existing Snapshot Profiles**.
7. Click **OK**.

Apply a Snapshot Profile to a Server

To add snapshot creation and expiration schedules to all volumes mapped to a server, associate a Snapshot Profile with the server.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the Snapshot Profile.
4. In the right pane, click **Apply to Server**.
   The **Apply to Server** dialog box opens.
5. Select the server to which you want to apply the Snapshot Profile. To select individual servers in a server cluster, expand the cluster and select each server individually.

   NOTE: If you apply a Snapshot Profile to a server cluster, the Snapshot Profile is applied only to the volumes that are mapped directly to the server cluster. Volumes that are mapped exclusively to servers that belong to the cluster are not affected.

6. (Optional) To remove existing Snapshot Profiles from the selected server, select **Replace existing Snapshot Profiles**.
7. Click **OK**.

Create a Snapshot for all Volumes Associated with a Snapshot Profile

You can create a snapshot for all volumes associated with a Snapshot Profile instead of manually creating a snapshot for each volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the Snapshot Profile.
4. In the right pane, click **Create Snapshot**.
   The **Create Snapshot** dialog box opens.
5. Click **New Snapshot**.
   The **New Snapshot** dialog box opens.
6. In the **Expire Time** field, type the number of minutes, hours, days, or weeks to keep the snapshot before deleting it. If you do not want the snapshot to expire, select **Do Not Expire**.
7. (Optional) In the **Description** field, type a description of the snapshot. The default descriptive text is "Manually Created."
8. Click **OK**.

Modifying Snapshot Profiles

Modify a snapshot profile to change the automated snapshot creation and expiration schedules that are applied to the associated volumes. Changes to a snapshot profile affect only new snapshots taken with the modified snapshot profile. Existing snapshots are not changed.

NOTE: For user interface reference information, click **Help**.

Rename a Snapshot Profile

Use the Edit Snapshot Profile dialog box to rename a snapshotprofile.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the snapshotprofile that you want to modify.
4. In the right pane, click **Edit Settings**.
   The **Edit Snapshot Profile** dialog box opens.
5. In the **Name** field, type a new name for the snapshotprofile.
6. Click **OK**.

Modify Rules for a Snapshot Profile

Snapshot Profile rules determine when snapshots are created and expired.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the Snapshot Profile that you want to modify.
4. In the right pane, click **Edit Settings**.
   The **Edit Snapshot Profile** dialog box opens.
5. (Optional) Add a rule to the snapshot profile.
   a. Click **Add Rule**. The **Add Rule** dialog box appears.
   b. From the drop-down menu, select the frequency at which the rule runs.
   c. Configure the dates and times at which you want snapshots to be created.

d. In the **Expiration** field, type the length of time to keep snapshots before deleting them.
e. Click **OK**.

6. (Optional) Modify the existing rules as needed.
   - To modify a rule, select the rule, then click **Edit Rule**.
   - To remove a rule, select the rule, then click **Remove Rule**.
7. Click **OK**.

Change the Snapshot Creation Method for a Snapshot Profile

The snapshot creation method controls how snapshots triggered by the snapshotprofile are created.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the Snapshot Profile that you want to modify.
4. In the right pane, click **Edit Settings**.
   The **Edit Snapshot Profile** dialog box opens.
5. From the **Snapshot Creation Method** drop-down menu, select an option to control how snapshots triggered by the snapshotprofile are created.
   - **Standard** – When selected, takes snapshots in series for all volumes associated with the snapshot.
   - **Parallel** – When selected, takes snapshots simultaneously for all volumes associated with the snapshot.
   - **Consistent** – When selected, halts I/O and takes snapshots for all volumes associated with the snapshot. Provides options for timing out snapshot creation and expiring incomplete snapshots.
6. Click **OK**.

Delete a Snapshot Profile

A snapshot profile cannot be deleted if it is being used by any volumes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the Snapshot Profile.
4. Make sure the snapshot profile is not in use by any volumes.
5. In the right pane, click **Delete**.
   The **Delete** dialog box opens.
6. Click **OK**.

Managing Expiration Rules for Remote Snapshots

By default, snapshot profiles applied to remote volumes have the same rules for expiration as for local volumes. However, you can specify different expiration rules for remote volumes if needed.

NOTE: For user interface reference information, click **Help**.

Create Snapshot Profile Expiration Rules for Remote Snapshots

Create remote expiration rules for a snapshot profile if you want the remote snapshots to expire on a different schedule than the local snapshots.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.

2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the Snapshot Profile.
4. In the **Schedule Rules** pane, right-click the schedule and select **Edit Remote Snapshot Expiration**.
   The **Edit Remote Snapshot Expiration** dialog box opens.
5. Configure the remote snapshot expiration rule.
   a. Select one or more Storage Centers for which you want to specify an expiration rule for remote snapshots.
   b. In the **Remote Expiration** field, specify the number of minutes, hours, days, or weeks to keep the remote snapshot before deleting it.
   c. Click **OK**.

Modify a Snapshot Profile Expiration Rule for Remote Snapshots

Modify a remote expiration rule for a snapshot profile to change the time at which remote snapshots are expired.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the Snapshot Profile.
4. In the right pane, click the **Remote Expiration Rules** tab.
5. Right-click the remote expiration rule to modify and select **Edit Remote Snapshot Expiration**.
   The **Edit Remote Snapshot Expiration** dialog box opens.
6. Configure the remote snapshot expiration rule.
   a. In the **Remote Expiration** field, specify the number of minutes, hours, days, or weeks to keep the remote snapshot before deleting it.
   b. Click **OK**.

Managing Storage Profiles

Storage Profiles determine the RAID level and tiers on which data is stored.

NOTE: For user interface reference information, click **Help**.

Related concepts

Managing Snapshot Profiles on page 130
Managing QoS Profiles on page 137

Create a Storage Profile (Storage Center 7.2.1 and Earlier)

Create a storage profile to specify custom RAID level and tier settings that can be applied to one or more volumes.

Prerequisites

In the Storage Center User Volume Defaults, the **Allow Storage Profile selection** checkbox must be selected.

About this task

NOTE: SCv2000 series controllers cannot create storage profiles.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the **Storage Profiles** node.
4. In the right pane, click **Create Storage Profile**.

The **Create Storage Profile** dialog box opens.

5. Configure the storage profile.
   a. Type a name for the storage profile in the **Name** field.
   b. Select the RAID levels to use for volumes associated with the storage profile from the **RAID Type Used** drop-down menu.
   c. In the **Storage Tiers** area, select the checkboxes of the storage tiers (disk classes) that can be used for volumes associated with the storage profile.
6. Click **OK**.

Create a Storage Profile (Storage Center 7.2.10 and Later)

Create a storage profile to specify custom RAID level and tier settings that can be applied to one or more volumes.

Prerequisites

In the Storage Center User Volume Defaults area, the **Allow Storage Profile selection** checkbox must be selected.

About this task

NOTE: SCv2000 series storage systems cannot create Storage Profiles.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the **Storage Profiles** node.
4. In the right pane, click **Create Storage Profile**.
   The **Create Storage Profile** dialog box opens.
5. Configure the storage profile.
   a. Type a name for the storage profile in the **Name** field.
   b. Select the storage tier (disk class) that will be used for data writes for volumes associated with the storage profile from the **Write Tier** drop-down menu.
   c. Select the RAID level to use for volumes associated with the storage profile from the **Write RAID Type** drop-down menu.
   d. Select the RAID level to use for snapshot data in tier 1 from the **Tier 1 Snapshot RAID Type** drop-down menu.
   e. Select the RAID level to use for snapshot data in tier 2 from the **Tier 2 Snapshot RAID Type** drop-down menu.
   f. Select the RAID level to use for snapshot data in tier 3 from the **Tier 3 Snapshot RAID Type** drop-down menu.
6. Click **OK**.

Apply a Storage Profile to One or More Volumes

Apply a storage profile to a volume to specify the RAID level and tiers used by the volume.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the storage profile to apply to a volume.
4. In the right pane, click **Apply to Volumes**.
   The **Apply to Volumes** dialog box opens.
5. Select the volumes to which you want to apply the storage profile.
6. Click **OK**.

Apply a Storage Profile to a Server

Apply a storage profile to a server to specify the RAID level and tiers used by all volumes that are mapped to the server.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the storage profile to apply to a server.
4. In the right pane, click **Apply to Server**.
   The **Apply to Server** dialog box opens.
5. Select the server to which you want to apply the storage profile.
6. Click **OK**.

Delete a Storage Profile

Delete a storage profile if it is no longer needed.

Prerequisites

- The **Allow Storage Profile Selection** checkbox must be selected in the **Configure User Preferences** dialog box of the Storage Center user.
- The storage profile cannot be applied to any volumes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the storage profile.
4. In the right pane, click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK**.

Related concepts

User Interface for Storage Center Management on page 45

Managing QoS Profiles

QoS profiles describe QoS settings that can be applied to volumes.

By defining QoS profiles to apply to volumes, you potentially limit I/Os that the volumes can perform, and also define their relative priority during times of congestion.

You can also define a group QoS profile that can be applied to multiple volumes to limit the I/Os that the volumes can do in aggregate.

Related concepts

Managing Storage Profiles on page 135
Managing Snapshot Profiles on page 130

Create a QoS Profile

QoS profiles include a set of attributes that control the QoS behavior for any volume to which it is applied.

Prerequisites

- To enable users to set QoS profiles for a Storage Center, the **Allow QoS Profile Selection** option must be selected on the Storage Center Preferences settings.
- To enable QoS profiles to be enforced, the **QoS Limits Enabled** and **Server Load Equalizer Enabled** options must be selected on the Storage Center Storage settings.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation tab, right-click **QoS Profiles** and select **Create QoS Profile**.
   The **Create QoS Profiles**. dialog box opens.
3. Configure the QoS profile.
   a. In the **Name** field, type a name for the QoS profile.
   b. Select a profile type: either **Volume QoS Profile** or **Group QoS Profile**.
   c. (Optional for volume QoS profiles only) In the Relative Priority field, type a number to identify the priority compared to other QoS profiles.
   d. (Optional for volume QoS profiles only) Select **Enable Latency Threshold Alert**, then type a latency threshold alert value is ms.
   e. (Optional) Select **Limit by IOPS**, then type a value for the maximum IOPS allowed.
   f. (Optional) Select **Limit by Bandwidth**, then type a value for the maximum MB/sec allowed.
4. Click **OK**.

Edit a QoS Profile

Modify the QoS profile to change the attributes that control the QoS for any volume or group to which it is applied.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation tab, right-click **QoS Profiles** and select **Edit Settings**.
   The **Edit QoS Profile** dialog box opens.
3. Where allowed, modify the values. The profile type field cannot be modified.
4. Click **OK**.

Delete a QoS Volume Profile

Delete a QoS profile for a volume.

Prerequisites

Only QoS profiles that are not currently in use by any volume can be deleted. The Default QoS Volume profile cannot be deleted even if there are no volumes assigned to it. Group QoS Profiles can be removed or reassigned; however, Volume QoS profiles can be reassigned only.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Storage** tab navigation tab, expand **QoS Profiles** and select the profile to be deleted.
3. Right-click the profile and select **Delete**.
   A confirmation dialog box opens to request approval for the deletion.
4. Click **OK**.

Apply a QoS Profile to a Volume

Apply a previously defined QoS profile to a volume.

Prerequisites

The QoS profile must already exist.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Expand the **QoS Profiles** navigation tree. Right-click the name of the QoS profile.
3. Select **Apply to Volumes**.
   The **Apply to Volumes** dialog box opens.
4. Select the checkbox next to each volume to which you want to apply the QoS profile.
5. Click **OK**.

Remove a Group QoS Profile From a Volume

Remove a Group QoS profile previously associated with one or more volumes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Expand the **QoS Profile** navigation tree and then expand the **Group QoS Profiles** navigation tree.
3. Right-click the Group QoS profile to be removed and select **Remove Group Profile from Volume**.
   A dialog box opens to show the volumes associated with the QoS profile.
4. Select the checkbox next to each volume from which you want to remove the QoS profile.
5. Click **OK**.

Importing Volumes from an External Storage Array

Storage Center can import volumes from an EqualLogic PS Series Storage Array or an MD Series Storage Array. There are two methods for importing data from an external device, offline and online.

- Offline import migrates a Volume from the source to the destination. The volume must then be mapped to the server after the import.
- Online import creates a destination volume, maps it to the server, then migrates the data to the destination volume. I/O from the server continues to both the destination and source volumes during the import process. Importing using the Online method can take longer than offline due to I/O continuing to the volume from the server.

Connect to an External Storage Array (iSCSI)

After cabling an external device to Storage Center using iSCSI, configure Storage Center to communicate with the external device.

Prerequisites

The external device must be connected to the controller using iSCSI.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. From the **Storage** tab navigation pane, select an iSCSI fault domain from the **Fault Domains** node.
4. Click **Create Remote Connection**.
   The **Configure iSCSI Connection** dialog box opens.

5. In the **Remote IPv4 Address** field, type the IPv4 address of the external device.
6. From the **iSCSI Network Type** drop-down menu, select the speed of the iSCSI network.
7. Click **Finish**.
   A confirmation dialog box appears.
8. Click **OK**.

PS Series Storage Array Import Requirements

A PS Series storage array must meet the following requirements to import data to a Storage Center storage system.

Component	Requirement
PS Series Firmware	Version 6.0.11 or higher
Connectivity	iSCSI
Network	Low-Latency, High-Bandwidth
Volume Settings	• Limit access to the volume by Storage Center IP or iSCSI initiator name. • Enable **Allow simultaneous connections from initiators with different IQNs** in the volume advanced settings. • Stop all IO from the server to the volume.

Storage Center Import Requirements

A Storage Center storage system must meet the following requirements to import data from a PS Series storage array.

Component	Requirement
Storage Center	Version 7.1 or later
Connectivity	iSCSI
Network	Low-latency, high-bandwidth

MD Series Import Requirements

A PowerVault MD Series must meet the following requirements to import data to a Storage Center storage system.

Component	Requirement
Hardware Platforms	MD3 series
Firmware Version	08.25.09

Supported Server Operating Systems for Online Import

Performing an online import of volumes from a PS Series storage array requires one of the following server operating systems:

- Red Hat Enterprise Linux 6.7
- Red Hat Enterprise Linux 7
- SUSE Linux Enterprise 11 or 12
- Oracle Linux 6.5
- Oracle Linux 7.0
- VMware ESXi 5.5 or later
- Windows Server 2008 R2 or later

Import Data from an External Device (Offline)

Importing data from an external device copies data from the external device to a new destination volume in Storage Center. Complete the following task to import data from an external device.

Prerequisites

- An external device must be connected into the Storage Center.
- The destination volume must be unmapped from the server.

About this task

NOTE: Before importing data from an external device, review *Data Migration from Dell PS Series or PowerVault MD3 to Dell EMC SC Series Storage using Thin Import* located in the Dell Knowledge Base.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. From the **External Devices** node in the **Storage** tab navigation pane, select an external device.
4. Click **Offline Import From External Device**.
   The **Offline Import From External Device** dialog box opens.
5. Modify the **Destination Volume Attributes** as needed.

   NOTE: For more information, click **Help**.

6. (Optional) Create a new Replication quality of service (QoS) definition.
   a. Click **Create QoS Node**.
      The **Create Replication QoS** dialog box appears.
   b. In the **Name** field, type a name for the QoS definition.
   c. In the **Link Speed** field, specify the speed of the link in megabits per second (Mbps) or gigabits per second (Gbps).
   d. Select the **Bandwidth Limited** check box, then click **Finish**.
7. Click **OK**.

Related concepts

Managing Volumes on page 97

Related tasks

Create a Storage Profile (Storage Center 7.2.1 and Earlier) on page 135
Create a Snapshot Profile on page 131
Create a QoS Definition on page 497

Import Data from an External Device (Online)

To import data from an external device in online mode, create a destination volume on the Storage Center and map it to the server. I/O from the server continues to both the destination and source volumes during the import. Importing using the Online method can take longer than offline due to I/O continuing to the volume from the server.

Prerequisites

- An external device must be connected into the Storage Center.
- The destination volume must be unmapped from the server.

About this task

NOTE: Before importing data from an external device, follow the instructions in the *Thin Import Data Migration Guide* located on Dell TechCenter.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. From the **External Devices** node in the **Storage** tab navigation pane, select an external device.
4. Click **Online Import from External Device**.
   The **Online Import from External Device** dialog box opens.
5. Modify the **Destination Volume Attributes** as needed.

   NOTE: For more information, click **Help**.

6. From the **Server** drop down box select the server to map to the destination volume.
7. (Optional) Create a new Replication quality of service (QoS) definition.
   a. Click **Create QoS Node**.
      The **Create Replication QoS** dialog box appears.
   b. In the **Name** field, type a name for the QoS definition.
   c. In the **Link Speed** field, specify the speed of the link in megabits per second (Mbps) or gigabits per second (Gbps).
   d. Select the **Bandwidth Limited** check box, then click **Finish**.
8. Click **OK**.

6

Storage Center Server Administration

Storage Manager allows you to allocate storage on a Storage Center to the servers in your SAN environment. Servers that are connected to Storage Centers can also be registered to Storage Manager to streamline storage management.

To present storage to a server, a server object must be added to the Storage Center.

Topics:

- Server Management Options
- Managing Servers on a Storage Center
- Managing Servers Centrally on the Servers View
- Installing and Using the Server Agent on a Windows Server

Server Management Options

To present storage to a server, a corresponding server object must be added to the Storage Center. You can manage servers individually for each Storage Center using Unisphere. You can also manage servers for multiple Storage Centers using Storage Manager.

Managing Storage Center Server Objects

Storage Center server objects are managed individually for each Storage Center from the **Storage** tabon the **Storage** view.Storage Centers have no knowledge about the servers other than the operating system, which must be manually specified.

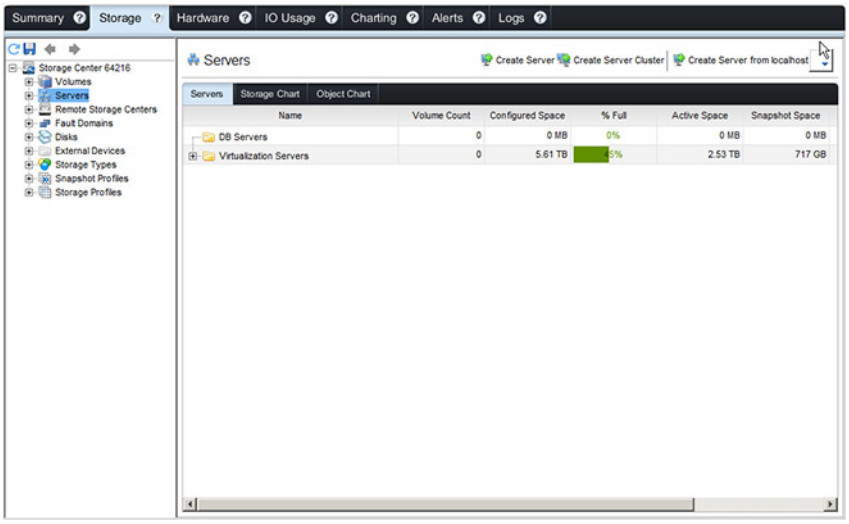


Figure 15. Storage Tab Servers Node

Managing Servers Centrally Using Storage Manager

Servers that are registered to Storage Manager are managed from the **Servers** view. Registered servers are centrally managed regardless of the Storage Centers to which they are connected.

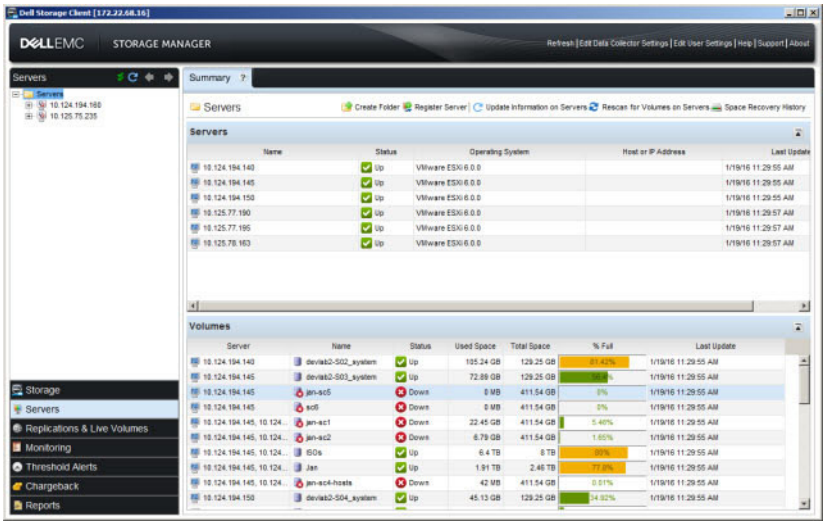


Figure 16. Servers View

The following additional features are available for servers that are registered to Storage Manager:

- Storage Manager gathers operating system and connectivity information from registered servers.
- Storage Manager can automatically add a corresponding Storage Center server object for each registered server.
- Storage Center volumes can be created, mounted, and formatted on the servers directly from the Storage Manager Client.
- When creating a volume for a Windows or VMware server, Storage Manager can recommend a Storage Center to host the volume based on capacity and performance.

Managing Servers on a Storage Center

Use the **Servers** view to create and manage server objects for a Storage Center.

Related concepts

Creating Servers on page 144
Modifying Servers on page 149
Mapping Volumes to Servers on page 152
Creating and Managing Server Folders on page 155
Deleting Servers and Server Folders on page 156

Creating Servers

Create a server to allow a Storage Center to pass I/O through the ports on that server. After a server is created, volumes can be mapped to it.

NOTE: For user interface reference information, click **Help**.

Create a Physical Server

Create a physical server object to represent a physical server in your environment.

Steps

1. Make sure the server HBAs have connectivity to the Storage Center HBAs.

- **iSCSI** – Configure the iSCSI initiator on the server to use the Storage Center HBAs as the target.
- **Fibre Channel** – Configure Fibre Channel zoning to allow the server HBAs and Storage Center HBAs to communicate.
- **SAS** – Directly connect the controller to a server using SAS ports configured as front-end connections.

2. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
3. Click the **Storage** tab.
4. Select **Servers** in the **Storage** tab navigation pane.
5. In the right pane, click **Create Server**.
   The **Create Server** dialog box appears.

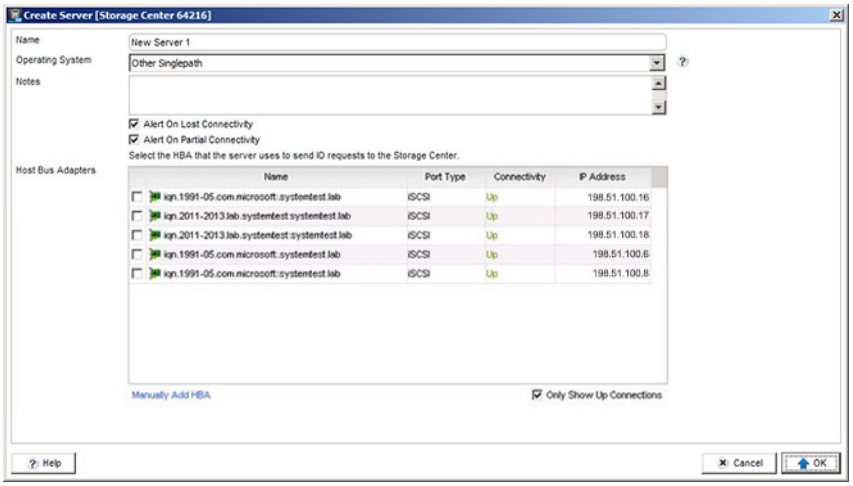


Figure 17. Create Server Dialog Box

6. Configure the server attributes.
   The server attributes are described in the online help.
   a. Enter a name for the server in the **Name** field.
   b. To add the server to a server folder, click **Change**, select a folder, and click **OK**.
   c. Select the operating system for the server from the **Operating System** drop-down menu.
   d. To generate Storage Center alerts when connectivity is lost between the Storage Center and the server, select **Alert On Lost Connectivity**.
   e. To generate Storage Center alerts when the Storage Center only has partial connection to the server, select **Alert On Partial Connectivity**.
   f. Select or define one or more HBAs for the server.
      - If one or more server HBAs are visible to the Storage Center, select the checkboxes of the HBAs to add from the **Host Bus Adapters** table.
      - If a server HBA is not visible to the Storage Center, click **Manually Add HBA** to define it manually. For SAS front-end connections, use the SAS device name as the World Wide Name (WWN) to manually add the HBA.

      NOTE: IP addresses can be added for HBAs that will be installed on the server in the future. When the HBA that uses that IP address is installed, it will be configured and ready to use.

7. Click **OK**.

Related tasks

Configure Front-End I/O Ports (Fibre Channel and SAS) on page 255
Configure Front-End I/O Ports (iSCSI) on page 255

Create a Virtual Server

Create a virtual server object to represent a virtual machine in your environment.

Prerequisites

The server that hosts the virtual server must be added as a physical server.

Steps

1. Make sure the server HBAs have connectivity to the Storage Center HBAs.
   - **iSCSI** – Configure the iSCSI initiator on the server to use the Storage Center HBAs as the target.
   - **Fibre Channel** – Configure Fibre Channel zoning to allow the server HBAs and Storage Center HBAs to communicate.
   - **SAS** – Directly connect the controller to a server using SAS ports configured as front-end connections.
2. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
3. Click the **Storage** tab.
4. Select the server that hosts the virtual server in the **Storage** tab navigation pane.
5. In the right pane, click **Create Virtual Server**.
   The **Create Virtual Server** dialog box opens.

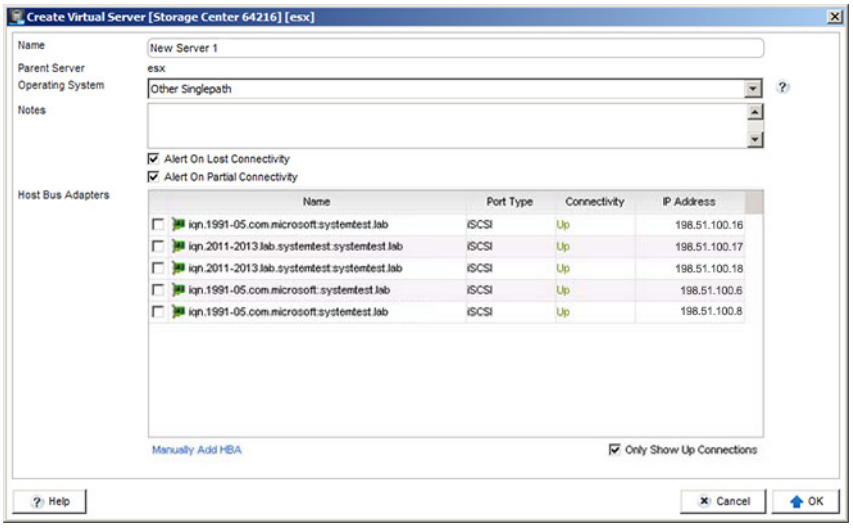


Figure 18. Create Virtual Server Dialog Box

6. Configure the server attributes.
   The server attributes are described in the online help.
   a. Enter a name for the server in the **Name** field.
   b. To add the server to a server folder, click **Change**, select a folder, and click **OK**.
   c. Select the operating system for the server from the **Operating System** drop-down menu.
   d. To generate Storage Center alerts when connectivity is lost between the Storage Center and the server, select **Alert On Lost Connectivity**.
   e. Select or define one or more HBAs for the server.
      - If one or more server HBAs are visible to the Storage Center, select the checkboxes of the HBAs to add from the **Host Bus Adapters** table.
      - If a server HBA is not visible to the Storage Center, click **Manually Add HBA** to define it manually. For SAS front-end connections, use the SAS device name as the World Wide Name (WWN) to manually add the HBA.

      NOTE: IP addresses can be added for HBAs that will be installed on the host server in the future. When the HBA that uses that IP address is installed, it will be configured and ready to use.
7. Click **OK**.

Related tasks

Configure Front-End I/O Ports (Fibre Channel and SAS) on page 255
Configure Front-End I/O Ports (iSCSI) on page 255

Create a Server Cluster

Create a server cluster object to represent a cluster of servers in your environment.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.

2. Click the **Storage** tab.
3. Select **Servers** in the **Storage** tab navigation pane.
4. In the right pane, click **Create Server Cluster**.
   The **Create Server Cluster** dialog box opens.

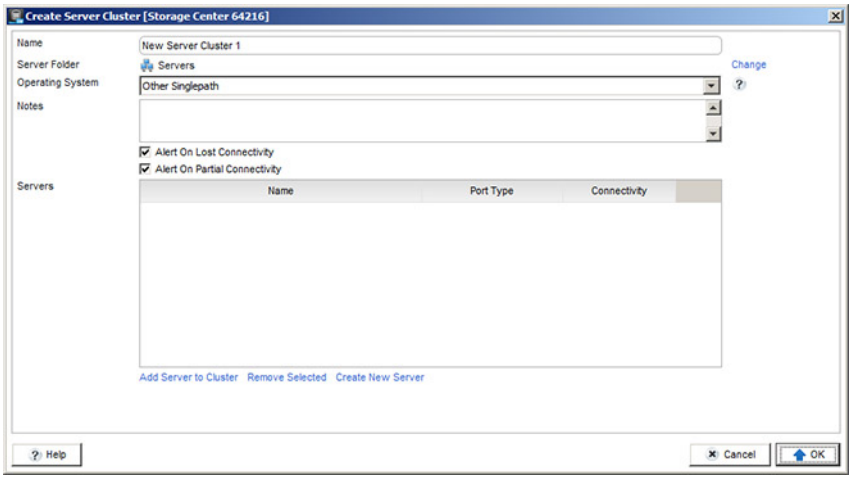


Figure 19. Create Server Cluster Dialog Box

5. Configure the server cluster attributes.
   The server attributes are described in the online help.
   a. Enter a name for the server in the **Name** field.
   b. To add the server cluster to a server folder, click **Change**, select a folder, and click **OK**.
   c. From the **Operating System** drop-down menu, select the operating system for the cluster.

      NOTE: All servers in a server cluster must be running the same operating system.

   d. To generate Storage Center alerts when connectivity is lost between the Storage Center and the servers, select **Alert On Lost Connectivity**.
   e. To generate Storage Center alerts when the Storage Center only has partial connectivity to the servers, select **Alert On Partial Connectivity**.
6. Add servers to the server cluster.
   - To add existing servers to the cluster, click **Add Server to Cluster**, select the server to add, and then click **OK**.
   - To define a new server, click **Create New Server**, configure the server attributes, and then click **OK**. For user interface reference information, click **Help**.
7. Click **OK**.

Create a Server from the localhost

Configure a localhost to access block level storage on the Storage Center.

Prerequisites

- Client must be running on a system with a 64-bit operating system.
- The local host must be running a supported Windows or Linux operating system.
- The Storage Manager Client must be run by a user with the Administrator privilege.
- The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator or Volume Manager privilege.
- On a Storage Center with Fibre Channel IO ports, configure Fibre Channel zoning before starting this procedure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab, click **Servers**.
4. Click **Create Server from localhost**.

The **Set up localhost for Storage Center** wizard opens.

- If the Storage Center has iSCSI ports and the host is not connected to any interface, the **Log into Storage Center via iSCSI** page appears. Select the target fault domains, and then click **Log In**.
- In all other cases, proceed to the next step.

5. On the **Verify localhost Information** page, verify that the information is correct. Then click **Create Server**.
   The server definition is created on the Storage Center for the connected and partially connected initiators.
6. The **Host Setup Successful** page displays the best practices that were set by the wizard and best practices that were not set. Make a note of any best practices that were not set by the wizard. It is recommended that these updates are applied manually before starting IO to the Storage Center.
7. (Optional) Place a check next to **Create a Volume for this host** to create a volume after finishing host setup.
8. Click **Finish**.

Create a Server from a VMware vSphere Host

Configure a VMware vSphere host to access block level storage on the Storage Center.

Prerequisites

- Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run by a user with the Administrator privilege.
- The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator or Volume Manager privilege.
- On a Storage Center with Fibre Channel IO ports, configure Fibre Channel zoning before starting this procedure.

About this task

NOTE: vSphere is not supported on servers connected to the Storage Center over SAS.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab, click **Servers**.
4. Click **Create Server from a VMware vSphere or vCenter**.
   The **Set Up VMware Host on Storage Center** wizard appears.
5. Enter the IP address or hostname, the user name and password. Then click **Next**.
   - If the Storage Center has iSCSI ports and the host is not connected to any interface, the **Log into Storage Center via iSCSI** page appears. Select the target fault domains, and then click **Log In**.
   - In all other cases, the **Verify vSphere Information** page appears. Proceed to the next step.
6. Select an available port, and then click **Create Server**.
   The server definition is created on the Storage Center.
7. The **Host Setup Successful** page displays the best practices that were set by the wizard and best practices that were not set. Make a note of any best practices that were not set by the wizard. It is recommended that these updates are applied manually before starting IO to the Storage Center.
8. (Optional) Place a check next to **Create a Volume for this host** to create a volume after finishing host setup.
9. Click **Finish**.

Create a Server from a VMware vCenter Host

Configure a VMware vCenter cluster to access block level storage on the Storage Center.

Prerequisites

- Client must be running on a system with a 64-bit operating system.
- The Storage Manager Client must be run by a user with the Administrator privilege.
- The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator or Volume Manager privilege.

- On a Storage Center with Fibre Channel IO ports, configure Fibre Channel zoning before starting this procedure.

About this task

NOTE: VMware vCenter is not supported on servers connected to the Storage Center over SAS.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab, click **Servers**.
4. Click **Create Server from a VMware vSpehere or vCenter**.
   The **Set Up VMware Host on Storage Center** wizard appears.
5. Enter the IP address or hostname, the user name and password. Then click **Next**.
   - If the Storage Center has iSCSI ports and the host is not connected to any interface, the **Log into Storage Center via iSCSI** page appears. Select the target fault domains, and then click **Log In**.
   - In all other cases, the **Verify vCenters Information** page appears. Proceed to the next step.
6. Select an available port, and then click **Create Servers**.
   The server definition is created on the Storage Center.
7. The **Host Setup Successful** page displays the best practices that were set by the wizard and best practices that were not set. Make a note of any best practices that were not set by the wizard. It is recommended that these updates are applied manually before starting IO to the Storage Center.
8. (Optional) Place a check next to **Create a Volume for this host** to create a volume after finishing host setup.
9. Click **Finish**.

Modifying Servers

Modify a server to change its attributes, apply a Snapshot Profile, and add or remove HBAs.

Apply One or More Snapshot Profiles to a Server

Associate a Snapshot Profile with a server to add snapshot creation and expiration schedules to all volumes that are currently mapped to a server. Volumes that are subsequently mapped to the server do not inherit the snapshot creation and expiration schedules.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server in the **Storage** tab navigation pane.
4. In the right pane, click **Apply Snapshot Profiles to Server**.
   The **Apply to Server** dialog box opens.
5. Select the Snapshot Profiles to assign to the server from the top pane of the dialog box.
6. To replace the existing Snapshot Profiles for each volume mapped to the server, select the **Replace Existing Snapshot Profiles** checkbox.
7. Click **OK**.

Add a Server to a Server Cluster

You can add a server to a server cluster.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the server to add to a cluster.

4. In the right pane, click **Add Server to Cluster**. The **Add Server to Cluster** dialog box opens.
5. Select the server cluster to which to add the server.
6. Click **OK**.

Remove a Server from a Server Cluster

You can remove a server object from a server cluster at any time.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server to remove from the server cluster in the **Storage** tab navigation pane.
4. In the right pane, click **Remove Server from Cluster**.
   The **Remove Server from Cluster** dialog box opens.
5. Click **OK**.

Convert a Physical Server to a Virtual Server

If you migrated a physical server to a virtual machine, change the physical server object to a virtual server object and select the host physical server.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the physical server to convert to a virtual server in the **Storage** tab navigation pane.
4. In the right pane, click **Convert to Virtual Server**.
   The **Convert to Virtual Server** dialog box opens.
5. Select the parent server or server cluster that hosts the virtual server.
6. Click **OK**.

Convert a Virtual Server to a Physical Server

If you migrated a virtual machine to a physical server, modify the corresponding virtual server object accordingly.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the virtual server to covert to a physical server in the **Storage** tab navigation pane.
4. In the right pane, click **Convert to Physical Server**.
   The **Convert to Physical Server** dialog box opens.
5. Click **OK**.

Rename a Server

A server object can be renamed at any time, and the name does not need to match the host name or IP address of the server.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. From the **STORAGE** menu, click **Servers**.
   The **Servers** view is displayed.
3. Click the **Storage** tab.

4. Select the server in the **Storage** tab navigation pane.
5. In the right pane, click **Edit Settings**. The **Edit Server Settings** dialog box opens.
6. Type a name for the server in the **Name** field.
7. Click **OK**.

Change the Operating System of a Server

If you installed a new operating system or upgraded the operating system on a server, update the corresponding server object accordingly.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server in the **Storage** tab navigation pane.
4. In the right pane, click **Edit Settings**.
   The **Edit Server Settings** dialog box opens.
5. Select the operating system for the server from the **Operating System** drop-down list.
6. Click **OK**.

Move a Server to a Different Server Folder

For convenience, server objects can be organized by folders.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server in the **Storage** tab navigation pane.
4. In the right pane, click **Edit Settings**. The **Edit Server Settings** dialog box opens.
5. Select the folder to which to move the server in the **Server Folder** navigation tree.
6. Click **OK**.

Add One or More HBAs to a Server

To map a volume to a server, the Storage Center must be able to communicate with at least one HBA on the server.

Steps

1. Make sure the server HBAs have connectivity with the Storage Center HBAs.
   - **Fibre Channel** – Configure Fibre Channel zoning to allow the server HBAs and Storage Center HBAs to communicate.
   - **iSCSI** – Configure the iSCSI initiator on the server to use the Storage Center HBAs as the target.
   - **SAS** – Directly connect the controller to a server using the SAS front-end connections.
2. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
3. Click the **Storage** tab.
4. Select the server in the **Storage** tab navigation pane.
5. In the right pane, click **Add HBAs to Server**.
   The **Add HBAs to Server** dialog box opens.
6. Select or define one or more HBAs for the server.
   - If one or more server HBAs are visible to the Storage Center, select the checkboxes of the HBAs for the server in the **Select HBAs to add to server** table.
   - If a server HBA is not visible to the Storage Center, click **Manually Add HBA** to define an HBA manually.

     NOTE: For SAS front-end ports, use the SAS device name as the world wide name to manually add the HBA.
7. Click **OK**.

Related tasks

Configure Front-End I/O Ports (Fibre Channel and SAS) on page 255
Configure Front-End I/O Ports (iSCSI) on page 255

Remove One or More HBAs from a Server

If a server HBA has been repurposed and is no longer used to communicate with the Storage Center, remove it from the server object.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server in the **Storage** tab navigation pane.
4. In the right pane, click **Remove HBAs from Server**.
   The **Remove HBAs from Server** dialog box opens.

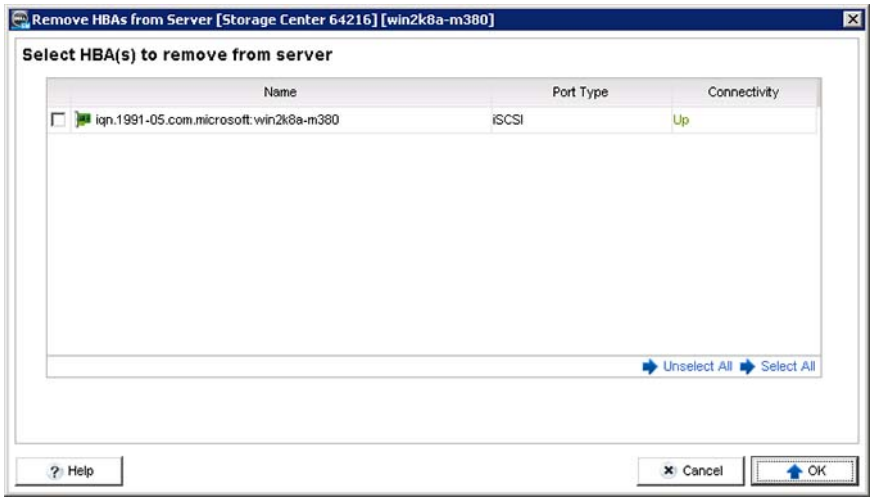


Figure 20. Remove HBAs from Server

5. Select the checkboxes of the HBAs to remove from the server.
6. Click **OK**.
   If the HBAs are used by one or more mapped volumes, a confirmation dialog box opens.
   - To keep the HBAs, click **Cancel**.
   - To remove the HBAs, click **OK**. Removing the HBAs might cause the server to lose visibility of the mapped volumes.

Mapping Volumes to Servers

Map a volume to a server to allow the server to use the volume for storage.

Map a Volume to a Server

Map a volume to a server to allow the server to use it.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server in the **Storage** tab navigation pane.
4. In the right pane, click **Map Volume to Server**.
   The **Map Volume to Server** wizard opens.
5. In the **Volume** navigation tree, select the volume you want to map to the server.

6. Click **Next**.
   The **Map Volume to Server** wizard advances to the next page.
7. (Optional) Click **Advanced Options** to configure LUN settings, restrict mapping paths, or present the volume as read-only.
8. Click **Finish**.

Unmap One or More Volumes From a Server

If a server no longer uses a volume, you can unmap the volume from the server.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server from which to unmap volumes in the **Storage** tab navigation pane.
4. In the right pane, click **Remove Mappings**.
   The **Remove Mappings** dialog box opens.
5. Select the checkboxes of the volumes to unmap from the server.
6. Click **OK**.

Create a Volume and Map it to a Server

If a server requires additional storage and you do not want to use an existing volume, you can create and map a volume to the server in a single operation.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server to which to map a new volume in the **Storage** tab navigation pane.
4. In the right pane, click **Create Volume**.
   The **Create Volume** dialog box opens.
5. Type a name for the volume in the **Name** field.
6. Select a unit of storage from the drop-down menu and enter the size for the volume in the **Size** field.
   The storage units are Bytes, KB, MB, GB, or TB.
7. Select the parent folder for the volume in the **Volume Folder** pane.
8. (Optional) Configure the remaining volume attributes as needed.
   - **Snapshot Profiles**—Click **Change** to select snapshot profiles for the volume.
   - **Server**—Click **Change** to select a server to which to map the volume.
   - **Advanced Mapping**—Click **Advanced Mapping** to configure LUN settings, restrict mapping paths, configure multipathing, or present the volume as read-only.
   - **Read Cache**—Clear the **Enabled** checkbox to disable read cache on the volume. **Read Cache** is enabled by default.
   - **Write Cache**—Clear the **Enabled** checkbox to disable write cache on the volume. **Write Cache** is enabled by default.
   - **Data Reduction Profile**—Select **Compression** or **Deduplication with Compression** as the data reduction profile for the volume. **None** is selected by default.
   - **Chargeback Department**—If Chargeback is enabled, click **Change** to select the department to charge for storage costs associated with the volume by clicking **Change**.
   - **Storage Profile**—Select the storage profile to assign to the volume. Selecting the **Recommended (All Tiers)** storage profile allows the volume to take full advantage of data progression.
   - **Storage Type**—Select the storage type to assign to the volume.
   - **Volume QoS Profile**—Click **Change** to select the volume QoS profile to assign to the volume.
   - **Group QoS Profile**—Click **Change** to select the group QoS profile to assign to the volume.
   - **Create as Replication**—Select this checkbox to create a replication volume.
   - **Create as Live Volume**—Select this checkbox to create a Live Volume.
   - **Preallocate Storage**—Select this checkbox to allocate storage to the volume before the volume is mapped to the server.

NOTE: When a volume is preallocated, the Storage Center allocates all of the space on the volume t>o the server. The Free Space of the volume is 0 MB and the Used/Active Space of the volume is the equal to the size of volume on Storage Center. To keep the volume preallocated when it is formatted on the server, the SCSI UNMAP feature must be disable on the server.

9. Click **OK**.

Related concepts

Modifying Volumes on page 102

Create Multiple Volumes Simultaneously and Map Them to a Server

If a server requires additional storage and you do not want to use existing volumes, you can create and map multiple volumes to the server in a single operation.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server to which to map new volumes in the **Storage** tab navigation pane.
4. In the right pane, click **Create Multiple Volumes**. The **Create Multiple Volumes** dialog box opens.
5. In the **Volume Count** field, type the number of volumes to create.
6. Type a name for the volume in the **Name** field.
7. Select a unit of storage from the drop-down menu and enter the size for the volume in the **Size** field.
   The storage units are Bytes, KB, MB, GB, or TB.
8. In the **Volume Folder** pane, select the parent folder for the volume.
9. (Optional) Configure the remaining volume attributes as needed.
   - **Snapshot Profiles**—Click **Change** to select snapshot profiles for the volume.
   - **Server**—Click **Change** to select a server to which to map the volume.
   - **Advanced Mapping**—Click **Advanced Mapping** to configure LUN settings, restrict mapping paths, configure multipathing, or present the volume as read-only.
   - **Read Cache**—Clear the **Enabled** checkbox to disable read cache on the volume. **Read Cache** is enabled by default.
   - **Write Cache**—Clear the **Enabled** checkbox to disable write cache on the volume. **Write Cache** is enabled by default.
   - **Data Reduction Profile**—Select **Compression** or **Deduplication with Compression** as the data reduction profile for the volume. **None** is selected by default.
   - **Chargeback Department**—If Chargeback is enabled, click **Change** to select the department to charge for storage costs associated with the volume by clicking **Change**.
   - **Storage Profile**—Select the storage profile to assign to the volume. Selecting the **Recommended (All Tiers)** storage profile allows the volume to take full advantage of data progression.
   - **Storage Type**—Select the storage type to assign to the volume.
   - **Volume QoS Profile**—Click **Change** to select the volume QoS profile to assign to the volume.
   - **Group QoS Profile**—Click **Change** to select the group QoS profile to assign to the volume.
   - **Create as Replication**—Select this checkbox to create a replication volume.
   - **Create as Live Volume**—Select this checkbox to create a Live Volume.
   - **Preallocate Storage**—Select this checkbox to allocate storage to the volume before the volume is mapped to the server.

     NOTE: When a volume is preallocated, the Storage Center allocates all of the space on the volume t>o the server. The Free Space of the volume is 0 MB and the Used/Active Space of the volume is the equal to the size of volume on Storage Center. To keep the volume preallocated when it is formatted on the server, the SCSI UNMAP feature must be disable on the server.
10. Click **OK**.
    The **Create Multiple Volumes** dialog box appears and displays the newly created volume.
11. Use the **Create Multiple Volumes** dialog box to create additional volumes.
    - To add a volume based on a previous volume, select the volume from the list and click **Clone Selected Volume**.
    - To manually define another volume, click **Add Volumes**.

- To modify a previous volume, select it from the list and click **Edit Volume**.
- To remove a previous volume, select it from the list and click **Remove Volume**.

12. Click **OK**. The volumes are created and mapped to servers.

Related concepts

Modifying Volumes on page 102

Creating and Managing Server Folders

Use server folders to group and organize servers defined on the Storage Center.

NOTE: For user interface reference information, click **Help**.

Create a Server Folder

Create a server folder to group servers together.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the **Servers** node.
4. In the right pane, click **Create Server Folder**.
   The **Create Server Folder** dialog box opens.
5. Type a name for the folder in the **Name** field.
6. (Optional) Type information about the server folder in the **Notes** field.
7. Select a parent folder for the new folder in the **Parent** navigation tree.
8. Click **OK**.

Rename a Server Folder

Select a different name for a server folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the server folder to rename.
4. In the right pane, click **Edit Settings**.
   The **Edit Server Folder Settings** dialog box opens.
5. Type a new name for the server folder in the **Name** field.
6. Click **OK**.

Move a Server Folder

Use the **Edit Settings** dialog box to move a server folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the server folder to rename.
4. In the right pane, click **Edit Settings**.
   The **Edit Server Folder Settings** dialog box opens.

5. Select a new parent folder in the **Parent** navigation tree.
6. Click **OK**.

Deleting Servers and Server Folders

Delete servers and server folders when they no longer utilize storage on the Storage Center.

NOTE: For user interface reference information, click **Help**.

Delete a Server

Delete a server if it no longer utilizes storage on the Storage Center. When a server is deleted, all volume mappings to the server are also deleted.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server to delete in the **Storage** tab navigation pane.
4. In the right pane, click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK**.

Delete a Server Folder

Delete a server folder if it is no longer needed.

Prerequisites

The server folder must be empty.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server folder to delete in the **Storage** tab navigation pane.
4. In the right pane, click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK**.

Managing Servers Centrally on the Servers View

Use the **Servers** view to register servers to Storage Manager and provision storage for registered servers.

Server Types That Can Be Centrally Managed

Servers running Windows and VMware operating systems can be registered to Storage Manager.

Server Type	Supported Versions/Models
Windows	• Windows Server 2012 R2 (full or core installation) • Windows Server 2016 (full) • Windows Server 2019 **NOTE:** The Storage Manager Server Agent must be installed on a Windows server before it can be registered.

Server Type	Supported Versions/Models
VMware	• ESXi 6.5 and later • vCenter Server 6.5 and later **NOTE:** SAS protocol for host connections is supported beginning in VMware ESXi version 6.5, and VMware vCenter Web Client Server version 6.5.

Storage Manager Server Agent for Windows Servers

To register a Windows server to Storage Manager, the Storage Manager Server Agent must be installed on the server. The Server Agent allows Storage Manager to communicate with the Windows server to retrieve information and streamline storage management for the server.

The Server Agent is required for Windows servers only. Other supported server types do not require the Server Agent.

IPMI Support for NAS Appliances

The Dell NAS appliances include Intelligent Platform Management Interface (IPMI) cards. Storage Manager communicates with the IPMI card to retrieve fan speed, temperature, voltage, and power supply information. The IPMI card also allows Storage Manager to clear the System Event Log (SEL), power off the server, and reset the server.

The IPMI card must be properly configured to allow Storage Manager to communicate with it. For IPMI configuration, see the documentation for your NAS product:

Product	Documentation
Dell NAS Server	• *Storage Center NAS Storage Solution Setup Guide* • *Storage Center NAS Storage Solution User Guide*

Registering Servers with Storage Manager

Register a physical or virtual server with Storage Manager to streamline the storage provisioning process.

Register a Windows-Based Server

Register the Storage Manager Server Agent on a Windows server to manage it on the **Servers** view.

Prerequisites

The Storage Manager Server Agent must be installed and running on the server.

Steps

1. Click the **Servers** view.
2. Select the **Servers** folder in the **Servers** pane.
3. In the right pane, click **Register Server** and select **Add Windows Server Agent**. The **Register Server** dialog box appears.
4. Enter the host name or IP address of a Windows server in the **Host or IP Address** field.

   NOTE: If the server is a member of a server cluster, enter the host name or IP address of a server, not a server cluster.

5. Enter the port number of the socket listening port on the Server Agent in the **Port** field.
6. Configure automatic management settings for the Storage Center(s) to which the server is connected.
   - To automatically create and manage the server on the Storage Center(s), select the **Auto Manage Storage Centers** check box.
   - To automatically create and manage virtual machines hosted by the server on the Storage Center(s), select **Auto Manage Virtual Machines On Storage Centers**.

NOTE: If the server has physical iSCSI HBAs, Storage Manager may not automatically recognize the WWNs for the server. In this situation, configure the iSCSI HBA(s) to target the Storage Center, create a server on the Storage Center, then manually map the Storage Center server to the Server Agent.

7. Select a parent folder for the server in the **Folder** navigation tree.
8. Click **OK**.

Related concepts

Install and Register the Server Agent on page 170
Manually Mapping a Windows Server to a Storage Center Server on page 167

Register a VMware vCenter Server

Register a VMware vCenter Server to manage it on the **Servers** view.

Steps

1. Click the **Servers** view.
2. Select the **Servers** folder in the **Servers** pane.
3. In the right pane, click **Register Server** and select **Add VMware vCenter Server**.
   The **Register Server** dialog box opens.
4. In the **Host or IP Address** field, enter the host name or IP address of a vCenter Server.
5. Type the user name and password of an administrator on the vCenter Server in the **User Name** and **User Password** fields.
6. Select a parent folder for the server in the **Folder** navigation tree.
7. Configure automatic management settings for the Storage Center for Storage Centers to which the server is connected.
   - To automatically create and manage the server on the Storage Center, select the **Auto Manage Storage Centers** checkbox.
   - To automatically create and manage virtual machines hosted by the server on the Storage Center, select **Auto Manage Virtual Machines On Storage Centers**.
8. To register a VASA provider, select the **Register VASA Provider** check box.
   A VASA provider must be registered to use VMware virtual volumes (VVols) in your storage environment.
   a. Select the version of VASA to use:
      - Select **VASA 1** for an ESXi 5.5 host. The format of the URL for VASA 1.0 is `https://host ID:3034/vasa-provider/vasa1/vasa-version.xml`
      - Select **VASA 2** for an ESXi 6.0 or later host. The format of the URL for VASA 2.0 is `https://host ID:3034/vasa-provider/vasa2/vasa-version.xml`

      The *host ID* is either the IP address or the Fully Qualified Domain Name (FQDN) of the host on which the Data Collector is installed.

      CAUTION: The host must use an FQDN known by DNS so that IP address changes do not cause vCenter to lose connection to the VASA provider. If FQDN use is not possible, IP address changes will not automatically be known by vCenter, and unregistering and reregistering the VASA provider will be required after each change. For this reason, nonphysical address locked DHCP addressing is discouraged.

      NOTE: If the VASA provider is unregistered and reregistered, the option for selecting VASA1 or VASA2 during VASA registration no longer displays because the Storage Manager Data Collector automatically selects the latest version of VASA that is supported by the ESXi host.

   b. Type the user name and password of the Storage Manager associated with the VASA provider.

      CAUTION: The user name for the VASA Provider should be a service account, not a user account. If a user account is specified in this field, and the user is deleted, the VASA information could be lost.
9. Click **OK**.

Results

NOTE: After a Storage Manager update, the VASA version number displayed in vCenter is not updated unless the VASA provider is unregistered and reregistered with that vCenter.

NOTE: If the VASA provider loses network access to the external database, the VASA provider needs to be unregistered and reregistered to continue with VVols operations.

Organizing and Removing Registered Servers

Use server folders to organize servers into groups.

Create a Server Folder

Create a server folder to group servers together.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the **Servers** node.
4. In the right pane, click **Create Server Folder**.
   The **Create Server Folder** dialog box opens.
5. Type a name for the folder in the **Name** field.
6. (Optional) Type information about the server folder in the **Notes** field.
7. Select a parent folder for the new folder in the **Parent** navigation tree.
8. Click **OK**.

Rename a Server Folder

Select a different name for a server folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the server folder to rename.
4. In the right pane, click **Edit Settings**.
   The **Edit Server Folder Settings** dialog box opens.
5. Type a new name for the server folder in the **Name** field.
6. Click **OK**.

Move a Server Folder

Use the **Edit Settings** dialog box to move a server folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the server folder to rename.
4. In the right pane, click **Edit Settings**.
   The **Edit Server Folder Settings** dialog box opens.
5. Select a new parent folder in the **Parent** navigation tree.
6. Click **OK**.

Move a Server to a Different Folder

Use the **Edit Settings** dialog box to move a server to a different folder.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select the server that you want to move.
3. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
4. In the **Folder** navigation tree, select a folder.
5. Click **OK**.

Enable or Disable Automatic Management of Storage Center Server Objects

You can configure Storage Manager to automatically create and manage the server and hosted virtual servers on the Storage Centers to which it is connected.

Steps

1. Click the **Servers** view.
2. Select the server to edit in the **Servers** pane.
3. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
4. Configure automatic management settings for the Storage Centers to which the server is connected.
   - To automatically create and manage the server on the Storage Centers, select the **Auto Manage Storage Centers** check box.
   - To automatically create and manage virtual machines hosted by the server on the Storage Centers, select **Auto Manage Virtual Machines On Storage Centers**.
5. Click **OK**.

Delete a Registered Server

Remove a registered server from the **Servers** view if you no longer want to manage it from Storage Manager. If **Auto Manage Storage Centers** is enabled for the server, deleting it removes the HBAs from the corresponding Storage Center server objects.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select the server.
3. In the right pane, click **Delete**. The **Delete Objects** dialog box appears.
4. Click **OK**.

Delete a Server Folder

Delete a server folder if it is no longer needed.

Prerequisites

The server folder must be empty.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Select the server folder to delete in the **Storage** tab navigation pane.
4. In the right pane, click **Delete**.
   The **Delete** dialog box opens.

5. Click **OK**.

Updating Server Information

You can retrieve current information from servers and scan for new volumes on servers.

Retrieve Current Information from a Single Server

Refresh the view to see the most current server data.

Steps

1. Click the **Servers** view.
2. Select a server in the **Servers** pane. The **Summary** tab appears.
3. In the right pane, click **Update Information**. The **Update Information** dialog box appears.

Scan for New Volumes on a Single Server

If volumes have been added to a server, scan the server to display them on the **Server** view.

Steps

1. Click the **Servers** view.
2. Select a server in the **Servers** pane. The **Summary** tab opens.
3. In the right pane, click **Rescan for Volumes**. The **Rescan for Volumes** dialog box opens.
4. Click **OK**.

Retrieve Current Information from All Servers

Trigger Storage Manager to refresh the data that is displayed for all servers. If **Auto Manage Storage Centers** is enabled one or more servers, this action adds corresponding server objects to the associated Storage Centers.

Steps

1. Click the **Servers** view.
2. Select the root **Servers** folder in the **Servers** pane. The **Summary** tab for all servers opens.
3. In the right pane, click **Update Information on Servers**. The **Update Information on Servers** dialog box opens.

   NOTE: This process can take several minutes to finish.

4. Click **OK**.

Scan for New Volumes on All Servers

If volumes have been added to multiple servers, scan all servers to display the volumes on the **Servers** view.

Steps

1. Click the **Servers** view.
2. Select the **Servers** folder in the **Servers** pane. The **Summary** tab for all servers opens.
3. In the right pane, click **Rescan for Volumes on Servers**. The **Rescan for Volumes on Servers** dialog box opens.
4. Click **OK**.

Change the Connection Timeout for a Windows Server

You can configure the maximum time in seconds that Storage Manager waits for a response for queries sent to the Server Agent.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select a Windows server.
3. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
4. In the **Connection Timeout** field, type a new timeout in seconds.
   - The default is 300 seconds.
   - The minimum value is 180 seconds.
   - The maximum value is 1200 seconds.
5. Click **OK**.

Managing Server Data Collection and Reporting Settings

Data collection and reporting settings apply to all servers added to the **Server** view.

Automatically Retrieve Information for All Registered Servers

If automated updating is enabled, information is updated every 30 minutes.

Steps

1. Click the **Servers** view.
2. In the Servers pane, click **Servers Properties**. The **Edit Settings** dialog box opens.
3. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
4. Click **Data Collector**.
   The **Data Collector** view is displayed.
5. Select the **Allow Automated Update Information** check box.

   When the **Allow Automated Update Information** check box is selected, the information that is displayed for all registered servers is updated every 30 minutes.
6. Click **OK**.

Configure Reporting Settings for All Registered Servers

You can specify the number of days for which data is gathered for all servers.

Steps

1. Click the **Servers** view.
2. In the Servers pane, click **Servers Properties**. The **Edit Settings** dialog box opens.
3. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
4. Click **Data Collector**.
   The **Data Collector** view is displayed.
5. In the **Days For Reporting** field, enter the number of days of data to gather from registered servers.
6. Click **OK**.

Creating Server Volumes and Datastores

Creating a volume on a Windows server or creating a datastore on a VMware server automatically creates a Storage Center volume and maps it to the server in one operation.

Related tasks

Create a Datastore and Map it to VMware ESX Server on page 164

Create a Volume and Map it to a Windows Server

You can create a volume, map it to a Windows server, format it, and mount it on the server in one operation.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select the Windows server on which to create the volume.
3. In the right pane, click **Create Volume**. The **Create Volume** dialog box opens.
4. Enter a name for the volume in the **Label** field. The name is displayed as the disk label in Windows.
5. Select a unit of storage from the drop-down menu and enter the size for the volume in the **Total Space** field. The available storage units are kilobytes (KB), megabytes (MB), gigabytes (GB), and terabytes (TB).
6. Select the smallest amount of disk space that can be allocated for a file in the **Allocation Size** drop-down menu. The default allocation value is dependent on the size of the volume.
7. Select how to format the volume from the **Format Type** drop-down menu:
   - **GPT**: Formats the volume using the GUID Partition Table disk partitioning scheme.
   - **MBR**: Formats the volume using the master boot record disk partitioning scheme.
8. Specify how to mount the volume in the **Drive or Mount Point** area:
   - **Use Next Available Drive Letter**: The volume is mounted on the server using the next unused drive letter.
   - **Assign to Drive Letter**: The volume is mounted on the server using the drive letter selected from the drop-down menu. To update the list of drive letters that are available on the server, click **Refresh**.
   - **Mount to Empty NTFS Folder**: The volume is mounted to an empty folder on the server. The path to the folder must be entered in the text field. To verify the path entered is valid, click **Verify mount point is available**.
9. Select the Storage Center on which to create the volume.
   - To manually choose a Storage Center, select it from the **Storage Center** drop-down menu.
   - To automatically choose a Storage Center based on capacity and performance, click **Recommend a Storage Center**. The drop-down menu displays the recommended Storage Center.
10. If you want to specify a custom LUN, restrict mapping paths, configure multipathing, or make the volume read-only, click **Advanced Mapping**.
11. To configure settings for the Storage Center volume that will be created, click **Volume Settings**. In the **Volume Settings** dialog box that appears, modify the options as needed, then click **OK**.
    a. Select the folder in which to create the volume from the **Volume Folder** drop-down menu.
    b. Type notes in the **Notes** field as needed.
    c. To schedule snapshot creation and expiration for the volume, apply one or more Snapshot Profiles by clicking **Change** across from **Snapshot Profiles**.
    d. If Chargeback is enabled, select the department to charge for storage costs associated with the volume by clicking **Change** across from **Chargeback Department**.
    e. To enable caching for reads on the volume, select the Enabled check box across from **Read Cache**.
    f. To enable caching for writes on the volume, select the Enabled check box across from **Write Cache**.
    g. To enable compression on eligible data in the volume, select the **Enable** check box across from **Compression**.
    h. To use specific tiers and RAID levels for volume data, select the appropriate Storage Profile from the **Storage Profile** drop-down menu. Using the **Recommended** Storage Profile allows the volume to take full advantage of data progression.
    i. If more than one Storage Type is defined on the Storage Center, select the Storage Type to provide storage from the **Storage Type** drop-down menu.

       To use a QoS profile, select a **Volume QoS Profile** or **Group QoS Profile** from the drop down lists.
12. Click **OK**.

Create an RDM Volume

You can create a volume, map it to a VMware virtual machine, and create a raw device mapping to the virtual machine in one operation.

Prerequisites

In order for the **Create RDM Volume** option to appear in Storage Manager, the virtual machine must be powered on. If Storage Manager determines that the VM is not powered on, the **Create RDM Volume** menu option is not displayed.

Steps

1. Click the **Servers** view.
2. Click the plus sign (+) next to the vSphere host, on which the virtual machine is located, to display the **Virtual Machines** node.
3. Click the plus sign (+) next to the **Virtual Machines** node to display the virtual machine.
4. Select the virtual machine on which to create the datastore.
5. Click **Create RDM Volume**.
6. Enter a name for the volume in the **Volume Name** field.
7. Select the unit of storage from the drop-down menu and enter the size of the volume in the **Total Space** field.
8. Select the Storage Center on which to create the volume.
   - To manually choose a Storage Center, select it from the **Storage Center** drop-down menu.
   - To automatically choose a Storage Center based on capacity and performance, click **Recommend a Storage Center**. The recommended Storage Center appears in the **Storage Center** drop-down menu.
9. To configure advanced volume mapping options, click **Advanced Mapping**.
10. To configure the volume creation settings, click **Volume Settings**. In the **Volume Settings** dialog box appears, modify the options as needed, then click **OK**.
    - To specify the name of the volume, type a name in the **Name** field.
    - To specify the folder in which the volume will be created, select a folder from the **Volume Folder** area.
    - To add notes to the volume, type notes in the **Notes** field.
    - To schedule snapshot creation and expiration for the volume, apply one or more Snapshot Profiles by clicking **Change** across from **Snapshot Profiles**.
    - If Chargeback is enabled, select the department to charge for storage costs associated with the volume by clicking **Change** across from **Chargeback Department**.
    - To enable caching for reads on the volume, select the **Enabled** check box across from **Read Cache**.
    - To enable caching for writes on the volume, select the **Enabled** check box across from **Write Cache**.
    - To enable compression on eligible data in the volume, select the **Enable** check box across from **Compression**.
    - To use specific tiers and RAID levels for volume data, select the appropriate Storage Profile from the **Storage Profile** drop-down menu. Using the **Recommended** Storage Profile allows the volume to take full advantage of data progression.
11. If more than one Storage Type is defined on the Storage Center, select the Storage Type to provide storage from the **Storage Type** drop-down menu.
12. Click **OK**.

Create a Datastore and Map it to VMware ESX Server

You can create a datastore, map it to a VMware ESX environment, and mount it to the cluster in one operation.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select the VMware ESXi cluster or host on which to create the datastore.
3. In the right pane, click **Create Datastore**.
   The **Create Datastore** dialog box opens.
4. Type a name for the datastore in the **Datastore Name** field.
5. Select the type of datastore to create:
   - **Standard Datastore (VMFS)**

- **VVol Datastore**

6. Click **Next**.
7. If you selected **Standard Datastore (VMFS)**, complete the following steps:
   a. Select a unit of storage from the drop-down menu and type the size for the datastore in the **Total Space** field. The available storage units are bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), and terabytes (TB).
   b. Select the size limit for virtual disks within the datastore from the **Max File Size** drop-down.
   c. Select the Storage Center on which to create the datastore from the **Storage Center** drop-down menu.
   d. To specify the folder in which to create the datastore, select a folder from the **Volume Folder** area.
   e. To add notes to the datastore, type notes in the **Notes** field.
   f. To specify a snapshot profile, click **Change**, select a profile in the **Select Snapshot Profiles** dialog box, and click **OK**.
   g. To specify a data reduction profile, select a profile from the **Data Reduction Profile** drop-down menu.
   h. To use specific tiers and RAID levels for datastore data, select the appropriate Storage Profile from the **Storage Profile** drop-down menu.
   i. If more than one storage type is defined on the Storage Center, select the storage type to provide storage from the **Storage Type** drop-down menu.
   j. If you want to specify a custom LUN, restrict mapping paths, configure multipathing, or make the datastore read-only, click **Advanced Mapping**.
8. If you selected **VVol Datastore**, select the radio button for the storage container to use for the VVol datasore
   - **Use Existing New Storage Container** – If you selected this option, a list of existing storage containers is displayed. Select the storage container to use and click **Finish**.
   - **Create a New Storage Container** – If you selected this option, complete the following steps:

   a. Select the Storage Center on which to create the datastore from the **Storage Center** drop-down menu.
   b. Select a unit of storage from the drop-down menu and type the size for the datastore in the **Size** field. The available storage units are bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), and terabytes (TB).
   c. To specify the folder in which to create a datastore, click **Change**, select a folder from the **Select Volume Folder** dialog box, and click **OK**.
   d. If more than one storage type is defined on the Storage Center, select the storage type to provide storage from the **Storage Type** drop-down menu.
   e. Specify whether to allow compression by selecting or clearing the **Compression Allowed** checkbox.
   f. Specify whether to allow deduplication by selecting or clearing the **Deduplication Allowed** checkbox.
   g. Specify whether to allow encryption by selecting or clearing the**Use Encryption** checkbox.
   h. (Optional) To specify the storage profiles to allow for new datastores, click **Change**, select the storage profiles to allow from the **Select Storage Profile** dialog box, and click **OK**.
   i. Select the default snapshot profile setting from the **Default Snapshot Profile** drop-down menu.
   j. Select the default data reductions profile setting from the **Default Data Reduction Profile** drop-down menu.
   k. Select the default storage profile setting from the **Default Storage Profile** drop-down menu.
   l. Select the default data reduction input setting from the **Default Data Reduction Input** drop-down menu.
9. Click **Finish**.

Related concepts

Creating Server Volumes and Datastores on page 163

Expand a Datastore

Expand a VMware datastore if it is running out of space.

Steps

1. Click the **Servers** view.
2. Select the datastore in the **Servers** pane.
3. In the right pane, click **Expand Datastore**. The **Expand Datastore** dialog box appears.
4. In the **New Size** field, type a new size for the datastore.
5. Click **OK**.

Delete a Volume or Datastore

Delete a volume or datastore if it is no longer needed by the server. Volumes that are not hosted on a Storage Center cannot be deleted.

Steps

1. Click the **Servers** view.
2. Select the volume or datastore to delete in the **Servers** pane.
3. In the right pane, click **Delete**. The **Delete Objects** dialog box appears.
4. Click **OK**.

Assigning/Creating Virtual Servers on Storage Centers

Virtual machines that are not automatically managed on a Storage Center must be manually assigned to server objects on the Storage Center(s) that provide storage.

Assign a Virtual Machine to a Storage Center server object

If a virtual server object has already been created on the Storage Center, assign the virtual server to that object.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select the virtual machine that needs to be assigned to a Storage Center.
3. In the right pane, click **Assign to Virtual Server on Storage Center**. The **Assign SC Server to Virtual Machine** dialog box appears.
4. Select the Storage Center on which to assign the server.
5. Click **Next**.
6. Select the server on the Storage Center to assign to the virtual machine.
7. Click **Finish**.

Create a Storage Center Server Object for a Virtual Machine

If there is no virtual server object on the Storage Center, create one for the virtual machine.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select the virtual machine that needs to be created on a Storage Center.
3. In the right pane, click **Create Virtual Server on Storage Center**. The **Create SC Server for Virtual Machine** dialog box appears.
4. Select the Storage Center on which to create the server.
5. Click **Next**.
6. Enter a name for the server in the **Server Name** field.
7. Select the operating system of the server from the **Server Operating System** field.
8. Click **Finish**.

Manually Mapping a Windows Server to a Storage Center Server

If the WWNs of a server are not correctly associated with the appropriate Storage Center server objects, you can manually create the mappings.

Add a Mapping Between a Windows Server and a Storage Center Server

If Storage Manager did not automatically recognize the WWNs of a Windows server when it was registered, manually associate the server with a Storage Center server.

Steps

1. Click the **Servers** view.
2. Select a Windows server in the **Servers** pane. The **Summary** tab appears.
3. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
4. Click **Add** in the **Manual Storage Center Server Mapping** area. The **Select Storage Center** dialog box appears.
5. Select the Storage Center to which you want to map a server and click **OK**. The **Select Server** dialog box appears.
6. Select the server object on the Storage Center to map to and click **OK**.
7. Click **OK**. The server mapping is added and the **Edit Settings** dialog box reappears.
8. Click **OK**.

Remove a Mapping Between a Windows Server and a Storage Center Server

If a Windows server no longer uses storage on a manually mapped Storage Center, you can remove the association.

Steps

1. Click the **Servers** view.
2. Select a Windows server in the **Servers** pane. The **Summary** tab appears.
3. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
4. Select the mapping to remove in the **Manual Storage Center Server Mapping** area.
5. Click **Remove**. The **Delete Objects** dialog box appears.
6. Click **OK**. The server mapping is removed and the **Edit Settings** dialog box reappears.
7. Click **OK**.

Managing NAS Appliances Powered by Windows Storage Server

The **Servers** view displays operating system and HBA connectivity information about Dell NAS appliances powered by Windows Storage Server. If the IPMI card is correctly configured, you can view hardware status, clear the system event log, and control the power.

View Operating System Information about a Windows-Based NAS Appliance

The **Summary** tab displays information about the NAS server software and hardware.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select a Windows-based NAS appliance. The **Summary** tab appears.

   The **Summary** tab displays information about the appliance operating system, connected Storage Centers, HBA ports, and volumes.

View HBA Connectivity Information for a Windows-Based NAS Appliance

The **Connectivity** tab displays information about the HBAs installed in the appliance. For each HBA, the **Storage Center Server Ports** pane displays the corresponding Storage Center server objects.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select a Windows-based NAS appliance. The **Summary** tab appears.
3. Click the **Connectivity** tab.

View Hardware Health Information for a Windows-Based NAS Appliance

The IPMI card in the Windows-based NAS appliance provides hardware monitoring and remote management functionality.

Prerequisites

- The IPMI card in the appliance must be configured.
- IPMI card information must be configured in Storage Manager.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select a Windows-based NAS appliance. The **Summary** tab appears.
3. Click the **IPMI** tab.

   The **IPMI** tab displays IPMI alerts, fan speed, temperature, voltage, and power supply information.

Clear the System Event Log (SEL) for a Windows-based NAS appliance

If the IPMI card is configured correctly, you can remotely clear the system event log.

Prerequisites

- The IPMI card in the appliance must be configured.
- IPMI card information must be configured in Storage Manager.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select a Windows-based NAS appliance. The **Summary** tab appears.
3. Click the **IPMI** tab.
4. Click **Clear SEL**. The **Clear SEL** dialog box appears.
5. Click **OK**. The system event log is cleared.

Shut Down a Windows-Based NAS Appliance

If the IPMI card is configured correctly, you can remotely shut down a Windows-based NAS appliance.

Prerequisites

- The IPMI card in the appliance must be configured.
- IPMI card information must be configured in Storage Manager.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select a Windows-based NAS appliance. The **Summary** tab appears.

3. Click the **IPMI** tab.
4. Click **Power Off**. The **Power Off** dialog box appears.
5. Click **OK**. The appliance is powered off.

Reset the Power for a Windows-Based NAS Appliance

If the IPMI card is configured correctly, you can remotely reset power for a Windows-based NAS appliance.

Prerequisites

- The IPMI card in the appliance must be configured.
- IPMI card information must be configured in Storage Manager.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select a Windows-based NAS appliance. The **Summary** tab appears.
3. Click the **IPMI** tab.
4. Click **Power Reset**. The **Power Reset** dialog box appears.
5. Click **OK**. The appliance power is reset.

Installing and Using the Server Agent on a Windows Server

To register a Windows server to Storage Manager, the Storage Manager Server Agent must be installed on the server. The Server Agent allows Storage Manager to communicate with the Windows server to retrieve information and streamline storage management for the server.

Download the Server Agent

Download the Server Agent Installer .msi file from the Data Collector website.

About this task

If you are installing the Server Agent on a full installation of Windows Server, perform this task from the server. If you are installing the Server Agent on a core installation of Windows Server, download the Server Agent on another computer and then transfer the file to the server.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Download** tab.
5. Click the **Download Windows Installer (.msi)** link located to the right of **Server Agent**.

Install and Register the Server Agent

Install the Storage Manager Server Agent on a Windows server to collect information and display information about the server. If you are using Microsoft Hyper-V virtualization, the Server Agent can be installed on the host server and virtual machines running Windows. If you are using VMware virtualization, the Server Agent can be installed on virtual machines running Windows.

Install the Server Agent on a Server Core Installation of Windows Server

Install Microsoft .NET Framework 2.0, open the required TCP ports, install the Server Agent, and register the Server Agent to the Data Collector.

Prerequisites

- The Server Agent must be downloaded.
- The server must meet the Server Agent requirements in the *Storage Manager 2020 R1 Release Notes*.
- The server must have network connectivity to the Storage Manager Data Collector.
- The firewall on the server must allow TCP port 27355 inbound and TCP port 8080 outbound.

Steps

1. Transfer the Server Agent Installer .msi file to the server.
2. Run the Server Agent installer from the command line to install the Server Agent on the server.
3. Complete the wizard to install the Server Agent.
4. On the last page of the wizard, select the **Launch Server Agent Manager** check box, then click **Finish**. The **Properties** dialog box appears.
5. Register the Server Agent with the Storage Manager Data Collector.

   NOTE: Server Agents can also be registered using the **Server** view in the Storage Manager Client.

   a. Specify the address and port of the Storage Manager Data Collector.
      - **Host/IP Address:** Enter the host name or IP address of the Data Collector.
      - **Web Services Port:** Enter the Legacy Web Service Port of the Data Collector. The default is 8080.
   b. (Optional) Configure Storage Manager to automatically add the server to the Storage Center(s) to which it has connectivity.
      - To automatically add the server, select the **Automatically Manage on Storage Center** check box.
      - To automatically add virtual machines hosted by the server, select the **Automatically Manage Virtual Machines on Storage Center** check box.

      NOTE: If the server has physical iSCSI HBAs, Storage Manager may not automatically recognize the WWNs for the server. In this situation, configure the iSCSI HBA(s) to target the Storage Center, create a server on the Storage Center, then manually map the Storage Center server to the Server Agent.
   c. Click **OK**.

Related concepts

Default Ports Used by Storage Manager on page 25
Manually Mapping a Windows Server to a Storage Center Server on page 167

Related tasks

Register a Windows-Based Server on page 157

Install the Server Agent on a Full Installation of Windows Server

Install the Server Agent and register it to the Data Collector.

Prerequisites

- The Server Agent must be downloaded.
- The server must meet the Server Agent requirements in the *Storage Manager 2020 R1 Release Notes*.
- The server must have network connectivity to the Storage Manager Data Collector.
- The firewall on the server must allow TCP port 27355 inbound and TCP port 8080 outbound.
- If you are installing the Server Agent on a NAS server, the IPMI card must be configured.

Steps

1. Double-click the downloaded Server Agent Installer .msi file.
2. Complete the wizard to install the Server Agent.
3. On the last page of the wizard, select the **Launch Server Agent Manager** check box, then click **Finish**. The **Properties** dialog box appears.
4. Register the Server Agent with the Storage Manager Data Collector.

   NOTE: Server Agents can also be registered using the **Server** view in the Storage Manager Client.

   a. Specify the address and port of the Storage Manager Data Collector.
      - **Host/IP Address:** Enter the host name or IP address of the Data Collector.
      - **Web Services Port:** Enter the Legacy Web Service Port of the Data Collector. The default is 8080.

   b. (Optional) Configure Storage Manager to automatically add the server to the Storage Center(s) to which it has connectivity.
      - To automatically add the server, select the **Automatically Manage on Storage Center** check box.
      - To automatically add virtual machines hosted by the server, select the **Automatically Manage Virtual Machines on Storage Center** check box.

      NOTE: If the server has physical iSCSI HBAs, Storage Manager may not automatically recognize the WWNs for the server. In this situation, configure the iSCSI HBA(s) to target the Storage Center, create a server on the Storage Center, then manually map the Storage Center server to the Server Agent.

   c. If the Server Agent is installed on a NAS server, enter the IPMI configuration settings in the following fields:
      - **IPMI IP Address:** Enter the IP address of the IPMI card.
      - **IPMI User Name:** Enter the IPMI user name.
      - **IPMI Password:** Enter the IPMI password.

   d. Click **OK**.

Related concepts

Default Ports Used by Storage Manager on page 25
Manually Mapping a Windows Server to a Storage Center Server on page 167

Related tasks

Register a Windows-Based Server on page 157

Manage the Server Agent with Server Agent Manager

Use the Server Agent Manager to manage and configure the Server Agent service.

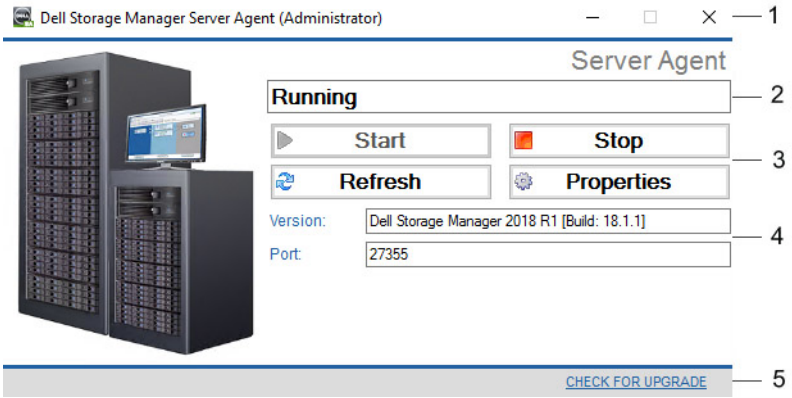


Figure 21. Server Agent Manager Dialog Box

The following table lists the objects in the Server Agent window.

Callout	Name
1	Minimize/Close
2	Status Message Area
3	Control Buttons
4	Version and Port
5	Commands

Start the Server Agent Manager

Under normal conditions, the Server Agent Manager is minimized to the Windows system tray.

About this task

To open the Server Agent Manager, perform either of the following actions on the server:

- If the Server Agent Manager is minimized, double-click the Server Agent Manager icon in the Windows system tray.
- If the Server Agent Manager is not running, start the **Storage Manager Server Agent Manager** application.
- If the Server Agent is installed on a server core installation of Windows Server, run the following command:

```
"c:\Program Files (x86)\Compellent Technologies\Enterprise Services
Agent\ServerAgentManager.exe"
```

The **Server Agent Manager** window appears.

Change the Listening Port of the Server Agent Service

If the default Server Agent listening port (27355) is already in use on the server, you can specify a custom port.

Steps

1. In Server Agent Manager, click **Properties**. The **Properties** dialog box appears.
2. Enter the port number in the **Socket Listening Port** field.
3. Click **OK**.

Modify the Connection to the Data Collector

If the Data Collector port, host name, or IP address has changed, use the Server Agent Manager to update the information.

Steps

1. In Server Agent Manager, click **Properties**. The **Properties** dialog box appears.
2. Specify the address and port of the Storage Manager Data Collector.
   - **Host/IP Address**: Enter the host name or IP address of the Data Collector.
   - **Web Services Port**: Enter the Legacy Web Service Port of the Data Collector. The default is 8080.
3. If the Server Agent is installed on a NAS server, enter the configuration settings of IPMI in the following fields:
   - **IPMI IP Address:** Enter the IP address of the IPMI card.
   - **IPMI User Name:** Enter the IPMI user name.
   - **IPMI Password:** Enter the IPMI password.
4. Click **OK**. The **Properties** dialog box closes.

Update the Server Agent to Match the Data Collector Version

If the Data Collector is updated to a new version, use the Server Agent Manager to update the Server Agent to a matching version.

Steps

1. In the Windows system tray, double-click the Server Agent icon. The **Server Agent Manager** window appears.
2. Click **CHECK FOR UPGRADE**. The Server Agent contacts the Data Collector to determine if an update is available.

   If a new Server Agent is available, the **Upgrade Available** dialog box appears.
3. Click **OK**. The Storage Manager website opens in the default browser and prompts you to download the updated Server Agent install file.
4. Save the Server Agent setup file to a local disk on the Windows server.
5. Double-click on the setup file. If the **Open File - Security Warning** dialog box appears, click **Run**.

   A Server Agent upgrade dialog box appears that asks if you want to continue.
6. Click **Yes**. The install wizard appears.
7. Complete the install wizard to update the Server Agent.

Uninstalling the Server Agent

Uninstall the Server Agent if you no longer need to automate storage management for the server.

7

Managing Virtual Volumes With Storage Manager

VVols is VMware's storage management and integration framework, which is designed to deliver a more efficient operational model for attached storage. This framework encapsulates the files that make up a virtual machine (VM) and natively stores them as objects on an array.

The VVols architecture enables granular storage capabilities to be advertised by the underlying storage. Storage containers, which define the available storage capabilities, can be created for vSphere Storage Policy-Based Management.

Topics:

- Configuring VVols in Storage Manager
- VMware Virtual Volume Concepts
- Setting Up VVols Operations on Storage Manager
- VASA Provider
- Managing Storage Containers
- Creating VVol Datastores
- Create a Datastore and Map it to VMware ESX Server
- View VVol and Datastore Information
- Protocol Endpoint Monitoring

Configuring VVols in Storage Manager

VMware vSphere 6 or later is required to run VVols in a storage environment with Storage Manager.

Requirements and Recommendations for Configuring VVols in Storage Manager

The following requirements and recommendations apply to setting up Storage Manager to use VVols:

- Storage Manager must be installed on a clustered hypervisor of choice with high-availability (HA) enabled.
- Fault Tolerance is recommended.
- Storage Manager must not be deployed or moved to a VVol datastore on the managed Storage Center. Storage Manager must be installed and remain on a traditional SAN volume
- Storage Manager must be installed on a separate management cluster.
- VVols is supported with the iSCSI and Fibre Channel interfaces only. FCoE and front end SAS are not supported for VVols.
- The network card must support the Secondary LUNID feature. For more information, search for I/O Devices with the Secondary LUNID in the *VMware Compatibility Guide*, available from http://www.vmware.com/resources/compatibility/search.php.

Safeguarding VVols Data

A critical component of the total VVols solution is the VM metadata.VMware's ESXi reads and writes this metadata to each VVol during control plane operations, such as power-on, power-off, and snapshots.

The Data Collector stores the VVols metadata written by the VASA provider in a database.

During Data Collector deployment (installation or migration) and during VASA provider registration, the production user is reminded to use an external database.

Use of the internal database is a consideration for lab deployments only. Depending upon the protection model used in deployment, failure to use the external database could result in the loss of some or all VVols metadata when the Data Collector is uninstalled or deleted. Use of the external database negates this risk during uninstall or delete.

The external database is expected to be deployed in a highly available manner including redundant switching connectivity.

Lab Experimentation Use of VVols

In a preproduction lab environment, a user could experiment with VVols and choose to purge all data on the array and restart with the intention of redeploying another VVols lab environment for experimentation purposes.

The proper steps for purging data in a LAB environment only are:

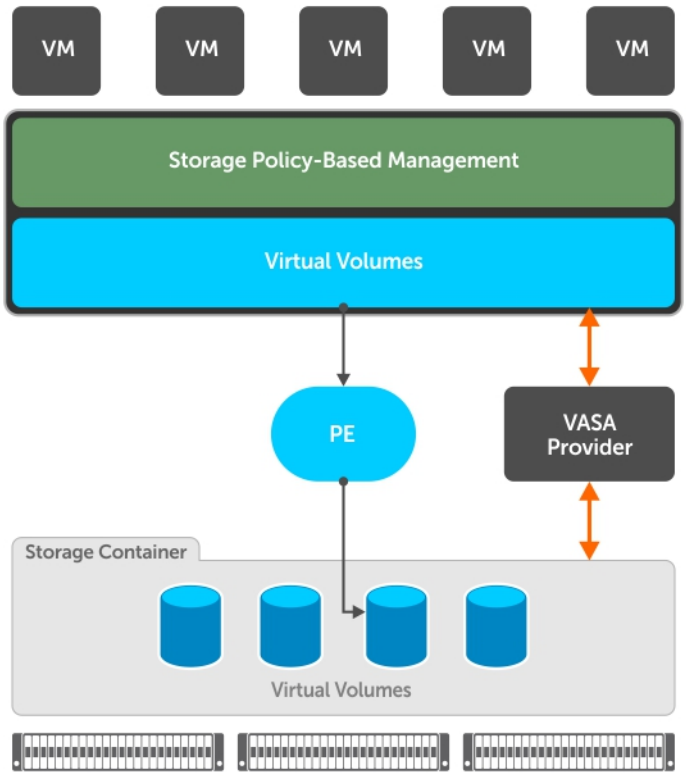
1. Using VMware vCenter — Delete all respective VVols VMs
2. Using Storage Center—Perform Purge

In the event the order is reversed, VVols metadata remains in the database even if the Data Collector is uninstalled. This metadata must be deleted to ensure a robust operating environment if a new lab environment is to be set up to use VVols. Failure to do so results in failures to some VVols VM operations to reference incorrect metadata.

If the order is reversed, contact technical support to work through the purge process.

VMware Virtual Volume Concepts

The following figure shows the virtual volumes (VVols) model defined by VMware.



The VVol framework introduces these components:

- VASA provider — A VASA provider (VP) is a software component that acts as a storage awareness service for vSphere. Storage vendors develop VASA providers to work with their specific storage arrays.
- Protocol endpoint (PE) — A protocol endpoint is the connection used for VVol storage, and the means by which you can access VVol storage containers. The protocol endpoint is also where access controls are placed and initiators are queried to ensure that they are permitted access to the storage containers and virtual volumes. Protocol endpoints are created and presented by Storage Manager when a VMware ESXi 6.0 server type is created in Storage Manager.

vSphere recognizes them as protocol endpoints after the VASA provider is registered and a Storage Container is created using Storage Manager.

- Storage container — A storage container is a quantity of storage made available for the placement of virtual volumes-based VMs. Each array has at least one storage container. Each storage container has one or more protocol endpoints associated with it.

  NOTE: Storage containers are not supported outside of the virtual volumes context.

  You must use Storage Manager (connected to a Data Collector Manager) to create storage containers.

Setting Up VVols Operations on Storage Manager

To set up and run operations for virtual volumes (VVols) in Storage Manager, you must:

- Register VMware vCenter Server in Storage Manager.
- Register VMware vCenter Server in Storage Center either by using **Auto manage Storage Center** option in Storage Manager or by manually adding vCenter server in Storage Center.
- Register the VASA provider on a vCenter server
- Create storage containers that are used to store the VVols objects created by the vCenter administrator
- Use Storage Manager to create datastores of type **VVOL**, which are mapped to the storage containers on the array using Storage Manager
- Use vCenter to create VVol-backed VMs

Storage Manager provides **Summary** and **Storage** views that provide information about storage containers, datastores, VVols, and protocol endpoints. These objects are managed using Storage Manager. Protocol endpoints are created automatically by Storage Manager and cannot be modified in any way.

Related concepts

Managing Storage Containers on page 179
VASA Provider on page 177

Virtual Volumes Restrictions

Volume operations on virtual volumes (VVols) are restricted to specific operations.

Storage administrators use Storage Manager to create storage container-backed vSphere datastores, also known as datastores of type **VVOL**. From within the vSphere web client these VVol datastores look no different from VMFS or NFS datastores. However, virtual machines stored within or on these VVol datastores are stored as virtual volumes on the array, organized within the storage container. Many of the same operations that can be performed again on traditional volumes can be performed against virtual volumes.

These volume operations are supported for VVols:

- Show
- Create Snapshot
- Set Snapshot Profiles
- Set Threshold Definitions

These volume operations are not supported for VVols:

- Edit Name
- Edit Properties
- Map Volume to Server
- Expand Volume
- Convert to Live Volume
- Delete
- Migrate
- Copy
- Mirror
- Replicate

Thick provisioning is not supported for operations such as creating or cloning a VVol VM. Only thin provisioning is supported.

VASA Provider

The VASA provider enables support for VMware VVols operations.

A VASA provider is a software interface between the vSphere vCenter server and vendor storage arrays. Dell provides its own VASA provider that enables vCenter to work with Dell storage. This VASA provider supports the VMware VASA 2.0 API specifications.

When the VASA provider is registered, vCenter can be used to create and manage VVols on the Storage Center.

You must configure the VASA provider if you intend to use VVols in your environment.

VASA Provider Restrictions

The following restrictions apply to the VASA provider:

- The Storage Manager VASA provider can be registered to only one vCenter Server.
- All ESXi and vCenter Server requests to the VASA provider are mapped to a single Storage Manager user.
- The VASA provider does not support user-defined storage profiles. Only default system-defined storage profiles can be used in VM Storage Policies.

Register the VASA Provider

You can register the VASA provider on a vCenter server, and manage it from the **Servers** view of Storage Center.

Register the VASA provider using one of the following methods:

- When initially registering a vCenter Server in the Storage Manager client, select the **Register VASA Provider** check box.
- For a vCenter Server that is already registered in the Storage Manager client, select **Edit Settings** and then select the **Register VASA Provider** check box.

NOTE: After a software update, the follow error might occur:

```
Error registering VASA provider: Error running VMware method

 [Method: RegisterVasaProvider] [Message: The VASA provider did not
respond]
```

Follow these steps to fix the error and register the VASA provider:

1. Open the file `:msaservice\plugins\module_manager\product-metadata.json .`
2. Change the VASA status to `deploy`.
3. Restart the Data Collector.

Related tasks

Register a VMware vCenter Server on page 158

Unregister a VASA Provider

Unregister a VASA provider to remove it from vCenter.

Prerequisites

CAUTION: The VASA provider must be unregistered before you initiate any of these tasks:

- **Any action related to uninstallation, migration, upgrade, reinstalling of Storage Manager on same host with same IP address**
- **Uninstalling Storage Manager with the intention of reinstalling on another host**
- **Changing the Storage Manager FQDN**

- **Changing the Storage Manager IP address**

Unregistering VASA will affects control plane operations on virtual volume VMs and datastores which are in use. It does not affect data transfer between an ESXi host and the respective SAN storage.

Unregistering the VASA provider results in powered-off VVol VMs being shown as inaccessible and datastores as inactive. To avoid prolonged control plane down time, minimize the period where the VASA provider remains unregistered. After re-reregistration, there could be a delay for powered-off VMs and datastores to recover from being inaccessible and inactive respectively.

Steps

1. Click the **Servers** view.
2. Select the **Servers** folder in the **Servers** pane.
3. Right-click the icon for the vCenter Server, and select **Edit Settings**.
   The **Edit VMware vCenter Server Settings** dialog box opens.
4. Click **Unregister VASA Provider**.
5. Click **OK**.

Using Storage Manager Certificates With VASA Provider

When you run the **Register VASA Provider** wizard, the URL of the VASA provider is automatically generated. This URL identifies the host on which the Data Collector is installed. The host is identified as either an IP address or fully qualified domain name (FQDN). Depending on how you installed or upgraded Storage Manager or if you changed the host for the Data Collector, you might need to take additional steps to update the certificates.

New Installation of Dell Storage Manager

If Storage Manager is registered with a name lookup service such as DNS server or Active Directory server, Storage Manager certificates are generated based on its FQDN. Any IP address changes do not affect certificates. If you change the FQDN, Storage Manager must be manually restarted if it is a Windows-based installation. It is automatically rebooted for the Virtual Appliance installation. If you were using the VASA provider before the IP changes, you must unregister and then register VASA Provider manually.

Upgrade of Dell Storage Manager

In Dell Storage Manager, certificates are based on IP addresses. After an upgrade to Dell Storage Manager, the existing certificates remain unchanged. If you need to modify the IP address of the host, the certificates need to be updated as described in the following table:

IP Change	Action Required
IP changes on Windows-based Storage Manager	If Storage Manager is not registered with a name lookup service such as DNS server or Active Directory, then Storage Manager and VASA certificates are based on the IP address of the Windows host. Before the IP address of the Windows host is changed, you must first unregister the VASA Provider. Then modify the IP address of the Windows host. Then manually restart Storage Manager to regenerate certificates based on the new IP address. After the restart, you must re-register the VASA Provider.
IP changes on the Virtual Appliance	On a Dell Storage Manager Virtual Appliance, network changes such as IP address happen through the Storage Manager and hence Storage Manager is aware of the changes. You must first unregister and the VASA Provider, then make the changes to the IP address. After the changes are done, Storage Manager restarts itself to regenerate certificates based on the new IP address. You then must re-register the VASA Provider.
Switch from an IP Address to an FQDN on Dell Storage Manager	To switch the certificates to use the FQDN instead of the IP address of the host, you must first unregister and the VASA Provider. Then register the Storage Manager host with a name lookup service. Then configure the

IP Change	Action Required
	networking properties on the host. Then follow the Dell Storage Manager procedure for deleting existing certificates and restart the Storage Manager. After the restart, re-register the VASA Provider.
FQDN changes on Windows or Virtual Appliance	If certificates are already using FQDN and you want to change the FQDN, unregister VASA Provider first. Then make changes to the name lookup service or Storage Manager host (or both) for the new FQDN. Then follow the old procedure for deleting certificates and restart Storage Manager. Re-register VASA Provider after Storage Manager is running. **NOTE:** Failure to unregister the VASA Provider before making changes in name lookup service results in initialization errors on vCenter for certain services and causes VASA registration to fail.
Switching from FQDN to IP Address on DellStorage Manager	If you want to stop using FQDN and go back to using IP addresses, unregister the VASA Provider first. Then make changes to the name lookup service or Storage Manager host (or both) to remove FQDN configuration. Restart Storage Manager for the changes to take effect and register VASA Provider again. **NOTE:** Failure to unregister the VASA Provider before making changes in name lookup service results in initialization errors on vCenter for certain services and causes VASA registration to fail.

Managing Storage Containers

A storage container is a pool of storage that is used in a VMware environment that supports VVols. Storage containers can be created using the following methods:

- From the **Storage** view in the Navigation pane of Storage Manager, select **Volumes**. Use the **Create Storage Container** function to create the storage container and specify its settings.
- From the **Servers** view in the Navigation pane of Storage Manager, select **Servers**. Use the **Create Datastore** function to create a datastore of the type **VVOL**. When you create a datastore using this function, you can also create a new storage container to be associated with the datastore, or map to an existing storage container to be associated with the datastore.

  NOTE: This is the recommended method.

After a storage container has been created, you can use vCenter to create a datastore and map it (mount it) to the storage container. The datastore can then be used to create VVol-based VMs.

Details about storage containers and VVols are shown in the **Summary** tab when you select the **Severs** node.

How Storage Container Options Affect vCenter Advertised Capabilities

Creating a storage container includes specifying options such as the use of compression, deduplication, encryption, snapshots and Storage Center Storage Profiles. These options are advertised as capabilities to vCenter. The following VASA version 2.0 system storage capabilities are supported by Storage Manager, and are shown on the vCenter **Summary** tab under **Capability Sets** and in Default Profiles in vCenter for individual datastores.

- compression
- dedupe
- encryption
- snapshotCapable
- SCstorageProfile

NOTE: These capabilities apply only to VVol datastores. They do not apply to legacy VMFS datastores.

A VMware administrator can use storage capabilities to create VM Storage Policies in vCenter.

Related tasks

Create a Datastore and Map it to VMware ESX Server on page 164

Data Reduction Options for VVols

You can specify data reduction options when creating storage containers. These options are advertised (made available) to the VMware administrator during VM Storage Profile creation.

When you use Storage Manager to create storage containers, you can optionally set these data reduction options:

- **Deduplication Allowed**
- **Compression Allowed**

Specifying one or both of these options indicates the data reduction preferences for VMs that are then created.

You can also specify options for **Data Reduction Input**:

- None
- Compression
- Deduplication with Compression

These options are presented as checkboxes on the **Create Storage Container** wizard.

NOTE: Even if the **Compression Allowed** and **Deduplication Allowed** checkboxes are selected, selecting the **None** profile option results in no action being taken.

You can also select the **Default Data Reduction Profile**, if one has been specified using the User Preferences.

After a storage administrator creates a storage container with data reduction options specified, these options are advertised (shown as being selected) on the VM Storage Profile wizard when a VMware administrator creates a storage profile. If you edit the storage container's Data Reduction option, you also change the advertised capabilities that are visible in the VM Storage Profile.

For information about using VM Storage Profiles, see the VMware vCenter documentation.

Factors That Affect Data Reduction Operation

When a new virtual volume is created, it can use any Data Reduction type supported by the storage container. The preference for the Data Reduction type on the virtual volume is influenced by either:

- The VM Storage Profile, if one is established and used
- The default Data Reduction Profile set for the storage center

The following factors affect how Data Reduction options are applied:

- If no VM Storage Policy is chosen, the Data Reduction type defaults to the value selected by the **Default Data Reduction Profile**.
- Editing an existing storage container's properties to change the value of the **Default Data Reduction Profile** does not affect existing virtual volumes. This change applies only to new volumes created afterward.
- If an existing volume has an enabled feature that is now disabled, the volume itself does not change. In the VM Storage Profile, the volume would now appear to be noncompliant. To bring the volume back into compliance, you can apply a compliant policy to the volume.

NOTE: The VM Storage Profile takes precedence when compatible storage exists.

NOTE: VM storage policies are applied only to data and config VVols and not to memory and swap VVols.

NOTE: When modifying VM storage policies especially for compression and deduplication, apply the VMware administrator policies to all volumes associated with VM. If these same changes are not applied to all volumes, some portion of the VM could be compressed while other portions could be uncompressed.

NOTE: The advertised capabilities only apply to VVols datastores and are not supported on legacy VMFS datastores.

NOTE: Any change to a storage container's Data Reduction profile might cause future fast cloned VMs to be created with mismatched Data Reduction profiles for the config and data VVols. A fast clone VM shares history with the VM from which it was created. Hence its data VVols inherit the settings of the data VVols of the original VM. There is another side effect of this shared history — if a user applies a VM Storage Policy to the original VM, the same changes apply to the data VVols of the fast clone VM and conversely.

NOTE: When applying a VM Storage Policy containing rules for the **ScStorageProfile** capability, the vCenter administrator can ignore the datastore compatibility warning `Datastore does not satisfy required properties.`. The VASA provider overrides the datastore's configured value and applies the user-provided value of **ScStorageProfile** for VVols of the VM.

Expected Behaviors for Data Reduction Scenarios

The settings specified in both the storage container Data Reduction options and in the VMware Storage Profile determine the results of VM and VVol creation. If the storage container Data Reduction settings conflict with the settings in the VM Storage Profile, creation of VMs and virtual volumes could fail.

The following table describes the expected behavior for new VM creation with the **Compression** option.

Table 6. Expected Behavior for New VM Creation with Compression

	VM Storage Policy = None Specified	VM Storage Policy = Compression Enabled	VM Storage Policy = Compression Disabled
Storage Container Compression Enabled	Volumes created with Default Data Reduction profile value from storage container	Volumes created with **Compression** Data Reduction Profile	Volumes created with the Data Reduction Profile set to **None**
Storage Container Compression Disabled	Volumes created with Default Data Reduction profile value from storage container	VM creation fails because user is trying to set an unsupported capability	Volumes created with the Data Reduction Profile set to **None**

The following table describes the expected behavior for new VM creation with the **Deduplication** option.

Table 7. Expected Behavior for New VM Creation with Deduplication

	VM Storage Policy = None Specified	VM Storage Policy = Deduplication Enabled	VM Storage Policy = Deduplication Disabled
Storage Container Deduplication Enabled	Volumes created with Default Data Reduction profile value from storage container	Volumes created with **Dedup with Compression** Data Reduction Profile	Volumes created with the Data Reduction Profile set to **None**
Storage Container Deduplication Disabled	Volumes created with Default Data Reduction profile value from storage container	VM creation fails because user is trying to set an unsupported capability	Volumes created with the Data Reduction Profile set to **None**

The following table describes the expected behavior for existing VMs when a vCenter user changes the associated VM policy. This table assumes that both Compression and Deduplication are enabled on the storage container.

Table 8. Expected Behavior for VM Storage Policy Update on Existing VMs

Old VM Storage Policy	New VM Storage Policy	Expected Behavior
Compression Enabled	Compression Disabled	Data Reduction Profile of associated VVols changes from **Compression** to **None**. Data is uncompressed at the next data progression cycle.
Compression Disabled/ None Specified	Compression Enabled	Data Reduction Profile of associated VVols changes from **None** to **Compression**. Data is compressed at the next data progression cycle.
Deduplication Disabled	Deduplication Enabled	Data Reduction Profile of associated VVols changes to **Deduplication with Compression**. Data is deduplicated at the next data progression cycle.
Deduplication Enabled	Deduplication Disabled	Data Reduction Profile of associated VVols changes from **Deduplication with Compression** to **None**. Data is rehydrated at the next data progression cycle.

The following table describes the expected behavior for existing VMs when a storage administrator selects or clears the **Compression** and **Deduplication** checkboxes on a storage container.

Table 9. Expected Behavior for Compression and Deduplication Checkboxes on Storage Container

Old Checkbox Value	New Checkbox Value	Expected Behavior
Compression Enabled	Compression Disabled	Data Reduction Profile of existing volumes remains unchanged. Compliance check warns that the VM is not compliant with storage container. Clone/Fast Clone of VM to the same storage container follows rules of Expected Behavior for New VM Creation with Compression on page 181 and might fail if the VM Storage Policy is now noncompliant. New volumes are created with the Data Reduction Profile set to **None**.
Compression Disabled	Compression Enabled	Data Reduction Profile of existing volumes remains unchanged. Clone/Fast Clone of VM to the same storage container follows rules of Expected Behavior for New VM Creation with Compression on page 181 and does not fail. New volumes are created with the Data Reduction Profile according to Expected Behavior for New VM Creation with Compression on page 181.
Deduplication Disabled	Deduplication Enabled	Data Reduction Profile of existing volumes remains unchanged. Clone/Fast Clone of VM to the same storage container follows rules of Expected Behavior for New VM Creation with Deduplication on page 181 and does not fail. New volumes are created with the Data Reduction Profile according to Expected Behavior for New VM Creation with Deduplication on page 181.
Deduplication Enabled	Deduplication Disabled	Data Reduction Profile of existing VVols remains unchanged. Compliance check warns that the VM is not compliant with the storage container. Clone/Fast Clone of VM to the same storage container follows rules of Expected Behavior for New VM Creation with Deduplication on page 181 and might fail if the VM Storage Policy is now noncompliant. New volumes are created with the Data Reduction Profile based on Expected Behavior for New VM Creation with Compression on page 181 if Compression is enabled or with the Data Reduction Profile set to **None**.

The following table describes the expected behavior for datastores related to migration.

Table 10. Expected Behavior Related to Migration

Source Datastore	Destination Datastore	Expected Behavior
Storage Container Deduplication = Supported	Storage Container Deduplication = Supported Destination VM Storage Policy = Deduplication Enabled	Migration succeeds. The volume on the destination is created with the **Deduplication with Compression** Data Reduction Profile.
Storage Container Deduplication = Supported	Storage Container Deduplication = Not Supported Destination VM Storage Policy = Deduplication Enabled	Migration fails because the source VM Storage Policy is invalid on the destination.
Storage Container Deduplication = Supported Default Data Reduction Policy on Container = **Deduplication with Compression**	Storage Container Deduplication = Not Supported Destination VM Storage Policy = None Specified	Migration succeeds. The volumes on the destination inherit the destination storage container's default Data Reduction Profile.

Table 10. Expected Behavior Related to Migration (continued)

Source Datastore	Destination Datastore	Expected Behavior
Storage Container Compression = Supported	Storage Container Compression = Not Supported VM Storage Policy = Compression Enabled	Migration fails because the source VM Storage Policy is invalid on the destination.
Storage Container Compression = Supported Default Data Reduction Policy on Container = **Compression**	Storage Container Compression = Not Supported VM Storage Policy = None Specified	Migration succeeds. The volumes on the destination inherit the destination storage container's default Data Reduction Profile.

Create a Storage Container Using the Storage View

Create a storage container to define storage options for virtual volumes (VVols).

About this task

NOTE: Storage Center supports a maximum of 50 storage containers per Storage Center.

NOTE: If you use the method described in the following steps to create a storage container, the resulting storage container is empty and does not have any VVols datastores associated with it. If you use the **Create Datastore** method instead, you can create a storage container at the same time and associate the new datastore to the storage container.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the navigation pane, select **Volumes**.
4. In the right pane, click **Create Storage Container**.
   The **Create Storage Container** dialog box opens.
5. Specify general information about the storage container:
   a. In the **Name** field, type the name of the storage container.
   b. In the **Size** field, type the size and select the unit of measurement from the drop-down menu.
   c. To specify a volume folder as the location for the new storage container, click **Change** and select the volume folder.
   d. In the **Storage Type** field, select a storage type from the drop-down list.
6. Specify the advertised capabilities for new volumes created within the storage container:
   a. Specify whether to allow compression by selecting or clearing the **Compression Allowed** checkbox.
   b. Specify whether to allow deduplication by selecting or clearing the **Deduplication Allowed** checkbox.
   c. Specify whether to allow encryption by selecting or clearing the **Use Encryption** checkbox.
   d. (Optional) To specify the storage profiles to allow for new volumes created within the storage container, click **Change** next to the right of **Allowed Storage Profiles** and select the storage profiles.
7. Specify the default settings for new volumes created within the storage container:
   a. Select the default snapshot profile setting from **Default Snapshot Profile** drop-down menu.
   b. Select the default storage profile setting from the **Default Storage Profile** drop-down menu.
   c. Select the default data reduction profile setting from the **Default Data Reduction Profile** drop-down menu.
   d. Select the default data reduction input setting from the **Default Data Reduction Input** drop-down menu.
8. Click **OK**.

Edit a Storage Container Using the Storage View

Modify a storage container to edit its settings.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the navigation pane, select **Volumes**.
4. Right-click on the storage container to modify and select **Edit Settings**.
   The **Edit Storage Container Settings** dialog box opens.
5. Modify the fields of the storage container as needed.
6. Click **OK**.

Delete a Storage Container

You can delete a storage container if it is not being used.

About this task

NOTE: The Delete Storage Container task fails if you try to delete a storage container while any virtual volumes are associated with it.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the navigation pane, select **Volumes**.
4. Right-click on the storage container to delete and select **Delete**.
   The **Delete** confirmation dialog box opens.
5. Click **OK**.

View Storage Container Information

Use the Volumes node in the Storage tab to display information about storage containers and virtual volumes (VVols).

Storage containers appear in the Storage Center **Storage** tab along with volumes. To view information about a storage container, click the name of the storage container.

When viewing information about a storage container, you can select the **Summary**, **Volumes**, **Charts**, and **Historical Usage** tabs.

Creating VVol Datastores

Storage containers must first be defined on the Storage Center before vCenter can use the storage container. After a storage container is created, vCenter is able to create VVol-based VMs in the storage container. When you use the **Create Datastore** action using Storage Manager, you create datastores of the type **VVOL** and specify the storage container to hold the datastore.

Create a Datastore and Map it to VMware ESX Server

You can create a datastore, map it to a VMware ESX environment, and mount it to the cluster in one operation.

Steps

1. Click the **Servers** view.
2. In the **Servers** pane, select the VMware ESXi cluster or host on which to create the datastore.

3. In the right pane, click **Create Datastore**.
   The **Create Datastore** dialog box opens.
4. Type a name for the datastore in the **Datastore Name** field.
5. Select the type of datastore to create:
   - **Standard Datastore (VMFS)**
   - **VVol Datastore**
6. Click **Next**.
7. If you selected **Standard Datastore (VMFS)**, complete the following steps:
   a. Select a unit of storage from the drop-down menu and type the size for the datastore in the **Total Space** field.
   The available storage units are bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), and terabytes (TB).
   b. Select the size limit for virtual disks within the datastore from the **Max File Size** drop-down.
   c. Select the Storage Center on which to create the datastore from the **Storage Center** drop-down menu.
   d. To specify the folder in which to create the datastore, select a folder from the **Volume Folder** area.
   e. To add notes to the datastore, type notes in the **Notes** field.
   f. To specify a snapshot profile, click **Change**, select a profile in the **Select Snapshot Profiles** dialog box, and click **OK**.
   g. To specify a data reduction profile, select a profile from the **Data Reduction Profile** drop-down menu.
   h. To use specific tiers and RAID levels for datastore data, select the appropriate Storage Profile from the **Storage Profile** drop-down menu.
   i. If more than one storage type is defined on the Storage Center, select the storage type to provide storage from the **Storage Type** drop-down menu.
   j. If you want to specify a custom LUN, restrict mapping paths, configure multipathing, or make the datastore read-only, click **Advanced Mapping**.
8. If you selected **VVol Datastore**, select the radio button for the storage container to use for the VVol datasore
   - **Use Existing New Storage Container** – If you selected this option, a list of existing storage containers is displayed. Select the storage container to use and click **Finish**.
   - **Create a New Storage Container** – If you selected this option, complete the following steps:

   a. Select the Storage Center on which to create the datastore from the **Storage Center** drop-down menu.
   b. Select a unit of storage from the drop-down menu and type the size for the datastore in the **Size** field. The available storage units are bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), and terabytes (TB).
   c. To specify the folder in which to create a datastore, click **Change**, select a folder from the **Select Volume Folder** dialog box, and click **OK**.
   d. If more than one storage type is defined on the Storage Center, select the storage type to provide storage from the **Storage Type** drop-down menu.
   e. Specify whether to allow compression by selecting or clearing the **Compression Allowed** checkbox.
   f. Specify whether to allow deduplication by selecting or clearing the **Deduplication Allowed** checkbox.
   g. Specify whether to allow encryption by selecting or clearing the**Use Encryption** checkbox.
   h. (Optional) To specify the storage profiles to allow for new datastores, click **Change**, select the storage profiles to allow from the **Select Storage Profile** dialog box, and click **OK**.
   i. Select the default snapshot profile setting from the **Default Snapshot Profile** drop-down menu.
   j. Select the default data reductions profile setting from the **Default Data Reduction Profile** drop-down menu.
   k. Select the default storage profile setting from the **Default Storage Profile** drop-down menu.
   l. Select the default data reduction input setting from the **Default Data Reduction Input** drop-down menu.
9. Click **Finish**.

Related concepts

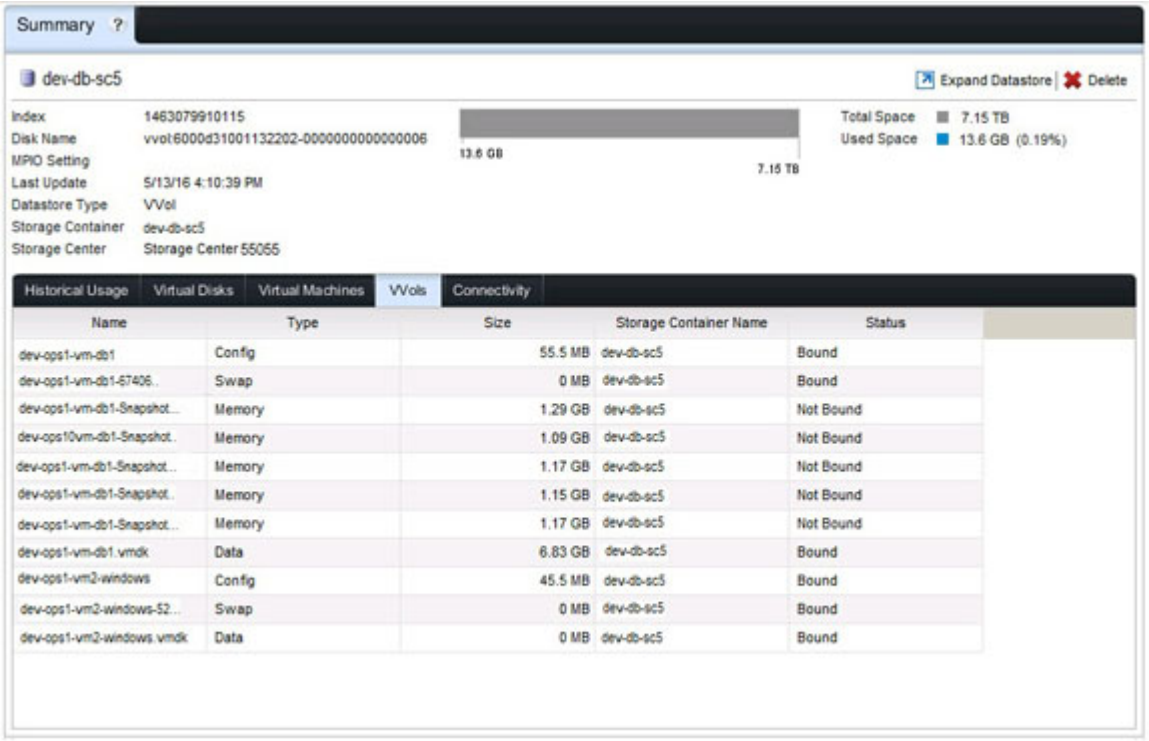
Creating Server Volumes and Datastores on page 163

View VVol and Datastore Information

The **Summary** view for a datastore shows details about the datastore.

Select the **Servers** node in Storage Manager and then select the datastores in the Storage Center hierarchy. To view details about a datastore, click the datastore name.

The following example shows the **Summary** view of a datastore.



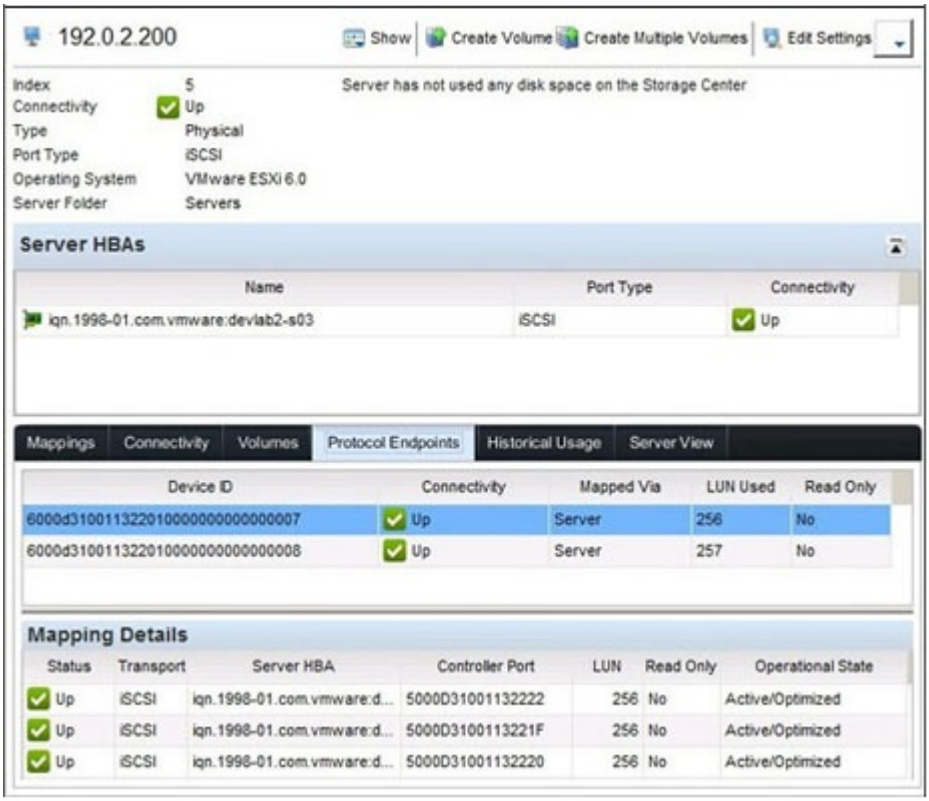
If the datastore was created with the type VVOL, the **VVols** tab identifies the virtual volumes stored in the storage container.

Protocol Endpoint Monitoring

You can view details about protocol endpoints that are associated with virtual volumes (VVols).

Protocol endpoints are automatically created when an ESXi 6.0 server is created in Storage Manager. Storage Manager exposes protocol endpoints in the **Storage** view. You can use Storage Manager to view protocol endpoint details for vSphere hosts.

The following example shows the protocol endpoints summary information displayed byStorage Manager.



If the host contains VVols, the **Storage** view for that host includes the following details about the protocol endpoints:

- Device ID
- Connectivity status
- Server HBA
- Mapped Via
- LUN Used
- Read Only (Yes or No)

8

PS Series Storage Array Administration

PS Series storage arrays optimize resources by automating performance and network load balancing. Additionally, PS Series storage arrays offer all-inclusive array management software, host software, and free firmware updates.

To manage PS Series storage arrays using Dell Storage Manager, the storage arrays must be running PS Series firmware version 7.0 or later.

Topics:

- About Groups
- About Volumes
- About Snapshots
- Managing Replication Schedules
- About Access Policies
- Monitoring a PS Series Group

About Groups

A PS Series group is a fully functional iSCSI storage area network (SAN).

You create a group when you configure one or more PS Series arrays and connect them to an IP network. In this virtualized storage system, the arrays become group *members* and share configuration data. A member belongs to a storage pool, and is configured with a specific RAID policy. Each member cooperates with other members to enable the virtualization of disk storage, controllers, caches, and network connections. Because the virtualization technology masks the underlying complexity of the storage configuration, client servers see the group as a single entity, giving you a centralized view of the storage data.

The following figure shows and example of PS Series groups. PS Series Group on page 188 explains the callouts used in the figure.

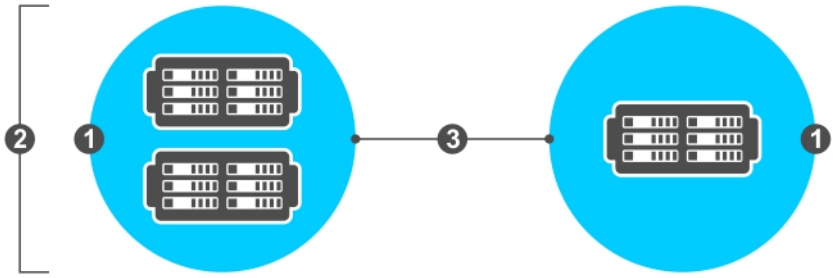


Figure 22. PS Series Group

Table 11. PS Series Group

Callout	Description
1	PS Series group Storage area network (SAN) comprising one or more PS Series arrays connected to an IP network. Arrays are high-performance (physical) block storage devices.
2	PS Series members One or more PS Series arrays represented as individual members within a pool to which it provides storage space to utilize.

Table 11. PS Series Group (continued)

Callout	Description
3	PS Series storage pools Containers for storage resources (disk space, processing power, and network bandwidth). A pool can have one or more members assigned to it.

A group can provide both block and file access to storage data. Access to block-level storage requires direct iSCSI access to PS Series arrays (iSCSI initiator). Access to file storage requires the FS Series NAS appliance using NFS or SMB protocols and the Dell FluidFS scale-out file system.

With storage data management features, you can:

- Manage a group through several built-in mechanisms such as ssh, serial line, telnet, and web-based user interfaces. You do not need an external management station or management software.
- Configure the system to alert you to management activity or problems through log files, SNMP traps, and email notification
- Add more arrays (up to 16) to a group to increase capacity and performance
- Secure data and management access with authorization and authentication mechanisms
- Protect storage data with replication and snapshots

Adding PS Series Groups

When PS Series groups are added to the Storage Manager Data Collector, they are associated with specific Storage Manager users. These users can view and manage only the PS Series groups to which they are mapped. PS Series groups that are visible to one Storage Manager user are not necessarily visible to another user.

When a Storage Manager user adds PS Series groups, they must provide credentials for a PS Series groups user account. The permission level assigned to a PS Series group user account determines the access that is allowed in the Storage Manager Client.

NOTE: A Storage Manager user with Reporter privileges cannot add PS Series groups to Storage Manager. To add PS Series groups to a user with Reporter privileges, log in to the Storage Manager Data Collector using a Storage Manager user with Administrator or Volume Manager privileges and map the PS Series groups to that reporter user on the **Users & User Groups** tab.

Add a PS Series Group

Add a PS Series group to Storage Manager to manage and monitor the PS Series group from the Dell Storage Manager Client.

Prerequisites

- You must have the user name and password for a PS Series group account.
- The Storage Manager Data Collector must have connectivity to the PS Series group management interface.
- A Storage Manager administrator cannot add the same PS Group that was already added by another administrator. However, a Storage Manager administrator can map that PS Group to his or her Storage Manager account using the Data Collector.

  Workaround: On a Windows installation, you can copy PS Group mappings to additional users from the **Data Collector Users & User Groups** tab. No workaround exists for the Data Collector Virtual Appliance.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the **PS Groups** node.
3. In the **Summary** tab, click **Add PS Group**. The **Add PS Group** wizard opens.
4. (Optional) Create a folder for the PS Series group.
   a. Click **Create Folder**.
   b. In the **Name** field, type a name for the folder.
   c. In the **Parent** field, select the **PS Groups** node or a parent folder.
   d. Click **OK**.
5. Enter PS Series group login information.

- **Hostname or IP Address** – Type the group or management IP address of the PS Series group.
  NOTE: Do not type the member IP address in this field.
- **User Name** and **Password** – Type the user name and password for a PS Series group user account.
- **Folder** – Select the **PS Groups** node or the folder to which to add the PS Series group.

NOTE: If you specify a PS Series group user account with Pool administrator or Volume administrator permissions, access to the PS Series group from Storage Manager is restricted based on the PS Series group user account permissions. You cannot add a PS Series group to Storage Manager using a user account with read-only account permissions.

6. Click **Finish**.

Reconnect to a PS Series Group

If Storage Manager cannot communicate with a PS Series group, Storage Manager marks the PS Series group as down. You can reconnect to a PS Series group that is marked as down.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the down PS Series group.
3. Right-click on the PS Series group and select **Reconnect to PS Group**. The **Reconnect PS Group** dialog box opens.
4. Enter PS Series group login information.
   - **Hostname or IP Address** — Type the host name or IP address of a PS Series group.
   - **User Name** and **Password** — Type the user name and password for a PS Series group user.
5. Click **OK**.

Configure Which Plugins Appear on the Summary Tab

Each summary plugin can be individually enabled or disabled.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. On the **Summary** tab, click **Select Summary Plugins**. The **Edit Summary Settings** dialog box appears.
4. Select the checkboxes of the plugins to display and clear the checkboxes of the plugins to hide.
5. Click **OK**.

Reorder Plugins on the Summary Tab

The summary plugins can be reordered using the arrow buttons on the **Edit Summary Settings** dialog box.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. On the **Summary** tab, click **Select Summary Plugins**. The **Edit Summary Settings** dialog box appears.
4. Reorder the summary plugins as needed.
   - To move a plugin up one level, click ^ once.
   - To move a plugin down one level, click v once.
   - To move a plugin to the top, click ^^ once.
   - To move a plugin to the bottom, click vv once.
5. Click **OK**.

Organizing PS Series Groups

Use folders to organize PS Series groups in Storage Manager.

Create a PS Group Folder

Use folders to group and organize PS Series groups.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the **PS Groups** node.
3. In the **Summary** tab, click **Create Folder**. The **Create Folder** dialog box opens.
4. In the **Name** field, type a name for the folder.
5. In the **Parent** field, select the **PS Groups** node or a parent folder.
6. Click **OK**.

Move a PS Series Group Into a Folder

A PS Series group can be moved to a PS Group folder at any time.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the PS Series group to move.
3. In the **Summary** tab, click **Move**. The **Select Folder** dialog box opens.
4. Select the folder to which to move the PS Series group.
5. Click **OK**.

Rename a PS Group Folder

Edit the settings of a PS Group folder to change the name of the folder.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the PS Group folder to modify.
3. In the **Summary** tab, click **Edit Settings**. The **Edit PS Group Folder Settings** dialog box opens.
4. In the **Name** field, type a name for the folder.
5. Click **OK**.

Move a PS Group Folder

Edit the settings of a PS Group folder to move the folder.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the PS Series group folder to move.
3. In the **Summary** tab, click **Edit Settings**. The **Edit PS Group Folder Settings** dialog box opens.
4. In the Parent area, select the PS Groups node or a parent folder.
5. Click **OK**.

Delete a PS Group Folder

Delete a PS Group folder if it is no longer needed.

Prerequisites

The PS Group folder must be empty to be deleted.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the PS Group folder to delete.
3. In the **Summary** tab, click **Delete**. The **Delete PS Group Folders** dialog box opens.
4. Click **OK**.

Remove a PS Series Group

Remove a PS Series group when you no longer want to manage it from Storage Manager.

About this task

NOTE: When a PS Series group is removed from all Storage Manager users with the Administrator or Volume Manager privilege, it is automatically removed from Storage Manager users with the Reporter privilege.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the PS Series group to remove.
3. In the **Summary** tab, click **Delete**. The **Delete PS Groups** dialog box opens.
4. Click **OK**.

Launch Group Manager

To manage a PS Series group using the Group Manager GUI, launch Group Manager from the PS Series group Summary tab.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. In the **Summary** tab, click **Launch Group Manager**. Group Manager opens in the default web browser.
4. Enter the user name and password for the PS Series group.
5. Click **Log In**.

About Volumes

Volumes provide the storage allocation structure within the PS Series group.

To access storage in a PS Series group, you allocate portions of a storage pool to volumes. You can create a volume on a single group member or one that spans multiple group members. You assign each volume a name, size, and a storage pool. The group automatically load balances volume data across pool members.

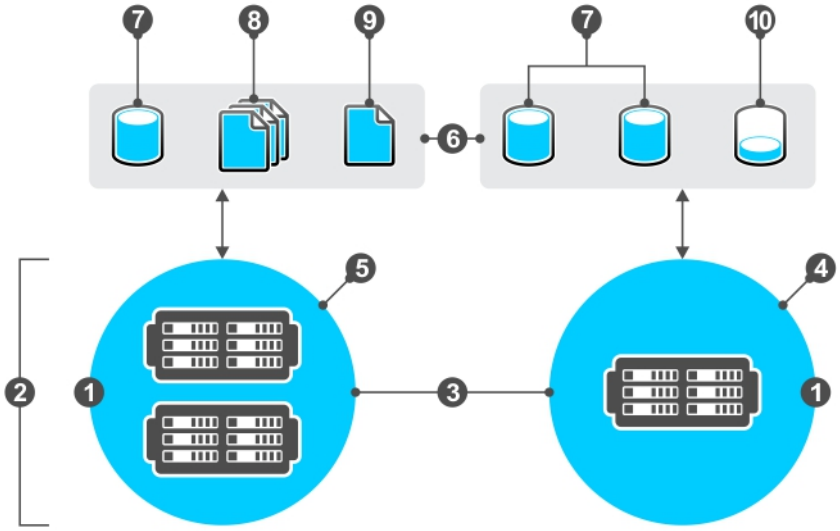


Figure 23. PS Series Volumes

Table 12. PS Series Volumes

Callout	Description
1	PS Series group Storage area network (SAN) comprising one or more PS Series arrays connected to an IP network. Arrays are high-performance (physical) block storage devices.
2	PS Series members Each PS Series array is a member in the group and is assigned to a storage pool.
3	PS Series storage pools Containers for storage resources (disk space, processing power, and network bandwidth).
4	PS Series single-member pool A PS Series array represented as a member within a pool to which it is assigned.
5	PS Series multimember pool Multiple PS Series arrays represented as individual members within a pool to which it is assigned.
6	Storage space Space received from PS Series arrays to allocate data as needed through various structures (volumes, snapshots, thin provisioning, replicas, containers, SMB/NFS, quotas, and local users and groups).
7	Volume Provides the structure for the PS Series group.
8	Snapshot collections A collection of snapshots within the PS Series group.
9	Snapshots A point-in-time copy of data from a volume or container. Snapshots can be created manually or automatically on a schedule.
10	Thin-provisioned volume (offline)

Table 12. PS Series Volumes (continued)

Callout	Description
	Thin provisioning allocates space based on how much is actually used, but gives the impression the entire volume size is available. (For example, a volume with 100GB storage can be allocated to use only 20GB, while the rest is available for other uses within the storage pool.) An offline volume indicates that it can no longer be accessed by the iSCSI initiator until it has been set online.

For each volume, the group generates an iSCSI target name, which you cannot modify. An iSCSI target name includes a prefix, a string, and the volume name. Initiators use the target name to connect to a volume. For example:

iqn.2001-05.com.equallogic:7-8b0900-6d0000000-001ebbc5d80sf0k0-db3

where:
prefix: iqn.2001-05.com.equallogic
string: 7-8b0900-6d0000000-001ebbc5d80sf0k0
volume name: db3

Each volume appears on the network as an iSCSI target. Hosts with iSCSI initiators use the volume's target name to connect to the volume.

Each iSCSI volume supports a set of features and capabilities:

- Snapshots — To protect volume data from mistakes, viruses, or database corruption, you can use snapshots.
- Replication — To protect against disasters, you can replicate volume data from one group to another.
- Thin Provisioning — To manage storage capacity utilization on demand, you can use thin provisioning.
- Clones — To create a boot image, full system backup, or transfer a system to another person, you can use cloning.
- Volume Undelete — To restore mistakenly deleted volumes, you might be able to use volume undelete.
  NOTE: The system permanently deletes volumes after 7 days, and sometimes sooner.
- Volume Folders — To organize volumes into folders for quick visual reference, you can use volume folders.
- Control Access to iSCSI Initiators — To protect your volumes from unauthorized and uncoordinated access by iSCSI initiators, you can use access control policies.
- Control Access to Hosts (servers) — To prevent inadvertent corruption of the volume caused by multiple hosts writing to it in an uncoordinated manner, enable multihost access to a volume.

Create a Volume

Create a volume to present a local unit of storage on a PS Series group.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select **Volumes**.
5. In the right pane, click **Create Volume**. The **Create Volume** dialog box opens.
6. In the **Name** field, type a name for the volume.
7. In the **Volume Folder** pane, select the Volumes node or a parent folder for the volume.
8. In the **Notes** field, type any notes to associate with this volume.
9. In the **Size** field, type a size for the volume in megabytes (MB), gigabytes (GB), or terabytes (TB).
10. (Optional) Configure the remaining volume attributes as needed.
    - To change the amount of space reserved for volume snapshots, type a percentage in the **Snapshot Reserve** field.
    - To copy ACL settings from an existing volume, click **Copy ACL**, select a volume from the dialog box, and click **OK**.
    - To change the storage pool assignment, click **Change**, select a storage pool from the dialog box, and click **OK**.
    - To change the sector size of the volume, select a size from the **Sector Size** area.
    - To enable thin provisioning, select the **Thin Provisioned Volume** checkbox:
      - In the **Minimum Volume Reserve** field, type the minimum reserve percentage of the volume.
      - In the **In-Use Warning Limit** field, type the in-use space warning limit percentage of the volume.

- To generate an warning event message when the in-use warning limit is exceeded, select the **Generate initiator error when in-use warning limit is exceeded.** checkbox.
- In the **Maximum In-Use Space** field, type the maximum in-use space percentage of the volume.
- To set the volume offline when the maximum in-use space is exceeded, select the **Set offline when maximum in-use space is exceeded** checkbox.

11. Click **OK**.

Modify a Volume

You can rename, move, or expand a volume after it has been created. You can also modify advanced volume attributes if needed.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Volumes** node and select a volume.
5. In the right pane, click **Edit Settings**. The **Edit Volume** dialog box opens.
6. In the **Name** field, type a name for the volume.
7. In the **Volume Folder** pane, select the Volumes node or a parent folder for the volume.
8. In the **Notes** field, type any notes to associate with this volume.
9. In the **Size** field, type a size for the volume in megabytes (MB), gigabytes (GB), or terabytes (TB).
10. (Optional) Configure the remaining volume attributes as needed.
    - To change the amount of space reserved for volume snapshots, type a percentage in the **Snapshot Reserve** field.
    - To change the warning threshold for snapshot space, type a percentage in the **Snapshot Space Warning Percent Threshold** field.
    - In the **Thin Provisioning Modes** area:
      - To enable thin provisioning, select the **Thin Provisioned Volume** checkbox:
      - In the **Minimum Volume Reserve** field, type the minimum reserve percentage of the volume.
      - In the **In-Use Warning Limit** field, type the in-use space warning limit percentage of the volume.
      - To generate an warning event message when the in-use warning limit is exceeded, select the **Generate initiator error when in-use warning limit is exceeded.** checkbox.
      - In the **Maximum In-Use Space** field, type the maximum in-use space percentage of the volume.
      - To set the volume offline when the maximum in-use space is exceeded, select the **Set offline when maximum in-use space is exceeded** checkbox.
    - In the **Volume iSCSI Settings** area:
      - Type a value in the **Public Alias** field to specify a public alias for the volume.
      - Select the **Allow simultaneous connections from initiators with different IQNs** checkbox if your environment supports multiple initiators accessing a volume.
11. Click **OK**.

Create a Volume Folder

Create a volume folder to organize volumes on a PS Series group.

Prerequisites

To use volume folders in Storage Manager, the PS Series group members must be running PS Series firmware version 8.0 or later.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.

4. In the **Storage** tab navigation pane, select the **Volumes** node.
5. In the right pane, click **Create Volume Folder**. The **Create Volume Folder** dialog box opens.
6. In the **Name** field, type a name for the folder.
7. (Optional) In the **Notes** field, type a description for the folder.
8. Click **OK**.

Edit a Volume Folder

Create a volume folder to organize volumes on a PS Series group.

Prerequisites

To use volume folders in Storage Manager, the PS Series group members must be running PS Series firmware version 8.0 or later.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Volumes** node.
5. Select the volume folder to edit.
6. In the right pane, click **Edit Settings**. The **Edit Volume Folder Settings** dialog box opens.
7. In the **Name** field, type a name for the folder.
8. (Optional) In the **Notes** field, type a description for the folder.
9. Click **OK**.

Delete a Volume Folder

Delete a volume folder if it is no longer needed.

Prerequisites

The volume folder must be empty to be deleted.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Volumes** node.
5. Select the volume folder to delete.
6. In the right pane, click **Delete**. The **Delete** dialog box opens.
7. Click **OK**.

Move a Volume to a Folder

Individual volumes can be organized by moving them to volume folders.

Prerequisites

To use volume folders in Storage Manager, the PS Series group members must be running PS Series firmware version 8.0 or later.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the volume to move.
5. In the right pane, click **Move to Folder**. The **Move to Folder** dialog box opens.
6. In the navigation pane, select a new volume folder.
7. Click **OK**.

Move Multiple Volumes to a Folder

Multiple volumes can organized by moving a selection of volumes to a volume folder.

Prerequisites

To use volume folders in Storage Manager, the PS Series group members must be running PS Series firmware version 8.0 or later.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the **Volumes** node or the volume folder that contains the volumes that you want to move.
5. In the right pane, select the volumes to move.
   - To select a group of volumes, select the first volume, then hold down Shift and select the last volume.
   - To select individual volumes, hold down Control while selecting them.
6. Right-click the selected volumes, then select **Move to Folder**. The **Move to Folder** dialog box opens.
7. In the navigation pane, select a new volume folder.
8. Click **OK**.

Rename a Volume

A volume can be renamed without affecting its availability.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the volume to modify.
5. In the right pane, click **Edit Settings**. The **Edit Volume** dialog box opens.
6. In the **Name** field, type a new name for the volume.
7. Click **OK**.

Clone a Volume

Clone a volume to create a copy of the volume.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.

3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume to clone.
5. In the right pane, click **Clone**. The **Clone Volume** dialog box opens.
6. In the **Name** field, type a name for the clone.
7. Click **OK**.

Modify Volume Access Settings

The read-write permission for a volume can be set to read-only or read-write. In addition, access to the volume from multiple initiators with different IQNs can be enabled or disabled.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume.
5. In the **Summary** tab, click **Set Access Type**. The **Set Access Type** dialog box opens.
6. Select the read-write permission for the volume.
   - **Set Read-Write** — You can add to, edit, and delete the contents of the volume.
   - **Set Read-Only** — You cannot add to, edit, or delete the contents of the volume.

     NOTE: Set a volume offline before changing the permission of the volume to read-only.
7. If your environment supports multiple initiators with different IQNs accessing a volume, select the **Allow simultaneous connections from initiators with different IQNs** checkbox. This option is disabled by default.
8. Click **OK**.

Set a Volume Online or Offline

When you create a volume, the PS Series group sets the volume online by default. An iSCSI initiator on a computer can discover or connect to an online volume.

About this task

To make a volume inaccessible to iSCSI initiators, set the volume offline. When a volume is set offline, the PS Series group closes all current iSCSI connections to the volume.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume.
5. If the volume is offline, click **Set Online** to set the volume online.

   If the volume is online, click **Set Offline** to set the volume offline.
6. Click **OK**.

Add Access Policy Groups to a Volume

To control volume access for a group of servers, add one or more access policy groups to a volume.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.

4. In the **Storage** tab navigation pane, select a volume.
5. In the right pane, click **Add Access Policy Groups**. The **Add Access Policy Groups to Volume** dialog box opens.
6. In the **Access Policy Groups** area, select the access policy groups to apply to the volume.
7. In the **Access Policy Group Targets** area, select whether the access policy groups apply to volumes and snapshots, volumes only, or snapshots only.
8. Click **OK**.

Add Access Policies to a Volume

To control volume access for individual servers, add one or more access policies to a volume.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume.
5. In the right pane, click **Add Access Policies**. The **Add Access Policies to Volume** dialog box opens.
6. In the **Access Policies** area, select the access policies to apply to the volume.
7. In the **Access Policy Targets** area, select whether the access policies apply to volumes and snapshots, volumes only, or snapshots only.
8. Click **OK**.

Create a Basic Access Point

A basic access point can be used to control access to a volume.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume.
5. In the right pane, click **Create Basic Access Point**. The **Create Basic Access Point** dialog box opens.
6. (Optional) In the **Description** field, type a description for the basic access point.
7. In the **CHAP Account** field, type the user name of the CHAP account that a computer must supply to access the volume.
8. In the **iSCSI Initiator** field, type the iSCSI initiator name of a computer to which you want to provide access to the volume.
9. In the **IPv4 Address** field, type the IPv4 address of a computer to which you want to provide access to the volume.
10. In the **Target Type** area, select whether the basic access point applies to the volume and snapshots, the volume only, or snapshots only.
11. Click **OK**.

Delete a Volume

Delete a volume from a PS Series group when you no longer need the volume.

Prerequisites

A volume must be offline to be deleted.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.

4. In the **Storage** tab navigation pane, expand the **Volumes** node and select the volume to delete.
5. Click **Delete**. The **Delete** dialog box opens.
6. Click **OK**.
   - If the volume does not contain data, the volume is permanently deleted.
   - If the volume does contain data, the volume is moved to the recycle bin.

Restore a Volume from the Recycle Bin

If you need to access a recently deleted volume, you can restore the volume from the recycle bin.

About this task

A volume in the recycle bin is permanently deleted at the date and time listed in the **Purge Time** column.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Volumes** node and expand the **Recycle Bin** node.
5. Select the volume to restore from the **Recycle Bin** node and click **Restore Volume**. A **Restore Volume** dialog box opens.
6. To change the name of the volume when it is restored, type a new name in the **Name** field.
7. Click **OK**.

Results

Empty the Recycle Bin

Empty the recycle bin to permanently delete all of the volumes in the recycle bin.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Volumes** node and select the **Recycle Bin** node.
5. Click **Empty Recycle Bin**. The **Empty Recycle Bin** dialog box opens.
6. Click **OK**.

Permanently Delete a Volume in the Recycle Bin

Instead of deleting all of the volumes in the recycle bin, you can delete a single volume in the recycle bin.

About this task

A volume in the recycle bin is permanently deleted at the date and time listed in the **Purge Time** column.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Volumes** node and expand the **Recycle Bin** node.
5. Select the volume to permanently delete from the **Recycle Bin** node and click **Delete**. A **Delete** dialog box opens.
6. Click **OK**.

About Snapshots

Snapshots enable you to capture volume data at a specific point in time without disrupting access to the volume.

A snapshot represents the contents of a volume at the time of creation. If needed, a volume can be restored from a snapshot.

Creating a snapshot does not prevent access to a volume, and the snapshot is instantly available to authorized iSCSI initiators. Similar to volumes, snapshots appear on the network as iSCSI targets, and can be set online and accessed by hosts with iSCSI initiators.

You can create a snapshot of a volume at the current time, or you can set up schedules to automatically create snapshots on a regular basis.

If you accidentally delete data, you can set a snapshot online and retrieve the data. If a volume is corrupted, you can restore the volume from a snapshot.

NOTE: Generally, snapshots will not be deleted unless you take action to delete them. In some instances, however, snapshots can be deleted by the system. For example, when a new snapshot is taken and not enough snapshot reserve space is available for the new snapshot and the previous one, the older one will be deleted. A snapshot can also be deleted during snapshot borrowing if you run out of borrowable space.

Create a Snapshot

You can create a snapshot of a single volume at the current time. Snapshot creation occurs immediately, with no impact on volume availability or performance.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume.
5. In the right pane, click **Create Snapshot**. The **Create Snapshot** dialog box opens.
6. (Optional) In the **Description** field, type a description for the snapshot.
7. To set the snapshot online after it is created, select the **Set snapshot online** checkbox.
8. To give read-write permissions to the snapshot, select the **Make snapshot read-write** checkbox.
9. Click **OK**.

Create a Snapshot Schedule

To specify how often to create snapshots of a volume, create a snapshot schedule.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume.
5. In the right pane, click **Create Schedule**. The **Create Schedule** dialog box opens.
6. In the **Name** field, type a name for the schedule.
7. In the **Frequency** drop-down list, select the frequency with which the schedule runs.
8. In the **Schedule Type** area, select the **Snapshot Schedule** option.
9. In the **Start and End Dates** area, select the date and time for the schedule to start and the date and time for the schedule to end.
10. In the **Snapshot Settings** area, type the maximum number of snapshots to keep.
11. Click **OK**.

Modify Snapshot Properties

After a snapshot is created, you can modify the settings of the snapshot.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Volumes** node and select a volume that contains a snapshot.
5. From the **Snapshots** tab, select a snapshot to modify.
6. Click **Edit Settings**. The **Modify Snapshot Properties** dialog box opens.
7. In the **Name** field, type a name for the snapshot.
8. (Optional) In the **Description** field, type a description for the snapshot.
9. In the **Snapshot iSCSI Settings** area, type a value in the **Public Alias** field to specify a public alias for the snapshot.
10. In the **Shared Access** area, select the **Allow simultaneous connections from initiators with different IQNs** checkbox if your environment supports multiple initiators accessing a volume.
11. In the **Read-Write Permissions** area, set the read-write permissions for the snapshot.
12. Click **OK**.

Control Snapshot Space Borrowing

You can control whether or not a volume is allowed to borrow space for snapshots. Snapshot space borrowing enables you to temporarily increase the available snapshot space for a volume by borrowing space from other sources. Borrowing can help prevent the oldest snapshots from potentially being deleted when the allocated snapshot reserve of a volume is depleted.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume.
5. In the right pane, click **Edit Snapshot Policy**. The **Edit Snapshot Policy** dialog box opens.
6. Select the action to perform when creating a snapshot exceeds the snapshot reserve.
   - **Set volume offline** — This option sets the volume and snapshots offline.
   - **Delete oldest snapshot** — This option deletes the oldest snapshots to free up space for new snapshots.
7. If the **Delete oldest snapshot** option is selected, you can select the **Borrow snapshot space as needed** checkbox to enable the PS Series group to borrow space for snapshots.
8. Click **OK**.

Set a Snapshot Online or Offline

When you create a snapshot, the PS Series group sets the snapshot offline by default. An iSCSI initiator on a computer cannot discover or connect to an offline snapshot. To make a snapshot accessible to iSCSI initiators, set the snapshot online.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume that contains a snapshot.
5. From the **Snapshots** tab, select a snapshot.
6. If the snapshot is offline, click **Set Online** to set the snapshot online.
   If the snapshot is online, click **Set Offline** to set the snapshot offline.

7. Click **OK**.

Restore a Volume from a Snapshot

You can restore a volume to the state of a snapshot.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume that contains a snapshot.
5. From the **Snapshots** tab, select a snapshot to restore.
6. Click **Restore Volume**. The **Restore Volume** dialog box opens.
7. To set the volume online after it is restored, select the **Set volume online after restore is complete** checkbox.
8. Click **OK**.

Delete a Snapshot

Delete a snapshot when you no longer need it.

Prerequisites

A snapshot must be offline to be deleted.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select a volume that contains a snapshot.
5. From the **Snapshots** tab, select a snapshot.
6. Click **Delete**. The **Delete Snapshot** dialog box opens.
7. Click **OK**.

Managing Replication Schedules

Replication schedules set when replications from a PS Series group run on a daily, hourly, or one-time basis. They also determine the number of snapshots the destination storage system retains for the replication.

Create an Hourly Replication Schedule

An hourly replication schedule determines how often a PS Series group replicates data to the destination volume at a set time or interval each day.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. Click **Create Schedule**.
   The **Create Schedule** dialog box opens.

6. Click the **Enable Schedule** checkbox.
7. In the **Name** field, type a name for the schedule.
8. From the **Frequency** drop-down menu, select **Hourly Schedule**.
9. Select the **Replication Schedule** radio button.
10. From the **Start Date** drop-down menu, select the start date of the schedule.
11. To enable an end date for the schedule, select the checkbox next to **End Date** then select a date from the **End Date** drop-down menu.
12. Specify when to start the replication.
    - To start the replication at a set time each day, select **At specific time**, then select a time of day.
    - To repeat the replication over a set amount of time, select **Repeat Interval**, then select how often to start the replication and the start and end times.
13. From the **Replica Settings** field, type the maximum number of replications the schedule can initiate.

Create a Daily Replication Schedule

A daily replication schedule determines how often a PS Series group replicates data to the destination volume at a set time or interval on specified days.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.

   The volume must be the source of a replication relationship.
5. Click **Create Schedule**.
   The **Create Schedule** dialog box opens.
6. Click the **Enable Schedule** checkbox.
7. In the **Name** field, type a name for the schedule.
8. From the **Frequency** drop-down menu, select **Daily Schedule**.
9. Select the **Replication Schedule** radio button.
10. From the **Start Date** drop-down menu, select the start date of the schedule.
11. To enable an end date for the schedule, select the checkbox next to **End Date** then select a date from the **End Date** drop-down menu.
12. In the **Run every** field, specify the how often to run the replication.
13. Specify the when to start the replication.
    - To start the replication at a set time each day, select **At specific time**, then select a time of day.
    - To repeat the replication over a set amount of time, select **Repeat Interval**, then select how often to start replication and the start and end times.
14. From the **Replica Settings** field, type the maximum number of replications the schedule can initiate.

Schedule a Replication to Run Once

Create a schedule for one replication to replicate the volume at a future date and time.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.

   The volume must be the source of a replication relationship.
5. Click **Create Schedule**.
   The **Create Schedule** dialog box opens.

6. Click the **Enable Schedule** checkbox.
7. In the **Name** field, type a name for the schedule.
8. From the **Frequency** drop-down menu, select **Run Once**.
9. From the **Date** field, select the start date of the replication.
10. In the **Time** field, specify the start time of the replication.
11. From the **Replica Settings** field, type the maximum number of replications the schedule can initiate.

Edit a Replication Schedule

After creating a replication schedule, edit it to change how often the schedule initiates replications.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. From the **Schedules** tab, select the replication schedule to edit.
6. Click **Edit**.
   The **Edit Schedule** dialog box appears.
7. Modify the schedule settings as needed.

   NOTE: For more information on the schedule settings, click **Help**.

8. Click **OK**.

Enable or Disable a Replication Schedule

After creating a replication schedule, enable or disable the schedule to allow the schedule to initiate replications or prevent the schedule from initiating replications.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. From the **Schedules** tab, select the replication schedule to enable or disable.
6. Click **Edit**.
   The **Edit Schedule** dialog box appears.
   - To enable the replication schedule, select the **Enable Schedule** checkbox.
   - To disable the replication schedule, clear the **Enable Schedule** checkbox.
7. Click **OK**.

Delete a Replication Schedule

Delete a replication schedule to prevent it from initiating replications after the schedule is no longer needed.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Group.
3. Click the **Storage** tab.

4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. From the **Schedules** tab, select the replication schedule to delete.
6. Click **Delete**.
   A confirmation dialog box appears.
7. Click **OK**.

About Access Policies

In earlier versions of the PS Series firmware, security protection was accomplished by individually configuring an access control record for each volume to which you wanted to secure access. Each volume supported up to 16 different access control records, which together constituted an access control list (ACL). However, this approach did not work well when large numbers of volumes were present. To address that issue, PS Series groups incorporated access policies and access policy groups that can be applied to one or more volumes.

Each access policy lets you specify one or more of the following authentication methods:

- CHAP user name (Challenge Handshake Authentication Protocol)
- IP address
- iSCSI initiator name

You can assign up to four access policies or access policy groups to a volume. The access policies or access policy groups assigned to a volume determine which hosts have access to that volume. In addition, you can allow or disallow volume access from multiple initiators, depending on your configuration needs.

An access policy or access policy group can apply to the volume, its snapshots, or both. For example, you can authorize computer access to a volume and its snapshots or to the volume only.

Create a Local CHAP Account

Use local CHAP accounts to make sure that only authorized users can access a PS Series group.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the **Access** node.
5. In the right pane, click **Create Local CHAP Account**. The **Create Local CHAP Account** dialog box opens.
6. In the **Username** field, type the CHAP user name.
7. In the **Password** field, type a password (otherwise known as a CHAP secret).
8. To enable the local CHAP account, select the **Enable** checkbox.
9. Click **OK**.

Edit a Local CHAP Account

Edit a local CHAP account to change the username/password and enable/disable the CHAP account.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the **Access** node.
5. In the Local CHAP Accounts area, select the local CHAP account to editt.
6. Click **Edit**. The **Edit Local CHAP Account** dialog box opens.
7. In the **Username** field, type the CHAP user name.

8. In the **Password** field, type a password (otherwise known as a CHAP secret).
9. To enable the local CHAP account, select the **Enable** checkbox.
   To disable the local CHAP account, clear the **Enable** checkbox.
10. Click **OK**.

Modify Target Authentication

A PS Series group automatically enables target authentication using a default user name and password. If needed, you can change these credentials.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the **Access** node.
5. In the right pane, click **Modify Target Authentication**. The **Modify Target Authentication** dialog box opens.
6. In the **Username** field, type a target authentication user name.
7. In the **Password** field, type a target authentication password (otherwise known as a CHAP secret).
8. Click **OK**.

Set the iSCSI Discovery Filter

You can prevent computers from discovering unauthorized targets by enabling the iSCSI discovery filter. If you enable the iSCSI discovery filter, initiators discover only those targets for which they have the correct access credentials.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the **Access** node.
5. In the right pane, click **Set iSCSI Filter**. The **Set iSCSI Filter** dialog box opens.
6. To enable the iSCSI discovery filter, select the **Prevent unauthorized host from discovery targets** checkbox.
   To disable the iSCSI discovery filter, clear the **Prevent unauthorized host from discovery targets** checkbox.
7. Click **OK**.

Create an Access Policy Group

Access policy groups combine individual access policies together so that they can be managed as a single entity.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the **Access** node.
5. In the right pane, click **Create Access Policy Group**. The **Create Access Policy Group** dialog box opens.
6. In the **Name** field, type a name for the access policy group.
7. (Optional) In the **Description** field, type a description for the access policy group.
8. In the **Access Policies** area, click **Add** to add access policies to the access policy group.
   To remove an access policy from the access policy group, select the access policy and click **Remove**.
9. Click **OK**.

Edit an Access Policy Group

After an access policy group is created, you can edit the settings of the access policy group.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select an access policy group.
5. In the right pane, click **Edit Settings**. The **Edit Access Policy Group** dialog box opens.
6. In the **Name** field, type a name for the access policy group.
7. (Optional) In the **Description** field, type a description for the access policy group.
8. In the **Access Policies** area, click **Add** to add access policies to the access policy group.
   To remove an access policy from the access policy group, select the access policy and click **Remove**.
9. Click **OK**.

Add Volumes to an Access Policy Group

You can select the volumes that you want to associate with an access policy group.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select an access policy group.
5. In the right pane, click **Add Volumes**. The **Add Volumes to Access Policy Group** dialog box opens.
6. In the **Volumes** area, select the checkboxes of the volumes to associate with the access policy group.
7. In the **Access Policy Group Targets** area, select whether the access policy group applies to volumes and snapshots, volumes only, or snapshots only.
8. Click **OK**.

Remove Volumes From an Access Policy Group

You can select the volumes that you want to unassociate from an access policy group.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select an access policy group.
5. In the right pane, click **Remove Volumes**. The **Remove Volumes from Access Policy Group** dialog box opens.
6. Select the checkboxes of the volumes to unassociate from the access policy group.
7. Click **OK**.

Delete an Access Policy Group

You can delete an access policy group if it is not in use.

Steps

1. Click the **Storage** view.

2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select the access policy group to delete.
5. In the right pane, click **Delete**. The **Delete Access Policy Group** dialog box opens.
6. Click **OK**.

Create an Access Policy

Access policies associate one or more authentication methods to available volumes.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the **Access** node.
5. In the right pane, click **Create Access Policy**. The **Create Access Policy** dialog box opens.
6. In the **Name** field, type a name for the access policy.
7. (Optional) In the **Description** field, type a description for the access policy.
8. In the **Access Points** area, click **Create** to create an access point.
   - To edit an access point, select the access point and click **Edit**. The **Edit Access Point** dialog box opens.
   - To remove an access point from the access policy, select the access point and click **Remove**
9. Click **OK**.

Edit an Access Policy

After an access policy is created, you can edit the settings of the access policy.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select an access policy.
5. In the right pane, click **Edit Settings**. The **Edit Access Policy** dialog box opens.
6. In the **Name** field, type a name for the access policy group.
7. (Optional) In the **Description** field, type a description for the access policy group.
8. In the **Access Policies** area, click **Create** to create an access point.
   - To edit an access point, select the access point and click **Edit**. The **Edit Access Point** dialog box opens.
   - To remove an access point from the access policy, select the access point and click **Remove**.
9. Click **OK**.

Create an Extended Access Point

Extended access points define the resources that represent the access policy.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select an access policy.
5. In the right pane, click **Edit Settings**. The **Edit Access Policy** dialog box opens.

6. In the **Access Points** area, click **Create**. The **Create Access Point** dialog box opens.
7. (Optional) In the **Description** field, type a description for the basic access point.
8. In the **CHAP Account** field, type the user name of the CHAP account that a computer must supply to access a volume.
9. In the **iSCSI Initiator** field, type the iSCSI initiator name of a computer to which you want to provide access to a volume.
10. In the text box in the **IPv4 Addresses** area, type the IPv4 addresses of the iSCSI initiators to which you want to provide access and then click **+ Add**. You can enter a single IP address or a range of IP addresses. IP addresses can also be entered in a comma separated list.

    To remove an IPv4 address from the **IPv4 Address** area, select the address and click **– Remove**.
11. Click **OK**.

Edit an Extended Access Point

After an extended access point is defined, you can edit the settings of the access point.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select an access policy.
5. In the right pane, click **Edit Settings**. The **Edit Access Policy** dialog box opens.
6. In the **Access Points** area, select the access point to edit and click **Edit**. The **Edit Access Point** dialog box opens.
7. (Optional) In the **Description** field, type a description for the basic access point.
8. In the **CHAP Account** field, type the user name of the CHAP account that a computer must supply to access a volume.
9. In the **iSCSI Initiator** field, type the iSCSI initiator name of a computer to which you want to provide access to a volume.
10. In the text box in the **IPv4 Addresses** area, type the IPv4 addresses of the iSCSI initiators to which you want to provide access and then click **+ Add**. You can enter a single IP address or a range of IP addresses. IP addresses can also be entered in a comma separated list.

    To remove an IP address from the **IPv4 Address** area, select the address and click **– Remove**.
11. Click **OK**.

Delete an Extended Access Point

You can delete an extended access point if it is no longer needed.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select an access policy.
5. In the right pane, click **Edit Settings**. The **Edit Access Policy** dialog box opens.
6. In the **Access Points** area, select the access point to delete and click **Remove**.
7. Click **OK**.

Add Volumes to an Access Policy

You can select the volumes that you want to associate with an access policy.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.

4. In the **Storage** tab navigation pane, expand the **Access** node and select an access policy.
5. In the right pane, click **Add Volumes**. The **Add Volumes to Access Policy** dialog box opens.
6. In the **Volumes** area, select the checkboxes of the volumes to associate with the access policy.
7. In the **Access Policy Targets** area, select whether the access policy applies to volumes and snapshots, volumes only, or snapshots only.
8. Click **OK**.

Remove Volumes From an Access Policy

You can select the volumes that you want to unassociate from an access policy.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select an access policy.
5. In the right pane, click **Remove Volumes**. The **Remove Volumes from Access Policy** dialog box opens.
6. Select the checkboxes of the volumes to unassociate from the access policy.
7. Click **OK**.

Delete an Access Policy

You can delete an access policy if it is not in use.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, expand the **Access** node and select the access policy to delete.
5. In the right pane, click **Delete**. The **Delete Access Policy** dialog box opens.
6. Click **OK**.

Monitoring a PS Series Group

Storage Manager provides access to logs, replications, and alerts for the managed PS Series group.

View Logs

You can view logs for the last day, last 3 days, last 5 days, last week, last month, or a specified period of time.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Monitoring** tab.
4. In the **Monitoring** tab navigation pane, select the **Logs** node.
5. Select the date range of the log data to display.

View Event Logs

You can view event logs for the last day, last 3 days, last 5 days, last week, last month, or a specified period of time.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Monitoring** tab.
4. In the **Monitoring** tab navigation pane, select the **Event Logs** node.
5. Select the date range of the event log data to display.

View Audit Logs

You can view audit logs for the last day, last 3 days, last 5 days, last week, last month, or a specified period of time.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Monitoring** tab.
4. In the **Monitoring** tab navigation pane, select the **Audit Logs** node.
5. Select the date range of the audit log data to display.

View Outbound Replications

You can view outbound replications for a PS Series group.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Monitoring** tab.
4. In the **Monitoring** tab navigation pane, select the **Outbound Replication** node.
   Information about outbound replications is displayed in the right pane.

View Inbound Replications

You can view inbound replications for a PS Series group.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Monitoring** tab.
4. In the **Monitoring** tab navigation pane, select the **Inbound Replication** node.
   Information about inbound replications is displayed in the right pane.

View Replication History

You can view the replication history for a PS Series group.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Monitoring** tab.
4. In the **Monitoring** tab navigation pane, select the **Replication History** node.
   Information about past replications is displayed in the right pane.

View Alerts

You can view the current alerts for a PS Series group.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Alerts** tab.
   Information about the PS Series group alerts is displayed in the right pane.

9

Storage Center Maintenance

Storage Manager can manage Storage Center settings, users and user groups, and apply settings to multiple Storage Centers.

Topics:

- Managing Storage Center Settings
- Configuring a Storage Center to Inherit Settings
- Managing Storage Center Users and Groups
- Managing Front-End I/O Ports
- Managing Back-End I/O Port Hardware
- Grouping Fibre Channel I/O Ports Using Fault Domains
- Grouping iSCSI I/O Ports Using Fault Domains
- Grouping SAS I/O Ports Using Fault Domains
- Managing Disks and Disk Folders
- Managing Secure Data
- Managing Data Redundancy
- Managing Disk Enclosures
- Managing Storage Center Controllers
- Updating Storage Center
- Shutting Down and Restarting a Storage Center
- Managing Field Replaceable Units (FRU)

Managing Storage Center Settings

This section describes how to configure general Storage Center settings.

Related concepts

Modifying Storage Center Network Settings on page 216
Configuring Storage Center User Preferences on page 218
Configuring Storage Center Data Settings on page 221
Configuring Storage Center Secure Console Settings on page 223
Configuring Storage Center SMTP Settings on page 224
Configuring Storage Center SNMP Settings on page 225
Configuring Storage Center Time Settings on page 226
Configuring Filters to Restrict Administrative Access on page 227

Related tasks

Viewing and Modifying Storage Center Information on page 214

Viewing and Modifying Storage Center Information

Storage Manager provides options for changing default properties for each individual Storage Center that is managed by Storage Manager.

About this task

NOTE: For user interface reference information, click **Help**.

Rename a Storage Center

Rename a Storage Center when the purpose of the Storage Center has changed or the name no longer applies.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **General** tab.
4. In the **Name** field, type a new name.
5. Click **OK**.

Rename an Individual Controller

The controller name can be changed without affecting the name of the Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, select the controller.
4. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
5. In the **Name** field, type a new name for the controller.
6. Click **OK**.

Change the Operation Mode of a Storage Center

Before performing maintenance or installing software updates, change the **Operation Mode** of a Storage Center to **Maintenance**.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **General** tab.
4. In the **Operation Mode** field, select **Production** or **Maintenance**.
   Selecting **Maintenance** hides alerts that occur during normal operation.
5. Click **OK**.

Related concepts

Storage Center Operation Modes on page 42

View Storage Center License Information

The Licence tab in the **Storage Center Settings** dialog box shows current license information. This information cannot be modified.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **License** tab to display license information.

4. Click **OK**.

Apply a New License to a Storage Center

If you add applications, or increase the number of disks licensed for your Storage Center, you may need to apply a new license. You can submit multiple licences in a zip file.

Prerequisites

- You must be able to access a Storage Center license file from the computer from which you are running Storage Manager .

About this task

NOTE: Applying the Flex Port license requires the Storage Center to restart. After the restart, Storage Center creates a fault domain for the flex port.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **License** tab.
4. Click **Submit License File**.
   The **Submit Storage Center License** and **Select License File** dialog boxes open.
5. Browse to and select a Storage Center license file, then click **Open**.
   The **Select License File** dialog box closes.
6. Click **Apply**.
7. Click **OK**.

Modifying Storage Center Network Settings

The shared management IP, controller management interfaces, and iDRAC can be managed using Storage Manager.

NOTE: For user interface reference information, click **Help**.

Modify the Storage Center Network Settings

In a dual-controller Storage Center, the shared management IP address is hosted by the leader under normal circumstances. If the leader fails, the peer takes over the management IP, allowing management access when the normal leader is down. An IPv6 management IP address can also be assigned.

Prerequisites

If the Storage Center is added to Storage Manager using a host name, the new IP address must be added to the DNS A or AAAA record for the Storage Center to avoid connectivity issues.

About this task

NOTE: A single-controller Storage Center does not have a shared management IP address by default, but it can be configured to facilitate a future transition to dual controllers.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Network** tab.
4. In the **IP Settings** area, type the IPv4 addresses for the management IP.

5. (Optional) In the **IP Settings** area, type the IPv6 addresses for the management IP.
6. (Optional) In the **Network Information** area, type the server addresses and domain name.
7. Click **OK**.

Modify Management Interface Settings for a Controller

The IP address, net mask, and gateway can be modified for the controller management interface.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, select the controller.
4. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
5. Modify the management interface settings.
   a. In the **IP Address** field, type a new IP address for the controller management interface.
   b. In the **IP Net Mask** field, type a network mask for the controller management interface.
   c. In the **IP Gateway** field, type the default route for the network.
6. Click **OK**.

Modify DNS Settings for a Controller

Storage Manager allows you to specify a primary DNS server, secondary DNS server, and the name of the domain to which the Storage Center belongs.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, select the controller.
4. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
5. Modify the DNS settings.
   a. In the **DNS Server** field, type the IP address of a DNS server on the network.
   b. (Optional) In the **Secondary DNS Server** field, type the IP address of a backup DNS server on the network.
   c. In the **Domain Name** field, type the name of the domain to which the Storage Center belongs.
6. Click **OK**.

Modify iDRAC Interface Settings for a Controller

The iDRAC interface provides out-of-band management for the controller. When you reach the **Configuration Complete** screen:

Steps

1. Scroll down to **Advanced Steps**.
2. Click the **Modify BMC Settings** link.
3. The **Edit BMC Settings** dialog box opens.
4. Specify the iDRAC interface settings for the bottom controller and the top controller.
   a. In the **BMC IP Address** field, type an IP address for the iDRAC interface.
   b. In the **BMC Net Mask** field, type the network mask.
   c. In the **BMC Gateway IPv4 Address** field, type the default route for the iDRAC.
5. Click **OK**.

Configuring Storage Center User Preferences

Storage Center user preferences establish defaults for the Storage Center user account that was used to add the Storage Center to Storage Manager . Storage Manager honors these preferences.

NOTE: For user interface reference information, click **Help**.

Set the Default Size for New Volumes

The default volume size is used when a new volume is created unless the user specifies a different value.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. In the **Volume Size** field, type a default size for new volumes in bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).
5. Click **OK**.

Set the Default Base Volume Name for New Volumes

The default base name is used as the name for a new volume unless the user specifies a different name. If one or more volumes with the base name already exist, a number is appended to the base name to create the new volume name.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. In the **Base Volume Name** field, type a name to use as a base for new volumes. The default base is **New Volume**.
5. Click **OK**.

Set Default Data Reduction Settings for New Volumes

The default data reduction settings are used when a new volume is created unless the user changes them. You can prevent the default data reduction settings from being changed during volume creation by clearing the **Allow Data Reduction Selection** checkbox.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. Configure data reduction defaults.
   - Select the **Compression Enabled** checkbox to reduce the amount of space used by a volume by encoding data.
   - Select the **Allow Data Reduction Selection** checkbox to allow users to enable or disable data reduction when creating volumes.
5. Click **Apply**.
6. Click **OK**.

Set Default Cache Settings for New Volumes

The default cache settings are used when a new volume is created unless the user changes them. You can prevent the default cache settings from being changed during volume creation by clearing the **Allow Cache Selection** checkbox.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. Select or clear the **Read Cache** and **Write Cache** checkboxes to set the default cache settings for new volumes.
5. Select or clear the **Allow Cache Selection** checkbox to allow or prevent users from configuring cache settings when creating volumes.
6. Click **OK**.

Set the Default Snapshot Options for New Volumes

The default snapshot options are used when a new volume is created unless the user changes them.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. Choose default Snapshot Profiles.
   a. In the **Snapshot** area, click **Change**.
      The **Select Snapshot Profiles** dialog box opens.
   b. In the top pane, select the Snapshot Profiles to assign to new volumes by default.
   c. Click **OK**.
      The **Select Snapshot Profiles** dialog box closes.
5. In the **Minimum Snapshot Interval** field, type the number of minutes that must pass after a snapshot is taken before a subsequent snapshot can be taken.
6. Click **OK**.

Allow or Disallow Advanced Volume Mapping Settings

Advanced volume mapping options include LUN configuration, mapping path options, and making the volume read-only.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. Select or clear the **Allow Advanced Mapping** checkbox to enable or disable advanced volume mapping options.
5. Click **OK**.

Set the Default Operating System for New Servers

The default operating system is used for new servers unless the user selects a different option. For convenience, choose the operating system that is most common in your environment.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.

2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. From the **Operating System** drop-down menu, select the default operating system for new servers.
5. Click **OK**.

Set the Default Storage Profile for New Volumes

The default Storage Profile is used when a new volume is created unless the user selects a different Storage Profile. You can prevent the Storage Profile from being changed during volume creation by clearing the **Allow Storage Profile Selection** checkbox.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. From the **Storage Profile** drop-down menu, select the Storage Profile to use as the default for new volumes.
5. To allow users to select a Storage Profile when creating a volume, select **Allow Storage Profile Selection**.
6. Click **OK**.

Set the Default Storage Type for New Volumes

The default Storage Type is used when a new volume is created unless the user selects a different Storage Type. You can prevent the Storage Type from being changed during volume creation by clearing the **Allow Storage Type Selection** checkbox.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. From the **Storage Type** drop-down menu, select the Storage Type to use as the default for new volumes.
5. To allow users to select a Storage Type when creating a volume, select **Allow Storage Type Selection**.
6. Click **OK**.

Set Default Volume QoS Profile

Specify the default Volume QoS Profiles to be used for new volumes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. In the **Quality of Service Profile** area, click **Change**.
   The **Select Volume QoS Profile to Apply** dialog box opens, which shows all QoS profiles that have been defined.
5. Select one of the profiles by clicking its name.
6. Click **OK**.

Allow QoS Profile Selection

To enable users to select QoS Profiles, set the option to enabled.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Preferences** tab.
4. In the **Quality of Service Profiles** area, select the **Allow QoS Profile Selection** checkbox.
5. Click **OK**.

Configuring Storage Center Data Settings

You can configure cache, Data Progression, snapshot, and RAID stripe width settings for the Storage Center.

NOTE: For user interface reference information, click **Help**.

Set Storage Center Cache Options

Global Storage Center cache settings override cache settings for individual volumes. Read cache improves read performance by anticipating the next read and holding it in volatile memory. Write cache increases write performance by holding written data in volatile memory until it can be safely stored on disk.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Storage** tab.
4. Select or clear the **Read Cache Enabled** and **Write Cache Enabled** checkboxes.
5. Click **OK**.

Schedule or Limit Data Progression

Schedule when Data Progression runs and limit how long it is allowed to run.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Storage** tab.
4. In the **Data Progression Start Time** field, select or type the time at which Data Progression starts running daily.
5. From the **Data Progression Max Run Time** drop-down menu, select the maximum time period that Data Progression is allowed to run.
6. Click **OK**.

Set RAID Stripe Width

The RAID stripe width controls the number of disks across which RAID data is striped. The stripe widths for RAID 5 and RAID 6 are independently configured.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Storage** tab.
4. From the **RAID 5 Stripe Width** drop-down menu, select a stripe width of 5 or 9 disks.
5. From the **RAID 6 Stripe Width** drop-down menu, select a stripe width of 6 or 10 disks.
6. Click **OK**.

Configure an iSNS Server

Set the host name or IP address of the Internet Storage Name Service (iSNS) server on your network.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Storage** tab.
4. In the **iSNS Server Host or IP Address** field, type the host name or IP address of an iSNS server that provides name services for initiators and targets on your network.
5. Click **OK**.

Apply Data Settings to Multiple Storage Centers

Data settings that are assigned to a single Storage Center can be applied to other Storage Centers.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Storage** tab.
4. Select the **Apply these settings to other Storage Centers** checkbox.
5. Click **Apply**.
   The **Select Storage Center** dialog box opens.
6. Select the checkbox for each Storage Center to which you want to apply the settings.
7. Click **OK**.

Configuring Storage Center Secure Console Settings

The secure console allows support personnel to access the Storage Center console without connecting through the serial port.

NOTE: Do not modify the secure console configuration without the assistance of technical support.

Enable Secure Console Access

Enable the secure console to allow support personnel to access the Storage Center console without connecting through the serial port.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Secure Console** tab.
4. Select the **Enable secure console access** checkbox.
5. In the **Reservation Server Host or IP Address**, type the host name or IP address of a secure console server provided by technical support.
6. In the **Session Time to Live** field, type the number of minutes, hours, or days to keep the session active.

   NOTE: The maximum time to live is 72 hours.

7. If a SOCKS proxy is required to allow the Storage Center to communicate with the secure console server specified in the previous step, configure the **Proxy Settings**.
   a. From the **Proxy Type** drop-down menu, select **SOCKS4** or **SOCKS5**.
   b. In the **IP Address** field, type the IP address of the proxy server.
   c. In the **Port** field, type the port used by the proxy server.
   d. If the proxy server requires authentication, complete the **User Name** and **Password** fields.
8. Click **OK**.

Restart the Storage Center Secure Console Server

Troubleshooting an issue may require restarting the secure console server.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Secure Console** tab.
4. Click **Restart Service**.
   A confirmation dialog box opens.
5. Click **OK** to confirm.
6. Click **OK**.

Apply Secure Console Settings to Multiple Storage Centers

Secure Console settings that are assigned to a single Storage Center can be applied to other Storage Centers.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Secure Console** tab.
4. Select the **Apply these settings to other Storage Centers** checkbox.
5. Click **Apply**.
   The **Select Storage Center** dialog box opens.
6. Select the checkbox for each Storage Center to which you want to apply the settings.
7. Click **OK**.
   - If the Secure Console proxy password is not configured or was modified, the dialog box closes.
   - If the Secure Console proxy password was configured previously and not modified, the **Secure Console Proxy** password dialog box opens.
8. (Proxy password only) In the **Password** field, type the password for the proxy, then click **OK**.

Configuring Storage Center SMTP Settings

SMTP server settings can be configured individually for each Storage Center or applied to multiple Storage Centers.

NOTE: For user interface reference information, click **Help**.

Configure Storage Center SMTP Server Settings

Configure SMTP settings to allow the Storage Center to send alert message emails to users who have specified a recipient address in their contact properties.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **SMTP Server** tab.
4. Configure the SMTP server settings.
   a. Select the **Enable SMTP Email** check box.
   b. In the **SMTP Mail Server** field, type the IP address or fully qualified domain name of the SMTP email server.
   c. (Optional) In the **Backup SMTP Server** field, type the IP address or fully qualified domain name of a backup SMTP email server.
   d. Click **OK**.
   e. Open the **SMTP Server** tab and click **Test Server** to verify connectivity to the SMTP server.
   f. If the SMTP server requires emails to contain a MAIL FROM address, specify an email address in the **Sender Email Address** field.
   g. (Optional) In the **Common Subject Line** field, type a subject line to use for all emails sent by the Storage Center.
   h. Configure how the Storage Center identifies itself to the SMTP server:
      - To use SMTP, type the Storage Center fully qualified domain name in the **Hello Message (HELO)** field.

- To use ESMTP, select the **Send Extended Hello (EHLO)** check box, then type the Storage Center fully qualified domain name in the **Extended Hello Message (EHLO)** field.

5. Click **OK**.

Apply SMTP Settings to Multiple Storage Centers

SMTP settings that are assigned to a single Storage Center can be applied to other Storage Centers.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **SMTP Server** tab.
4. Select the **Apply these settings to other Storage Centers** checkbox.
5. Click **Apply**.
   The **Select Storage Center** dialog box opens.
6. Select the checkbox for each Storage Center to which you want to apply the settings.
7. Click **OK**.
   - If a password is not configured or was modified, the dialog box closes.
   - If a password was configured previously and not modified, the **SMTP Server Password** dialog box opens.
8. (Password only) In the **Password** field, type the password for SMTP, then click **OK**.

Configuring Storage Center SNMP Settings

SNMP allows the Storage Center to be monitored over the network.

NOTE: For user interface reference information, click **Help**.

Configure SNMP Settings for a Storage Center

Configure SNMP if you want to monitor the Storage Center with a network management system.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **SNMP Server** tab.
4. From the **SNMP Version** drop-down menu, select the version of SNMP to configure.
5. Click **Apply**.
   The contents of the dialog box change depending on the version of SNMP selected.
6. If you selected SNMP v1/v2c, set the community strings that allow access to the Storage Center SNMP agent.
   a. In the **Read Only Community String** field, type a password for allowing network management systems to read from the Storage Center SNMP agent.
   b. In the **Read Write Community String** field, type a password for allowing network management systems to read from or write to the Storage Center SNMP agent.
7. If you selected SNMP v3, you can create an SNMP v3 user if one does not exist.

To create a new user:

a. Click **Create SNMP v3 User**.
The **Create SNMP v3 User** dialog box opens.
b. In the **Name** field, type a user name.
c. In the **Password** field, type a password.
d. Select an authentication method from the **Authentication Type** drop-down menu.
e. Select an encryption type from the **Encryption Type** drop-down menu.
f. Click **OK**.
g. Select the user from the SNMP v3 Settings table.

8. Specify settings for the network management system to which Storage Center will send SNMP traps.
   a. Click **Create Trap Destination**.
   The **Create SNMP Trap Destination** dialog box opens.
   b. In the **Trap Destination** field, type the host name or IP address of the network management system that is collecting trap information
   c. From the **Type** drop-down menu, select the type of the SNMP trap request or SNMP inform request to use.
   d. In the **Port** field, type the port number of the network management system.
   e. If **SNMPv1 Trap**, **SNMPv2 Trap**, or **SNMPv2 Inform** is selected from the **Type** drop-down menu, type a password in the **Community String** field.
   f. If **SNMPv3 Trap** or **SNMPv3 Inform** is selected from the **Type** drop-down menu, select a user from the **SNMP v3 User** drop-down menu.
   g. Click **OK**.
9. If the **SNMP Running** status is **No**, click **Start SNMP**.
10. Click **OK**.

Apply SNMP Settings to Multiple Storage Centers

SNMP settings that are assigned to a single Storage Center can be applied to other Storage Centers.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **SNMP Server** tab.
4. Select the **Apply these SNMP v1/v2c settings to other Storage Centers** checkbox.
5. Click **Apply**.
   The **Select Storage Center** dialog box opens.
6. Select the checkbox for each Storage Center to which you want to apply the settings.
7. Click **OK**.

Configuring Storage Center Time Settings

Date and time settings can be configured individually for each Storage Center or applied to multiple Storage Centers.

NOTE: For user interface reference information, click **Help**.

Set the Date and Time for a Storage Center

Select the time zone, then set the date and time or configure the Storage Center to synchronize with an NTP server.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.

2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Time Settings** tab.
4. From the **Region** drop-down menu, select the region where the Storage Center is located.
5. From the **Time Zone** drop-down menu, select the time zone where the Storage Center is located.
6. Set the date and time.
   - To set the date and time manually, clear **Use NTP Server**, then select **Set Current Time** and set the date and time in the **Curent Time** fields.
   - To configure the Storage Center to synchronize the date and time with a Network Time Protocol server, select **Use NTP Server**, then type the host name or IP address of an NTP server in the **Server Host or IP Address** field.
7. Click **OK**.

Apply Date and Time Settings to Multiple Storage Centers

Date and time settings that are assigned to a single Storage Center can be applied to other Storage Centers.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Time Settings** tab.
4. Select the **Apply these settings to other Storage Centers** checkbox.
5. Click **Apply**.
   The **Select Storage Center** dialog box opens.
6. Select the checkbox for each Storage Center to which you want to apply the settings.
7. Click **OK**.

Configuring Filters to Restrict Administrative Access

Access filters can be created to selectively allow administrative access to a Storage Center based on IP address, user privilege level, or user name. When one or more access filters are defined, administrative connections that do not match an access filter are denied.

- Storage Manager does not allow you to create an access filter policy that would reject your current administrative connection.
- Access filters apply to new administrative connections only; existing administrative connections are not affected.

NOTE: For user interface reference information, click **Help**.

Create an Access Filter for a Storage Center

Create an access filter to explicitly allow administrative connections from a user privilege level, specific user, IP address, or range of IP addresses.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **IP Filtering** tab.
4. Click **Create Filter**.
   The **Create IP Filter** dialog box opens

5. Select the Storage Center user or user privilege level to allow.
   - To allow access to a Storage Center user privilege level, select **User Privilege Level**, then select a privilege level from the drop-down menu.
   - To allow access to an individual Storage Center user, select **Specific User**, then select a user from the drop-down menu.
6. Specify which source IP addresses to allow.

   NOTE: If network address translation (NAT) is enabled in your network environment, be sure to specify the IP address(es) visible to the Storage Center.

   - To allow all source IP addresses, select **All Hosts**.
   - To allow access to a specific IP address, select **Single IP Address**, then type the IP address in the field.
   - To allow access to a range of IP addresses, select **Range of IP Addresses**, then type the first and last IP addresses in the fields.
7. Click **OK**.

Modify an Access Filter for a Storage Center

Modify an access filter to change the users or IP addresses it allows.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **IP Filtering** tab.
4. Select the access filter that you want to modify, then click **Modify Filter**.
   The **Modify IP Filter** dialog box opens.
5. Modify the access filter settings as needed. For user interface reference information, click **Help**.
6. (Optional) Modify the allowed Storage Center user or user privilege level.
   - To allow access to a Storage Center user privilege level, select **User Privilege Level**, then select a privilege level from the drop-down menu.
   - To allow access to an individual Storage Center user, select **Specific User**, then select a user from the drop-down menu.
7. (Optional) Modify the allowed source IP addresses.

   NOTE: If network address translation (NAT) is enabled in your network environment, be sure to specify the IP address(es) visible to the Storage Center.

   - To allow all source IP addresses, select **All Hosts**.
   - To allow access to a specific IP address, select **Single IP Address**, then type the IP address in the field.
   - To allow access to a range of IP addresses, select **Range of IP Addresses**, then type the first and last IP addresses in the fields.
8. Click **OK**.

Delete an Access Filter for a Storage Center

Delete an access filter if it is no longer needed or you want to revoke administrative access to the users and IP addresses that the filter matches.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **IP Filtering** tab.
4. Select the access filter that you want to delete, then click **Delete Filter**.
   The **Delete IP Filter** dialog box opens.
5. Click **OK** to confirm.
6. Click **OK**.

View and Delete Access Violations for a Storage Center

View access violations to determine who has unsuccessfully attempted to log in. A maximum of 100 access violations are recorded and displayed for a Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **IP Filtering** tab.
4. Click **Show Access Violations**.
   The **Show Access Violations** dialog box opens.
5. (Optional) Delete access violations.
   a. Select the corresponding checkbox for each violation that you want to delete.
   b. Click **Delete Selected Violations**.
      A confirmation dialog box opens.
   c. Click **OK**.
      The confirmation dialog box closes.
   d. Click **OK**.
      The **Show Access Violations** dialog box closes.
6. Click **OK**.

Apply Access Filtering Settings to Multiple Storage Centers

Access filtering settings that are assigned to a single Storage Center can be applied to other Storage Centers.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **IP Filtering** tab.
4. Select the **Apply these settings to other Storage Centers** checkbox.
5. Click **Apply**.
   The **Select Storage Center** dialog box opens.
6. Select the checkbox for each Storage Center to which you want to apply the settings.
7. Click **OK**.

Configuring a Storage Center to Inherit Settings

A Storage Center can be configured to inherit settings from another Storage Center to save time and ensure that Storage Centers are configured consistently.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

About this task

NOTE: For user interface reference information, click **Help**

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Inherit Settings**.
   The **Inherit Settings** wizard opens.
3. Select the Storage Center from which you want to inherit settings, then click **Next**. The wizard advances to the next page.
4. Select the checkbox for each category of settings that you want to inherit. For user interface reference information, click **Help**.
5. Click **Finish**.
   - If you modified passwords for the SupportAssist proxy, Secure Console proxy, or SMTP server (or if passwords are not configured), the dialog box closes.
   - If a password for the SupportAssist proxy, Secure Console proxy, or SMTP server was configured previously and not modified, you are prompted to reenter the required passwords.
6. Type the required passwords.

Managing Storage Center Users and Groups

Storage Center users have access to folders, volumes, views, and commands depending on their privilege level and the user groups to which they belong. User accounts can be created locally and/or exist externally in a directory service.

User Privilege Levels

Each user is assigned a single privilege level. Storage Center has three levels of user privilege.

Table 13. Storage Center User Privilege Levels

Privilege Level	Allowed Access
Administrator	Read and write access to the entire Storage Center (no restrictions). All Administrators have the same predefined privileges. Only Administrators can manage users and user groups.
Volume Manager	Read and write access to the folders associated with the assigned user groups. Users with this privilege level can create volumes in the allowed volume folders and map them to existing servers in the allowed server folders.
Reporter	Read-only access to the folders associated with the assigned user groups.

User Groups

User groups grant access to volume, server, and disk folders.

- Users with the Administrator privilege have access to all folders and cannot be added to user groups.
- Users with the Volume Manager or Reporter privilege must be associated with one or more user groups, and can access only the volume, server, and disk folders made available to them.

User Account Management and Authentication

Storage Center access is granted using either of the following methods:

- **Local users and user groups**: User accounts can be created and maintained on the Storage Center.
- **External directory service**: In environments that use Active Directory or OpenLDAP, Storage Center can authenticate directory users. Access can be granted to individual directory users and directory user groups. These users access the Storage Center using their domain credentials.

Managing Local Storage Center Users

This section describes how to create, manage, and delete local Storage Center users.

NOTE: For user interface reference information, click **Help**.

Create a Local Storage Center User

Create a local Storage Center user to assign privileges to a new user.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, click **Create Local User**.
   The **Create Local User** dialog box opens.
5. In the **Name** field, type a name for the user.

   NOTE: To avoid user name conflicts with directory service users, do not use the @ or \ characters in local user names.

6. From the **Privilege** drop-down menu, select the privilege level to assign to the user.
   - **Administrator** – When selected, the local user has full access to the Storage Center.
   - **Volume Manager** – When selected, the local user has read and write access to volumes, servers, and disks in the folders associated with the assigned user groups.
   - **Reporter** – When selected, the local user has read-only access to volumes, servers, and disks in the folders associated with the assigned user groups.
7. From the **Session Timeout** drop-down menu, select the maximum length of time that the local user can be idle while logged in to the Storage Center System Manager before the connection is terminated.
8. From the **Preferred Language** drop-down menu, select a language. That language will be used for email alerts.
9. (Volume Manager and Reporter only) Add one or more local user groups to the local user.
   a. In the **Local User Groups** area, click **Change**.
      The **Select Local User Groups** dialog box opens.
   b. (Optional) To create a new local user group, click **Create Local User Group**, then complete the **Create Local User Group** wizard. For user interface reference information, click **Help**.
   c. Select the checkbox for each local user group you want to associate with the local user.
   d. Click **OK**.
      The **Select Local User Groups** dialog box closes.
10. Specify and confirm a password for the user in the **Password** and **Confirm Password** fields.
11. (Optional) Specify more information about the user in the **Details** area.
12. Click **OK**.
    The **Create Local User** dialog box closes.
13. Click **OK**.

Configure the Default User Preferences for New Storage Center Users

The default user preferences are applied to new Storage Center users. The preferences can be individually customized further after the user is created.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, click **Configure Default User Preferences**.
   The **Configure Default User Preferences** dialog box opens.
5. Modify the user preferences as needed, then click **OK**.

   NOTE: For user interface reference information, click **Help**.

6. Click **OK**.
   The **Configure Default User Preferences** dialog box closes.

7. Click **OK**.

Related tasks

Configure Preferences for a Local Storage Center User on page 234

Increase the Privilege Level for a Local Storage Center User

The privilege level can be increased for local users that have the Volume Manager or Reporter privilege. The privilege level for a user cannot be decreased.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Local User Settings** dialog box opens.
5. From the **Privilege** drop-down menu, select the privilege level to assign to the user.
   - **Administrator** – When selected, the local user has full access to the Storage Center.
   - **Volume Manager** – When selected, the local user has read and write access to the folders associated with the assigned user groups.
   - **Reporter** – When selected, the local user has read-only access to the folders associated with the assigned user groups.
6. Click **OK**.
   The local user **Edit Local User Settings** dialog box closes.
7. Click **OK**.

Change the Preferred Language for a Storage Center User

The preferred language for a Storage Center user determines the languages used in email alerts and automated reports from the Storage Center.

Prerequisites

The Storage Center must support the preferred language.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Local User Settings** dialog box opens.
5. From the **Preferred Language** drop-down menu, select a language.
6. Click **OK**.

Change the Session Timeout for a Local Storage Center User

The session timeout controls the maximum length of time that the local user can be idle while logged in to the Storage Center before the connection is terminated.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.

3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Local User Settings** dialog box opens.
5. From the **Session Timeout** drop-down menu, select the maximum length of time that the local user can be idle while logged in to the Storage Center before the connection is terminated.
6. Click **OK**.
   The **Edit Settings** dialog box closes.
7. Click **OK**.

Enable or Disable Access for a Local Storage Center User

When a local Storage Center user is disabled, the user is not allowed to log in.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Local User Settings** dialog box opens.
5. In the **Allow User to Log In** field, enable or disable access for the local user.
   - To enable access, select the **Enabled** checkbox.
   - To disable access, clear the **Enabled** checkbox.
6. Click **OK**.
   The local user **Edit Settings** dialog box closes.
7. Click **OK**.

Modify Local Group Membership for a Local Storage Center User

User groups grant access to volume, server, and disk folders for users with the Volume Manager or Reporter privilege level.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Local User Settings** dialog box opens.
5. Modify local group membership for the user.
   a. In the **Local User Groups** field, click **Change**.
      The **Select Local User Groups** dialog box opens.
   b. (Optional) To create a new local user group, click **Create Local User Group**, then complete the **Create Local User Group** wizard. For user interface reference information, click **Help**.
   c. Select the checkbox for each local user group you want to associate with the local user.
   d. To remove the local user from a local group, clear the checkbox for the group.
   e. Click **OK**.
      The **Select Local User Groups** dialog box closes.
6. Click **OK**.
   The **Edit Local User Settings** dialog box closes.
7. Click **OK**.

Configure Preferences for a Local Storage Center User

By default, each Storage Center user inherits the default user preferences. If necessary, the preferences can be individually customized for a user.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Local User Settings** dialog box opens.
5. Click **Configure User Preferences**.
   The **Configure User Preferences** dialog box opens.
6. Modify the user preferences as needed, then click **OK**.

   NOTE: For user interface reference information, click **Help**.

7. Click **OK**.
   The **Edit Local User Settings** dialog box closes.
8. Click **OK**.

Related tasks

Configure the Default User Preferences for New Storage Center Users on page 231

Modify Descriptive Information About a Local Storage Center User

The descriptive information about a local user includes his or her real name, department, title, location, telephone numbers, email address(es), and notes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Local User Settings** dialog box opens.
5. Modify the **Real Name** field as necessary.
6. Modify the fields in the **Details** area as necessary, then click **OK**.

   NOTE: For user interface reference information, click **Help**.

7. Click **OK**.
   The **Edit Local User Settings** dialog box closes.
8. Click **OK**.

Change the Password for a Local Storage Center User

Changing the password for a local Storage Center user through Storage Manager automatically updates any Storage Center mappings that were made using the user's credentials.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.

3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, select the user, then click **Change Password**.
   The **Change Password** dialog box opens.
5. Type the old password.
6. Type and confirm a new password for the local user, then click **OK**.
7. Click **OK**.

Delete a Local Storage Center User

Delete a Storage Center user if he or she no longer requires access. The local user that was used to add the Storage Center to Storage Manager cannot be deleted. The last user with the Administrator privilege cannot be deleted because Storage Center requires at least one Administrator.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, select the user, then click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK** to confirm.
6. Click **OK**.

Restore a Deleted Local Storage Center User

A new password must be provided when restoring a deleted user. If you are restoring a deleted user with the Volume Manager or Reporter privilege, the user must be added to one or more local user groups.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local Users** subtab, click **Restore Deleted User**.
   The **Restore Deleted User** wizard opens.
5. Select the local user that you want to restore, then click **Next**.
   The wizard advances to the next page.
6. (Volume Manager and Reporter only) Add the local user to one or more local user groups.
   a. In the **Local User Groups** area, click **Change**.
      The **Select Local User Groups** dialog box opens.
   b. (Optional) To create a new local user group, click **Create Local User Group**, then complete the **Create Local User Group** wizard. For user interface reference information, click **Help**.
   c. Select the checkbox for each local user group you want to associate with the local user.
   d. Click **OK**. The **Select Local User Groups** dialog box closes.
7. Type and confirm a new password for the local user in the **New Password** and **Confirm Password** fields.
8. Modify the remaining user settings as needed.

   NOTE: For user interface reference information, click **Help**.

9. Click **Finish**.
10. Click **OK**.

Managing Local Storage Center User Groups

User groups grant access to volume, server, and disk folders.

NOTE: For user interface reference information, click **Help**.

Create a Local User Group

Create a local Storage Center user group to grant access to specific volume, server, and disk folders.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local User Groups** subtab, click **Create Local User Group**.
   The **Create Local User Group** wizard opens.
5. Add volume folders to the local user group.
   a. If you need to create a volume folder, click **Create Volume Folder**, then complete the fields in the **Create Volume Folder** dialog box.
   b. Click **OK** to create the volume folder.
   c. Click **Next**.
      The wizard advances to the next page.
6. Add server folders to the local user group.
   a. If you need to create a server folder, click **Create Server Folder**, then complete the fields in the **Create Server Folder** dialog box.
   b. Click **OK** to create the server folder.
   c. Click **Next**.
      The wizard advances to the next page.
7. Add disk folders to the local user group.
   a. Select the disk folder(s) you want to add to the local user group, then click **Next**.
      The wizard advances to the next page.
   b. In the **Name** field, type a name for the local user group, then click **Finish**.
8. Click **OK**.

Manage User Membership for a Local Storage Center User Group

Local Storage Center users and directory users that have been individually granted access can be added to local Storage Center user groups.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local User Groups** subtab, select the local user group, then click **Manage Users**.
   The **Manage Users** dialog box opens.
5. Manage user membership for the user group.
   - To add users, select the user(s) you want to add in the upper table, then click **Add Users**. The users move from the upper table to the lower table.
   - To remove users, select the user(s) you want to remove in the lower table, then click **Remove Users**. The users move from the upper table to the lower table.
6. Click **OK**.
   The **Manage Users** dialog box closes.

7. Click **OK**.

Manage Directory User Group Membership for a Local Storage Center User Group

Add a directory user group to a local user group to grant access to all directory users in the directory user group.

Prerequisites

- The Storage Center must be configured to authenticate users with an external directory service.
- The directory user group(s) you want to add to a local Storage Center user group must have been granted Volume Manager or Reporter access to the Storage Center.
- The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**. The **Edit Settings** dialog box appears.
3. Click the **Users and User Groups** tab.
4. On the **Local User Groups** subtab, select the local user group, then click **Manage Directory User Groups**. The **Manage Directory User Groups** dialog box appears.
5. Manage directory user group membership for the user group.
   - To add directory user groups, select the directory user group(s) you want to add in the upper table, then click **Add Directory User Groups**. The directory user group(s) move from the upper table to the lower table.
   - To remove directory user groups, select the directory user group(s) you want to remove in the lower table, then click **Remove Directory User Groups**. The directory user groups move from the upper table to the lower table.
6. When you are finished, click **OK** to close the **Manage Directory User Groups** dialog box.
7. Click **OK** to close the **Edit Settings** dialog box.

Manage Folder Access Granted by a Local Storage Center User Group

The folders that are associated with a local Storage Center user group determine the access that is granted by the user group.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local User Groups** subtab, select the local user group, then click **Manage Folders**.
   The **Manage Folders** wizard opens.
5. Manage volume folders for the local user group.
   a. If you need to create a volume folder, click **Create Volume Folder**, then complete the fields in the **Create Volume Folder** dialog box.
   b. Click **OK**.
   c. Click **Next**.
   The wizard advances to the next page.
6. Manage server folders for the local user group.
   a. If you need to create a server folder, click **Create Server Folder**, then complete the fields in the **Create Server Folder** dialog box.
   b. Click **OK**.
   c. Click **Next**.
   The wizard advances to the next page.
7. Manage disk folders for the local user group.
   a. Select the disk folders you want to add.
   b. Click **Finish**.

The wizard closes.

8. Click **OK**.

Delete a Local Storage Center User Group

Delete a local Storage Center user group if it is no longer needed.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Local User Groups** subtab, select the local user group, then click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK** to confirm.
6. Click **OK**.

Enabling Directory Services Authentication

Before you can grant Storage Center access to directory users and directory user groups, you must first configure Storage Center to communicate with one or more Active Directory/OpenLDAP servers. If you use Kerberos authentication, you must also configure Storage Center to communicate with the Kerberos Key Distribution Center (KDC).

Prerequisites

- An Active Directory or OpenLDAP directory service must be deployed in your environment.
- Storage Center must have network connectivity to the directory service.
- You must be familiar with the Active Directory/OpenLDAP configuration of the directory service.
- Storage Center requires credentials from a directory service user that is allowed to query the directory service and who has sufficient privileges to perform a bind operation.
- (Active Directory only) Joining the controller to the domain requires credentials from a directory service user who is an administrator and who has sufficient privileges to create a computer record in the directory.
- (Active Directory only) To join the controller to the domain, forward and reverse DNS records for the Storage Center must be created in the domain. For a single-controller Storage Center system, create DNS records for the controller IP address. For a dual-controller Storage Center system, create DNS records for the management IP address.
- (OpenLDAP only) To use password authentication with OpenLDAP, an SSL certificate is required to communicate with the directory service using SSL/TLS.

Discover Directory Service Settings Automatically

Use the Configure Directory Service Automatic Discovery wizard to allow the Storage Center to discover available directory services automatically.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Directory Services** tab.
4. Click **Configure Directory Services Automatic Discovery**.
   The Storage Center automatically discovers directory server settings and displays the settings in the **Configure Directory Service Automatic Discovery** wizard.
5. (Optional) Clear the checkbox next to any setting you want to change, and then type a new value into that field.
   - In the **URI** field, type the uniform resource identifier (URI) for one or more servers to which Storage Center connects.

     NOTE: Use the fully qualified domain name (FQDN) of the servers.

Example URIs for two servers:

ldap://server1.example.com ldap://server2.example.com:1234

NOTE: Adding multiple servers ensures continued authorization of users in the event of a resource outage. If Storage Center cannot establish contact with the first server, Storage Center attempts to connect to the remaining servers in the order listed.

- In the **Directory Server Connection Timeout** field, type the maximum time (in minutes) that Storage Center waits while attempting to connect to an Active Directory server. This value must be greater than zero.
- In the **Base DN** field, type the base distinguished name for the LDAP server. The Base DN is the starting point when searching for users.
- In the **Storage Center Hostname** field, type the fully qualified domain name (FQDN) of the Storage Center.
  - For a single-controller Storage Center system, this is the fully qualified host name for the controller IP address.
  - For a dual-controller Storage Center system, this is the fully qualified host name for the management IP address.
- In the **LDAP Domain** field, type the LDAP domain to search.

6. (Optional) Click **Test Server** to verify that the Storage Center can communicate with the specified directory servers using the selected protocol.
7. (Optional) If Transport Layer Security (TLS) is enabled, upload a Certificate Authority PEM file.
   a. Click **Upload Certificate Authority PEM**.
   b. Browse to the location of the PEM file, select the file, and click **Select**. The **Upload TLS Certificate** dialog box opens.

      NOTE: If you select the wrong PEM file, click **Upload Certificate** in the **Upload TLS Certificate** dialog box to select a new file.

   c. Click **OK** to upload the certificate.
8. Click **Next**.
   The **Kerberos Settings** page opens.
9. (Optional) Select the **Enabled** checkbox to enable Kerberos authentication.
10. To change any of the Kerberos settings, clear the **Auto-Discover** checkbox, and then type a new value into that field.
    - **Kerberos Domain Realm**: Kerberos domain realm to authenticate against. In Windows networks, this is the domain name in uppercase characters.
    - **KDC Hostname or IP Address**: Fully qualified domain name (FQDN) or IP address of the Key Distribution Center (KDC) to which Storage Center will connect.
    - **Password Renew Rate (Days)**: Number of days before the keytab is regenerated. The default value is 0, which equates to a password renew rate of 14 days.
11. Click **Next**.
    The **Join Domain** page opens.
12. Type the user name and password of a domain administrator.
13. Click **Next**.
    The **Summary** page opens.
14. If you want to change any setting, click **Back** to return to the previous page.
15. Click **Finish**.
16. Click **OK**.

Configure Directory Services Manually

Use the Directory Service Manual Configuration wizard to enter directory service settings manually. Use manual configuration for OpenLDAP or special Active Directory configurations.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Directory Services** tab.
4. Click **Configure Directory Services Manually**.

The **Directory Service Manual Configuration** wizard opens.

5. From the **Directory Type** drop-down menu, select **Active Directory** or **OpenLDAP**.
6. Type the settings for the directory server.
   - In the **URI** field, type the uniform resource identifier (URI) for one or more servers to which Storage Center connects.

     NOTE: Use the fully qualified domain name (FQDN) of the servers.

     Example URIs for two servers:

     ldap://server1.example.com ldap://server2.example.com:1234

     NOTE: Adding multiple servers ensures continued authorization of users in the event of a resource outage. If Storage Center cannot establish contact with the first server, Storage Center attempts to connect to the remaining servers in the order listed.
   - In the **Directory Server Connection Timeout** field, type the maximum time (in minutes) that Storage Center waits while attempting to connect to an Active Directory server. This value must be greater than zero.
   - In the **Base DN** field, type the base distinguished name for the LDAP server. The Base DN is the starting point when searching for users.
   - In the **Relative Base** field, type the Relative Base information. A Relative Base is a list of Relative Distinguished Names (RDN) prepended to the Base DN, indicating where the controller should be joined to the domain. An RDN contains an attribute and a value, such as:

     OU=SAN Controllers

     OU is the attribute, and **SAN Controllers** is the value.

     The following special characters used within an RDN value must be escaped using a backslash:

     , + " \ < > ; = / CR and LF

     For example:

Relative Base:	OU=SAN Controllers
(No escapes necessary)	
Relative Base:	OU=SAN****+Controllers
(The plus character is escaped)	
Relative Base:	OU=Buildings A****,B\,C,OU=SAN ****+Controllers
(Commas and plus sign are escaped *except* for the comma separating the RDNs.)	
   - In the **Storage Center Hostname** field, type the fully qualified domain name (FQDN) of the Storage Center.
     - For a single-controller Storage Center system, this is the fully qualified host name for the controller IP address.
     - For a dual-controller Storage Center system, this is the fully qualified host name for the management IP address.
   - In the **LDAP Domain** field, type the LDAP domain to search.
   - In the **Authentication Bind DN** field, type the Distinguished Name or User Principal Name of the user that the Storage Center uses to connect to and search the LDAP server.
   - In the **Authentication Bind Password** field, type the password for the authentication bind Distinguished Name.
7. (Optional) Click **Test Server** to verify that the Storage Center can communicate with the specified directory servers using the selected protocol.
8. (Optional) If Transport Layer Security (TLS) is enabled, upload a Certificate Authority PEM file.
   a. Click **Upload Certificate Authority PEM**.
   b. Browse to the location of the PEM file, select the file, and click **Select**. The **Upload TLS Certificate** dialog box opens.

      NOTE: If you select the wrong PEM file, click **Upload Certificate** in the **Upload TLS Certificate** dialog box to select a new file.

   c. Click **OK** to upload the certificate.
9. Click **Next**. The **Kerberos Settings** page opens.

10. (Optional) Select the **Enabled** checkbox to enable Kerberos authentication.
11. To change any of the Kerberos settings, clear the **Auto-Discover** checkbox, and then type a new value into that field.
    - **Kerberos Domain Realm**: Kerberos domain realm to authenticate against. In Windows networks, this is the domain name in uppercase characters.
    - **KDC Hostname or IP Address**: Fully qualified domain name (FQDN) or IP address of the Key Distribution Center (KDC) to which Storage Center will connect.
    - **Password Renew Rate (Days)**: Number of days before the keytab is regenerated. The default value is 0, which equates to a password renew rate of 14 days.
12. Click **Next**.
    The **Join Domain** page opens.
13. Type the user name and password of a domain administrator.
14. Click **Next**.
    The **Summary** page opens.
15. If you want to change any setting, click **Back** to return to the previous page.
16. Click **Finish**.
17. Click **OK**.

Managing Directory Service Users

Directory service users can be individually granted access to a Storage Center.

NOTE: For user interface reference information, click **Help**.

Grant Access to a Directory User

Grant access to a directory user to allow the user to log in to the Storage Center using directory credentials.

Prerequisites

The Storage Center must be configured to authenticate users with an external directory service.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory Users** subtab, click **Actions** > **Grant Access to Directory User**.
   The **Grant Access to Directory User** dialog box opens.
5. In the **User Principal Name** field, type the principal name for the directory user. The following formats are supported:
   - *username*@*domain*
   - *domain**username*
6. In the **Distinguished Name** field, type the distinguished name for the directory user.
   For example: `CN=Firstname Lastname,CN=Users,DC=example,DC=com`
7. In the **Real Name** field, type the real name of the directory user.
8. From the **Privilege** drop-down menu, select the privilege level to assign to the user.
   - **Administrator**: When selected, the user has full access to the Storage Center.
   - **Volume Manager**: When selected, the user has read and write access to the folders associated with the assigned user groups.
   - **Reporter**: When selected, the user has read-only access to the folders associated with the assigned user groups.
9. From the **Session Timeout** drop-down menu, select the maximum length of time that the user can be idle while logged in to the Storage Center before the connection is terminated.
10. (Volume Manager and Reporter only) Add one or more local user groups to the user.
    a. In the **Local User Groups** area, click **Change**.
       The **Select Local User Groups** dialog box opens.

b. (Optional) To create a new local user group, click **Create Local User Group** , then complete the **Create Local User Group** wizard. For user interface reference information, click **Help**.
c. Select the checkbox for each local user group you want to associate with the user.
d. Click **OK**.
The **Select Local User Groups** dialog box closes.

11. (Optional) Specify more information about the user in the **Details** area. For user interface reference information, click **Help**.
12. Click **OK**.
The **Grant Access to Directory User** dialog box closes.
13. Click **OK**.

Increase the Privilege Level for a Directory Service User

The privilege level can be increased for directory service users that have the Volume Manager or Reporter privilege. The privilege level for a user cannot be decreased.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory Users** subtab, select the user, then click **Edit Settings**.
The **Edit Settings** dialog box opens.
5. From the **Privilege** drop-down menu, select the privilege level to assign to the user.
   - **Administrator** – When selected, the local user has full access to the Storage Center.
   - **Volume Manager** – When selected, the local user has read and write access to the folders associated with the assigned user groups.
   - **Reporter** – When selected, the local user has read-only access to the folders associated with the assigned user groups.
6. Click **OK**.
The local user **Edit Settings** dialog box closes.
7. Click **OK**.

Change the Session Timeout for a Directory Service User

The session timeout controls the maximum length of time that the user can be idle while logged in to the Storage Center before the connection is terminated.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory Users** subtab, select the user, then click **Edit Settings**.
The **Edit Settings** dialog box opens.
5. From the **Session Timeout** drop-down menu, select the maximum length of time that the user can be idle while logged in to the Storage Center before the connection is terminated.
6. Click **OK**.
The **Edit Settings** dialog box closes.
7. Click **OK**.

Enable or Disable Access for a Directory Service User

When a directory service user is disabled, the user is not allowed to log in.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. Enable or disable access for the directory service user.
   - To enable access, select the **Enabled** checkbox.
   - To disable access, clear the **Enabled** checkbox.
6. Click **OK**.
   The local user **Edit Settings** dialog box closes.
7. Click **OK**.

Modify Local Group Membership for a Directory Service User

User groups grant access to volume, server, and disk folders for users with the Volume Manager or Reporter privilege level.

Prerequisites

- The directory service user must have been individually granted access to the Storage Center. Users that have been granted access based on a directory group inherit local group membership from the directory group settings.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. Modify local group membership for the user.
   a. In the **Local User Groups** area, click **Change**.
      The **Select Local User Groups** dialog box opens.
   b. (Optional) To create a new local user group, click **Create Local User Group**, then complete the **Create Local User Group** wizard. For user interface reference information, click **Help**.
   c. Select the checkbox for each local user group you want to associate with the local user.
   d. To remove the local user from a local group, clear the checkbox for the group.
   e. Click **OK**.
      The **Select Local User Groups** dialog box closes.
6. Click **OK**.
   The local user **Edit Settings** dialog box closes.
7. Click **OK**.

Configure Preferences for a Directory Service User

By default, each Storage Center user inherits the default user preferences. If necessary, the preferences can be individually customized for a user.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.

2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. Click **Configure User Preferences**. The **Configure User Preferences** dialog box opens.
6. Modify the user preferences as needed, then click **OK**.

   NOTE: For user interface reference information, click **Help**.

7. Click **OK**.
   The local user **Edit Settings** dialog box closes.
8. Click **OK**.

Modify Descriptive Information About a Directory Service User

The descriptive information about a local user includes his or her real name, department, title, location, telephone numbers, email address(es), and notes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory Users** subtab, select the user, then click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. Click **Configure User Preferences**.
   The **Configure User Preferences** dialog box opens.
6. Modify the **Real Name** field as necessary.
7. Modify the fields in the **Details** area as necessary, then click **OK**.

   NOTE: For user interface reference information, click **Help**.

8. Click **OK**.
   The local user **Edit Settings** dialog box closes.
9. Click **OK** .

Delete a Directory Service User

Delete a directory service user if he or she no longer requires access. The user that was used to add the Storage Center to Storage Manager cannot be deleted. The last user with the Administrator privilege cannot be deleted because Storage Center requires at least one Administrator.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory Users** subtab, select the user, then click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK** to confirm.
6. Click **OK**.

Restore a Deleted Directory Service User

If you are restoring a deleted user with the Volume Manager or Reporter privilege, the user must be added to one or more local user groups.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory Users** subtab, click **Actions** > **Restore Deleted User**.
   The **Restore Deleted User** wizard opens.
5. Select the directory service user that you want to restore, then click **Next**.
   The wizard advances to the next page.
6. (Volume Manager and Reporter only) Add the local user to one or more local user groups.
   a. In the **Local User Groups** area, click **Change**.
      The **Select Local User Groups** dialog box opens.
   b. (Optional) To create a new local user group, click **Create Local User Group**, then complete the **Create Local User Group** wizard. For user interface reference information, click **Help**.
   c. Select the checkbox for each local user group you want to associate with the local user.
   d. Click **OK**.
      The **Select Local User Groups** dialog box closes.
7. Modify the remaining user settings as needed.

   NOTE: For user interface reference information, click **Help**.

8. Click **Finish**.
   The **Restore Deleted User** wizard closes.
9. Click **OK**.

Managing Directory User Groups

Granting access to a directory user group grants access to all directory users that belong to the group.

NOTE: For user interface reference information, click **Help**.

Grant Access to a Directory User Group

Grant access to a directory user group to allow directory users in the group to log in to the Storage Center.

Prerequisites

- The Storage Center must be configured to authenticate users with an external directory service.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory User Groups** subtab, click **Grant Access to Directory User Groups**.
   The **Grant Access to Directory User Groups** dialog box opens.
5. In the **Display Name** field, type a name to identify the directory user group.
6. In the **Distinguished Name** field, type the distinguished name for the directory user group.

   Example: CN=Groupname,CN=Users,DC=example,DC=com

7. From the **Privilege** drop-down menu, select the privilege level to assign to the user group.

- **Administrator**: When selected, directory users in the group have full access to the Storage Center.
- **Volume Manager**: When selected, directory users in the group have read and write access to the folders associated with the assigned user groups.
- **Reporter**: When selected, directory users in the group have read-only access to the folders associated with the assigned user groups.

8. (Volume Manager and Reporter only) Add one or more local user groups to the directory user group.
   a. In the **Local User Groups** area, click **Change**.
   The **Select Local User Groups** dialog box opens.
   b. (Optional) To create a new local user group, click **Create Local User Group**, then complete the **Create Local User Group** wizard. For user interface reference information, click **Help**.
   c. Select the checkbox for each local user group you want to associate with the directory user group.
   d. Click **OK**.
   The **Select Local User Groups** dialog box closes.
9. Click **OK**.
   The **Grant Access to Directory User Groups** dialog box closes.
10. Click **OK**.

Increase the Privilege Level for a Directory User Group

The privilege level can be increased for directory service groups that have the Volume Manager or Reporter privilege. The privilege level for a directory service group cannot be decreased.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory User Groups** subtab, select the directory user group, then click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. From the **Privilege** drop-down menu, select the privilege level to assign to the user group.
   - **Administrator** – When selected, directory users in the group have full access to the Storage Center.
   - **Volume Manager** – When selected, directory users in the group have read and write access to the folders associated with the assigned user groups.
   - **Reporter** – When selected, directory users in the group have read-only access to the folders associated with the assigned user groups.
6. Click **OK**.
   The **Edit Settings** dialog box closes.
7. Click **OK**.

Modify Local Group Membership for a Directory User Group

Local user groups grant access to volume, server, and disk folders for directory user groups with the Volume Manager or Reporter privilege level.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory User Groups** subtab, select the directory user group, then click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. Modify local group membership for the directory user group.
   a. In the **Local User Groups** area, click **Change**.
   The **Select Local User Groups** dialog box opens.

b. (Optional) To create a new local user group, click **Create Local User Group**, then complete the **Create Local User Group** wizard. For user interface reference information, click **Help**.
c. Select the checkbox for each local user group you want to associate with the directory user group.
d. To remove the directory user group from a local group, clear the checkbox for the local group.
e. Click **OK**.
The **Select Local User Groups** dialog box closes.

6. Click **OK**.
The **Edit Settings** dialog box closes.
7. Click **OK**.

Delete a Directory User Group

Delete a directory user group if you no longer want to allow access to the directory users that belong to the group.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
The **Edit Storage Center Settings** dialog box opens.
3. Click the **Users and User Groups** tab.
4. On the **Directory User Groups** subtab, select the directory user group, then click **Delete**.
The **Delete** dialog box opens.
5. Click **OK** to confirm.
6. Click **OK**.

Managing Local Storage Center User Password Requirements

Setting password requirements for local Storage Center users increases the password security for all Storage Center local users.

Configure Local Storage Center User Password Requirements

Set local user password requirements to increase the complexity of local user passwords and improve the security of the Storage Center.

About this task

NOTE: For user interface reference information, click **Help**.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
The **Edit Storage Center Settings** dialog box opens.
3. Click the **Password Configuration** tab.
4. Select the **Enabled** checkbox.
5. Configure the password requirements as necessary.
   - To set the number of previous passwords that Storage Center checks against when validating a password, type a value in the **History Retained** field. To disable previous password validation, type 0.
   - To set the minimum number of characters in a new password, type a value in the **Minimum Length** field. To match the Storage Center minimum password length, set the value to 1.
   - To set the number of login failures that lock out an account, type a number in the **Account Lockout Threshold** field. To disable the account lockout threshold, type 0.
     NOTE: Only administrator-level accounts can unlock other Storage Center accounts. Have more than one Storage Center administrator-level account so that other Storage Center accounts can be unlocked.
   - To require new passwords to follow complexity standards, select the **Complexity Enabled** checkbox. To disable the password complexity requirement, clear the **Complexity Enabled** checkbox.

- To set the number of days before a user can change his or her password, type a value in the **Minimum Age** field. To disable the minimum age requirement, type 0.
- To set the number of days after which a password expires, type a value in the **Maximum Age** field. To disable the maximum age requirement, type 0.
- To set the number of days before a password expires when the expiration warning message is issued, type a value in the **Expiration Warning Time** field. To disable the expiration warning message, type 0.
- To specify the password expiration warning message that a user receives, type a warning message in the **Expiration Warning Message**. The expiration warning message is blank if this field is left empty.

6. Click **OK**.

Reset the Password Aging Clock

The password aging clock determines when a password expires based on the minimum and maximum age requirements. Reset the password aging clock to start the password aging clock from the current date and time.

Prerequisites

Password Configuration must be enabled.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Password Configuration** tab.
4. Select the **Enabled** checkbox.
5. Select the **Reset Aging Clock** checkbox.
6. Click **OK**.

Apply Password Requirements to Other Storage Centers

The password requirements set on a Storage Center can also be applied to another Storage Center managed by Storage Manager.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**. The **Edit Settings** dialog box opens.
3. Click the **Apply these settings to other Storage Centers** check box.
4. Click OK. The Select Storage Center dialog box opens.
5. Select a Storage Center.
   - To select an individual Storage Center, place a check next to a Storage Center.
   - To select all Storage Centers, click **Select All**.
   - To deselect all Storage Centers, click **Unselect All**.
6. Click **OK**.

Require Users to Change Passwords

The new password requirements apply to new user passwords only. Require users to change passwords at next login so the password complies with the new password requirements.

Prerequisites

Password Configuration must be enabled.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Password Configuration** tab.
4. Select the **Enabled** checkbox.
5. Select the **Requires Password Change** checkbox.
6. Click **OK**.

Managing Front-End I/O Ports

Fibre Channel (FC), iSCSI, and SAS ports on a storage system may be designated for use as front-end I/O ports. Front-end I/O ports can connect to Fibre Channel fabrics or Ethernet networks that contain servers that require storage, or directly to a server using SAS connections.

NOTE: When a Storage Manager Client is connected to a storage system through a Data Collector, information about front-end SAS connections is not displayed in the Servers view of the Storage Manager Client.

Front-End Connectivity Modes

Storage Center uses either legacy mode, virtual port mode, or ALUA port mode to transport data to servers that use SAN storage. In legacy mode, front-end I/O ports are configured in pairs of primary and reserved ports. In virtual port mode, all ports are active, and if one port fails the load is distributed between the remaining ports within the same fault domain. In ALUA port mode, volumes are mapped using two paths, active and passive.

NOTE: In Legacy mode, reserve ports and primary ports reside on separate controllers, providing controller-level failover only. Legacy mode does not provide port-level failover.

The front-end connectivity mode is configured independently for Fibre Channel and iSCSI. Both transport types can be configured to use the same mode or different modes to meet the needs of the network infrastructure. For example, a Storage Center can be configured to use virtual port mode for iSCSI and legacy mode for FC.

- The front-end connectivity mode for FC and iSCSI ports is initially selected during Storage Center deployment.
- After deployment, the front-end FC and iSCSI ports can be changed from legacy mode to virtual port mode.
  - After FC and iSCSI ports are configured for virtual port mode, they cannot be changed back to legacy mode.

    NOTE: Use legacy port mode only if the network environment does not meet the requirements for virtual port mode.
- The front-end connectivity mode for SAS front-end is always ALUA port mode and cannot be changed.

Virtual Port Mode

Virtual port mode provides port and controller redundancy by connecting multiple active ports to each Fibre Channel or Ethernet switch.

In virtual port mode, each physical port has a WWN (World Wide Name), and is also assigned an additional virtual WWN. Servers target only the virtual WWNs. During normal conditions, all ports process I/O. In the event of a port or controller failure, a virtual WWN will move to another physical WWN in the same fault domain. When the failure is resolved and ports are rebalanced, the virtual port returns to the preferred physical port.

Virtual port mode provides the following advantages over legacy mode:

- **Increased performance**: Because all ports are active, additional front-end bandwidth is available without sacrificing redundancy.
- **Improved redundancy**: Ports can fail over individually instead of by controller.
- **Simplified iSCSI configuration**: Each fault domain has an iSCSI control port that coordinates discovery of the iSCSI ports in the domain. When a server targets the iSCSI port IP address, it automatically discovers all ports in the fault domain.

ALUA Port Mode

Asymmetric Logical Unit Access (ALUA) provides port and controller redundancy for SAS front-end connections.

Volumes mapped to a server using SAS front-end also have port and controller redundancy. Volumes mapped over SAS are mapped to both controllers. The volume mapping is Active/Optimized on one controller and Standby on the other controller. If the port or controller fails on the active controller, the paths to the other controller become Active/Optimized. The mapping on the first controller switches to Standby. When the port or controller recovers, the mapping to the first controller returns to Active/Optimized and the mapping to the second controller returns to Standby status.

Legacy Mode

Legacy mode provides controller redundancy for a dual-controller Storage Center by connecting multiple primary and reserved ports to each Fibre Channel or Ethernet switch.

NOTE: Legacy mode is not available on SCv2000 or SCv3000 series storage systems.

In Legacy mode, each primary port on a controller is paired with a corresponding reserved port on the other controller. During normal conditions, the primary ports process I/O and the reserved ports are in standby mode. If a controller fails, the primary ports fail over to the corresponding reserved ports on the other controller. This approach ensures that servers connected to the switch do not lose connectivity if one of the controllers fails. For optimal performance, the primary ports should be evenly distributed across both controllers. When possible, front-end connections should be made to separate controller I/O cards to improve redundancy.

About Fault Domains and Ports

Fault domains group front-end ports that are connected to the same transport media, such as a Fibre Channel fabric or Ethernet network. Ports that belong to the same fault domain can fail over to each other because they have the same connectivity.

Front-end ports are categorized into fault domains that identify the allowed port movement when a controller reboots or a port fails. Failure modes and port activity depend on whether the Storage Center is configured for Legacy mode, ALUA port mode, or Virtual port mode.

Fault Domains for SCv2000 Series Storage Systems

The Storage Center handles all fault domain creation and modification on SCv2000 series.

Depending on the hardware configuration, the following fault domains are automatically created on SCv2000 series storage systems:

- For SCv2000 series storage systems with Fibre Channel HBAs, two fault domains are created for the Fibre Channel ports.
- For SCv2000 series storage systems with iSCSI HBAs, two fault domains are created for the iSCSI ports.
- For SCv2000 series storage systems with SAS HBAs, four fault domains are created for the SAS ports.
- Fault domains are automatically created for Flex/Embedded Ethernet ports.

NOTE: Additional front-end fault domains cannot be created on SCv2000 series storage systems . In addition, existing fault domains cannot be modified or deleted on SCv2000 series storage systems .

Fault Domains for SCv3000 Series Storage Systems

The Storage Center handles all fault domain creation and modification on SCv3000 series storage systems.

Depending on the hardware configuration, the following fault domains are automatically created on SCv3000 series storage systems:

- For SCv3000 series storage systems with Fibre Channel HBAs, two fault domains are created for the Fibre Channel ports.
- For SCv3000 series storage systems with iSCSI HBAs, two fault domains are created for the iSCSI ports.
- For SCv3000 series storage systems with SAS HBAs, four fault domains are created for the SAS ports.
- For SCv3000 series storage systems with iSCSI mezzanine cards, two fault domains are created for the iSCSI ports.
- For SCv3000 series storage systems with iSCSI mezzanine cards and iSCSI HBAs, four fault domains are created for iSCSI ports

NOTE: Additional front-end fault domains cannot be created on SCv3000 series storage systems. In addition, existing fault domains cannot be modified or deleted on SCv3000 series storage systems.

Fault Domains for Front-End SAS Ports for SC4020 Storage Systems

Users can select the number of fault domains to create for front-end SAS ports on SC4020 Storage Systems.

Fault domain behavior on SC4020 Storage Systems:

- Storage Center generates the SAS fault domains by pairing un-used front-end SAS ports into fault domains. If all SAS front-end ports are already included in fault domains, fault domains cannot be created.
  - Storage Center uses one port from each controller.
  - The paired ports have the same port number.
- Users can modify fault domain names and notes about the fault domain.
- Users can delete SAS fault domains.
- Users cannot add, move or remove ports within SAS fault domains.

Fault Domains in Virtual Port Mode

In virtual port mode, fault domains group front-end ports that are connected to the same Fibre Channel fabric or Ethernet network. All ports in a fault domain are available for I/O. If a port fails, I/O is routed to another port in the fault domain.

The following requirements apply to fault domains in virtual port mode:

- Fault domains are created for each front-end Fibre Channel fabric or Ethernet network.
- A fault domain must contain a single type of transport media (FC or iSCSI, but not both).

  CAUTION: For iSCSI only, servers initiate I/O to iSCSI ports through the control port of the fault domain. If an iSCSI port moves to a different fault domain, its control port changes. This change disrupts any service initiated through the previous control port. If an iSCSI port moves to a different fault domain, you must reconfigure the server-side iSCSI initiators before service can be resumed.
- For each fault domain, it is a best practice to connect at least two cables from each controller to the Fibre Channel fabric or Ethernet network.

Fault Domains in Legacy Mode

In Legacy Mode, each pair of primary and reserved ports are grouped into a fault domain. The fault domain determines which ports are allowed to fail over to each other.

The following requirements apply to fault domains in legacy mode on a dual-controller Storage Center:

- A fault domain must contain one type of transport media (FC or iSCSI, but not both).
- A fault domain must contain one primary port and one reserved port.
- The reserved port must be located on a different controller than the primary port.

  NOTE: For a single-controller Storage Center, only one fault domain is required for each transport type (FC or iSCSI) because there are no reserved ports.

Failover Behavior

Legacy mode, ALUA port mode, and virtual port mode behave differently during failure conditions because they use different mechanisms to provide fault tolerance.

Table 14. Front-End I/O Ports Failover Behavior

Scenario	Virtual Port Mode	Legacy Mode	ALUA Port Mode
Normal operating conditions	All ports are active and pass I/O.	• Primary ports pass I/O. • Reserved ports remain in a standby mode until a controller failure.	• Active/Optimized ports pass I/O. • Standby ports remain in a standby mode until a controller or port failure.

Table 14. Front-End I/O Ports Failover Behavior (continued)

Scenario	Virtual Port Mode	Legacy Mode	ALUA Port Mode
A controller fails in a dual-controller Storage Center	Virtual ports on the failed controller move to physical ports on the functioning controller.	Primary ports on the failed controller fail over to reserved ports on the functioning controller.	Active/Optimized ports on the failed controller fail over to the Standby ports on the functioning controller.
A single port fails (single- or dual-controller Storage Center)	[1]An individual port fails over to another port on the same controller in the same fault domain.	The port does not fail over because there was no controller failure. If a second path is available, MPIO software on the server provides fault tolerance.	The port fails over to the Standby port on the functioning controller.

NOTE: [1]To support port level failover, a controller must have at least two ports in the same fault domain using the same transport media, such as FC or iSCSI.

Rebalance Front-End Ports

If a controller has been restarted, front-end ports can become unbalanced. If front-end ports are unbalanced, a message at the top of the Summary tab prompts you to rebalance the ports.

About this task

NOTE: Front-end ports are automatically rebalanced when using SCv2000 and SCv3000 series controllers. Manual port rebalance is not necessary.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Summary** tab.
3. Click **Rebalance Ports** in the banner message.
   A **Rebalance Ports** dialog box is displayed, which shows the progress of the rebalance operation.

Managing Front-End I/O Port Hardware

Front-end FC and iSCSI ports can be renamed and monitored with threshold definitions. iSCSI ports can be assigned network configuration and tested for network connectivity.

For a Storage Center in virtual port mode, the **Hardware** tab displays a virtual port for each physical port. For physical ports, the physical identity, speed, and hardware are given. For virtual ports, the current and preferred physical ports are shown.

NOTE: For user interface reference information, click **Help**.

Rename a Front-End I/O Port

Set a display name for a physical or virtual I/O port to make it more identifiable.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click the **Front End Ports** subtab.
4. Double-click the desired I/O port.
   The **Hardware** tab for the I/O port opens.
5. Click **Edit Settings**.
   The **Edit Controller Port Settings** dialog box opens.
6. In the **Name** field, type a descriptive name for the I/O port.

7. Click **OK**.
   The **Edit Controller Port Settings** dialog box closes.

Reset a Front-End IO Port Name to the WWN

Reset a physical or virtual IO port name to the World Wide Name if you no longer need the descriptive name defined by an administrator.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Controllers**→ controller name→ **IO Ports**→*transport type*, then select the IO port.
4. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
5. Click **Reset name to WWN**.
6. Click **OK**.

Change the Preferred Physical IO Port for a Virtual IO Port

Under normal operating conditions, a FC or iSCSI virtual port is hosted by its preferred physical port.

Prerequisites

The fault domain must be configured for virtual port mode.

- If a Storage Center has IO ports with different performance characteristics, you may want to configure a virtual port to use a particular physical port.
- If a physical port is removed from a Storage Center, the corresponding virtual port must be assigned to a different physical port.
- A single physical port can be the preferred port for multiple virtual ports.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Controllers**→ *controller name*→ **IO Ports**→*transport type*→*physical IO port*, then select the virtual IO port.
4. In the right pane, click **Edit Settings**. The **Edit Settings** dialog box appears.
5. From the **Preferred Parent** drop-down menu, select the WWN of the physical IO port that should host the virtual port when possible.
6. Click **OK**.

Set or Modify the IP Address and Gateway for a Single iSCSI Port

Servers target the iSCSI port IP address to initiate iSCSI connections to the Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click the **Front End Ports** subtab.
4. Double-click the desired I/O port.
   The **Hardware** tab for the IO port opens.
5. Click **Edit Settings**.
   The **Edit Controller Port Settings** dialog box opens.
6. In the **IPv4 Address** field, type the new IPv4 address for the iSCSI I/O port.

7. Click **OK**.
   The **Edit Controller Port Settings** dialog box closes.

Test Network Connectivity for an iSCSI Port

Test connectivity for an iSCSI I/O port by pinging a port or host on the network.

About this task

NOTE: If multiple virtual fault domains (VLANs) are associated with the port, the physical fault domain is used for ping tests issued from the **Hardware** tab. To test network connectivity for a VLAN, initiate a ping test from a physical port in a fault domain on the **Storage** tab.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click the **Front End Ports** subtab.
4. Double-click the desired IO port.
   The **Hardware** tab for the I/O port opens.
5. Click **Ping Address**.
   The **Ping Address** dialog box opens.
6. If the port uses an IPv4 address, in the **IPv4 Address** field, type the IP address of the host to which you want to test connectivity.
7. If the port uses either an IPv4 or IPv6 address, in the **IP Address** field, type the IP address of the host to which you want to test connectivity.
8. From the **Ping Size** drop-down menu, select a size in bytes for the ping packets, not including overhead. If you select **Other**, type a value between 1 and 17000 bytes in the field below the menu.

   NOTE: The **Ping Size** drop-down menu might not be displayed depending on the hardware I/O cards used by the Storage Center.

9. Click **OK**. A message displays the results of the test.
10. Click **OK**.

Related tasks

Test Network Connectivity for an iSCSI Port in a Fault Domain on page 266

Set Threshold Alert Definitions for a Front-End IO Port

Configure one or more Threshold Alert Definitions for an IO port if you want to be notified when an IO port reaches specific bandwidth or latency thresholds.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click the **Front End Ports** subtab.
4. Double-click the IO port.
   The **Hardware** tab for the IO port opens.
5. Click **Set Threshold Alert Definitions**.
   The **Set Threshold Alert Definitions** dialog box opens.
6. From the **Selected Alert Definitions** table, select the alert definition for which you want to configure a threshold alert and click **Create Threshold Definition**.
   The **Create Threshold Definition** dialog box opens.
7. Configure the threshold definition attributes as needed, then click **OK**. These attributes are described in the online help.
8. From the **Available Alert Definitions** table, click the new alert definition.

The threshold alert is automatically set for the selected alert definition.

9. (Optional) To remove the Threshold Alert Definition, hold **Ctrl** and click the alert definition in the .**Selected Alert Definitions** table, then hold **Ctrl** and click the threshold alert in the .**Available Alert Definitions** table.
   The alert threshold is removed from the alert definition.
10. Click **OK**.

Configure Front-End I/O Ports (Fibre Channel and SAS)

On SCv2000 series and SCv3000 series storage systems, unconfigured Fibre Channel and SAS ports must be configured before they can be used as front-end ports.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click the **Unconfigured Ports** subtab.
4. In the right pane, select an unconfigured Fibre Channel or SAS I/O port.
5. Click **Configure Port**.

Configure Front-End I/O Ports (iSCSI)

On SCv2000 series and SCv3000 series storage systems, unconfigured iSCSI ports must be configured before they can be used as front-end ports..

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click the **Unconfigured Ports** subtab.
4. In the right pane, select an unconfigured iSCSI I/O port.
5. Click **Configure Port**.
6. Type an IP address for the port.
7. Click **OK**.

Unconfigure Front-End I/O Ports

On SCv2000 series and SCv3000 series storage systems, unconfigure I/O ports that are not connected to the storage network and are not intended for use.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click the **Front End Ports** subtab.
4. In the right pane, select a down I/O port and click **Unconfigure Port**.
   The **Unconfigure Port** confirmation dialog box opens.
5. Click **OK**.

Converting Front-End Ports to Virtual Port Mode

Using the Convert to Virtual Port Mode tool converts all front-end iSCSI or Fibre Channel IO ports to virtual port mode. After the conversion is complete, the ports can not be converted back to legacy mode.

Convert Fibre Channel Ports to Virtual Port Mode

Use the Convert to Virtual Port Mode tool to convert all Fibre Channel ports on the Storage Center controllers to virtual port mode.

Prerequisites

The Fibre Channel ports must be in legacy port mode.

About this task

NOTE: This operation cannot be undone. After the ports are converted to virtual port mode, they cannot converted back.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. From the Storage tab navigation pane, expand **Fault Domains** then select the **Fibre Channel** folder.
4. Click **Convert to Virtual Port Mode**.
   The **Convert to Virtual Port Mode** confirmation dialog box appears.
5. Click **OK**.

Convert iSCSI Ports to Virtual Port Mode

Use the Convert to Virtual Port Mode tool to convert all iSCSI ports on the Storage Center controllers to virtual port mode.

Prerequisites

The iSCSI ports must be in legacy port mode.

About this task

NOTE: This operation cannot be undone. After the ports are converted to virtual port mode, they cannot be converted back.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. From the Storage tab navigation pane, expand **Fault Domains** then select the **iSCSI** folder.
4. Click **Convert to Virtual Port Mode**.
   The **Convert to Virtual Port Mode** dialog box opens.
5. In the Domain field of each fault domain you want to convert, type a new IP address to use as the primary port for each iSCSI fault domain.
6. Click **OK**.

Managing Back-End I/O Port Hardware

Back-end ports can be renamed and monitored with threshold definitions.

Configure Back-End Ports

Use the Generate Default Back End Port Configuration dialog box to configure back-end ports. After the ports are configured, they can be used to connect enclosures.

Prerequisites

- Supported only on CT-SC040, SC8000, or SC9000 storage systems.
- Back-end ports have not been previously configured during Storage Center configuration.
- An enclosure must be connected to the ports.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, click **Fault Domains**.
4. Click **Generate Default Back End Port Configuration**.
   The **Generate Default Back End Port Configuration** dialog box opens and displays the status of all SAS ports.
5. Select the ports with a status of **Up** and click **Finish** to configure the ports as back-end ports.

Configure Individual Back-End I/O Ports

A back-end port must be configured before the port can be used for back-end connectivity.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click the **Unconfigured Ports** subtab.
4. Right-click a SAS I/O port and select **Configure as Back End** from the menu.
   The port is configured as a back-end port.

Rename a Back-End I/O Port

Set a display name for an I/O port to make it more identifiable.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click the **Back End Ports** subtab.
4. Double-click the desired I/O port.
   The **Hardware** tab for the I/O port opens.
5. Click **Edit Settings**.
   The **Edit Controller Port Settings** dialog box opens.
6. In the **Name** field, type a descriptive name for the I/O port.
7. Click **OK**.
   The **Edit Controller Port Settings** dialog box closes.

Grouping Fibre Channel I/O Ports Using Fault Domains

Front-end ports are categorized into fault domains that identify allowed port movement when a controller reboots or a port fails. Ports that belong to the same fault domain can fail over to each other because they have connectivity to the same resources.

NOTE: Fault domains cannot be added or modified on SCv2000 or SCv3000 series storage systems. Storage Center creates and manages fault domains on these systems.

Create a Fibre Channel Fault Domain

Create a Fibre Channel fault domain to group Fibre Channel ports for failover purposes.

Prerequisites

The Fibre Channel ports to add to the fault domain must be unconfigured. Ports that are already added to a fault domain or designated as back-end ports cannot be added to a new fault domain.

- In virtual port mode, all Fibre Channel ports that are connected to the same Fibre Channel fabric should be added to the same fault domain.
- In legacy mode, each pair of primary and reserved ports connected to the same Fibre Channel fabric should be added to a unique fault domain. The primary port should be located on a different controller than the secondary port.

About this task

NOTE: Fibre Channel ports are always configured in Virtual Port Mode on SCv2000 and SCv3000 series storage systems. Legacy Mode is not supported.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, click **Fault Domains**, then click **Create Fibre Channel Fault Domain**.
   The **Create Fault Domain** dialog box opens.
4. In the **Name** field, type a name for the fault domain.
5. In the **Ports** table, select the Fibre Channel ports to add to the fault domain. All Fibre Channel ports in the fault domain should be connected to the same Fibre Channel fabric
6. Click **OK**.

Rename a Fibre Channel Fault Domain

The fault domain name allows administrators to identify the fault domain.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **Fibre Channel** and select a fault domain.
   The **FC Fault Domain** view is displayed.
4. Click **Edit Settings**.
   The **Edit Fault Domain Settings** dialog box opens.
5. In the **Name** field, type a name for the fault domain.
6. Click **OK**.

Remove Ports from an Fibre Channel Fault Domain

To repurpose front-end Fibre Channel ports, remove the ports from the fault domain.

About this task

- If the front-end ports are configured for virtual port mode, the storage system must be running Storage Center 7.5.1 or later to remove all ports from a fault domain.
- If the front-end ports are configured for virtual port mode, but the storage system is running a version of Storage Center earlier than Storage Center 7.5.1, an error occurs if the port being removed is the last port in the fault domain.
- If front-end ports are configured for legacy mode, all the ports in a fault domain can be removed from a storage system running any supported version Storage Center.

NOTE: You cannot remove the last port in the fault domain for an SCv2000 Series or SCv3000 Series system.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **Fibre Channel** and select the fault domain.
4. If you are using an SCv2000 Series or SCv3000 Series storage system, click **Edit Settings**, clear the check boxes of the ports to remove from the fault domain, and click **OK**.

   Otherwise, perform the following steps to remove ports from a fault domain:

   a. Click **Edit Settings**.
   b. In the **Ports** area, click **Remove Ports from Fault Domain**.
   c. In the **Remove Ports from Fault Domain** dialog box, select the ports to remove from the fault domain.
   d. Click **OK** to remove the selected ports from the fault domain.
   e. Click **OK** to close the **Edit Fault Domain Settings** dialog box.

Delete a Fibre Channel Fault Domain

Delete a Fibre Channel fault domain if all ports have been removed and it is no longer needed.

About this task

- If the front-end ports were configured for virtual port mode, the storage system must be running Storage Center 7.5.1 or later to remove a fault domain.
- If the front-end ports were configured for legacy mode, a fault domain can be removed from a storage system running any supported version Storage Center.

NOTE: You cannot delete fault domains on SCv2000 Series or SCv3000 Series storage systems.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, expand **Fibre Channel**, and select the fault domain to delete.
   The **Fault Domain** view is displayed.
4. Click **Delete**.
   The **Delete Fault Domain** dialog box opens.
5. Click **OK**.

Grouping iSCSI I/O Ports Using Fault Domains

Front-end ports are categorized into fault domains that identify allowed port movement when a controller reboots or a port fails. Ports that belong to the same fault domain can fail over to each other because they have connectivity to the same resources.

NOTE: Fault domains cannot be added or modified on SCv2000 or SCv3000 series storage systems. Storage Center creates and manages fault domains on these systems.

iSCSI VLAN Tagging Support

iSCSI ports in a fault domain can be configured to use a VLAN ID. For each Storage Center, one of two levels of VLAN functionality is available depending on the Storage Center OS version, Storage Center controller model, and iSCSI hardware. Basic VLAN functionality is referred to as single-VLAN tagging, and enhanced VLAN functionality is referred to as multi-VLAN tagging.

Single-VLAN Tagging

If a Storage Center supports single-VLAN tagging, a maximum of 1 VLAN ID can be configured for each iSCSI I/O port. An iSCSI I/O port can belong to only one fault domain, and all ports in the same fault domain use the same VLAN ID.

Single VLAN tagging is supported by all Storage Center versions compatible with Storage Manager.

Multi-VLAN Tagging

If a Storage Center supports multi-VLAN tagging, a maximum of 64 VLAN IDs can be configured for each iSCSI I/O port. An iSCSI I/O port can belong to up to 64 fault domains—one for each VLAN.

Multi-VLAN tagging is supported by Storage Centers that meet the multi-VLAN tagging requirements.

Multi-VLAN Tagging Requirements

The following table lists the requirements that a Storage Center must meet to support multi-VLAN tagging.

Requirement	Description
Storage Center controller model	Multi-VLAN Tagging is not supported on SCv3000 or SCv2000 storage systems.
Storage Center iSCSI I/O card hardware	Chelsio T3, T5, or T6 iSCSI cards must be installed in the Storage Center.
Storage Center front-end connectivity mode	The Storage Center iSCSI ports must be configured for virtual port mode. Legacy mode is not supported.

Types of iSCSI Fault Domains

When a Storage Center meets the multi-VLAN tagging requirements, two types of iSCSI fault domains can be created.

- **Physical** – The first fault domain configured for a given set of iSCSI ports.
  - Physical fault domains do not require a VLAN ID, but can be configured to use a VLAN ID.
  - Physical fault domains support iSCSI replication to and from remote Storage Centers.
- **Virtual** – Subsequent VLAN fault domains configured for the same set of iSCSI ports are referred to as virtual fault domains.
  - Virtual fault domains must be assigned a VLAN ID.
  - Virtual fault domains do not support iSCSI replication.
  - Virtual fault domains do not support IPv6.

Creating iSCSI Fault Domains

Create an iSCSI fault domain to group ports that can fail over to each other because they have connectivity to the same resources.

NOTE: For user interface reference information, click **Help**.

Create a Physical iSCSI Fault Domain

Create a physical iSCSI fault domain to group physical ports for failover purposes.

Prerequisites

- In virtual port mode, all iSCSI ports that are connected to the same iSCSI network should be added to the same fault domain.
- In legacy mode, each pair of primary and reserved ports that are connected to the same iSCSI network should be added to a unique fault domain. The primary port should be located on a different controller than the secondary port.
- Physical ports cannot be selected and added to a fault domain if they are already added to another fault domain.
- Each iSCSI port that you want to add to the fault domain must be assigned an IP address, subnet mask, and gateway in the same network as the iSCSI control port for the fault domain.

About this task

NOTE: iSCSI ports must be configured in virtual port mode when using SCv2000 and SCv3000 series controllers. Legacy mode is not supported.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then select **iSCSI**.
4. In the right pane, click **Create Fault Domain**. The **Create Fault Domain** dialog box opens.
5. In the **Name** field, type a name for the fault domain.
6. (Virtual port mode only) Configure an IP address and gateway for the iSCSI control port in the fault domain. Servers target this IP address using iSCSI initiators, and the Storage Center redirects individual iSCSI connections to the appropriate virtual port.
   a. In the **Target IPv4 Address** field, type an IP address to assign to the iSCSI control port.
   b. In the **Subnet Mask** field, type the subnet mask for the well-known IP address.
   c. In the **Gateway IPv4 Address** field, type the IP address for the iSCSI network default gateway.
7. (Optional) In the **Target IPv6 Address** field, type an IP address to assign to the iSCSI control port.
8. (Optional) If necessary, assign a VLAN ID to the fault domain.

   NOTE: If the Storage Center does not meet the multi-VLAN tagging requirements, a VLAN ID cannot be specified at this time. Instead, modify the fault domain after it is created to add a VLAN ID.

   a. Select the **Physical** option if you want to create a physical fault domain, that is, a fault domain that consists of physical ports.
   b. Select the **Virtual** option if you want to create a fault domain that consists of virtual ports.
   c. Select the **VLAN Tagged** check box if you want to create a tagged fault domain that consist of physical ports.
   d. In the **VLAN ID** field, type a VLAN ID for the fault domain. Allowed values are 1–4096.
   e. (Optional) To assign a priority level to the VLAN, type a value from 0–7 in the **Class of Service Priority** field. 0 is best effort, 1 is the lowest priority, and 7 is the highest priority.
9. In the **Ports** table, select the iSCSI ports to add to the fault domain. All iSCSI ports in the fault domain should be connected to the same Ethernet network.
   If creating a physical fault domain, physical ports appear in the list only if they are not assigned to any fault domain yet.
10. Click **OK**.

Next steps

(Optional) Configure VLANs for the iSCSI ports in the fault domain by creating a virtual fault domain for each VLAN. Base the virtual fault domains on the physical fault domain.

Related concepts

iSCSI VLAN Tagging Support on page 260

Related tasks

Set or Modify the IP Address and Gateway for a Single iSCSI Port on page 253
Create a Virtual iSCSI Fault Domain on page 262
Add a VLAN ID to a Physical iSCSI Fault Domain on page 263

Create a Virtual iSCSI Fault Domain

To add a VLAN ID to iSCSI ports that are already in use, use an existing iSCSI fault domain as the basis for a new VLAN iSCSI fault domain.

Prerequisites

- The Storage Center must meet the multi-VLAN tagging requirements.
- Virtual fault domains do not support IPv6.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains→ iSCSI**, then select the fault domain.
4. In the right pane, click **Create VLAN Copy**. The **Create VLAN** dialog box opens.
5. In the **Name** field, type a name for the fault domain.
6. Configure an IP address and gateway for the iSCSI control port in the fault domain. Servers target this IP address using iSCSI initiators, and the Storage Center redirects individual iSCSI connections to the appropriate virtual port.
   a. In the **Target IPv4 Address** field, type an IP address to assign to the iSCSI control port.
   b. In the **Subnet Mask** field, type the subnet mask for the well known IP address.
   c. In the **Gateway IPv4 Address** field, type the IP address for the iSCSI network default gateway.
7. Configure VLAN tagging.
   a. In the **VLAN ID** field, type VLAN ID for the fault domain. Allowed values are 1–4096.
   b. (Optional) To assign a priority level to the VLAN, type a value from 0–7 in the **Class of Service Priority** field. 0 is best effort, 1 is the lowest priority, and 7 is the highest priority.
8. Assign a VLAN IP address to each selected port in the **Ports** table by editing the corresponding field in the **VLAN IP Address** column. Each port must have an IP address in the same network as the iSCSI control port, which is specified in the **Well Known IP Address** field.
9. Click **OK**.

Related concepts

iSCSI VLAN Tagging Support on page 260
Multi-VLAN Tagging Requirements on page 260

Related tasks

Create a Virtual iSCSI Fault Domain on page 262

Modifying iSCSI Fault Domains

Modify an iSCSI fault domain to change its name, modify network settings for iSCSI ports in the domain, add or remove iSCSI ports, or delete the fault domain.

NOTE: For user interface reference information, click **Help**.

Rename an iSCSI Fault Domain

The fault domain name allows administrators to identify the fault domain.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Edit Settings**.
   The **Edit Fault Domain Settings** dialog box opens.
5. In the **Name** field, type a name for the fault domain.
6. Click **OK**.

Modify iSCSI Fault Domain Control Port Network Settings

Configure an IP address and gateway for the iSCSI control port in the fault domain. Servers target this IP address using iSCSI initiators, and the Storage Center redirects individual iSCSI connections to the appropriate virtual port.

Prerequisites

The Storage Center iSCSI ports must be configured for virtual port mode.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Edit Settings**.
   The **Edit Fault Domain Settings** dialog box opens.
5. In the **Target IPv4 Address** field, type an IP address to assign to the iSCSI control port.
6. In the **Subnet Mask** field, type the subnet mask for the well-known IP address.
7. In the **Gateway IPv4 Address** field, type the IP address for the iSCSI network default gateway.
8. (Optional) If IPv6 is supported, in the **Target IPv6 Address** field, type an IP address to assign to the iSCSI control port.
9. Click **OK**.

Add a VLAN ID to a Physical iSCSI Fault Domain

Add a VLAN ID to an existing iSCSI fault domain if the ports in the fault domain are connected to a tagged network.

Prerequisites

The Storage Center iSCSI ports must be configured for virtual port mode.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Edit Settings**.

The **Edit Fault Domain Settings** dialog box opens.

5. Select the **VLAN Tagged** checkbox.
6. In the **VLAN ID** field, type a VLAN ID for the fault domain. Allowed values are 1–4096.
7. (Optional) To assign a priority level to the VLAN, type a value from 0-7 in the **Class of Service Priority** field. 0 is best effort, 1 is the lowest priority, and 7 is the highest priority.
8. Click **OK**.

Related concepts

iSCSI VLAN Tagging Support on page 260

Modify the MTU for an iSCSI Fault Domain

The Maximum Transmission Unit (MTU) specifies the largest packet size supported by the iSCSI network.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Edit Settings**.
   The **Edit Fault Domain Settings** dialog box opens.
5. From the **MTU** drop-down menu, select the largest packet size supported by the iSCSI network.
6. Click **OK**.

Modify the TCP Port for an iSCSI Fault Domain

By default, iSCSI ports accept iSCSI connections on TCP port 3260. Modify the port as needed to integrate with iSCSI network infrastructure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Edit Settings**.
   The **Edit Fault Domain Settings** dialog box opens.
5. Click **Edit Advanced Port Settings**.
   The **Edit Advanced Port Settings** dialog box opens.
6. In the **Port Number** field, type the TCP port to use for iSCSI traffic.
7. Click **OK** to close the **Edit Advanced Port Settings** dialog box.
8. Click **OK**.

Modify the iSCSI Window Size for an iSCSI Fault Domain

The window size specifies the amount of data that can be in transit at any given time.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Edit Settings**.
   The **Edit Fault Domain Settings** dialog box opens.
5. Click **Edit Advanced Port Settings**.
   The **Edit Advanced Port Settings** dialog box opens.

6. In the **Window Size** field, type a value for the window size.
   - Allowed values are 16 KB to 32 MB.
   - The window size must be divisible by 16 KB.
7. Click **OK** to close the **Edit Advanced Port Settings** dialog box.
8. Click **OK**.

Modify Digest Settings for an iSCSI Fault Domain

The iSCSI digest settings determine whether iSCSI error detection processing is performed.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Edit Settings**.
   The **Edit Fault Domain Settings** dialog box opens.
5. Click **Edit Advanced Port Settings**.
   The **Edit Advanced Port Settings** dialog box opens.
6. In the **Digest Settings** area, select or clear the **Immediate Data Write** checkbox as needed.
7. Click **OK** to close the **Edit Advanced Port Settings** dialog box.
8. Click **OK**.

Modify Timeout Settings for an iSCSI Fault Domain

iSCSI timeout settings determine how the Storage Center handles idle connections.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Edit Settings**.
   The **Edit Fault Domain Settings** dialog box opens.
5. Click **Edit Advanced Port Settings**.
   The **Edit Advanced Port Settings** dialog box opens.
6. In the **Timeout Settings** area, modify the timeout values as needed. These options are described in the online help.
7. Click **OK** to close the **Edit Advanced Port Settings** dialog box.
8. Click **OK**.

Add Ports to an iSCSI Fault Domain

After you connect additional iSCSI ports to an existing iSCSI network, add the iSCSI ports to the fault domain that corresponds to the network.

Prerequisites

- If the fault domain is physical, the iSCSI ports that will be added to the fault domain must not belong to a fault domain.
- If the fault domain is physical, each iSCSI port that you want to add to the fault domain must be assigned an IP address, subnet mask, and gateway in the same network as the iSCSI control port for the fault domain.
- If the fault domain is virtual, the iSCSI ports you want to add to the fault domain must support the Multi-VLAN Tagging feature.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.

2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Edit Settings**.
   The **Edit Fault Domain Settings** dialog box opens.
5. In the **Ports** table, click **Add Ports to Fault Domain**.
   The **Add Ports to Fault Domain** dialog box opens.
6. In the **Select the ports to add** table, select the iSCSI ports to add to the fault domain. All iSCSI ports in the fault domain should be connected to the same Ethernet network.
7. (Virtual fault domain only) Assign a VLAN IP address to each selected port by editing the corresponding field in the **VLAN IP Address** column. Each port must have an IP address in the same network as the iSCSI control port.
8. Click **OK** to close the **Add Ports to Fault Domain** dialog box.
9. Click **OK**.

Related concepts

iSCSI VLAN Tagging Support on page 260

Related tasks

Set or Modify the IP Address and Gateway for a Single iSCSI Port on page 253

Test Network Connectivity for an iSCSI Port in a Fault Domain

Test connectivity for an iSCSI physical or virtual I/O port by pinging a port or host on the network.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, right-click the physical port for which you want to test connectivity, then select **Ping Address**.
   The **Ping Address** dialog box opens.
5. Type the IP address of the host to which you want to test connectivity.
   - If the host uses either IPv4 or IPv6 addressing, type the IP address of the host to which you want to test connectivity in the **IP Address** field.
   - If the host uses IPv4 addressing only, type the IPv4 address in the **IPv4 Address** field.
6. Click **OK**. A message displays the results of the test.
7. Click **OK**.

Related tasks

Test Network Connectivity for an iSCSI Port on page 254

Remove Ports from an iSCSI Fault Domain

To repurpose front-end iSCSI ports, remove the ports from the fault domain.

About this task

- If the front-end ports are configured for virtual port mode, the storage system must be running Storage Center 7.5.1 or later to remove all ports from a fault domain.
- If the front-end ports are configured for virtual port mode, but the storage system is running a version of Storage Center earlier than Storage Center 7.5.1, an error occurs if the port being removed is the last port in the fault domain.
- If front-end ports are configured for legacy mode, all the ports in a fault domain can be removed from a storage system running any supported version Storage Center.

NOTE: You cannot remove the last port in the fault domain for an SCv2000 Series or SCv3000 Series system.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, expand **iSCSI**, and select a fault domain.
4. If you are using an SCv2000 Series or SCv3000 Series storage system, click **Edit Settings**, clear the check boxes of the ports to remove from the fault domain, and click **OK**.

   Otherwise, perform the following steps to remove ports from a fault domain:

   a. Click **Edit Settings**.
   b. In the **Ports** area, click **Remove Ports from Fault Domain**.
   c. In the **Remove Ports from Fault Domain** dialog box, select the ports to remove from the fault domain.
   d. Click **OK** to remove the selected ports from the fault domain.
   e. Click **OK** to close the **Edit Fault Domain Settings** dialog box.

Delete an iSCSI Fault Domain

Delete an iSCSI fault domain if all ports have been removed and it is no longer needed.

About this task

- If the front-end ports were configured for virtual port mode, the storage system must be running Storage Center 7.5.1 or later to remove a fault domain.
- If the front-end ports were configured for legacy mode, a fault domain can be removed from a storage system running any supported version Storage Center.

NOTE: You cannot delete fault domains on SCv2000 Series or SCv3000 Series storage systems.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, expand **iSCSI**, and select the fault domain to delete.
   The **Fault Domain** view is displayed.
4. Click **Delete**.
   The **Delete Fault Domain** dialog box opens.
5. Click **OK**.

Configuring NAT Port Forwarding for iSCSI Fault Domains

Port forwarding allows iSCSI initiators (servers or remote Storage Centers) located on a public network or different private network to communicate with Storage Center iSCSI ports on a private network behind a router that performs Network Address Translation (NAT).

For each Storage Center iSCSI control port and physical port, the router performing NAT must be configured to forward connections destined for a unique public IP address and TCP port pair to the private IP address and TCP port for the iSCSI port. These port forwarding rules must also be configured in parallel on the Storage Center fault domains to make sure that iSCSI target control port redirection functions correctly. Fault domains can only be modified by administrators.

NOTE: If Storage Center iSCSI ports are configured for legacy mode, the port forwarding rules do not need to be defined on the Storage Center because there is no control port redirection.

iSCSI NAT Port Forwarding Requirements for Virtual Port Mode

The following requirements must be met to configure NAT port forwarding for an iSCSI fault domain in virtual port mode.

- For each Storage Center iSCSI control port and virtual port, a unique public IP address and TCP port pair must be reserved on the router that performs NAT.
- The router that performs NAT between the Storage Center and the public network must be configured to forward connections destined for each public IP address and port pair to the appropriate Storage Center private target iSCSI IP address and private port (by default, TCP port 3260).

iSCSI NAT Port Forwarding Example Configuration

In this example, a router separates the Storage Center on a private network (192.168.1.0/24) from a server (iSCSI initiator) on the public network (1.1.1.60). To communicate with Storage Center iSCSI target ports on the private network, the server connects to a public IP address owned by the router (1.1.1.1) on ports 9000 and 9001. The router forwards these connections to the appropriate private IP addresses (192.168.1.50 and 192.168.1.51) on TCP port 3260.

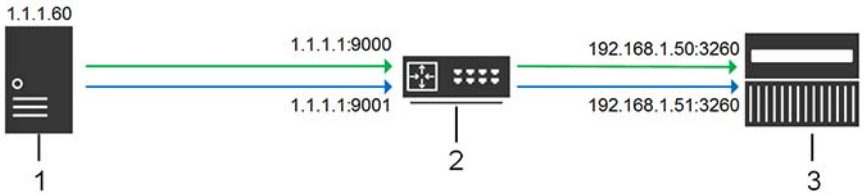


Figure 24. iSCSI NAT Port Forwarding Diagram

Item	Description
1	iSCSI initiator (server or remote Storage Center)
2	Router performing NAT/port forwarding
3	Storage Center

Configure NAT Port Forwarding for an iSCSI Fault Domain

Configure NAT port forwarding for a fault domain to make sure that control port redirection works correctly.

Prerequisites

When the router that performs NAT and port forwarding receives inbound iSCSI connections destined for the specified public IP and public port, it forwards the connections to the private Storage Center iSCSI IP address and private port (by default, TCP port 3260).

- The Storage Center iSCSI ports must be configured for virtual port mode.
- For each Storage Center iSCSI control port and virtual port, a unique public IP address and TCP port pair must be reserved on the router that performs NAT.
- The router that performs NAT between the Storage Center and the public network must be configured to forward connections destined for each public IP address and port pair to the appropriate Storage Center private iSCSI IP address and appropriate port (by default, TCP 3260).

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Configure NAT Port Forwarding**.
   The **Configure NAT Port Forwarding** dialog box opens.
5. In the **Port Forwarding Configuration** area, configure port forwarding information for a Storage Center iSCSI port.
   a. Click **Add**.
      The **Create iSCSI NAT Port Forward** dialog box opens.
   b. From the **Port Name** drop-down menu, select the iSCSI control port or a physical port.
      - Control ports are labeled with the name of the fault domain.
      - Physical ports are labeled with a WWN.
   c. In the **Public IPv4 Address** field, type the IPv4 address that iSCSI initiators (servers and remote Storage Centers) communicate with on the public network to reach the Storage Center iSCSI port.
   d. In the **Public Port** field, type the TCP port that iSCSI initiators communicate with on the public network to reach the Storage Center iSCSI port.
   e. Click OK.
      The **Create iSCSI NAT Port Forward** dialog box closes.

6. Repeat the preceding steps for each additional iSCSI control port and physical port in the fault domain.
7. In the **Public Networks/Initiators** area, define an iSCSI initiator IP address or subnet that requires port forwarding to reach the Storage Center because it is separated from the Storage Center by a router performing NAT.
   a. Click **Add**.
   The **Create iSCSI NAT Public Network/Initiator** dialog box opens.
   b. In the **Public IPv4 Address** field, type the IPv4 address for the iSCSI initiator or subnet for which NAT port forwarding is required.
   c. In the **Subnet Mask** field, type the subnet mask for the iSCSI initiator IP address or subnet.
   d. Click OK.
   The **Create iSCSI NAT Public Network/Initiator** dialog box closes.
8. Repeat the preceding steps for each additional iSCSI initiator IP address or subnet that requires port forwarding.
9. Click **OK**.

Modify NAT Port Forwarding for an iSCSI Fault Domain

Modify NAT port forwarding to change the port forwarding configuration or change the iSCSI initiators and subnets that require port forwarding.

Prerequisites

- The Storage Center iSCSI ports must be configured for virtual port mode.
- For each Storage Center iSCSI control port and virtual port, a unique public IP address and TCP port pair must be reserved on the router that performs NAT.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Configure NAT Port Forwarding**.
   The **Configure NAT Port Forwarding** dialog box opens.
5. In the **Port Forwarding Configuration** area, modify port forwarding information for a Storage Center iSCSI port.
   - To add port forwarding information for an iSCSI port, click **Add**.
   - To modify port forwarding information for an iSCSI port, select the port, then click **Edit**.
   - To delete port forwarding information for an iSCSI port, select the port, then click **Remove**.
6. In the **Public Networks/Initiators** area, add or modify iSCSI initiator IP addresses or subnets that require port forwarding to reach the Storage Center because it is separated from the Storage Center by a router performing NAT.
   - To add an iSCSI initiator IP address or subnet, click **Add**.
   - To modify an iSCSI initiator IP address or subnet, select it, then click **Edit**.
   - To delete an iSCSI initiator IP address or subnet, select it, then click **Remove**.
7. Click **OK**.

Configuring CHAP for iSCSI Fault Domains

When Challenge Handshake Authentication Protocol (CHAP) authentication is enabled, the Storage Center challenges each iSCSI initiator in the fault domain for a shared secret (password). When CHAP is enabled it applies to all servers and remote Storage Centers that connect to the fault domain.

NOTE: When CHAP is enabled for an iSCSI fault domain, all iSCSI initiators in the fault domain (servers and Storage Centers) must be configured to use CHAP. All iSCSI initiators that are not configured to use CHAP are no longer able to communicate with the Storage Center iSCSI ports in the fault domain.

Configure CHAP for Servers in an iSCSI Fault Domain

When Challenge Handshake Authentication Protocol (CHAP) authentication is enabled (for unidirectional CHAP only), the Storage Center (target) challenges each iSCSI initiator for a shared secret (password). Servers (remote initiators) must provide

the correct shared secret to access Storage Center (target) volumes. To enable bidirectional CHAP authentication, unique shared secrets (passwords) must be configured for the remote initiator and the target Storage Center.

About this task

NOTE: Changing CHAP settings will cause existing iSCSI connections between SAN systems using the selected fault domain to be lost. You will need to use the **Configure iSCSI Connection** wizard to reestablish the lost connections after changing CHAP settings.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Configure CHAP**.
   The **Configure CHAP** dialog box opens.
5. Select the **CHAP Enabled** checkbox.
6. (Bidirectional CHAP only) In the **Bidirectional CHAP Secret** field, type the shared secret that the Storage Center (target) must provide when challenged by the remote initiator. If this field is empty, bidirectional CHAP authentication is not enabled.
7. Define the CHAP configuration for each server in the fault domain that initiates iSCSI connections to the Storage Center.
   a. Click **Add**.
      The **Add Remote CHAP Initiator** dialog box opens.
   b. In the **iSCSI Name** field, type the iSCSI name of the remote initiator.
   c. In the **Remote CHAP Name** field, type the CHAP name of the remote initiator.
   d. In the **Remote CHAP Secret** field, type the shared secret that the remote initiator must provide when challenged by the Storage Center (target).
   e. (Bidirectional CHAP only) In the **Local CHAP Secret** field, type the shared secret that the Storage Center (target) must provide when challenged by the remote initiator. This secret is required if bidirectional CHAP is enabled on the remote iSCSI initiator. This is the same shared secret that is typed into the **Bidirectional CHAP Secret** field for **Local CHAP Configuration** on the **Configure CHAP** dialog box.
   f. Click **OK**.
      The **Add Remote CHAP Initiator** dialog box closes.
8. Click **OK**.
   The **Configure CHAP** dialog box closes.
9. Configure each remote iSCSI initiator to use the shared secrets that you defined.

Modify CHAP Settings for a Server in an iSCSI Fault Domain

Modify CHAP settings for a server to change one or more shared secrets for the server.

About this task

NOTE: Changing CHAP settings will cause existing iSCSI connections between SAN systems using the selected fault domain to be lost. You will need to use the **Configure iSCSI Connection** wizard to reestablish the lost connections after changing CHAP settings.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Configure CHAP**.
   The **Configure CHAP** dialog box opens.
5. In the **Remote CHAP Configuration** table, select a CHAP configuration, then click **Edit**.
   The **Edit Remote CHAP Initiator** dialog box opens.
6. Modify the options as needed, then click **OK**.
   The **Edit Remote CHAP Initiator** dialog box closes.
7. Click **OK**.

Remove CHAP Settings for a Server in an iSCSI Fault Domain

Remove CHAP settings for a server to prevent it from targeting the Storage Center while CHAP is enabled for the fault domain.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Configure CHAP**.
   The **Configure CHAP** dialog box opens.
5. In the **Remote CHAP Configuration** table, select a CHAP configuration, then click **Remove**.
   The CHAP configuration is removed from the table.
6. Click **OK**.
   The **Configure CHAP** dialog box closes.

Enable Bidirectional CHAP for iSCSI Replication in a Fault Domain

When bidirectional CHAP is enabled for iSCSI replication, the source Storage Center (initiator) challenges the destination Storage Center (target) for a shared secret.

Prerequisites

CHAP must be enabled for the fault domain.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **iSCSI** and click the fault domain.
4. In the right pane, click **Configure CHAP**.
   The **Configure CHAP** dialog box opens.
5. Type a shared secret in the **Bidirectional CHAP Secret** field.

Related tasks

Configure an iSCSI Connection for Remote Storage Systems on page 495

Grouping SAS I/O Ports Using Fault Domains

Front-end ports are categorized into fault domains that identify allowed port movement when a controller reboots or a port fails. Ports that belong to the same fault domain can fail over to each other because they have connectivity to the same resources.

NOTE: Fault domains cannot be added or modified on SCv2000 or SCv3000 series storage systems. Storage Center creates and manages fault domains on these systems.

Create a SAS Fault Domain

Create a SAS fault domain to group SAS front-end ports for failover purposes on SC4020 or SC5020 controllers.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Fault Domains**, then click **Create SAS Fault Domain**.
   The **Create Fault Domain** dialog box opens.
4. In the **Name** field, type a name for the fault domain.

5. In the **Ports** table, select the SAS ports to add to the fault domain.
   When pairing SAS ports into the fault domain:
   - Use one port from each controller.
   - Make sure the paired ports have the same port number and are connected to the same server.
6. Click **OK**.

Delete a SAS Fault Domain

Delete a SAS fault domain if it is no longer needed.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Fault Domains**, then expand **SAS** and click the fault domain link.
   The **Fault Domain** view is displayed.
4. In the right pane, click **Delete**.
   The **Delete Fault Domain** dialog box opens.
5. Click **OK**.

Managing Disks and Disk Folders

Manage disks by adding new disks and organizing disks in disk folders.

Add disks and enclosures to accommodate greater data needs. The supported number of enclosures attached to Storage Center depends on the controller and enclosure being used.

When adding disks be aware of the following.

- After disks are added, additional space may not be immediately available. Make sure to allow enough time for Storage Manager to allocate space for writes.
- Create a new disk folder only to address specific application program requirements. Creating a second disk folder may cause storage to be used inefficiently.
- Data cannot be written to unassigned disks.
- The Assigned disk folder was created during initial configuration of the Storage Center. Managing unassigned disks means moving the disk to a managed disk folder.
- When Storage Manager detects self-encrypting drives (SEDs) that are Federal Information Processing Standard (FIPS) 140-2 certified, it formats the drives for Secure Data use.
  - If Self-Encrypting Drives is licensed, disks will be managed in a Secure Data folder.
  - If Self-Encrypting Drives is not licensed, disks will be treated as unsecured drives, but may be upgraded to Secure Data status if a license is purchased in the future.

Storage Center Disk Management

For SC7020, SC5020, and SCv3000 storage systems, Storage Center manages disks automatically. When configuring a storage system, Storage Center manages the disks into folders based on function of the disk. FIPS-certified Self-Encrypting Drives (SEDs) are managed into a separate folder than other disks. When Storage Center detects new disks, it manages the disk into the appropriate folder.

In Storage Center version 7.3 and later, the Automatic Drive Placement function can be turned on or off for all storage systems (except SCv2000 series) using the Storage Center Storage settings.

Disk Management on SCv2000 Series Storage Systems

SCv2000 series storage systems manage disks automatically, limiting the disk management options. After adding disks, Storage Center recognizes the new disks, creates a new disk folder if necessary, then manages the disks in the disk folder. If a disk is intentionally down for testing purposes, then is deleted, you can restore the disk to manage the disk again in a disk folder.

The following disk management options are not available for SCv2000 series storage systems:

- Creating disk folders
- Adding disks to disk folders
- Managing disk spares

Related tasks

Restore a Disk on page 276

Scan for New Disks

Scanning for disks recognizes new disks and allows them to be assigned to a disk folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Disks**, then click **Scan For Disks**.
   The **Scan For Disks** operation runs. After the scan completes, a confirmation dialog box opens.
4. Click **OK**.

Create a Disk Folder

Creating a disk folder manages unassigned disks in the new disk folder.

About this task

NOTE: Having multiple disk folders may cause storage to be used inefficiently.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Disks**, then click **Create Disk Folder**.
   The **Create Disk Folder** dialog box opens.
4. Type a name in the **Name** field.
5. To select the disks to be managed, click **Change**.
   The **Select Unmanaged Disks** dialog box opens.
6. Select the disks to be included in the disk folder.
7. Click **OK**.
   The **Select Unmanaged Disks** dialog box closes.
8. Click **OK**.

Related tasks

Create Secure Data Disk Folder on page 280

Delete Disk Folder

Delete a disk folder if all disks have been released from the folder and the folder is not needed.

Prerequisites

The disk folder does not contain disks.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Disks**, then select a disk folder.
   The **Disk Folder** view is displayed.
4. Click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK**.

Modify a Disk Folder

The disk folder Edit Settings dialog box allows you to change the name of the folder, add notes, or change the Storage Alert Threshold.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Disks**, then select a disk folder.
   The **Disk Folder** view is displayed.
4. Click **Edit Settings**.
   The **Edit Disk Folder Settings** dialog box opens.
5. Modify the following attributes as needed.
   - To change the name of the disk folder, type a name into the **Name** field.
   - To add notes to the disk folder, type text into the **Notes** field.
   - To change the percent of remaining data that initiates a threshold warning, select a value from the **Storage Alert Threshold** drop-down menu.
   - If the folder is a Secure Data disk folder, enable or disable the Rekey option by clicking the **Rekey** checkbox.
   - If the folder is a Secure Data disk folder, specify a rekey interval by typing a value in the field.
6. Click **OK**.

Manage Unassigned Disks

Manage Unassigned Disks assigns disks to an existing disk folder. A RAID rebalance is required to complete managing disks.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Disks**, then select an unassigned disk folder.
   The **Disk Folder** view is displayed.
4. Click **Manage Unassigned Disks**.
   The **Manage Unassigned Disks** dialog box opens.
5. From the **Disk Folder** drop-down menu, select a disk folder.
6. In the **Unassigned Disks** pane, select the disks to be assigned.
7. To schedule a RAID rebalance select one of the following options.
   - To start a RAID rebalance after creating the disk folder, select **Perform RAID rebalance immediately**.
   - To schedule a RAID rebalance for a later time, select **Schedule RAID rebalance** then select a date and time.
8. To skip the RAID rebalance, select **I will start RAID rebalance later**.

   NOTE: To use all available space, perform a RAID rebalance.

9. Click **OK**.

Enable or Disable the Disk Indicator Light

The drive bay indicator light identifies a drive bay so it can be easily located in an enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Disks**.
   The **Disks** view is displayed.
5. In the right pane, click the **Disks** subtab and select a disk.
6. Enable or disable the disk indicator light for the selected disk.
   - If the indicator light is off, click **Indicator On** to enable the indicator light.
   - If the indicator light is on, click **Indicator Off** to disable the indicator light.

Release a Disk

Release a disk before removing it from an enclosure. The disk is fully released after performing a RAID rebalance.

About this task

NOTE: Do not release disks from a disk folder unless the remaining disks have enough free space for the re-striped data.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the enclosure and select **Disks**.
   The **Disks** view is displayed.
4. In the right pane, click the **Disks** subtab, then select a disk and click **Release Disk**.
   The **Release Disks** dialog box opens.
5. Schedule a RAID rebalance.
   - To start a RAID rebalance after releasing the disk, select **Perform RAID rebalance immediately**.
   - To schedule a RAID rebalance, select **Schedule RAID rebalance** then select a date and time.
6. To skip the RAID rebalance, select **I will start RAID rebalance later**.
7. Click **OK**.

Cancel Releasing a Disk

After releasing a disk, the data remains on the disk until the RAID rebalance is complete. Cancel releasing a disk if the RAID rebalance has not completed and the data is still on the disk. Canceling the release reassigns the disk to the disk folder to which it was previously assigned.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the enclosure and select **Disks**.
   The **Disks** view is displayed.
4. In the right pane, click the **Disks** subtab, then select a disk marked for release and click **Cancel Release Disk**.
   The **Cancel Release Disks** dialog box opens.
5. Click **OK**.

Delete a Disk

Deleting a disk removes that disk object from Unisphere. Before deleting the disk object, you must release the disk, moving the data off the disk.

Prerequisites

- The disk failed and it does not have any allocated blocks.
- The disk was removed from the enclosure.
- If the disk was in an enclosure that has been removed, that enclosure object must be deleted first.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the enclosure and select **Disks**.
   The **Disks** view is displayed.
4. In the right pane, click the **Disks** subtab, then select the disk and click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK**.

Related tasks

Restore a Disk on page 276

Restore a Disk

After a disk fails, Storage Center does not allow that disk to be managed again. If the disk is down for testing purposes then deleted, the disk can be restored so that Storage Center can manage the disk again.

Prerequisites

The disk must be down, removed from the enclosure, and deleted from Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the enclosure and select **Disks**.
   The **Disks** view is displayed.
4. In the right pane, click the **Disks** subtab, then select the disk and click **Restore**.
   The **Restore Disk** dialog box opens.
5. Click **OK**.
   Storage Center restores the disk and adds it to a disk folder.

Replace a Failed Disk

The Replace Failed Disk wizard identifies the disk to replace and provides steps for replacing the disk.

Prerequisites

The status of the disk must be Down to be replaced.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the enclosure and select **Disks**.
   The **Disks** view is displayed.

4. In the right pane, select the failed disk to replace and click **Replace Disk**.
   The **Replace Failed Disk** wizard opens.
5. Locate the failed disk in the enclosure and click **Next**.
6. Follow the instructions to physically remove the failed disk from the enclosure and click **Next**.
7. Follow the instructions to insert the replacement disk into the enclosure and click **Next**.
   Storage Center attempts to recognize the replacement disk.

   If the disk replacement succeeds, Storage Center confirms that the disk replacement occurred successfully and displays information about the replacement disk.
8. Click **Finish** to close the wizard.

Managing Secure Data

Secure Data provides data-at-rest encryption with key management for self-encrypting drives (SED). The Self-Encrypting Drives feature must be licensed to use Secure Data.

How Secure Data Works

Using Secure Data to manage SEDs requires an external key management server. If a key management server has not been configured or is unavailable, Storage Center allows SEDs to be managed; however, it will not secure the SEDs until the key management server is available and configured, at which point they will be secured.

NOTE: Create a backup for the key management server before removing an SED and after managing an SED.

Each FIPS disk in Storage Center has an internal Media Encryption Key (MEK). The key resides on the disk, providing encryption for data written to the disk and decryption for data as it is read from the disk. Destroying the key makes any data on the disk immediately and permanently unreadable, a process referred to as a crypto erase. When you add an SED to, or release an SED from a Secure Data folder, the MEK is destroyed and a new key is generated. Creating a new key allows the disk to be reused, although all previous data is lost.

WARNING: Managing a FIPS SED and assigning it to a Secure Data folder destroys the encryption key on the disk, which makes any previous data on the disk unreadable.

Not to be confused with the MEK, the Storage Center manages a separate set of keys for providing data-at-rest encryption. These keys are referred to as authority credentials. The purpose of these keys is to protect the theft of any number of drives. If a secured drive from a Secure Data folder is removed from the system such that power is removed, the drive will be locked and customer data will be unreadable.

WARNING: Storage Center will not be able to manage a previously-managed drive as an SED if the key has been deleted from the drive or the key management server.

Authenticating to the drive using the authority credential is the only means of unlocking the drive while preserving customer data, which can only be obtained by successfully authenticating to the related key management server through a secure channel.

Use the **Copy Volumes to Disk Folder** operation to copy volumes from a Secure Data folder to another folder. The destination folder can be either a secure folder or a nonsecure folder.

To protect data at rest, all SEDs in a Secure Data disk folder lock when power is removed (lock on reset enabled). When power is removed from the drive, the drive cannot be unlocked without an authority credential.

When replicating from a Secure Data volume to a non-Secure Data folder, that volume is no longer secure after it leaves the Secure Data folder. When replicating a non-Secure Data volume to a Secure Data folder, that volume is not secure until it replicates to the Secure Data folder and Data Progression runs.

Configure Key Server

Before managing SEDs in a Secure Data folder, configure communication between Storage Center and the key management server.

Prerequisites

The Storage Center must have the Self-Encrypting Drives license.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Secure Data** tab.
4. In the **Hostname** field, type the host name or IP address of the key management server.
5. In the **Port** field, type the number of a port with open communication with the key management server.
6. In the **Timeout** field, type the amount of time in seconds after which Storage Center should stop attempting to reconnect to the key management server after a failure.
7. To add alternate key management servers, type the host name or IP address of another key management server in the **Alternate Hostnames** area. Then click **Add**.

   NOTE: Alternate hostnames should be added to the configuration after all drives in the system have initially been managed and fully secured. To ensure optimized access times during initial Key creation, alternate hostnames should be added only after the drives in the Storage Center have been initially managed and fully secured.

8. If the key management server requires a user name to validate the Storage Center certificate, type the name in the **Username** field.
9. If the key management server requires a password to validate the Storage Center certificate, type the password in the **Password** field.
10. Configure the key management server certificates.
    a. Click **Configure Key Management Server Certificates**.
       The **Configure Key Management Server Certificates** dialog box opens.
    b. Click **Browse** next to the **Root CA Certificate**. Navigate to the location of the root CA certificate on your computer and select it.
    c. Click **Browse** next to the certificate fields for the controllers Navigate to the location of the controller certificates on your computer and select them.
    d. Click **OK**.
11. Click **OK**.

Results

After you configure the key server, the **Server Connectivity** status is shown as **Up** on the **Edit Storage Center Settings** dialog box.

Configure Rekey Interval for Disk Folder

Specify a rekey interval for a Secure Disk folder. When that interval has been reached, a rekey is triggered on each disk in the folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Click the **Disks** node.
   The **Disks** view is displayed.
4. Right-click the name of a Secure Disk folder and select **Edit Settings**.
   The **Edit Disk Folder Settings** dialog box opens.
5. If the Rekey option is not enabled, select the checkbox to enable it.
6. Type a value in the Rekey interval field to specify the amount of time after which a rekey will be triggered on each disk in the folder.
7. Click **OK**.

Rekey a Disk Folder

Perform an on-demand rekey of a Secure Disk folder.

Prerequisites

The disk or disk folder must be enabled as Secure Disk.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Click the **Disks** node.
   The **Disks** view is displayed.
4. Right-click the name of a Secure Disk folder and select **Rekey Disk Folder**.
   The **Rekey Disk Folder** dialog box opens.
5. Click **OK**.

Rekey a Disk

Perform an on-demand rekey of a Secure Disk.

Prerequisites

The disk or disk folder must be enabled as Secure Disk disk.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Click the **Disks** node.
   The **Disks** view is displayed.
4. Right-click the name of a Secure Disk disk and select **Rekey Disk**.
   The **Rekey Disk** dialog box opens.
5. Click **OK**.

Copy Volumes to Disk Folder

Copy volumes from one Secure Disk folder to another folder. The target folder can be either a secure folder or a nonsecure folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Click the **Disks** node.
   The **Disks** view is displayed.
4. Right-click the name of a Secure Disk folder and select **Copy Volumes to Disk Folder**.
   The **Copy Volumes to Disk Folder** dialog box opens.
5. Choose the source volume by selecting the checkbox next to the name of the disk folder.
6. Use the drop-down menu to select the destination disk folder.
7. Click **OK**.

Create Secure Data Disk Folder

A Secure Data folder can contain only SEDs that are FIPS certified. If the Storage Center is licensed for Self-Encrypting Drives and unmanaged SEDs are found, the Create Disk folder dialog box shows the Secure Data folder option.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Click the **Disks** node.
   The **Disks** view is displayed.
4. Click **Create Disk Folder**.
   The **Create Disk Folder** dialog box opens. The dialog box displays all unmanaged disks and designates spare disks.
5. Select the **Create as a Secure Data folder** checkbox.

   NOTE: All non-SEDs must be removed from the Unmanaged Disks table before creating a Secure Data folder.

6. Type a name in the **Name** field.
7. Select the disks to be managed and click **OK**.
   The Secure Data Disk folder is created.
8. To modify the tier redundancy, select the **Create Storage Type** checkbox and then modify the redundancy for each tier as needed.
   - **Single Redundant**: Single-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 (each drive is mirrored)
     - RAID 5-5 (striped across 5 drives)
     - RAID 5-9 (striped across 9 drives)
   - **Dual redundant**: Dual redundant is the recommended redundancy level for all tiers. It is enforced for 3 TB HDDs and higher and for 18 TB SSDs and higher. Dual-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 Dual-Mirror (data is written simultaneously to three separate drives)
     - RAID 6-6 (4 data segments, 2 parity segments for each stripe)
     - RAID 6-10 (8 data segments, 2 parity segments for each stripe.)
9. Click **OK**.

Managing Data Redundancy

Manage data redundancy by modifying tier redundancy or creating Storage Types.

Redundancy Requirements

Drive size is used to determine the redundancy level to apply to a tier of drives. If any drive in a tier surpasses a threshold size, a specific redundancy level can be applied to the tier containing that drive. If a redundancy level is required, the Storage Center operating system sets the level and it cannot be changed.

Table 15. HDD Redundancy Recommendations and Requirements

Disk Size	Level of Redundancy Recommended or Enforced
Up to 3 TB	Dual redundant is the recommended level **NOTE:** Non-redundant storage is not an option for SCv2000 Series storage systems.
3 TB and higher	Dual redundant is required and enforced

Table 16. SSD Redundancy Recommendations and Requirements

Disk Size	Level of Redundancy Recommended or Enforced
Up to 18 TB	Dual redundant is the recommended level

Table 16. SSD Redundancy Recommendations and Requirements (continued)

Disk Size	Level of Redundancy Recommended or Enforced
	NOTE: Non-redundant storage is not an option for SCv2000 Series storage systems.
18 TB and higher	Dual redundant is required and enforced

Managing RAID

Modifying tier redundancy, or adding or removing disks can cause data to be unevenly distributed across disks. A RAID rebalance redistributes data over disks in a disk folder.

Rebalance RAID

Rebalancing RAID redistributes data over the disks according to the Storage Type. Rebalance the RAID after releasing a disk from a disk folder, when a disk fails, or after adding a disk.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Disks**.
4. Click **Rebalance RAID**.
   The **RAID Rebalance** dialog box opens. If a RAID rebalance is needed, the dialog box shows RAID rebalance options.
5. Select **Perform RAID Rebalance immediately**.
6. Click **OK**.

Cancel a RAID Rebalance

Cancel a RAID rebalance to stop an on-going RAID rebalance. Cancelling a RAID rebalance does not cancel the need to rebalance. You will still be prompted to rebalance RAID.

About this task

NOTE: The RAID rebalance stops after completing the current rebalance pass.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Disks**.
4. Click **Rebalance RAID**.
   The **RAID Rebalance** dialog box opens.
5. Click **Stop Rebalancing**. After rebalance stops, a confirmation dialog box opens.
6. Click **OK**.

Schedule a RAID Rebalance

Schedule a RAID rebalance to rebuild the data on all of the disks at a later date.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Disks**.

4. Click **Rebalance RAID**.
   The **RAID Rebalance** dialog box opens. If a RAID rebalance is needed, the dialog box shows RAID rebalance options. If a RAID rebalance is needed, the dialog box shows RAID rebalance options.
5. Select **Schedule RAID rebalance**.
6. Select a date and time.
7. Click **OK**.

Check the Status of a RAID Rebalance

The RAID Rebalance displays the status of an in-progress RAID rebalance and indicates whether a rebalance is needed.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select **Disks**.
4. Click **Rebalance RAID**.
   The **RAID Rebalance** dialog box shows the status of a RAID rebalance.
5. Click **OK**.

Managing Storage Types

Storage Types determine how Data Progression moves data within a disk folder. Each disk folder has a corresponding Storage Type.

NOTE: Modifying tier redundancy requires a RAID rebalance to be completed, and should not be performed unless sufficient free disk space is available within the disk folder.

Create a Storage Type

Creating a Storage Type sets the redundancy level for each tier and assigns the Storage Type to a disk folder.

Prerequisites

SCv2000 series storage systems do not support creating new Storage Types.

About this task

NOTE: Do not assign multiple Storage Types to one disk folder. Data Progression may not perform as intended with multiple Storage Types assigned to one disk folder.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, click **Storage Types**, then click **Create Storage Type**.
   The **Create Storage Type** dialog box opens.
4. Select a disk folder from the **Disk Folder** drop-down menu.
5. Select a redundancy type.
   - **Redundant**: Protects against the loss of any one drive (if single redundant) or any two drives (if dual redundant).
   - **Non-Redundant**: Uses RAID 0 in all classes, in all tiers. Data is striped but provides no redundancy. If one drive fails, all data is lost.
     NOTE: Non-Redundant is not recommended because data is not protected against a drive failure. Do not use non-redundant storage for a volume unless the data has been backed up elsewhere.
6. For Redundant Storage Types, you must select a redundancy level for each tier unless the drive type or size requires a specific redundancy level
   - **Single Redundant**: Single-redundant tiers can contain any of the following types of RAID storage:

- RAID 10 (each drive is mirrored)
- RAID 5-5 (striped across 5 drives)
- RAID 5-9 (striped across 9 drives)

- **Dual redundant**: Dual redundant is the recommended redundancy level for all tiers. It is enforced for 3 TB HDDs and higher and for 18 TB SSDs and higher. Dual-redundant tiers can contain any of the following types of RAID storage:
  - RAID 10 Dual-Mirror (data is written simultaneously to three separate drives)
  - RAID 6-6 (4 data segments, 2 parity segments for each stripe)
  - RAID 6-10 (8 data segments, 2 parity segments for each stripe.)

7. **Drive Addition** is selected by default. Leave this option selected.
8. Click **OK**.

Modify Tier Redundancy

Modify tier redundancy to change the redundancy level for each tier in a Storage Type. After modifying tier redundancy, a RAID rebalance is required to move data to the new RAID levels.

About this task

NOTE: Do not modify tier redundancy if there is insufficient space in the tier for a RAID rebalance.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, click **Storage Types**, then click the **Storage Types** subtab.
4. Right-click the Storage Type to modify and select **Modify Tier Redundancy**.
   The **Modify Tier Redundancy** dialog box opens
5. Modify the redundancy for each tier as needed.
   - **Redundant**: Protects against the loss of any one drive (if single redundant) or any two drives (if dual redundant).
   - **Non-Redundant**: Uses RAID 0 in all classes, in all tiers. Data is striped but provides no redundancy. If one drive fails, all data is lost.

     NOTE: Non-Redundant is not recommended because data is not protected against a drive failure. Do not use non-redundant storage for a volume unless the data has been backed up elsewhere.
6. For Redundant Storage Types, you must select a redundancy level for each tier unless the drive type or size requires a specific redundancy level
   - **Single Redundant**: Single-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 (each drive is mirrored)
     - RAID 5-5 (striped across 5 drives)
     - RAID 5-9 (striped across 9 drives)
   - **Dual redundant**: Dual redundant is the recommended redundancy level for all tiers. It is enforced for 3 TB HDDs and higher and for 18 TB SSDs and higher. Dual-redundant tiers can contain any of the following types of RAID storage:
     - RAID 10 Dual-Mirror (data is written simultaneously to three separate drives)
     - RAID 6-6 (4 data segments, 2 parity segments for each stripe)
     - RAID 6-10 (8 data segments, 2 parity segments for each stripe.)
7. **Drive Addition** is selected by default. Leave this option selected.
8. Click **OK**.
   A RAID rebalance starts.

Managing Disk Enclosures

Use the Hardware view to rename an enclosure, set an asset tag, clear the swap status for replaceable hardware modules in a disk enclosure, mute alarms, reset the temperature sensors, and delete an enclosure from a Storage Center.

Add an Enclosure

This step-by-step wizard guides you through adding a new enclosure to the system.

Prerequisites

This wizard is available only for SCv2000 series and SCv3000 series arrays. This procedure can be performed without a controller outage.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, click **Enclosure**.
   The **Enclosure** view is displayed.
4. Click **Add Enclosure**.
   The **Add New Enclosure** wizard opens.
5. Confirm the details of your current install, and click **Next** to validate the cabling.

   If the cabling is wrong, an error message is displayed. You can proceed to the next step once the error is corrected and validated.
6. If prompted, select the enclosure type and click **Next**.
7. Follow the instructions to insert disks into the new enclosure and turn on the enclosure. Click **Next** when finished.
8. If displayed, follow the instructions to disconnect the A side chain cable from an existing enclosure.
9. Click **Next**.
10. Connect the A side chain cables to the new enclosure by following the displayed instructions. Click **Next** to validate the cabling.

    If the enclosure cannot be detected, an error message is displayed. You can proceed to the next step once the cabling is validated.
11. If displayed, follow the instructions to disconnect the B side chain cables from the existing enclosure.
12. Click **Next**.
13. Connect the B side chain cables to the new enclosure by following the displayed instructions.
14. Click **Next** to validate the cabling.

    If the enclosure cannot be detected, an error message is displayed. You can proceed to the next step once the cabling is validated.
15. Click **Finish** to exit the wizard.

Remove an Enclosure

This step-by-step wizard guides you through removing an enclosure to the system without a controller outage.

Prerequisites

- This wizard is only available for the SCv2000 series controllers.
- The option will display only if Storage Center has the ability to remove enclosures and data has been removed from all disks in the selected enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.

3. In the **Hardware** tab navigation pane, expand **Enclosure**.
   The **Enclosure** view is displayed.
4. Select the enclosure you want to remove and click **Remove Enclosure**.
   The **Remove Enclosure** wizard opens.
5. Confirm the details of your current install, and click **Next**.
6. Locate the enclosure in the Storage Center and click **Next**.
7. Follow the directions to disconnect the A side chain cables connecting the enclosure to the Storage Center. Click **Next**.
8. Reconnect the A side chain cables by following the directions to exclude the enclosure. Click **Next**.
9. Follow the directions to disconnect the B side chain cables connecting the enclosure to the Storage Center. Click **Next**.
10. Reconnect the B side chain cables by following the directions to exclude the enclosure. Click **Next** to validate the cabling and delete the enclosure.

    If the cabling is invalid, an error message is displayed. You can proceed to the next step once the error is corrected and validated.
11. Click **Finish** to exit the wizard.

Replace an Enclosure

The Replace Enclosure wizard guides you through replacing an enclosure in the storage system.

Prerequisites

- Requires a controller outage
- Available only for the SCv2000 series controller
- Available only if data has been released from all disks in the selected enclosure and the situation allows the replacement of an enclosure

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, click **Enclosure**.
   The **Enclosure** view is displayed.
4. Select the enclosure you want to replace and click **Replace Enclosure**.
   The **Replace Enclosure** wizard opens.
5. Click **Next** to accept the warning of service interruption.
6. Follow the instruction for locating the enclosure in the rack.
7. Click **Next**.
8. Follow all instructions to remove disks from the enclosure.
9. Click **Next**.
10. Disconnect the enclosure from the Storage Center.
11. Click **Next**.
12. Add disks to your enclosure by following the instructions.
13. Click **Next**.
14. Follow the instructions to connect the A-side chain.
15. Click **Next**.
    The wizard checks that the enclosure is connected.
16. Follow the instructions to connect the B-side chain.
17. Click **Next**.
    The wizard validates the cabling.
18. Click **Finish** to exit the wizard.

Rename a Disk Enclosure

Change the display name of a disk enclosure to differentiate it from other disk enclosures.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosure**, then select an enclosure.
   The **Enclosure** view is displayed.
4. In the right pane, click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. In the **Name** field, type a new name for the enclosure.
6. Click **OK**.

Set an Asset Tag for a Disk Enclosure

An enclosure asset tag can be used to identify a specific component for company records. .

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosure**, then select an enclosure.
   The **Enclosure** view is displayed.
4. In the right pane, click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. In the **Asset Tag** field, type an asset tag for the enclosure.
6. Click **OK**.

Delete an Enclosure

Delete an enclosure if it will be physically removed from the Storage Center.

Prerequisites

- All data must be moved off the enclosure by releasing the disks and rebalancing RAID.
- The enclosure must be down.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosure**.
   The **Enclosure** view is displayed.
4. Select the enclosure you want to delete and click **Delete Enclosure**. The **Delete Enclosure** dialog box opens.
   NOTE: If there are no disks currently in that enclosure, the dialog will not be displayed. The enclosure will be removed without a request for confirmation.
5. Click **OK**.

Mute an Enclosure Alarm

Mute an enclosure alarm to prevent it from sounding.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosure** and select an enclosure.
   The **Enclosure** view is displayed.
4. Under **Enclosure**, select **Audible Alarms**.
5. In the right pane, right-click the audible alarm, then select **Request Mute**.

Unmute an Enclosure Alarm

Unmute an enclosure alarm to allow it to sound.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures** and select an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Audible Alarms**.
5. In the right pane, right-click the audible alarm, then select **Request Mute Off**.

Clear the Swap Status for an Enclosure Cooling Fan

Clear the swap status for an enclosure cooling fan to acknowledge that it has been replaced.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Cooling Fan Sensors**.
   The **Cooling Fan Sensors** view is displayed.
5. In the right pane, select the cooling fan, then click **Request Swap Clear**.

Clear the Swap Status for an Enclosure I/O Module

Clear the swap status for an enclosure I/O module to acknowledge that it has been replaced.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **I/O Modules**.
   The **I/O Modules** view is displayed.
5. In the right pane, select the I/O module, then click **Request Swap Clear**.

Clear the Swap Status for an Enclosure Power Supply

Clear the swap status for an enclosure power supply to acknowledge that it has been replaced.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Power Supplies**.
   The **Power Supplies** view is displayed.
5. In the right pane, select the power supply, then click **Request Swap Clear**.

Replace a Failed Power Supply

This step-by-step wizard guides you through replacing a failed power supply in an enclosure in the Storage Center.

Prerequisites

This wizard is only available for the SCv2000 series, and can be completed without a controller outage.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand the enclosure with the failed power supply.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Power Supplies**.
   The **Power Supplies** view is displayed.
5. In the right pane, select the failed power supply, then click **Replace Power Supply**.
   The **Replace Failed Power Supply** wizard opens.
6. Refer to the graphic in the wizard to locate the failed power supply. Click **Next**.
7. Follow the instructions to remove the failed power supply. Click **Next**.
8. Follow the instructions to insert the replacement power supply. Click **Next** to verify the replacement.

   If this verification fails, an error message is displayed. You can proceed to the next step once the error is corrected and validated.
9. Click **Finish** to exit the wizard.

Clear the Under Voltage Status for a Power Supply

Clear the under voltage status for an enclosure power supply to acknowledge that you are aware of it.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Power Supplies**.
   The **Power Supplies** view is displayed.
5. In the right pane, select the power supply, then click **Request DC Undervoltage Clear**.

Clear the Swap Status for a Temperature Sensor

The swap status for a temperature sensor is set when the component that contains the sensor is replaced.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Temperature Sensor**.
   The **Temperature Sensor** view is displayed.
5. In the right pane, select the temperature sensor, then click **Request Swap Clear**.

Clear the Minimum and Maximum Recorded Values for Temperature Sensor

Clear the minimum and maximum recorded values for a temperature sensor to reset them.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Temperature Sensor**.
   The **Temperature Sensors** view is displayed.
5. In the right pane, select the temperature sensor, then click **Request Min/Max Temps Clear**.

Replace a Failed Cooling Fan Sensor

This step-by-step wizard guides you through replacing a failed cooling fan sensor in the Storage Center without a controller outage.

Prerequisites

This wizard is only available for the SCv2000 series and SCv3000 series Storage Centers.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand either **Controllers** or **Enclosures**, then select and expand either a controller or an enclosure.
   Either the **Enclosure** or **Controller** view is displayed.
4. Under the selected enclosure or controller, click **Fan Sensors**.
   The **Fan Sensors** view is displayed.
5. In the right pane. select the failed sensor and click **Replace Failed Cooling Fan Sensor**.
   The **Replace Failed Cooling Fan Sensor** wizard opens.
6. Refer to the graphic in the wizard to locate the failed cooling fan sensor. Click **Next**.
7. Follow the instructions to remove the power supply from the enclosure. Click **Next**.
8. Follow the instructions to insert the replacement power supply. Click **Next** to verify the replacement.
   If this verification fails, an error message is displayed. You can proceed to the next step once the error is corrected and validated.
9. Click **Finish** to exit the wizard.

Enable or Disable the Disk Indicator Light

The drive bay indicator light identifies a drive bay so it can be easily located in an enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Disks**.
   The **Disks** view is displayed.
5. In the right pane, click the **Disks** subtab and select a disk.
6. Enable or disable the disk indicator light for the selected disk.
   - If the indicator light is off, click **Indicator On** to enable the indicator light.
   - If the indicator light is on, click **Indicator Off** to disable the indicator light.

Clear the Swap Status for a Disk

Clear the swap status for a disk to acknowledge that it has been replaced.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Enclosures**, then select and expand an enclosure.
   The **Enclosure** view is displayed.
4. Under the selected enclosure, click **Disks**.
   The **Disks** view is displayed.
5. In the right pane, click the **Disks** subtab, select a disk, then click **Request Swap Clear**.

Managing Storage Center Controllers

Storage Manager can help you manage and maintain the controllers in your Storage Center by walking you through the process for adding a controller and replacing parts.

Add a Controller

This step-by-step wizard guides you through adding a new controller to the storage system.

Prerequisites

- This wizard is only available for SC4020, SC8000, and SC9000 controllers.
- The new controller must have a Hardware Serial Number (HSN) and Eth 1 IP address assigned to it before starting this procedure. To see the new controller information, run the following command from the serial console:

```
controller show
```

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, click **Controllers**.
   The **Controllers** view is displayed.
4. Click **Add Controller**.

The **Add New Controller** wizard opens.

5. Confirm the details of your current install, and click **Next**.
6. Insert the controller into the existing enclosure. Click **Next** to validate the install.
7. Click **Finish** to exit the wizard.

Replace a Failed Controller

This step-by-step wizard guides you through replacing a failed controller in the Storage Center without an additional controller outage.

Prerequisites

This wizard is only available for the SCv2000 series controllers

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, click **Controllers**.
   The **Controllers** view is displayed.
4. In the right pane, select the controller you want to replace and click **Replace Controller**.
   The **Replace Controller** wizard opens.
5. Refer to the graphic in the wizard to located the failed controller. Click **Next**.
6. Follow the instructions to remove the battery from the failed controller. Click **Next**.
7. Follow the instructions to remove the failed controller from the Storage Center. Click **Next**.
8. Insert the battery from the failed controller into the new controller. Click **Next**.
9. Follow the instructions to insert the new controller into the Storage Center. Click **Next** to validate the installation.
   If the installation fails, an error message is displayed. You can proceed to the next step once the error is corrected and validated.
10. Click **Finish** to exit the wizard.

Enable or Disable a Controller Indicator Light

Enable a controller indicator light to assist in locating the controller in the rack.

Prerequisites

The controller indicator light is visible only on SC8000 or SC9000 storage controllers.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Controllers**, then select a controller.
   The **Controller** view is displayed.
4. Enable or disable the disk indicator light for the selected disk.
   - If the indicator light is off, click **Indicator On** to enable the indicator light.
   - If the indicator light is on, click **Indicator Off** to disable the indicator light.

Replace a Failed Cooling Fan Sensor

This step-by-step wizard guides you through replacing a failed cooling fan sensor in the Storage Center without a controller outage.

Prerequisites

This wizard is only available for the SCv2000 series and SCv3000 series Storage Centers.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand either **Controllers** or **Enclosures**, then select and expand either a controller or an enclosure.
   Either the **Enclosure** or **Controller** view is displayed.
4. Under the selected enclosure or controller, click **Fan Sensors**.
   The **Fan Sensors** view is displayed.
5. In the right pane. select the failed sensor and click **Replace Failed Cooling Fan Sensor**.
   The **Replace Failed Cooling Fan Sensor** wizard opens.
6. Refer to the graphic in the wizard to locate the failed cooling fan sensor. Click **Next**.
7. Follow the instructions to remove the power supply from the enclosure. Click **Next**.
8. Follow the instructions to insert the replacement power supply. Click **Next** to verify the replacement.
   If this verification fails, an error message is displayed. You can proceed to the next step once the error is corrected and validated.
9. Click **Finish** to exit the wizard.

Managing I/O Card Changes

The Configure I/O Card Changes wizard simplifies the task of moving, replacing, upgrading, or repurposing I/O cards in Storage Center controllers. The wizard is used to configure I/O card hardware changes on a per-port basis after physical I/O card changes have been made. The wizard is typically used when upgrading I/O cards or controllers.

About this task

For each local port, you can specify:

- Whether to link an I/O card to an existing configuration
- Whether the I/O card is new hardware
- Whether to delete the configuration for a removed I/O card

The wizard guides you through the following actions:

- Associating I/O cards with existing port configurations
- Indicating which I/O cards are new hardware
- Deleting configurations for I/O cards that have been removed

Before using the wizard, you should be aware of the following:

- Changes should be performed by a certified installer or with the assistance of technical support.
- At least one back-end port must remain in its original location.
- A controller restart is required to implement changes.
- Do not rebalance any ports until controllershave been replaced and all hardware configuration changes are complete.

Plan a Hardware Change

Upon boot, the Storage Center searches back-end targets for the configuration. Because a controller cannot boot without configuration information, back-end access must be maintained during the controller replacement procedure. This can be done in two ways:

About this task

- Keep at least one common back-end slot/port defined and connected in the same manner on the new hardware configuration as it was on the old hardware configuration.
- Connect the back-end to a port that is *undefined* on the new hardware configuration. Storage Center is able to detect iSCSI targets and acquire the boot configuration from the drives even though the slot/port is marked as *undefined*.

When the appropriate back-end slot/port is identified, record this information on the Port Usage Work Sheet and continue the upgrade process.

Change the Hardware

Changing hardware follows these general tasks. Refer to upgrade documentation for the specific change for more detailed instructions.

Steps

1. Power down and unplug the controller. This reduces downtime by facilitating re-cabling. In a dual-controller Storage Center, the second controller takes on all functions of the Storage Center, preventing a system outage.
2. Record/tag the cabling for the affected card.
3. Disconnect the cables on the I/O card.
4. Replace, move, or remove the I/O cards and reconnect as recorded on the Port Usage Work Sheet.
5. Plug in and power on the controller.

Manage I/O Card Changes

After a change to an I/O card in a Storage Center controller, the Configure I/O Card Changes wizard applies old port configurations to the new or modified ports. Changes can include replacing an I/O card, moving the I/O card to a different PCI slot, and removing an I/O card. Use the Configure I/O Card Changes wizard to apply existing I/O card port configuration settings to new or modified I/O card ports.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
   The **Hardware** view is displayed.
3. In the **Hardware** navigation pane, select a controller, then click **Configure I/O Card Change**.

   NOTE: If the controller must be restarted to move configurations to the other controller, the **Configure I/O Card Changes** wizard shows the option to restart the controller.

   The **Configure I/O Card Changes** wizard opens.
4. (Optional) Click **Restart Controller**.
5. Click **Next**.
6. From the **Fibre Channel**, **iSCSI**, or **SAS** table, identify ports that have been modified.
7. From the **Card Location** drop-down menu, select a port configuration.
8. Click **Finish**.

Add a UPS to a Storage Center

An uninteruptable power supply (UPS) provides power redundancy to a Storage Center. When a UPS is added to a Storage Center, the status of the UPS is displayed in Storage Manager.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the right pane, select **Actions** > **UPS** > **Create UPS**.
   The **Create UPS** dialog box opens.
3. In the **IPv4 Address** field, type the IP address of the UPS.
4. In the **Community String** field, type the community string configured on the UPS. The default is Public.
5. From the **UPS Type** drop-down menu, select the brand of the UPS.
6. Click **OK**.

Updating Storage Center

Update a Storage Center to the latest version by connecting directly to the Storage Center or by connecting through a Data Collector. If the Storage Center to update does not have SupportAssist enabled you can use the Storage Center Update Utility to update software. For more information on the Storage Center Update Utility, see *Using the Storage Center Update Utility*.

The Storage Manager Client displays the current update status of all Storage Centers managed by the Data Collector in the Summary tab.

NOTE: Updating from Storage Center version 6.6 to a later version is a separate guided process. See the *Storage Center OS Version 7 Software Update Guide* for details.

Update Storage Center Software

Follow this procedure if SupportAssist is enabled on the Storage Center.

Prerequisites

SupportAssist must be enabled on the Storage Center.

About this task

The options displayed in the Storage Center software update dialog boxes depend on the type of update performed on the Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the right pane, select **Actions** > **System** > **Check for Update**.
   The **Update Storage Center** dialog box opens and checks for an update.
3. (Optional) Click **Release Notes** for information about the update.
4. Select an Installation Type:
   - To apply only non-service affecting updates, select **Apply non-service affecting updates**.
   - To apply non-service affecting updates to required components, select **Apply required components — Non-Service Affecting**.
   - To apply all updates including those affecting service, select **Apply all updates — Service Affecting**.

   NOTE: Service-affecting installation types require a controller outage. Service will be interrupted.
5. Click **OK**.
6. (Optional) If you select **Apply all updates** and **Download and Install now**, the **Download and Install Update Confirmation** dialog opens. Type the Storage Center Administrator Username and Password to continue.

The **Update Storage Center** dialog opens. This dialog displays details of the installation process and updates those details every 30 seconds. This is also displayed as a blue message bar in the Summary tab, and in the update status column of the Storage Center details. In case of an update failure, click **Retry** to restart the interrupted process.

7. Click **OK**.

   If the update is service affecting, the connection to the Storage Center will be lost.

Using the Storage Center Update Utility

The Storage Center Update Utility acts as an update server for Storage Centers without an internet connection or with SupportAssist disabled. To use the Storage Center Update Utility to update Storage Center software, install the utility, load an update package, and start the service. Then, if the Storage Center is configured to use the Storage Center Update Utility, manually check for an update and update the Storage Center software. If a Storage Center is configured to use the Storage Center Update Utility, you must check for updates manually.

For more information on installing and setting up the Storage Center Update Utility, see the *Dell Storage Center Update Utility Administrator's Guide*.

Configure Storage Center to Use the Storage Center Update Utility

If the Storage Center is not connected to the internet, configure it to use the Storage Center Update Utility when checking for updates. Before Storage Center can receive an update from the Storage Center Update Utility, a Storage Center distro must be loaded and the Storage Center Update Utility service must be running.

Prerequisites

The Storage Center Update Utility must be setup and running.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **SupportAssist** tab.
4. Disable SupportAssist. Click **Turn Off SupportAssist**.
5. Under **Configure Update Utility**, select the **Enabled** checkbox.
6. In the **Update Utility Host or IP Address** field, type the IP address of the Storage Center Update Utility.
7. In the **Update Utility Port** field, type the port of the Storage Center Update Utility.
8. Click **OK**.

Shutting Down and Restarting a Storage Center

Shutting down or restarting a Storage Center affects all controllers. Controllers can also be shut down or restarted individually.

NOTE: For user interface reference information, click **Help**.

Shut Down All Controllers in Storage Center

Shutting down a Storage Center creates a system outage, during which time no I/O is processed. Use this process only as directed, for example to replace hardware, to move the Storage Center to another location, or to shut down for data center power maintenance.

Prerequisites

- An outage must be scheduled so that halting I/O does not impact your network.
- I/O to the controllers must be halted.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the right pane, click **Actions→ System→ Shutdown/Restart**.
   The **Shut Down/Restart** dialog box opens.
3. From the first drop-down menu, select **Shut Down**.
4. Click **OK**.
5. After the controllers have shut down, shut down the disk enclosures by physically turning off the power supplies.

Next steps

After the outage is complete, see the Owner's Manual for your controller for instructions on how to start the controllers in the proper order.

Related tasks

Set Storage Center Cache Options on page 221

Restart All Controllers in a Storage Center

If the Storage Center has dual-controllers, the controllers can be restarted in sequence or simultaneously.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the right pane, click **Actions→ System→ Shutdown/Restart**.
   The **Shut Down/Restart** dialog box opens.
3. From the first drop-down menu, select **Restart**.
4. (Dual-controllers only) From the **Restart options** drop-down menu, choose how you want the controllers to restart.
   - To restart the controllers one after the other, avoiding an outage, select **Restart in Sequence**.
   - To restart the controllers at the same time, causing an outage, select **Restart Simultaneously**.
5. Click **OK**.

Shut Down a Controller

If the Storage Center has dual-controllers, the remaining controller continues to process I/O. If the Storage Center has only one controller, shutting it down creates an outage.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Controllers** and select the controller.
   The **Controller** view is displayed.
4. In the right pane, click **Shut Down/Restart Controller**.
   The **Shut Down/Restart Controller** dialog box opens.
5. From the drop-down menu, select **Shutdown**.
6. Click **OK**.

Restart a Controller

If the Storage Center has dual-controllers, the remaining controller continues to process I/O. If the Storage Center has only one controller, restarting it down creates an outage.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.

2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Controllers** and select the controller.
   The **Controller** view is displayed.
4. In the right pane, click **Shut Down/Restart Controller**.
   The **Shut Down/Restart Controller** dialog box opens.
5. From the drop-down menu, select **Restart**.
6. Click **OK**.

Reset a Controller to Factory Default

Reset a controller to apply the factory default settings, erase all data stored on the controller, and erase all data on the drives.

Prerequisites

The Storage Center must be an SCv2000 or SCv3000 series storage system.

About this task

CAUTION: Resetting the controller to factory defaults erases all information on the controller and all data on the drives.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the right pane, click **Actions→ System→ Reset to Factory Defaults**.
   The **Reset Storage Center to Factory Defaults** dialog box opens.
3. In the **Factory Reset Token** field, type the text above the **Factory Reset Token** field exactly as it appears in the dialog box.
4. In the **Storage Center Administrator Username** field type the username of a Storage Center user with administrator-level privileges.
5. In the **Storage Center Administrator Password** field type the password of a Storage Center user with administrator-level privileges.
6. To restart the controller after the reset, select the **Power on the Storage Center after resetting to factory defaults** checkbox.
7. Click **OK**.
   The Storage Center resets to the factory default settings.

Managing Field Replaceable Units (FRU)

The FRU Manager maintains the status of FRUs and issues action tickets when a unit needs to be replaced. Storage Manager displays FRU tickets that contain specific information on each FRU, and provides the ability to close tickets.

NOTE: The FRU Manager is not supported on SC8000 or CT-SC040 series storage systems.

Managing FRU Tickets

Storage Manager can display information on FRU tickets, and can also close FRU tickets.

NOTE: If FRUs and FRU Manager are not enabled, Storage Manager does not display options or tickets.

View a FRU Ticket

To view the status of a replacement Field Replacement Unit (FRU) view the FRU ticket from the Alerts tab.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.

2. Click the **Alerts** tab.
3. Select a FRU ticket.
4. Click **View FRU Ticket**.
   The **FRU Ticket Information** dialog opens.
5. Click **OK**.

Close a FRU Ticket

Close a FRU ticket if the FRU ticket is not needed.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Alerts** tab.
3. Select a FRU ticket.
4. Click **Close FRU Ticket**.
   The **Close FRU Ticket** dialog opens.
5. Click **OK**.

10

Viewing Storage Center Information

Storage Manager provides access to summary information about managed Storage Centers, including I/O performance and hardware status. Use this information to monitor the health and status of your Storage Centers.

Topics:

- Viewing Summary Information
- Viewing Detailed Storage Usage Information
- Viewing Historical IO Performance
- Viewing Current IO Performance
- Configuring Chart Options
- Configure the Storage Center Data Gathering Schedule
- Exporting Usage Data
- Monitoring Storage Center Hardware

Viewing Summary Information

Storage Center summary plugins provide summary information for individual Storage Centers. The summary plugins can also be used to compare multiple Storage Centers.

Storage Center Summary Plugins

The following plugins can be configured to display on the **Summary** tab and **Comparison** tab.

Summary Plugin	Description
System Status	Displays a summary of disk space and alerts for a Storage Center.
Storage Summary	Displays a a bar chart that shows the disk space on a Storage Center and a graph that shows available disk space, used disk space, and the low disk space alert threshold for a Storage Center.
Frond End IO Summary	Displays a graph that shows front end IO from a Storage Center to the servers for the past four weeks.
Current Alerts	Displays a table that shows all of the storage objects that currently have an alert status for a Storage Center.
Replication Validation	Displays a table that shows replications and the corresponding replication statuses for a Storage Center.
Top 10 Fastest Growing Volumes	Displays a table that shows the fastest growing volumes on a Storage Center.
Current Threshold Alerts	Displays a table that shows all of the current threshold alerts for a Storage Center.

Viewing Summary Information for a Storage Center

When a Storage Center is selected from the **Storage** pane, information about the Storage Center is displayed on the panes of the **Summary** tab.

NOTE: Disk Space details and graphs are displayed in Storage Center version 7.4.10 and later.

System RAID Overhead Ratio and Estimated Usable Space are displayed in Storage Center version 7.5.1 and later.

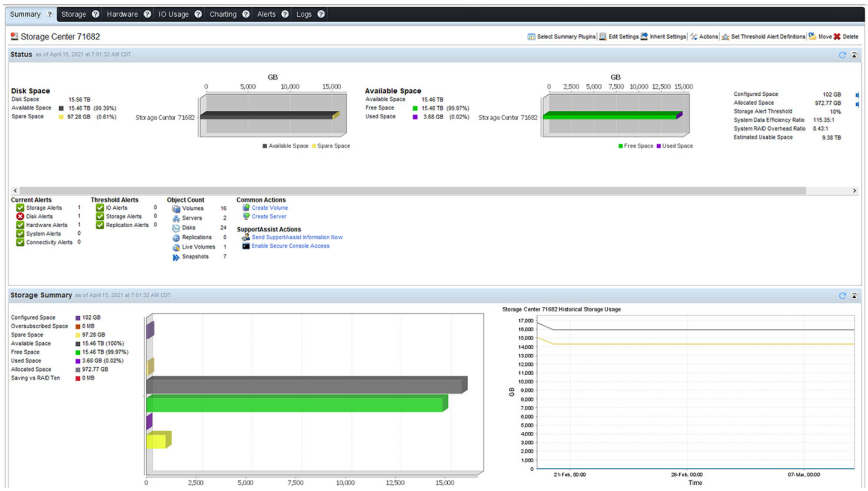


Figure 25. Summary Tab

View Summary Plugins for a Storage Center

Use the **Summary** tab to view the summary plugins that are currently enabled.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Summary** tab.

Related concepts

Using the Status Plugin on page 302
Using the Storage Summary Plugin on page 304
Using the Front End IO Summary Plugin on page 306
Using the Current Alerts Plugin on page 307
Using the Replication Validation Plugin on page 307
Using the Top 10 Fastest Growing Volumes Plugin on page 308
Using the Current Threshold Alerts Plugin on page 308

Configure Which Plugins Appear on the Summary Tab

Each summary plugin can be individually enabled or disabled.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. On the **Summary** tab, click **Select Summary Plugins**. The **Edit Summary Settings** dialog box appears.
3. Select the check boxes of the plugins to display and clear the check boxes of the view plugins to hide.
4. Click **OK** to save changes to the plugins of the **Summary** tab.

Reorder Plugins on the Summary Tab

The summary plugins can be reordered as needed.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. On the **Summary** tab, click **Select Summary Plugins**. The **Edit Summary Settings** dialog box appears.
3. Reorder the summary plugins as needed.

- To move a plugin up one level, press **Move Up** once.
- To move a plugin down one level, press **Move Down** once.
- To move a plugin to the top, press **Move to Top** once.
- To move a plugin to the bottom, press **Move to Bottom** once.

4. Click **OK** to save changes to the plugins of the **Summary** tab.

Viewing Summary Information for Multiple Storage Centers

Storage Manager provides two ways to view summary information for multiple Storage Centers. When the **Storage Centers** node or a Storage Center folder is selected, the **Summary** tab provides general summary information, and the **Comparison** tab allows you to compare the Storage Centers using a specific summary plugin.

View General Summary Information for Multiple Storage Centers

General summary information includes aggregate storage usage information and summary information for each Storage Center.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center folder or the **Storage Centers** node.
3. Click the **Summary** tab.

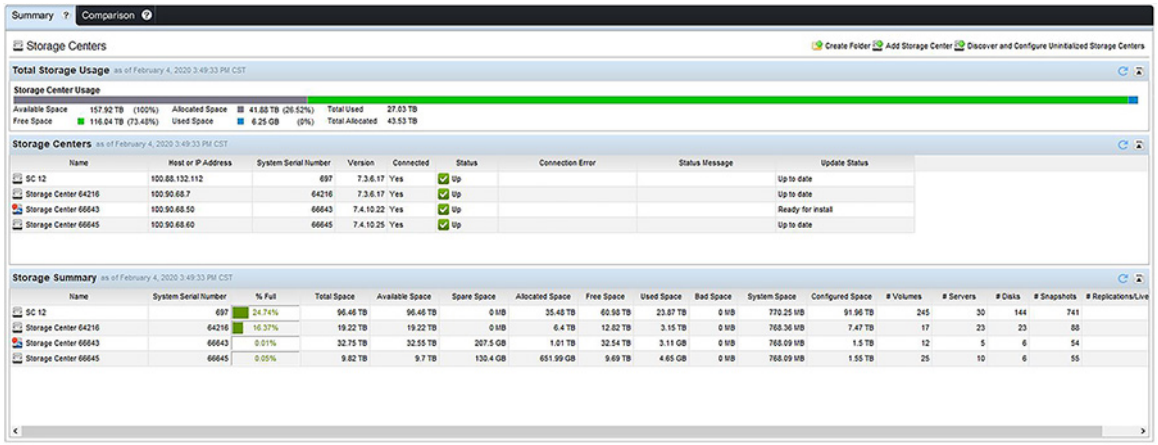


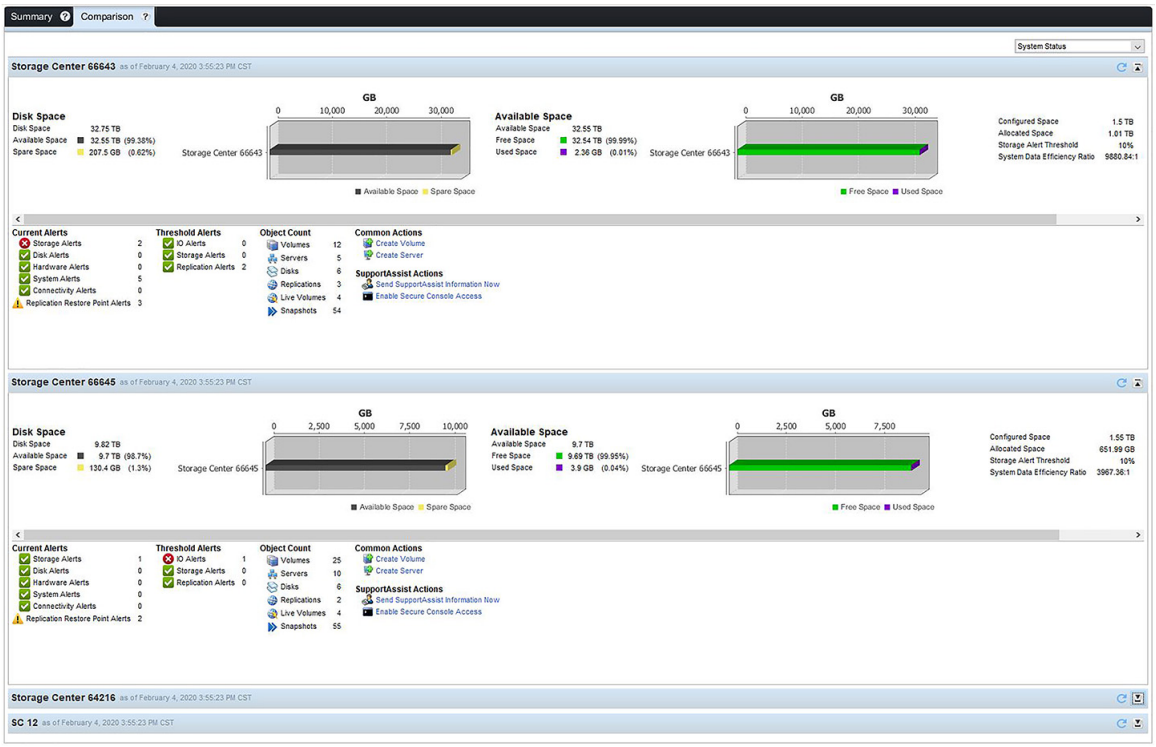
Figure 26. Storage Centers Summary Tab

Use a Summary Plugin to Compare Storage Centers

Storage Center summary information can be compared using the summary plugins.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center folder or the **Storage Centers** node.
3. Click the **Comparison** tab.



4. From the drop-down menu in the top right corner, select the summary plugin that you want to use to compare the Storage Centers.

Related concepts

Using the Status Plugin on page 302
Using the Storage Summary Plugin on page 304
Using the Front End IO Summary Plugin on page 306
Using the Current Alerts Plugin on page 307
Using the Replication Validation Plugin on page 307
Using the Top 10 Fastest Growing Volumes Plugin on page 308
Using the Current Threshold Alerts Plugin on page 308

Using the Status Plugin

The **Status** plugin displays Storage Center disk space information and the status of alerts.

- Use the top part of the **Status** plugin to view disk space usage on the Storage Center, the current alert threshold, and data savings information.
- Use the bottom part of the **Status** plugin to view a summary of alerts on a Storage Center.

NOTE: Disk Space details and graphs are displayed in Storage Center version 7.4.10 and later.

System RAID Overhead Ratio and Estimated Usable Space are displayed in Storage Center version 7.5.1 and later.

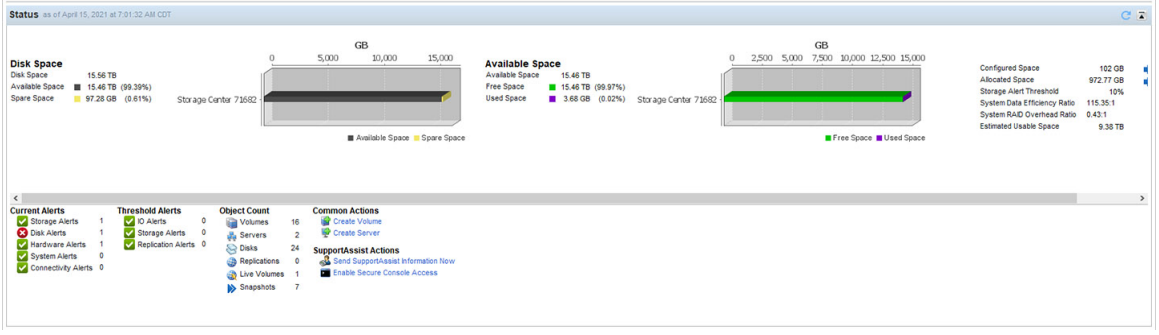


Figure 27. Status Plugin

Status Information

The top portion of the **Status** plugin displays information about disk space usage.

NOTE: The information displayed varies with the Storage Center version.

Disk Space

- **Disk**—Total amount of raw disk space on all drives in the Storage Center.
- **Spare**—Amount of space distributed across all drives that is reserved for balancing drive usage and recovering from a drive failure. For Storage Center version 7.3 and earlier, this value will appear as zero, because a hard drive is dedicated to spare space usage.

Available Space

- **Available**—Amount of space allocated for volumes on the Storage Center. Calculated as:
  - Storage Center version 7.4.10 and later—Used space + Free space
  - Storage Center versions 7.3-7.4.2—Allocated + Free space
- **Free**—Amount of disk space available for use by a Storage Center. Calculated as:
  - Storage Center version 7.4.10 and later—Storage Type Free space + Disk Free space
  - Storage Center versions 7.3-7.4.2—Free space = Disk Free space
- **Used**—Amount of configured space used by the Storage Center plus RAID overhead. The calculation includes used space on different objects, depending on the Storage Center software version and the use of hot spares versus distributed spares:
  - Version 7.4.10 and later—sum of all used space for each Storage Type.
  - Earlier versions—combination of the sum of used space on hot spares, distributed spares, and Storage Type, depending on the system configuration.

Configured Space—Total amount of space available on all of the configured volumes in the Storage Center. Calculated as:

- Storage Center version 7.4.10 and later—Configured space is equal Total space
- Storage Center version 7.2 and earlier, Configured space is equal to Available space

Allocated Space—Amount of disk space allocated on the disks for volumes plus RAID overhead. (Not used in Storage Center versions 7.1 or 7.2).

Storage Alert Threshold—Remaining disk space percentage that causes a storage alert to occur.

System Data Efficiency Ratio—Ratio that indicates the efficiency of compression, deduplication, RAID, and Thin Provisioning.

System RAID Overhead Ratio—The RAID overhead ratio for the entire system calculated using the RAID overhead from the existing storage types.

Estimated Usable Space—Calculation of the free space that is usable based on the current usage of the system.

Alert Information

The top portion of the **Status** plugin displays information about the alerts for a Storage Center.

The alert icons indicate the highest active alert level.

Alert Icon	Description
	Indicates no unacknowledged alerts for a category
	Indicates that the highest unacknowledged alert level is Warning
	Indicates that the highest unacknowledged alert level is Error

The following types of alerts are summarized on the **Status** plugin.

Alert Type	Description
Current Alerts	Displays the total number of Storage Center alerts and the number of alerts for the each of following categories: • Storage Alerts • Disk Alerts • Hardware Alerts • System Alerts

Alert Type	Description
	• Connectivity Alerts The Current Alerts status icon indicates the highest unacknowledged alert level for the categories under Current Alerts.
Threshold Alerts	Displays the total number of Storage Manager threshold alerts and the number of alerts for each of the following categories: • IO Alerts • Storage Alerts • Replication Alerts The Threshold Alerts status icon indicates the highest active alert level for the categories under Threshold Alerts.
Replication Restore Point Alerts	Displays the total number of restore point alerts.

Viewing More Detailed Status Information

The **Status** plugin provides shortcuts to areas that display more detailed information.

To View ...	Click ...
Disk space usage details for the Storage Center	**More Details** located to the right of the disk space information.
More information about the Data Savings Ratios	**More Information** located to the right of the disk space information.
Details about current alerts for the Storage Center	**Current Alerts**, which opens the **Storage Alerts** tab on the **Monitoring** view.
Restore point details for the Storage Center	**Replication Restore Point Alerts**, which opens the **Restore Points** tab on the **Replications & Live Volumes** view
Threshold alert details for the Storage Center	**Threshold Alerts**, which opens the **Definitions** tab on the **Threshold Alerts** view

Using the Storage Summary Plugin

The **Storage Summary** plugin displays current storage usage in numerical and bar chart formats and historical storage usage in line chart format.

Use the bar chart to compare the amount of used disk space to the amount of available disk space on a Storage Center. Use the line chart to compare the historical used disk space to the historical available disk space and alert threshold.

Storage Summary Bar Chart

Use the bar chart to view available disk space, allocated disk space, used disk space, free disk space, and Savings vs RAID 10. In addition, the amount of configured disk space and oversubscribed disk space is displayed below the bar chart.

The following information is displayed in the bar chart on the **Storage Summary** plugin:

Field/Option	Description
Configured Space	Total amount of space available on all of the configured volumes in the Storage Center. Calculated as: • Storage Center version 7.4.10 and later—Configured space is equal Total space • Storage Center version 7.2 and earlier, Configured space is equal to Available space
Oversubscribed	Configured Space minus the Available Space.
Spare Space	Amount of space distributed across all drives that is reserved for balancing drive usage and recovering from a drive failure. (Displayed in Storage Center version 7.4.2 and later.)

Field/Option	Description
Available Space	Amount of space allocated for volumes and the free space that can be used by the Storage Center. Calculated as: ● Storage Center version 7.4.10 and later —Used space + Free space ● Storage Center versions 7.3-7.4.2—Allocated + Free space
Free Space	Amount of disk space available for use by a Storage Center. Calculated as: ● Storage Center version 7.4.10 and later—Storage Type Free space + Disk Free space ● Storage Center versions 7.3-7.4.2—Free space is equal to Disk Free space
Used Space	Amount of configured space used by the Storage Center plus RAID overhead.
Allocated Space	Amount of disk space allocated on the disks for volumes plus RAID overhead. (Not used in Storage Center versions 7.1 or 7.2).
Savings vs RAID Ten	Amount of disk space saved by effective use of RAID 5/6 and/or Data Reduction compared to possible disk space savings from RAID 10.

Historical Storage Usage

The following information is displayed about past disk space usage on the **Historical Storage Usage** plugin:

Field/Option	Description
Available Space	Total amount of raw disk space available on all of the disks of a Storage Center.
Used Space	Amount of disk space used by a Storage Center.
Alert Threshold Space	Low disk space threshold for a Storage Center.

Manipulating the Storage Summary Chart or Graph

You can change the zoom level of the chart or graph, save it as an image, or print it.

Zoom in on an Area of the Chart or Graph

Zoom in if you want to view more details.

Steps

1. Click and hold the right or left mouse button.
2. Drag the mouse to the right to select.
3. Release the mouse button to zoom into the selected area of the bar chart.

Return to the Normal View of the Chart or Graph

If you have changed the zoom level of the chart or graph, you can return to the normal view.

Steps

1. Click and hold the right or left mouse button on the chart or graph.
2. Drag the mouse to the left to return to the normal zoom level.

Save a Chart or Graph as a PNG Image

Save the chart or graph as an image if you want to use it elsewhere, such as in a document or an email.

Steps

1. Right-click the chart or graph and select **Save As**. The **Save** dialog box appears.

2. Select a location to save the image and enter a name for the image in the **File name** field.
3. Click **Save** to save the image.

Print the Bar Chart

Print the chart if you want a paper copy.

Steps

1. Right-click the bar chart and select **Print**. The **Page Setup** dialog box appears.
2. Select the paper size to print to from the **Size** drop-down menu.
3. Select the **Landscape** radio button to allow the entire bar chart to print.
4. Click **OK**. The Print dialog box appears.
5. Select the printer to use from the **Name** drop-down menu.
6. Click **OK**. The bar chart is printed to the selected printer.

Using the Front End IO Summary Plugin

The **Front End IO Summary** plugin displays two graphs that show historical front end performance data.

Use the Storage Center FE MB Report to view the read, write, and total front end activity measured in MB/sec. Use the FE IO Report to view the read, write, and total front end activity measured in IO/sec.

Zoom in on an Area of the Graph

Zoom in if you want to view more details.

Steps

1. Use the mouse to select an area of the graph in which to zoom.
   a. Click and hold the right or left mouse button on the graph.
   b. Drag the mouse to the right to select an area of the graph.
2. Release the mouse button to zoom into the selected area of the graph.

Return to the Normal View of the Graph

If you have changed the zoom level of the graph, you can return to the normal view.

Steps

1. Click and hold the right or left mouse button on the graph.
2. Drag the mouse to the left to return to the normal zoom level of the graph.

Save the Graph as a PNG Image

Save the graph as an image if you want to use it elsewhere, such as in a document or an email.

Steps

1. Right-click the graph and select **Save As**. The **Save** dialog box appears.
2. Select a location to save the image and enter a name for the image in the **File name** field.
3. Click **Save** to save the graph.

Print the Graph

Print the graph if you want a paper copy.

Steps

1. Right-click the graph and select **Print**. The **Page Setup** dialog box appears.
2. Select the paper size to print to from the **Size** drop-down menu.
3. Select the **Landscape** radio button to allow the entire graph to print.
4. Click **OK**. The Print dialog box appears.
5. Select the printer to use from the **Name** drop-down menu.
6. Click **OK**. The graph is printed to the selected printer.

Using the Current Alerts Plugin

The **Current Alerts** plugin displays a table that lists alerts for a Storage Center and associated storage objects.

Use this plugin to monitor and acknowledge Storage Center alerts.

Related concepts

Viewing Storage System Alerts on page 610

Acknowledge an Alert

Alerts can be acknowledged to indicate to the Storage Center that you have read the alert message and are aware of the problem. Unacknowledged alerts displays a status of **No** in the **Acknowledge** field.

Steps

1. Select the unacknowledged alert(s) to acknowledge.
2. Right-click the selected alert(s) and select **Acknowledge**. The **Acknowledge Alert** dialog box appears.

   NOTE: The **Acknowledge** option does not appear if one of the selected alerts is already acknowledged.

3. Click **OK** to acknowledge the selected alert(s).

   The **Acknowledged** status of the selected alert(s) changes to **Yes**.

Update the List of Alerts

Update the list of alerts to view the most recent information.

About this task

Click **Refresh** to update the list of alerts.

Using the Replication Validation Plugin

The **Replication Validation** plugin displays a table that lists replications and corresponding statuses. Use this plugin to monitor the status of replications from the current Storage Center to a destination Storage Center.

Related concepts

Saving and Validating Restore Points on page 542
Test Activating Disaster Recovery on page 544
Activating Disaster Recovery on page 546

Using the Top 10 Fastest Growing Volumes Plugin

The **Top 10 Fastest Growing Volumes** plugin displays a table that lists the volumes on a Storage Center that are growing at the fastest rate. Use this plugin to monitor the growth of the ten fastest growing volumes a Storage Center.

Figure 28. Top 10 Fastest Growing Volumes Plugin

Related concepts

Modifying Live Volumes on page 527

Related tasks

Replicating Volumes on page 505

Using the Current Threshold Alerts Plugin

The **Current Threshold Alerts** plugin displays a table that lists active threshold alerts for a Storage Center and associated storage objects. Use this plugin to monitor current threshold alerts for a Storage Center.

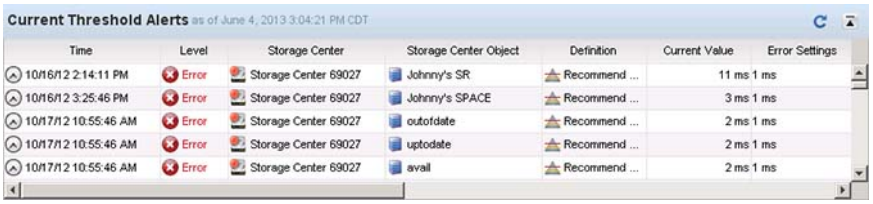


Figure 29. Current Threshold Alerts Plugin

Related concepts

Viewing and Deleting Threshold Alerts on page 575

Display the Threshold Definition for an Alert

If you want to view the threshold definition that generated an alert in detail, you can go to the definition directly from the alert.

Steps

1. Select the alert for which you want to display the threshold definition.
2. Right-click the alert and select **Go to Definition**, or double-click the alert.
   The threshold definition of the selected alert is displayed on the **Definitions** tab of the **Threshold Alerts** view.

Related concepts

Configuring Threshold Definitions on page 569

Update the List of Threshold Alerts

Refresh the list of threshold alerts to see an updated list of alerts.

About this task

Click **Refresh** to update the list of alerts.

Viewing Detailed Storage Usage Information

Detailed storage usage information is available for each Storage Type that is configured for a Storage Center.

View Storage Usage by Tier and RAID Type

Storage usage by tier and RAID type is displayed for each Storage Type.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Storage Type**, then select the individual storage type you want to examine.
4. Click the **Summary** subtab to view storage usage by tier and RAID type.

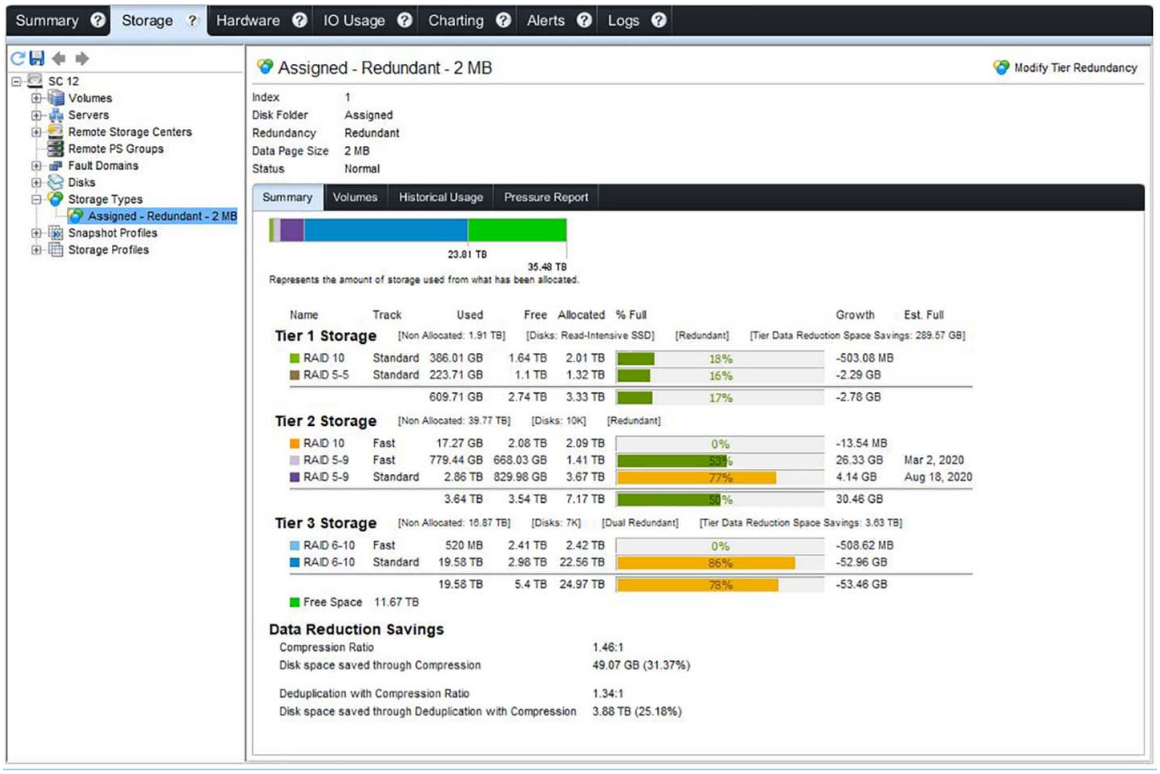


Figure 30. Storage Tab Storage Type Node

View Storage Usage by Volumes

Storage usage by volume is displayed for each Storage Type.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.

2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Storage Type**, then select the individual storage type you want to examine.
4. Click the **Volumes** subtab to view storage usage by volume.

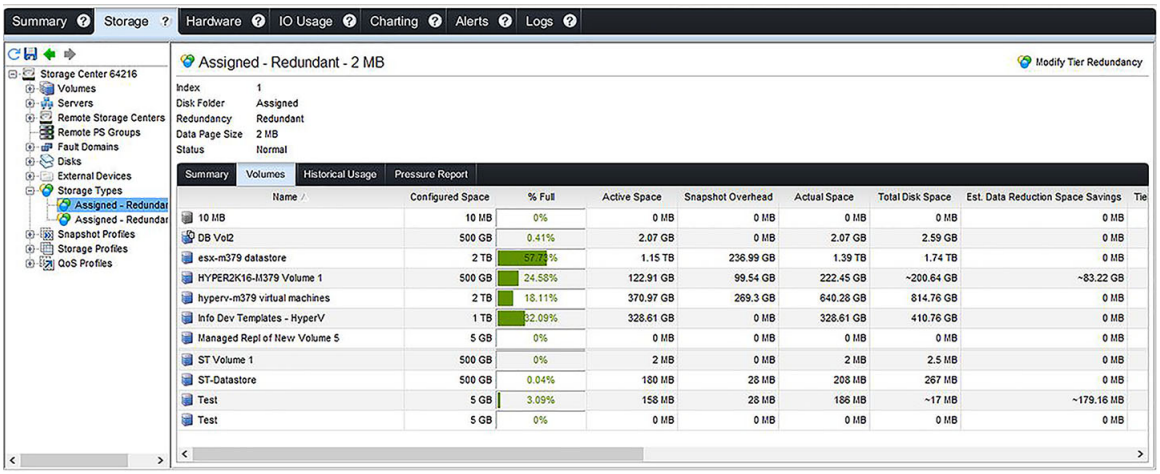


Figure 31. Storage Type Volumes Subtab

View Historical Storage Usage

Allocated space and used space over time is displayed for each Storage Type.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Storage Type**, then select the individual storage type you want to examine.
4. Click the **Historical Usage** subtab to view allocated space and used space over time.

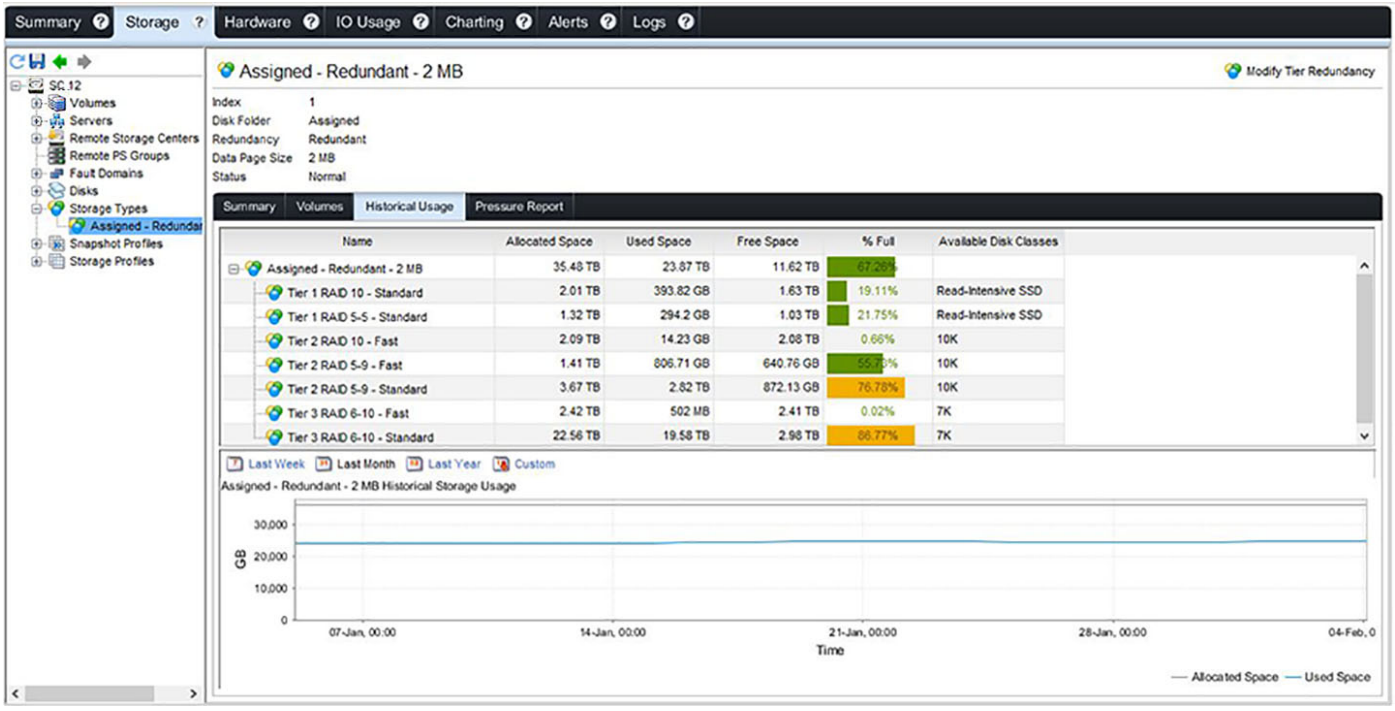


Figure 32. Storage Type historical Usage Tab

5. (Optional) Change the time span of the graph by clicking **Last Week**, **Last Month**, **Last Year**, or **Custom**.

View a Data Progression Pressure Report

For each storage type, the data progression pressure report displays how space is allocated, consumed, and scheduled to move across different RAID types and storage tiers. Use the data progression pressure report to make decisions about the types of disks to add to a Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, expand **Storage Type**, then select the individual storage type that you want to examine.
4. Click the **Pressure Report** subtab to view the data progression pressure report. By default, the most recent data gathered from the Storage Center is displayed.
5. To view a previously generated data progression report, select a report from the drop-down menu. Reports are identified by the date and time at which they were generated.

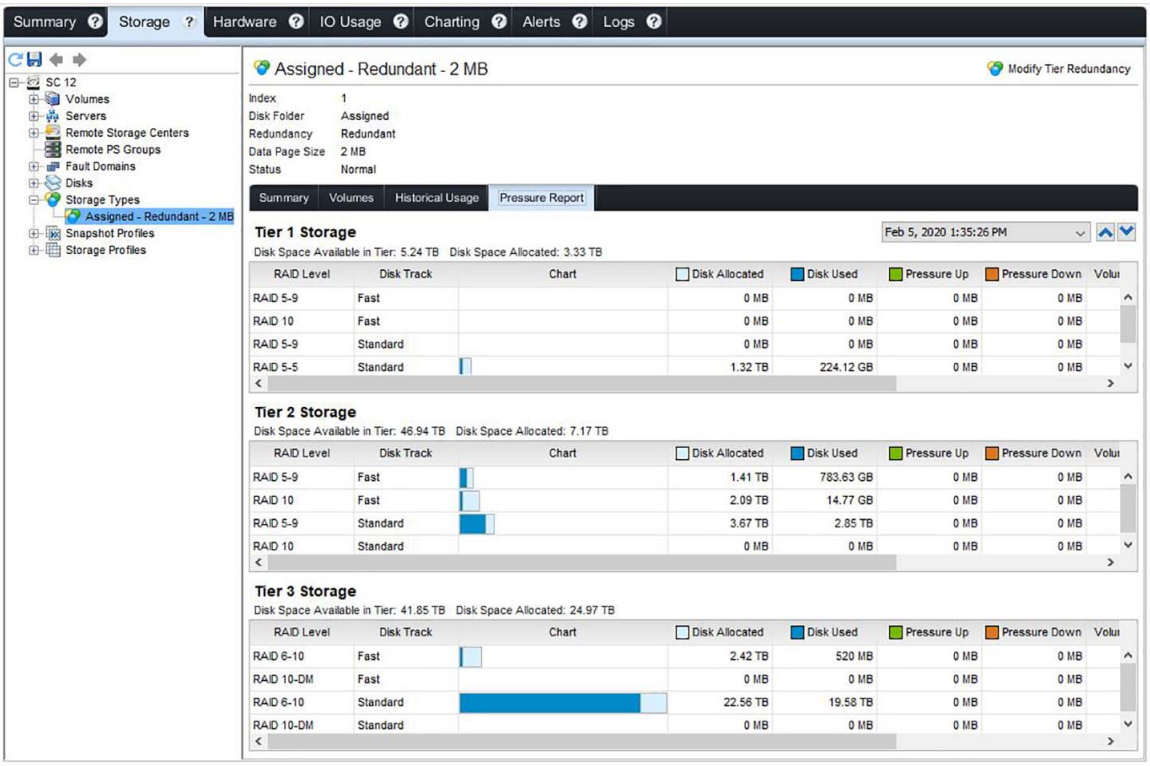


Figure 33. Storage Type Pressure Report Tab

The data progression Pressure Report tab displays the following information for each RAID level:

Pressure Report Column	Description
RAID Level	RAID level in the storage tier.
Disk Track	Type of track, which may be **Fast** or **Standard**.
Chart	Bar charts that display allocated disk space and used disk space.
Disk Allocated	Amount of raw disk space allocated.
Disk Used	Amount of raw disk space consumed.
Pressure Up	Amount of data scheduled to move to a faster storage tier during the next Data Progression cycle. Indicated by a green bar and up arrow in the bar chart.

Pressure Report Column	Description
Pressure Down	Amount of data scheduled to move to a slower storage tier during the next Data Progression cycle. Indicated by an orange bar and a down arrow in the bar chart.
Volume Allocated	Amount of usable space for volumes after RAID is applied.
Volume Used	Amount of volume allocated space that is consumed.
Saved vs RAID 10	Amount of space saved by moving less-accessed data to RAID 5 or RAID 6 instead of using RAID 10 for all data.

Viewing Historical IO Performance

The **IO Usage** tab is used to view and monitor historical IO performance statistics for a Storage Center and associated storage objects. The **Comparison View** on the **IO Usage** tab is used to display and compare historical IO usage data from multiple storage objects.

Using the IO Usage Tab

Use the **IO Usage** tab to view historical IO usage data for a Storage Center or associated storage object, and to compare IO usage data from multiple storage objects.

NOTE: For user interface reference information, click **Help**.

View Historical IO Usage Data for a Storage Center

Select a Storage Center on the **IO Usage** tab to view historical IO usage data.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **IO Usage** tab.
3. Select a Storage Center object from the **IO Usage** navigation pane.

   The **IO Charts** tab displays a chart that shows the historical IO usage data of the Storage Center.
4. To refresh the displayed IO usage data, click **Refresh** on the **IO Usage** navigation pane.

View Historical IO Usage Data for a Storage Object

Select a specific object in the **IO Usage** tab navigation pane to view historical IO usage data for the object.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **IO Usage** tab.
3. Select a storage object from the **IO Usage** navigation pane.
4. Depending on the type of storage objects selected in Step 4 one or both of the following tabs appear:
   - **IO Charts**: Displays charts that shows historical IO usage data.
     - If a Storage Center is selected, the **IO Charts** tab displays IO usage data for the front end and back end connections of the Storage Center.
     - If a storage object is selected that has other storage objects assigned to it, the **IO Charts** tab displays calculated averages of the IO usage data for all of the objects assigned to the selected storage object.
     - If a storage object is selected that does not have storage objects assigned to it, the **IO Charts** tab displays the IO usage data of the selected storage object.

- **Most Active Report**: Displays a table that shows the minimum, maximum, average, and standard deviation values of the historical IO usage data.

  The **Most Active Report** tab is displayed only if the selected storage object is one of the following container objects:

  - Volumes or a volume folder
  - Servers or a server folder
  - Remote Storage Centers
  - Disks or disk speed folder

5. To refresh the displayed IO usage data, click **Refresh** on the **IO Usage** navigation pane.

Change the Period of Data to Display on the IO Usage Tab

You can display data for the last day, last 3 days, last 5 days, last week, last month, or a custom time period.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **IO Usage** tab.
3. Click one of the following buttons to change the period of IO usage data to display:
   - **Last Day**: Displays the past 24 hours of IO usage data.
   - **Last 3 Days**: Displays the past 72 hours of IO usage data.
   - **Last 5 Days**: Displays the past 120 hours of IO usage data.
   - **Last Week**: Displays the past 168 hours of IO usage data.
   - **Last Month**: Displays IO usage data for the past month.
   - **Custom**: Displays options that allow you to specify the start time and the end time of the IO usage data to display.
4. If you clicked **Custom**, perform the following tasks to specify the start time and end time of the IO usage data to display.

   To specify the start time:

   a. Select **Other** from the **Start Time** drop-down menu.
   b. Select the start date of the time period to display from the date drop-down menu calendar.
   c. Specify the start time of the time period in the time field.

      To set the start time to the beginning of the day, select the **Start of Day** check box.

   d. Click **Update** to display IO usage data using the specified start time.

      To specify the end time:

   a. Clear the **Use Current** check box.
   b. Select the stop date of the time period to display from the date drop-down menu calendar.
   c. Specify the stop time of the time period in the time field.

      To set the stop time to the end of the day, select the **End of Day** check box.

   d. Click **Update** to display IO usage data using the specified end time.

Display the Comparison View

Use the Comparison View to compare historical IO usage for storage objects.

Steps

1. Click the **Storage** view.
2. Select a Storage Center from the **Storage** pane.
3. Click **IO Usage** tab.
4. Click **Select View** on the **IO Usage** navigation pane.
5. Select **Comparison View** from the drop-down menu.

   The options on the **IO Usage** navigation pane are replaced with **Comparison View** options.

6. Select the check boxes of the storage objects to compare from the **IO Usage** navigation pane.

   NOTE: The **Comparison View** cannot compare more than 10 objects at one time.

7. Click **Update**.

   The **Total IO/Sec** and **Total MB/Sec** charts appear by default and display the total IO usage for writes and reads, in IO/sec and MB/Sec, for the selected storage objects.

8. Select the check boxes of additional charts to display:

   NOTE: The charts that can be displayed depend on the storage objects that were selected in Step 6.

   - **Write IO/Sec**: Displays writes, in IO/sec, for the selected storage objects in a single chart.
   - **Read IO/Sec**: Displays reads, in IO/sec, for the selected storage objects in a single chart.
   - **Write MB/Sec**: Displays writes, in MB/sec, for the selected storage objects in a single chart.
   - **Read MB/Sec**: Displays reads, in MB/sec, for the selected storage objects in a single chart.
   - **Read Latency**: Displays read latencies, in ms, for the selected storage objects in a single chart.
   - **Write Latency**: Displays write latencies, in ms, for the selected storage objects in a single chart.
   - **Xfer Latency**: Display data transfer latencies, in ms, for the selected servers or remote Storage Centers in a single chart.
   - **Avg IO Size**: Displays average IO sizes for the selected storage objects in a single chart.
   - **IO Pending**: Displays pending IOs for the selected storage objects in a single chart.

9. Click **Update**.

Viewing Current IO Performance

The **Charting** tab is used to view and monitor current IO performance statistics for a Storage Center and associated storage objects. The **Comparison View** on the **Charting** tab is used to display and compare IO usage data from multiple storage objects.

Using the Charting Tab

Use the **Charting** tab to view current IO usage data for a Storage Center or associated storage object and compare IO usage data for multiple storage objects.

NOTE: For user interface reference information, click **Help**.

View Current IO Usage Data for a Storage Center

Select a Storage Center on the **Charting** tab to view current IO usage data.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Charting** tab.
3. Select the Storage Center from the **Charting** navigation pane.

   The **IO Charts** tab displays a chart that shows the IO usage data for the Storage Center.

4. To refresh the IO usage data, click **Refresh** on the **Charting** navigation pane.
5. To stop collecting IO usage data from the Storage Center, click the **Stop** button. To resume collecting IO usage data, click the **Start** button.

View Current IO Usage Data for a Storage Object

Select a specific object in the **Charting** tab navigation pane to view current IO usage data for the object.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Charting** tab.
3. Select a storage object from the from the **Charting** navigation pane.
4. Depending on the type of storage objects selected in the previous step, one or both of the following tabs appear:
   - **IO Charts**: Displays charts that shows IO usage data.
     - If a Storage Center is selected, the **IO Charts** tab displays IO usage data for the front end and back end connections of the Storage Center.
     - If a storage object is selected that has other storage objects assigned to it, the **IO Charts** tab displays calculated averages of the IO usage data for all of the objects assigned to the selected storage object.
     - If a storage object is selected that does not have storage objects assigned to it, the **IO Charts** tab displays the IO usage data of the selected storage object.

     IO Chart During Replications

     During replications (either for a one-time replication or for a Live Volume) the IO graph shows usage data related to the replication.

     For remote Storage Centers, the chart shows usage activity of the current Storage Center receiving data from the remote Storage Center. For example, when replicating from Storage Center *A* to Storage Center *B*:
     - Selecting Storage Center *A* in the left navigation pane, and viewing remote Storage Center *B* usage data will show little activity.
     - Selecting Storage Center *B* in the left navigation pane, and viewing Storage Center *A* usage data will show the IO activity related to Storage Center *A* writing data to Storage Center *B*.

     For volumes, the graph shows the IO received by the volume from the server or Storage Center:
     - During a one-time replication, the graph shows IO written from the primary Storage Center to the destination volume.
     - During a Live Volume replication, the graph shows IO written from the mapped server.

   - **Most Active Report**: Displays a table that shows the minimum, maximum, average, and standard deviation values of the IO usage data, which the Storage Manager collects every 5 minutes by default.

     The **Most Active Report** tab is displayed only if the selected storage object is one of the following container objects:

     - Volumes or a volume folder
     - Servers or a server folder
     - Remote Storage Centers
     - Disks or disk speed folder
5. To refresh the IO usage data, click **Refresh** on the **Charting** navigation pane.
6. To stop collecting IO usage data from the Storage Center, click the **Stop** button. To resume collecting IO usage data, click the **Start** button.

Change the Period of Data to Display on the Charting Tab

You can display data for the last 5 minutes, last 15 minutes, last 30 minutes, or last hour.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Charting** tab.
3. Select the period of the IO usage data to display on the **Charting** tab from the **Show Last** drop-down menu.
   - **5 Minutes**: Displays the past 5 minutes of IO usage data.
   - **15 Minutes**: Displays the past 15 minutes of IO usage data.
   - **30 Minutes**: Displays the past 30 minutes of IO usage data.
   - **1 Hour**: Displays the past 60 minutes of IO usage data.

Display the Comparison View on the Charting tab

Use the Comparison View to compare current IO usage for storage objects.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click **Charting** tab.
3. Click **Select View** on the **Charting** navigation pane.
4. Select **Comparison View** from the drop-down menu.

   The options on the **Charting** navigation pane are replaced with **Comparison View** options.

5. Select the check boxes of the storage objects to compare from the **Charting** navigation pane.

   NOTE: The **Comparison View** cannot compare more than 10 objects at one time.

6. Click **Update**.

   The **Total IO/Sec** and **Total MB/Sec** charts appear by default and display the total IO usage for writes and reads, in IO/sec and MB/Sec, for the selected storage objects.

7. Select the check boxes of additional charts to display:

   NOTE: The charts that can be displayed depend on the storage objects that were selected in Step 6.

   - **Write IO/Sec**: Displays writes, in IO/sec, for the selected storage objects in a single chart.
   - **Read IO/Sec**: Displays reads, in IO/sec, for the selected storage objects in a single chart.
   - **Write MB/Sec**: Displays writes, in MB/sec, for the selected storage objects in a single chart.
   - **Read MB/Sec**: Displays reads, in MB/sec, for the selected storage objects in a single chart.
   - **Read Latency**: Displays read latencies, in ms, for the selected storage objects in a single chart.
   - **Write Latency**: Displays write latencies, in ms, for the selected storage objects in a single chart.
   - **Xfer Latency**: Display data transfer latencies, in ms, for the selected servers or remote Storage Centers in a single chart.
   - **Avg IO Size**: Displays average IO sizes for the selected storage objects in a single chart.
   - **IO Pending**: Displays pending IOs for the selected storage objects in a single chart.

8. Click **Update**.

Configuring Chart Options

User Settings affect the charts on the **Summary**, **IO Usage**, and **Charting** tabs, and the Chart Settings affect the charts on the **IO Usage** and **Charting** tabs.

Related concepts

Configuring User Settings for Charts on page 316
Configuring Chart Settings on page 317

Configuring User Settings for Charts

Modify the User Settings for your user account to display alerts on the charts and change the chart colors.

NOTE: For user interface reference information, click **Help**.

Display Alerts on Charts

You can configure charts to display the relationships between the reported data and the configured threshold alerts and Storage Center alerts.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box appears.
2. In the **Charting Options** area of the **General** tab, select the check box(es) of the alert(s) to display on charts:
   - **Show threshold alert levels on charts**: Displays a horizontal line parallel to the X axis that shows the relationship between the reported data and the threshold level. The default is to hide threshold alerts.
   - **Show Storage Center alerts on charts**: Displays a vertical line parallel to the Y axis that shows the relationship between the reported data and Storage Center alerts. The default is to hide Storage Center alerts.

     NOTE: Charts display only alerts relating to controller failures or remote Storage Center failures.
3. Click **OK**.

Customize Chart Colors

You can choose the background color, gridline color, and crosshair color for charts.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box appears.
2. Click on the **General** tab. The following colors are displayed in the **Charting Options** area:
   - **Background Color**: Color of the background behind the chart.
   - **Gridline Color**: Color of the gridlines in the chart.
   - **Crosshair Color**: Color of the crosshairs in the chart.
3. To customize a color, click the **Change** link located to the right of the current color swatch. The **Select Color** dialog box appears.
   - To select a color from a list of color swatches, click the **Swatches** tab, and click on a color to select it.
   - To select a color based on an HSB value, click the **HSB** tab, then enter the HSB value by specifying hue (**H**), saturation (**S**), and brightness (**B**) values.
   - To select a color based on an RGB value, click the **RGB** tab, then enter the RGB value by specifying red (**R**), green (**G**), and blue (**B**) values.
4. Click **OK** to close the **Select Color** dialog box.
5. Click **OK**. The customized color settings will appear the next time a chart is updated.

Display Data Point Sliders on Charts

Chart sliders display specific data for a selected data point. When chart sliders are enabled, a table displays the specific data values for the selected data point.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box appears.
2. Click on the **General** tab.
3. Under **Charting Options**, select the **Show sliders on charts** check box.
4. Click **OK**.

Configuring Chart Settings

The chart configuration options include displaying threshold and Storage Center alerts on charts and changing the colors of charts.

NOTE: For user interface reference information, click **Help**.

Combine Usage Data into One Chart

You can combine IO usage data into a single chart with multiple Y axes.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **IO Usage** or **Charting** tab.
3. Select the **Combine Charts** check box to combine the IO usage data into a single chart with multiple Y axes.

Scale Usage Data in a Chart

You can change the scale for MB/Sec, IO/Sec, and Latency.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **IO Usage** or **Charting** tab.
3. Select the check box of the usage metric to scale.
   - To scale the MB/Sec metric, select the **Set MB/Sec Scale** check box.
   - To scale the IO/Sec metric, select the **Set IO/Sec Scale** check box.
   - To scale the latency metric, select the **Set Latency Scale** check box.
4. Enter a value in the selected usage metric field to scale the Y axis.
5. Press **Enter**. The data in the chart scales to fit the new Y axis.

Select the Usage Data to Display in a Chart

You can show or hide usage data for a chart.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **IO Usage** or **Charting** tab.
3. Select a Storage Center or storage object from the **IO Usage** or **Charting** navigation pane.
4. Select the check boxes of the usage metrics to display in the chart and clear the check boxes of the usage metrics to not display in the chart.

   NOTE: Reducing the number of usage metrics to display reduces the time required to update the IO Chart tab.

Configure the Storage Center Data Gathering Schedule

You can configure the intervals at which Storage Manager gathers IO Usage, Replication Usage, and Storage Usage data from managed Storage Centers.

Steps

1. In the top pane of the Storage Manager Client, click **Edit Data Collector Settings**. The **Edit Data Collector Settings** dialog box appears.
2. Click the **Schedules** tab.
3. Click **Edit**. The **Schedules** dialog box opens.
4. Configure the data collection schedules, in the **Storage Center Report Gathering Settings** area, by performing the following steps:
   - To change how often IO usage data is collected, select a different period of time from the **IO Usage** drop-down menu.

- To change how often replication usage data is collected, select a different period of time from the **Replication Usage** drop-down menu.
- To change how often storage usage data is collected, select a different period of time from the **Storage Usage** drop-down menu.

  If **Daily** is selected from the Storage Usage drop-down menu, the time of day that storage usage data is collected can be selected from the **Storage Usage Time** drop-down menu.

5. Click **OK**.

Exporting Usage Data

You can export Storage Usage and IO Usage data to CSV, Text, Excel, HTML, XML, or PDF.

Export Storage Usage Data

You can export storage usage data for Storage Centers, volumes, and servers.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. Click **(Save Storage Usage Data)** located in the **Storage** navigation pane.

   The **Save Storage Usage Data** dialog box opens.

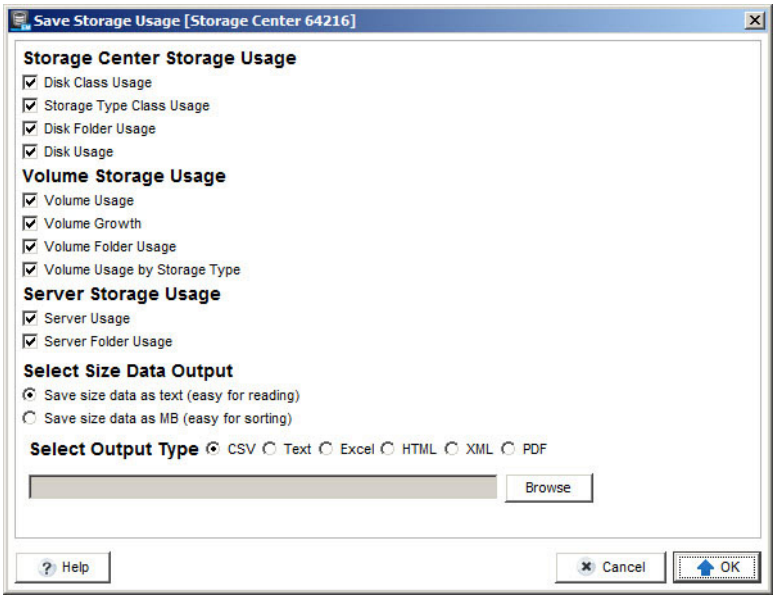


Figure 34. Save Storage Usage Dialog Box

4. Specify the storage usage data to export by selecting or clearing the check boxes in the **Storage Center Storage Usage**, **Volume Storage Usage**, and **Server Storage Usage** areas of the dialog box.

   By default, all of the storage usage data is selected to be exported.

5. Specify how to display the size data in the output by selecting one of the following radio buttons:
   - **Save size data as text (easy for reading)** – Displays size data using the units that are the most appropriate for the displayed values. For example, 2097152 megabytes is displayed as 2 TB.
   - **Save size data as MB (easy for sorting)** – Displays size data in megabytes, without a unit of measure label. For example, 2 TB is displayed as 2097152 (megabytes).
6. Select a file type for the output: **CSV** (.csv), **Text** (.txt), **Excel** (.xls), **HTML** (.htm), **XML** (.xml), or **PDF** (.pdf).
7. Click **Browse** and specify the file name and location to save the file.

8. Click **OK**.

Export I/O Usage Data

You can export I/O usage data for the most active volumes, servers. disks, remote Storage Centers, controllers, and fault domains. You can also export Chart I/O usage data for Storage Centers, volumes, servers, disks, controllers, storage profiles, and fault domains.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the**IO Usage** or **Charting** tab.
3. Click **(Save IO Usage Data)** located in the **IO Usage** or **Charting** navigation pane.

   The **Save IO Usage Data** dialog box opens.

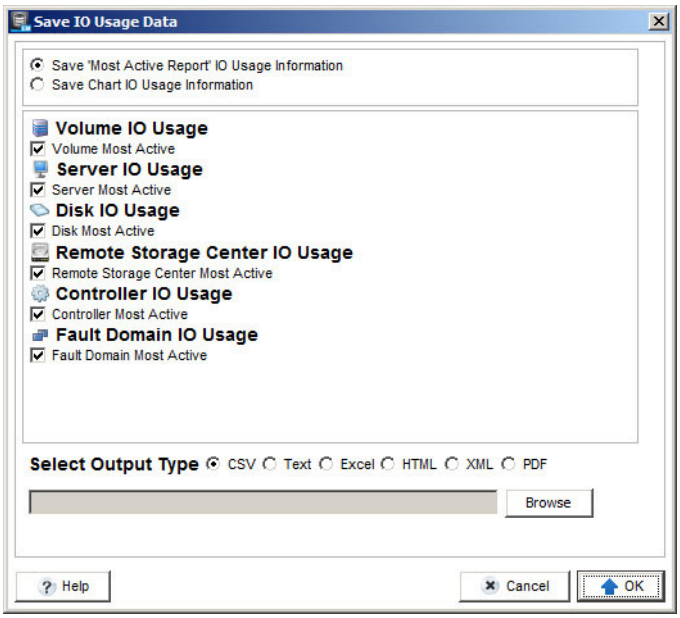


Figure 35. Save IO Usage Data Dialog Box

4. Specify the type of I/O usage data to export by selecting one of the following radio buttons:
   - **Save 'Most Active Report' IO Usage Information**
   - **Save Chart IO Usage Information**
5. If you selected the **Save 'Most Active Report' IO Usage Information** radio button, select the check boxes of the I/O usage data to export:
   - **Volume Most Active** – Exports I/O usage data for the volumes.
   - **Server Most Active** – Exports I/O usage data for the servers.
   - **Disk Most Active** – Exports I/O usage data for the disks.
   - **Remote Storage Center IO Usage** – Exports I/O usage data for remote Storage Centers.
   - **Controller Most Active** – Exports I/O usage data for the controllers.
   - **Fault Domain Most Active** – Exports I/O usage data for fault domains.
6. If you selected the **Save Chart IO Usage Information** radio button:
   a. Select the storage object from which to export I/O usage data from the **Select Object Type** drop-down menu.
   b. If you selected an object other than a Storage Center, select the check boxes of the storage objects for which you want to export I/O usage data.
      - To select all of the storage objects, click **Select All**.
      - To deselect all of the storage objects, click **Unselect All**.
7. Select a file type for the output: **CSV** (.csv), **Text** (.txt), **Excel** (.xls), **HTML** (.htm), **XML** (.xml), or **PDF** (.pdf).
8. Click **Browse** and specify the file name and location to save the file.
9. Click **OK**.

Monitoring Storage Center Hardware

Use the Hardware tab of the Storage view to monitor Storage Center hardware.

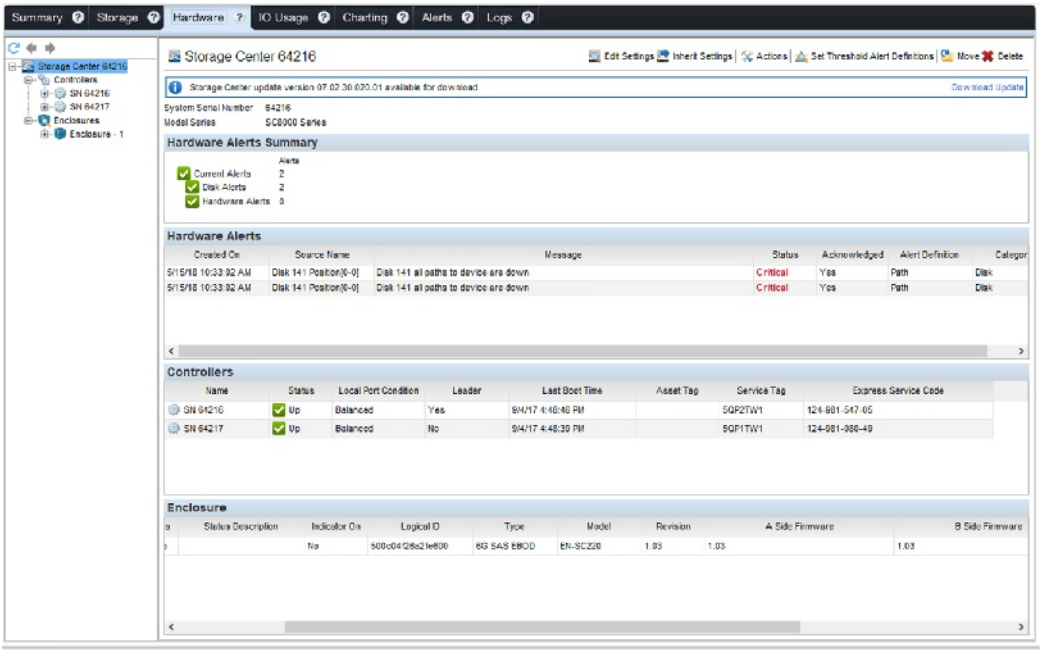


Figure 36. Hardware Tab

Related concepts

Monitoring a Storage Center Controller on page 321
Monitoring a Storage Center Disk Enclosure on page 324
Monitoring SSD Endurance on page 327
Viewing UPS Status on page 328
Managing Disk Enclosures on page 284
Shutting Down and Restarting a Storage Center on page 295

Monitoring a Storage Center Controller

The Hardware tab displays status information for the controller(s) in a Storage Center.

NOTE: For user interface reference information, click **Help**.

View Summary Information for All Controllers in a Storage Center

The Controllers node on the Hardware tab displays summary information for all controllers in a Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, select **Controllers**.
4. Use the tabs in the right pane to view summary information for the controllers and controller components.

View Summary Information for a Controller

The controller node on the Hardware tab displays summary information for the controller, including name, version, status, and network settings.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, select the controller. The right pane displays controller summary information.

View a Diagram of a Controller

The Hardware tab displays a diagram of the back of a controller selected from the Hardware tab navigation pane.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Controllers** node then select a controller. The right pane displays a diagram of the controller

   The hardware view indicates failed components with a red overlay.
4. To view more information about hardware components, mouse over a hardware component. A tool tip appears and displays information including the name and status of the hardware component.
5. To adjust the zoom on the controller diagram, change the position of the zoom slider located to the right of the controller diagram.
   - To zoom in, click and drag the zoom slider up.
   - To zoom out, click and drag the zoom slider down.
6. To move the controller diagram in the **Controller View** tab, click and drag the controller diagram.

View IO Port Information and Status for a Controller

The controller node on the Hardware tab displays summary and status information for all Fibre Channel, iSCSI, and SAS ports on IO cards installed in the controller.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Controllers** node, expand the node for a specific controller, then select **IO Ports**. The right pane displays summary and status information for all IO port types present in the controller.
4. To view more detailed information for a particular protocol, select **Fibre Channel**, **iSCSI**, or **SAS** in the **Hardware** tab navigation pane.

Locate a Port in the Controller Diagram

The Hardware tab displays the location of a port in the controller diagram when that port is selected from the Hardware tab navigation pane.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Controllers** node, expand the node for a specific controller, then select **IO Ports**.

4. Select an IO port from the **Fibre Channel**, **iSCSI**, or **SAS** nodes. The **Port View** tab in the right pane highlights the selected port in the controller diagram.

View Fan Status for a Controller

The Fan Sensors node on the Hardware tab displays summary and status information for fans in the controller.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Controllers** node, expand the node for a specific controller, then click **Fan Sensor**. The right pane displays summary and status information for the fans in the controller.

View Power Supply Status for a Controller

The Power Supply node on the Hardware tab displays summary and status information for power supplies in the controller.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Controllers** node, expand the node for a specific controller, then click **Power Supply**. The right pane displays summary and status information for the power supplies in the controller.

View Temperature Information for a Controller

The Temperature Sensor node on the Hardware tab displays summary and status information for temperature sensors in the controller.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Controllers** node, expand the node for a specific controller, then click **Temperature Sensor**. The right pane displays summary and status information for temperature sensors in the controller.

View Voltage Sensor Status for a Controller

The Voltage Sensor node on the Hardware tab displays status information for voltage sensors in the controller.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Controllers** node, expand the node for a specific controller, then click **Voltage Sensor**. The right pane displays status information for voltage sensors in the controller.

View Cache Card Status for a Controller

The Cache Card node on the Hardware tab displays status information for the cache card in the controller.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.

3. In the **Hardware** tab navigation pane, expand the **Controllers** node, expand the node for a specific controller, then click **Cache Card**. The right pane displays summary and status information for cache card in the controller.

Monitoring a Storage Center Disk Enclosure

The Hardware tab displays status information for the disk enclosure(s) in a Storage Center.

NOTE: For user interface reference information, click **Help**.

View Summary Information for All Enclosures in a Storage Center

The Enclosures node on the Hardware tab displays summary information for all disk enclosures in a Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, select **Enclosures**.
4. Use the tabs in the right pane to view summary information for the enclosures and enclosure components.

View Summary Information for an Enclosure

The enclosure node on the Hardware tab displays summary information for the enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, select an enclosure. The right pane displays summary information.

View a Diagram of an Enclosure

The Hardware tab displays a graphical representation of an enclosure selected from the Hardware tab navigation pane.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosures** node.
4. Select an enclosure. The **Enclosure View** tab in the right pane displays a front and back diagram of the selected enclosure.

   The hardware view indicates failed components with a red overlay.
5. To view more information about hardware components, mouse over a hardware component. A tool tip appears and displays information including the name and status of the hardware component.
6. To adjust the zoom on the enclosure diagram, change the position of the zoom slider located to the right of the enclosure diagram.
   - To zoom in, click and drag the zoom slider up.
   - To zoom out, click and drag the zoom slider down.
7. To move the enclosure diagram in the **Enclosure View** tab, click and drag the enclosure diagram.

View Alarm Status for an Enclosure

The Audible Alarms node on the Hardware tab displays alarm status for the enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, select **Audible Alarms**. The right pane displays summary information.

View Disk Status for an Enclosure

The Disks node in the Hardware tab displays the statuses of all disks in the enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosure** node then the node for a specific enclosure.
4. Click the **Disks** node. The right pane displays the status of all disks in the enclosure.

Locate a Disk in the Enclosure Diagram

The Hardware tab shows the location of a disk selected from the Disks tab in the right pane.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosures** node, then the node for a specific enclosure.
4. Click the **Disks** node. The right pane displays the disks in the enclosure in the **Disks** tab.
5. Select a disk from the **Disks** tab. The **Disk View** tab highlights the disk in the enclosure diagram.

   NOTE: Storage Manager groups disks in an SC280 enclosure into drawers. If the enclosure is an SC280, you must expand a drawer to select a disk.

View Cooling Fan Status for an Enclosure

The Cooling Fan Sensors node on the Hardware tab displays cooling fan status for the enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosures** node, then the node for a specific enclosure.
4. Select **Cooling Fan Sensors**. The right pane displays summary information.

Locate a Cooling Fan Sensor in the Enclosure Diagram

The Hardware tab highlights the location of a cooling fan sensor in the enclosure diagram.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosures** node, then the node for a specific enclosure.

4. Click the **Cooling Fan Sensors** node. The right pane lists the cooling fan sensors in that enclosure.
5. Select a cooling fan sensor from the **Cooling Fans** tab. The **Fan View** tab highlights the selected fan in the enclosure diagram.

View IO Module Status for an Enclosure

The I/O Modules node on the Hardware tab displays IO module status for the enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosures** node, then the node for a specific enclosure.
4. Click **I/O Modules**. The right pane displays status information for the IO module selected from the **I/O Modules** tab.

Locate an IO Module in the Enclosure Diagram

The Hardware tab highlights the location of an IO module in the enclosure diagram.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosures** node then, the node for a specific enclosure.
4. Select the **I/O Modules** node. The right pane lists the IO modules in the enclosure.
5. Select an IO module from the **I/O Modules** tab. The **IO Module View** tab highlights the selected IO module in the enclosure diagram.

View Power Supply Status for an Enclosure

The Power Supplies node on the Hardware tab displays power supply status for the enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosures** node, then the node for a specific enclosure.
4. Click **Power Supplies**. The right pane displays status information for the power supply selected from the **Power Supplies** tab.

Locate a Power Supply in the Enclosure Diagram

The Hardware tab highlights the location of a power supply in the enclosure diagram.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosures** node, then the node for a specific enclosure.
4. Select the **Power Supplies** node. The right pane lists the power supplies in the enclosure.
5. Select a power supply from the **Power Supplies** tab. The Power Supply View tab highlights the selected power supply in the enclosure diagram.

View Temperatures for an Enclosure

The Temperature Sensor node on the Hardware tab displays temperatures for the enclosure.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand the **Enclosures** node, then the node for a specific enclosure.
4. Click **Temperature Sensor**. The right pane displays temperature sensor information.

Monitoring SSD Endurance

The lifespan of a Solid State Drive (SSD) is determined by how much data is written to it. The endurance level for an SSD is displayed as a percentage that indicates the amount of wear life remaining. Some SSDs track and report endurance status and some do not.

A fresh drive starts with an endurance level of 100%, and the endurance level decreases as data is written to the drive. A Storage Center triggers an alert when it determines that an SSD will reach its endurance limit within 120 days.

NOTE: For user interface reference information, click **Help**.

View Current Endurance and Endurance History for an SSD

The current endurance level for an SSD is displayed as a percentage. The endurance level for an SSD is also recorded over time and can be displayed in a graph.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the SSD.
4. View endurance information for the SSD.
   - To view the current endurance level for the SSD, see the **Endurance** value displayed in the right pane.
   - To view endurance history information for the SSD, click the **Endurance History** subtab.

View the Current Endurance Level for All SSDs in a Disk Folder

If a disk folder contains SSDs, the summary table displays the percentage of wear life remaining for each SSD and a corresponding endurance chart.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Storage** tab.
3. In the **Storage** tab navigation pane, select the disk folder.
4. On the **Disks** subtab, locate the **Endurance** and **Endurance Chart** columns in the table.

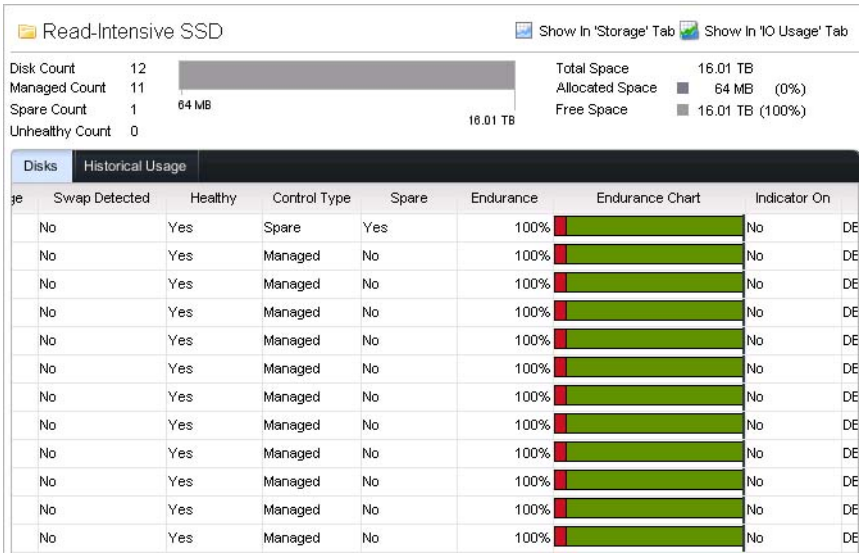


Figure 37. SSD Endurance

The **Endurance Chart** column shows a wear gauge that indicates the amount of wear life remaining and when an alert will be sent. The gauge indicators are:

- **Red**: Fail zone calculated from disk data that estimates when 120 days remain in the life of the disk. An alert is sent when the wear life moves from the green zone to the red zone.
- **Green**: Safe operating zone.
- **Black Tick Mark**: Current Endurance level, in which the far right position indicates 100% endurance (new disk, no wear) and the far left position indicates 0% (end of life). This is also shown as the Endurance percentage in the **Endurance** column.

Viewing UPS Status

A UPS provides power redundancy to a Storage Center with the use of a backup battery.

If the power to a Storage Center is cut off, the UPS immediately switches over to the battery giving a Storage Center administrator time to properly power down the Storage Center or fix the power issue. When the UPS switches to the battery, it sends an on battery message to the Storage Center. The Storage Center registers the battery message as an alert, turns off write cache, and flushes the cache to disk. The Storage Center continues to operate in this way until it shuts down or the UPS sends an online message allowing it to return to normal operations.

NOTE: For user interface reference information, click **Help**.

Related tasks

Add a UPS to a Storage Center on page 294

View Summary Information for All UPS Units that Serve the Storage Center

The **UPS** node on the **Hardware** tab displays summary information for the UPS units that provide backup power for the Storage Center.

Prerequisites

A UPS unit must have been configured for the Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.

3. In the **Hardware** tab navigation pane, select **UPS**. The right pane displays summary information.

View Summary Information for a UPS Unit that Serves the Storage Center

The **Hardware** tab displays summary information for the UPS units that provide backup power for the Storage Center.

Prerequisites

A UPS must have been configured for the Storage Center.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, under the **UPS** node, select the name of a UPS unit. The right pane displays summary information.

11

SMI-S

The Storage Management Initiative Specification (SMI-S) is a standard interface specification developed by the Storage Networking Industry Association (SNIA). Based on the Common Information Model (CIM) and Web-Based Enterprise Management (WBEM) standards, SMI-S defines common protocols and data models that enable interoperability between storage vendor software and hardware.

Topics:

- SMI-S Provider
- Setting Up SMI-S
- Using the Dell SMI-S Provider with Microsoft SCVMM

SMI-S Provider

The SMI-S Provider is included with the Data Collector. You can configure SMI-S during initial Data Collector installation or post-installation by modifying the Data Collector properties. When SMI-S is enabled and configured, the Data Collector automatically installs and manages the SMI-S Provider; no additional installation is required.

NOTE: The Storage Manager Data Collector must be installed in a Microsoft Windows environment. SMI-S is not supported on a Virtual Appliance.

Supported Management Solutions

Storage Manager SMI-S is compatible with the following combinations of Microsoft System Center Virtual Machine Manager (SCVMM) and Microsoft Server versions.

- SCVMM 2012 SP1 running on Windows Server 2012
- SCVMM 2012 R2 running on Windows Server 2012
- SCVMM 2012 R2 running on Windows Server 2012 R2
- SCVMM 2016 R2 running on Windows Server 2016

Supported SMI-S 1.6 Profiles

An SMI-S profile describes the management interfaces for a storage subsystem.

The Dell SMI-S provider packaged with Storage Manager supports the following SMI-S 1.6 profiles:

- Access Points
- Array
- Block Services
- Block Server Performance
- Copy Services
- Disk Drive Lite
- Extent Composition
- FC Target Ports
- Health
- iSCSI Target Ports
- Job Control
- Masking and Mapping
- Multiple Computer System
- Physical Package
- Replication Services
- Server

- Software
- Thin Provisioning

SMI-S Namespace

Use the following namespace parameters to access SMI-S.

- Interop namespace - **/interop**
- Array namespace - **/root/compellent**

Setting Up SMI-S

To set up SMI-S, enable SMI-S for the Data Collector, then add the required SMI-S user. HTTPS is the default protocol for the SMI-S provider.

Steps

1. SMI-S Prerequisites on page 331
2. Enable SMI-S for the Data Collector on page 331

SMI-S Prerequisites

Complete the following prerequisite tasks before configuring SMI-S on the Storage Manager Data Collector.

Steps

1. Make sure that a user for the SMI-S Provider is created on the Data Collector.
2. Make sure that the following Microsoft software is installed on the server that hosts the Data Collector:
   - Microsoft .NET Framework 4.6 Full
   - Windows PowerShell 3.0 or later
3. For Windows Server 2012, open the required SMI-S ports on server that hosts the Data Collector.

   NOTE: SLP does not support using a static IP on the adapter. The adapter on the server that hosts the Data Collector must acquire its IP address using DHCP.

   a. Start the **Windows PowerShell** application.
   b. Run the following commands to open the required ports:
      - `netsh advfirewall firewall add rule name="CIM-XML" dir=in protocol=TCP localport=5988-5989 action=allow`
      - `netsh advfirewall firewall add rule name="CIM-XML" dir=out protocol=TCP localport=5990 action=allow`
   c. Run the following commands to open the SLP ports:
      - `netsh advfirewall firewall add rule name="SLP-udp" dir=in protocol=UDP localport=427 action=allow`
      - `netsh advfirewall firewall add rule name="SLP-udp" dir=out protocol=UDP localport=427 action=allow`

Enable SMI-S for the Data Collector

If the SMI-S Service is disabled on the Storage Manager Data Collector, use Unisphere Central to enable the SMI-S service.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:

https://*data_collector_host_name_or_IP_address*:3033/

c. Press Enter.
The Unisphere Central login page is displayed.

d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.

e. Click **Log In**.

2. Click **Data Collector**.
The **Data Collector** view is displayed.
3. Click the **General** tab, and then select the **Ports** subtab.
4. Click **Edit**.
The **Edit Port** dialog box opens.
5. Select **SMI-S Service** from the list of ports.
6. Select the **Enabled** checkbox.
7. Click **OK**.
The **Data Collector Restart** dialog box opens.
8. Click **Yes**.
The Data Collector service stops and restarts.

Using the Dell SMI-S Provider with Microsoft SCVMM

Complete the following tasks to discover the Dell SMI-S provider using System Center Virtual Machine Manager (SCVMM) 2012 or SCVMM 2016:

Steps

1. SCVMM Prerequisites on page 332
2. Limitations for SCVMM 2012 on page 333
3. Modify the SCVMM 2012 Management Server Registry to Allow HTTPS on page 333
4. Use SCVMM to Discover the SMI-S Provider on page 334

SCVMM Prerequisites

Make sure that the following prerequisites are met before using SCVMM to discover the Dell SMI-S provider and Storage Centers.

About this task

- SCVMM and the Storage Manager Data Collector must be installed on separate servers, and both servers must be members of the same Active Directory domain.
- If the SCVMM server is running Windows Server 2012 R2:
  - Install Update Rollup 14 for SCVMM on the server – https://support.microsoft.com/en-us/help/4043306/description-of-update-rollup-14-for-microsoft-system-center-2012-r2
  - Enable TLS v1.2 on the server – https://support.microsoft.com/en-us/help/4055768/tls-1-2-protocol-support-deployment-guide-for-system-center-2012-r2
- If the SCVMM sever is running Windows Server 2016:
  - Install latest version of SCVMM on the server
  - Enable TLS v1.2 on the server – https://support.microsoft.com/en-us/help/4051111/tls-1-2-protocol-support-deployment-guide-for-system-center-2016
- SMI-S must be enabled and configured for the Storage Manager Data Collector.
- The Storage Centers that you want to manage with SMI-S must be added to Data Collector and mapped to the SMI-S user.

Limitations for SCVMM 2012

Review the following limitations before you use Microsoft SCVMM 2012 to discover the Dell SMI-S provider and Storage Centers.

Thin Provisioning

The SCVMM 2012 console limits the maximum volume size at creation time to the available capacity of the storage pool. Storage Center thin provisioning does not have this restriction. This limitation can also cause the SCVMM 2012 console to display an error for "Allocated Storage" if allocated storage exceeds the available physical storage.

To create a volume that is larger than the available storage pool, use the PowerShell cmdlet `New-SCStorageLogicalUnit` instead of the SCVMM 2012 console.

Adding Server WWNs

If a WWN is not associated with a Storage Center server object, SMI-S creates one new server object for each available WWN. If a server has more than one WWN, SMI-S creates one server object for each WWN instead of creating one server object with multiple WWNs.

If a server has more than one WWN, create the server object manually instead of allowing SMI-S to automatically create the object(s).

Volume Names

SCVMM 2012 does not allow spaces or special characters such as underscores or dashes in volume names. However, volumes that have been created prior to discovery can include spaces in their names.

When creating LUNs using SCVMM 2012, do not include spaces in volume names.

Storage Center Controller Failover

In the event of a Storage Center controller failover, some operations may appear to fail in SCVMM due to timeouts. For instance, if controller failover occurs when creating a volume in SCVMM, the volume is created successfully on the Storage Center but the operation appears to fail in SCVMM.

In the event of a Storage Center controller failover, refresh the Dell SMI-S Provider in SCVMM. Refreshing the provider after failover helps ensure that the information in SCVMM remains accurate.

Modify the SCVMM 2012 Management Server Registry to Allow HTTPS

If you configured the Data Collector to use HTTPS for SMI-S connections, certificate errors can occur when SCVMM 2012 imports the Dell SMI-S Provider certificate. To prevent these errors, edit the registry on the SCVMM 2012 management server.

About this task

CAUTION: Serious problems might occur if you modify the registry incorrectly. For added protection, back up the registry before you modify it.

Steps

1. Start the **Registry Editor** application.
2. If the **User Account Control** dialog box appears, click **Yes** to continue. The **Registry Editor** window appears.
3. Disable CN verification for the storage provider certificate.
   a. In **Registry Editor**, navigate to the following folder:

Windows Server 2012: Select **HKEY_LOCAL_MACHINE**→ **Software**→ **Microsoft**→ **Windows**→ **CurrentVersion**→ **Storage Management**

b. If the **DisableHttpsCommonNameCheck** entry does not exist, select **Edit**→ **New**→ **DWORD (32-bit) Value**, and then type `DisableHttpsCommonNameCheck` to create it.

c. Double-click **DisableHttpsCommonNameCheck**.

d. In the **Value data** box, type `1`, then click **OK**.

4. If the server that hosts SCVMM is running Windows Server 2012, disable client certificate checking.

a. In **Registry Editor**, select **HKEY_LOCAL_MACHINE**→ **Software**→ **Microsoft** → **Windows**→ **CurrentVersion**→ **Storage Management**.

b. Double-click **EnableHTTPListenerClientCertificateCheck**.

c. In the **Value data** box, type `0`, then click **OK**.

5. If the server that hosts SCVMM is running Windows Server 2012 with the January 2012 Microsoft Security Update KB2585542 installed, perform the following steps to modify the registry.

a. In **Registry Editor**, select **HKEY_LOCAL_MACHINE**→ **System**→ **CurrentControlSet**→ **Control**→ **SecurityProviders**→ **SCHANNEL**.

b. If the **SendExtraRecord** entry does not exist, select **Edit**→ **New**→ **DWORD (32-bit) Value**, and then type `SendExtraRecord` to create it.

c. Double-click **SendExtraRecord**.

d. In the **Value data** box, type `2`, then click **OK**.

NOTE: For more information, see http://support.microsoft.com/kb/2643584

6. Close **Registry Editor**.

Prepare the SCVMM 2012 Server for Indications

If you are using the Dell SMI-S Provider with SCVMM 2012 running on Windows Server 2012 or later, configure the SCVMM server to accept SMI-S indications.

Steps

1. Make sure the Windows Standards-Based Storage Management feature is installed.
2. In Windows PowerShell, run the following command to open the required ports:

```
netsh advfirewall firewall add rule name="CIM-XML" dir=in protocol=TCP localport=5990 action=allow
```

3. In Windows PowerShell, run the following command to allow the Network Service to bind to the HTTPS port:

```
netsh http add urlacl url=https://*:5990/ user="NT AUTHORITY\NETWORK SERVICE"
```

Use SCVMM to Discover the SMI-S Provider

The **Add Storage Devices** wizard allows you to add the SMI-S Provider.

About this task

Depending on the configuration of your Storage Center, it might take several minutes to discover the SMI-S provider.

Steps

1. Start the Microsoft SCVMM Administrator Console.
2. Open the **Fabric** workspace.
3. On the **Home** tab, click **Add Resources**, and then select **Add Storage Devices**.
   The **Add Storage Devices Wizard** opens.
4. On the **Select Provide Type** wizard page, select **SAN and NAS devices discovered and managed by a SMI-S provider** and click **Next**.
5. Complete the fields in the **Specify Discovery Scope** wizard page.

a. In the **Provider IP address or FQDN** field, type the IP address or the fully qualified domain name of the Storage Manager Data Collector server that hosts the SMI-S provider.

b. In the TCP/IP port field, type the connection port of the SMI-S Provider.
   The default port is 5989.
c. Select the **Use Secure Socket Layers (SSL) connection** check box.
d. Click **Browse**.
   The **Select a Run As Account** dialog box opens
e. Select the SMI-S user account that you added to the SMI-S Provider and click **OK**.
   By default, **Run As account** users that are assigned to the **Storage Device** category are listed.
   NOTE: If no **Run As account** user exists, click **Create Run As Account** in the **Select a Run As Account** dialog box.

6. Complete the **Gather Information** wizard page.
   SCVMM automatically attempts to discover and import the storage device information
   a. If you selected the **Use Secure Socket Layers (SSL) connection** option, the **Import Certificate** dialog appears. Review the certificate information and click **Import**.
      When the discovery process succeeds, the discovered storage arrays, storage pools, manufacturer, model, and capacity are listed on the page.
      NOTE: If an error appears, make sure you have modified the registry of the SCVMM 2012 server to allow HTTPS connections. See Modify the SCVMM 2012 Management Server Registry to Allow HTTPS.

7. Complete the **Select Storage Devices** wizard page to select storage devices that you want SCVMM to manage.
   a. If the classification for the storage array does not exist, click **Create classification** and create a classification for the storage array
      A classification is a means for providing descriptive information about the array, such as location, purpose, or capacity.
   b. Select the storage device that you want SCVMM to manage.
   c. In the **Classification** column, select the storage classification you want to assign to the storage array.
   d. Select storage arrays and associated classifications for all storage pools you want SCVMM to manage.
   e. When you have finished selecting storage pools, click **Next**.
8. Confirm all settings on the **Summary Page** and click **Finish**
9. Verify the newly discovered storage information.
   NOTE: It can take several minutes for SCVMM to discover storage pools. Use the **Jobs** view to monitor discovery process.
   a. On the **Home** tab of the Fabric workspace, click **Fabric Resources**.
   b. Expand the **Storage** node, and verify any of the following:
      - To view the storage pools that are assigned to a classification, click **Classifications and Pools**. Expand the classification where you added storage; expand a storage pool to view logical unit information for the storage pool.
      - To view storage provider information, click **Providers**. You can view the storage provider name, management address, managed arrays, and the provider status.
      - To view discovered storage arrays, click **Arrays**. You can view the name of the array, total and used capacity, the number of managed storage pools, the provider name and port, and the provider status.

12

FluidFS Administration

This chapter describes how to use Storage Manager to manage FluidFS clusters for file storage.

Topics:

- How FS8600 Scale-Out NAS Works
- FluidFS System Management for FS Series Appliances
- FluidFS Networking
- FluidFS Account Management and Authentication
- FluidFS NAS Volumes, Shares, and Exports
- FluidFS Data Protection
- File Access Notification
- FluidFS Monitoring
- FluidFS Maintenance
- FS Series VAAI Plugin
- FluidFS Troubleshooting

How FS8600 Scale-Out NAS Works

Dell FS8600 scale-out NAS leverages the Dell Fluid File System (FluidFS) and Storage Centers to present file storage to Microsoft Windows, UNIX, and Linux clients. The FluidFS cluster supports the Windows, UNIX, and Linux operating systems installed on a dedicated server or installed on virtual systems deploying Hyper-V or VMware virtualization.

The Storage Centers present a certain amount of capacity (NAS pool) to the FluidFS cluster. This NAS pool is then divided into NAS volumes, which in turn are used to create SMB shares and NFS exports.

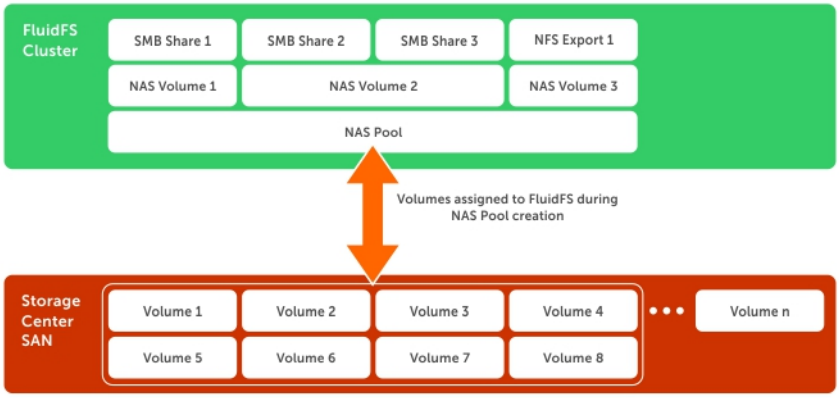


Figure 38. NAS Storage

To the client, the FluidFS cluster presents itself as a single file server, hosting multiple SMB shares and NFS exports, with a single IP address and namespace. Clients connect to the FluidFS cluster using their respective operating system's NAS protocols:

- UNIX and Linux users access files through the NFS protocol
- Windows users access files through the SMB protocol
- Users can also access files through the FTP and FTPS protocols

The FluidFS cluster serves data to all clients concurrently.

FS8600 Scale-Out NAS Terminology

The following table defines terminology related to FS8600 scale-out NAS.

Term	Description
Fluid File System (FluidFS)	High-performance, scalable file system software installed on NAS controllers.
Appliance (NAS appliance)	A rack-mounted 2U chassis that contains two hot-swappable NAS controllers in an active-active configuration in a FluidFS cluster. Cache data is mirrored between the paired NAS controllers within the NAS appliance.
Controller (NAS controller)	The two primary components of a NAS appliance, each of which functions as a separate member in the FluidFS cluster.
Peer controller	The NAS controller with which a specific NAS controller is paired in a NAS appliance.
Standby controller	A NAS controller that is installed with the FluidFS software but is not part of a FluidFS cluster. For example, a new or replacement NAS controller from the Dell factory is considered a standby controller.
Backup power supplies	Each NAS controller contains a backup power supply that provides backup battery power in the event of a power failure.
FluidFS cluster	One to six FS8600 scale-out NAS appliances configured as a FluidFS cluster.
Storage Center	Up to eight Storage Centers that provide the NAS storage capacity.
Storage Manager	Multisystem management software and user interface required for managing the FluidFS cluster and Storage Centers(s).
FS8600 Scale-out NAS	A fully configured, highly available, and scalable FluidFS cluster, providing NAS (SMB and NFS) services. The cluster comprises NAS appliances, storage provided by one or more Storage Centers and Storage Manager.
FTP	File Transport Protocol, used to transfer files to and from the FluidFS cluster.
NAS pool	The sum of all storage provided by up to eight Storage Centers minus space reserved for internal system use.
NAS volume	A virtualized volumes that consumes storage space in the NAS pool. Administrators can create SMB shares and NFS exports on a NAS volume and share them with authorized users.
LAN or client network	The network through which clients access SMB shares or NFS exports. This network is also used by the storage administrator to manage the FluidFS cluster.
Client VIP	One or more virtual IP addresses that clients use to access SMB shares and NFS exports hosted by the FluidFS cluster.
SMB Share	A directory in a NAS volume that is shared on the network using the Server Message Block (SMB) protocol.
NFS export	A directory in a NAS volume that is shared on the network using the Network File System (NFS) protocol.
Network Data Management Protocol (NDMP)	Protocol used for NDMP backup and restore operations.
Replication	Copies NAS volume data between two FluidFS clusters or between two NAS volumes.
Replication partners	FluidFS clusters participating in a replication operation.
Snapshot	An image of all the NAS volume data frozen as read-only at a specific point in time.

Key Features of the Scale-Out NAS

The following table summarizes key features of scale-out NAS.

Feature	Description
Shared back-end infrastructure	The Storage Center SAN and scale-out NAS leverage the same virtualized disk pool.
File management	Storage Center SAN and scale-out NAS management and reporting using Storage Manager.
High-performance, scale-out NAS	Support for a single namespace spanning up to four NAS appliances (eight NAS controllers).
Capacity scaling	Ability to scale a single namespace up to 4-PB capacity with up to eight Storage Centers.
Connectivity options	Offers 1GbE and 10GbE copper and optical options for connectivity to the client network.
Highly available and active-active design	Redundant, hot-swappable NAS controllers in each NAS appliance. Both NAS controllers in a NAS appliance process I/O.
Multitenancy	Multitenancy enables a single physical FluidFS cluster to be connected to several separated environments and manage each environment individually.
Automatic load balancing	Automatic balancing of client connections across network ports and NAS controllers, as well as back-end I/O across Storage Center volumes.
Multiprotocol support	Support for SMB (on Windows), NFS (on UNIX and Linux), and FTP/FTPS protocols with ability to share user data across all protocols.
Client authentication	Controls access to files using local and remote client authentication, including LDAP, Active Directory, and NIS.
Quota rules	Control client space usage.
File security style	Choice of file security mode for a NAS volume (UNIX, Windows, or Mixed).
Storage Center Data progression	Automatic migration of inactive data to less-expensive drives.
Storage Center Dynamic capacity	Thin-provisions the block-level storage allocated to the NAS pool and NAS volumes and consumes space only when writes occur.
Cache mirroring	The write cache is mirrored between NAS controllers, which ensures a high-performance response to client requests and maintains data integrity in the event of a NAS controller failure.
Journaling mode	In the event of a NAS controller failure, the cache in the peerg NAS controller is written to storage and the peer NAS controller continues to write directly to storage, which protects against data loss.
Backup power supply	Maintains data integrity in the event of a power failure by keeping a NAS controller online long enough to write the cache to the internal storage device.
NAS volume thin clones	Clones NAS volumes without needing to physically copy the data set.
Deduplication	Policy-driven post-process deduplication technology that eliminates redundant data at rest.
Compression	LZPS (Level Zero Processing System) compression algorithm that intelligently shrinks data at rest.
Metadata protection	Metadata is constantly checksummed and stored in multiple locations on both the FS Series appliance and within the Storage Centers for data consistency and protection.
Snapshots	Redirect-on-write snapshots that are user-accessible over the network.
Replication	NAS volume-level, snapshot-based, asynchronous replication to remote FluidFS clusters to enable disaster recovery.
NDMP backup	Snapshot-based, asynchronous, two-way backup (direct NDMP), or three-way backup (remote NDMP) over Ethernet to certified third-party backup solutions.

Feature	Description
Antivirus scanning	SMB antivirus scanning offloading using certified third-party, Internet Content Adaptation Protocol (ICAP)-enabled antivirus solutions.
Monitoring	Built-in performance monitoring and capacity planning.

Overview of the FS8600 Hardware

Scale-out NAS consists of one to six FS8600 appliances configured as a FluidFS cluster. Each NAS appliance is a rack-mounted 2U chassis that contains two hot-swappable NAS controllers in an active-active configuration. In a NAS appliance, the second NAS controller with which one NAS controller is paired is called the peer controller. Scale-out NAS supports expansion, that is, you can start with one NAS appliance and add NAS appliances to the FluidFS cluster as needed to increase performance.

NAS appliance numbers start at 1 and NAS controller numbers start at 0. Appliance 1 contains Controller 0 and Controller 1, Appliance 2 contains Controller 2 and Controller 3, and so on. To identify the physical hardware displayed in Storage Manager, you must match the service tag shown in Storage Manager with the service tag printed on a sticker on the front-right side of the NAS appliance.

The following FS8600 appliance configurations are available. All NAS appliances in a FluidFS cluster must use the same configuration—mixing 1GbE and 10GbE, or Fibre Channel and iSCSI, is not supported.

- 1Gb Ethernet client connectivity with 8Gb Fibre Channel back-end connectivity to the Storage Center
- 10Gb Ethernet client connectivity with 8Gb Fibre Channel back-end connectivity to the Storage Center
- 10Gb Ethernet client connectivity with 10Gb Ethernet iSCSI back-end connectivity to the Storage Center

NOTE: There are two RAM configurations for the 10GbE models - 24GB and 48GB, which should not be mixed in the same appliance, but can be mixed in the cluster.

Internal Backup Power Supply

Each NAS controller is equipped with an internal backup power supply (BPS) that protects data during a power failure. The BPS provides continuous power to the NAS controllers for a minimum of 5 minutes in case of a power failure and has sufficient battery power to allow the NAS controllers to safely shut down. In addition, the BPS provides enough time for the NAS controllers to write all data from the cache to nonvolatile internal storage.

The NAS controllers regularly monitor the BPS battery status, which requires the BPS to maintain a minimum level of power for normal operation. To ensure the BPS battery status is accurate, the NAS controllers routinely undergo battery calibration cycles. During a battery calibration cycle, the BPS goes through charge and discharge cycles; therefore, battery error events during this process are expected. A battery calibration cycle takes up to 7 days to complete. If a NAS controller starts a battery calibration cycle, and the peer NAS controller BPS has failed, the NAS controllers enter journaling mode. Entering this mode might impact performance, so you should repair a failed BPS as soon as possible.

Internal Storage

Each NAS controller has an internal storage device that is used only for the FluidFS images and for a cache storage offload location in the event of a power failure. The internal hard drive does not provide the NAS storage capacity.

Internal Cache

Each NAS controller has an internal cache that provides fast reads and reliable writes.

Overview of the FS8600 Architecture

Scale-out NAS consists of these components:

- Hardware
  - FluidFS cluster
  - Storage Center
- NAS appliance network interface connections
  - SAN network

- Internal network
- LAN/client network

The following figure shows an overview of the scale-out FS8600 architecture.

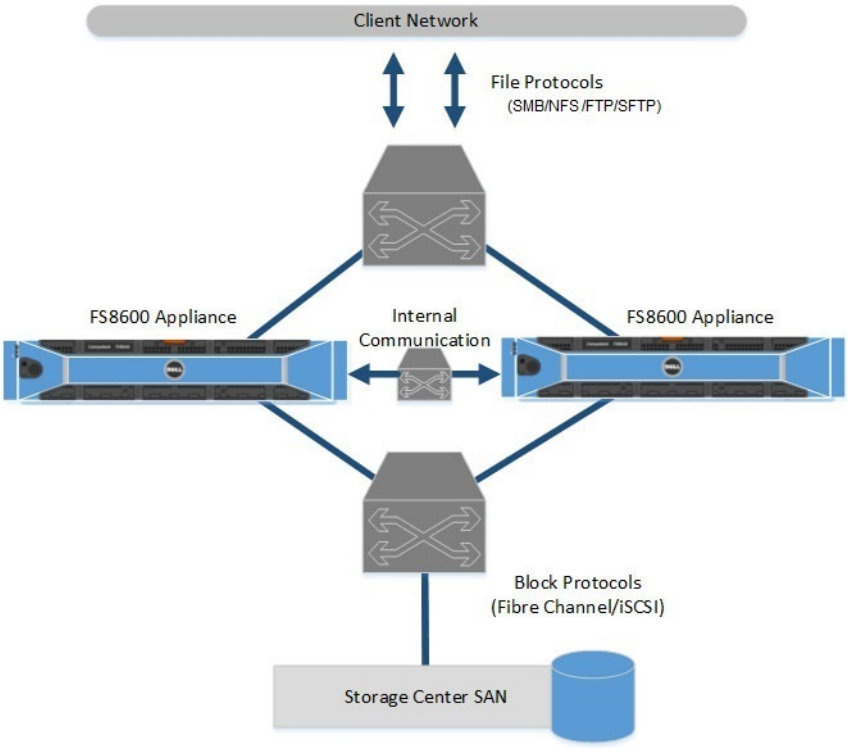


Figure 39. FS8600 Architecture

Storage Center

The Storage Center provides the FS8600 scale-out NAS storage capacity; the FS8600 cannot be used as a standalone NAS appliance. Storage Centers eliminate the need to have separate storage capacity for block and file storage. In addition, Storage Center features, such as Dynamic Capacity and Data Progression, are automatically applied to NAS volumes.

SAN Network

The FS8600 shares a back-end infrastructure with the Storage Center. The SAN network connects the FS8600 to the Storage Center and carries the block-level traffic. The FS8600 communicates with the Storage Center using either the iSCSI or Fibre Channel protocol, depending on which NAS appliance configuration you purchased.

Internal Network

The internal network is used for communication between NAS controllers. Each of the NAS controllers in the FluidFS cluster must have access to all other NAS controllers in the FluidFS cluster to achieve the following goals:

- Provide connectivity for FluidFS cluster creation
- Act as a heartbeat mechanism to maintain high availability
- Enable internal data transfer between NAS controllers
- Enable cache mirroring between NAS controllers
- Enable balanced client distribution between NAS controllers

LAN/Client Network

The LAN/client network is used for client access to the SMB shares, NFS exports, and the FTP landing directory. It is also used by the storage administrator to manage the FluidFS cluster. The FluidFS cluster is assigned one or more virtual IP addresses

(client VIPs) on the client network that allow clients to access the FluidFS cluster as a single entity. The client VIP also enables load balancing between NAS controllers, and ensures failover in the event of a NAS controller failure.

If client access to the FluidFS cluster is not through a router (in other words, a flat network), define one client VIP per NAS controller. If clients access the FluidFS cluster through a router, define a client VIP for each client interface port per NAS controller.

Data Caching and Redundancy

New and modified files are first written to the cache, and then cache data is immediately mirrored to the peer NAS controller (mirroring mode). Data caching provides high performance, while cache mirroring between peer NAS controllers ensures data redundancy. Cache data is ultimately transferred to permanent storage asynchronously through optimized data-placement schemes.

When cache mirroring is not possible, such as a single NAS controller failure or when the BPS battery status is low, NAS controllers write directly to storage (journaling mode).

File Metadata Protection

The FluidFS cluster has several built-in measures to store and protect file metadata (which includes information such as name, owner, permissions, date created, date modified, and a soft link to the file's storage location).

- All metadata updates are recorded constantly to storage to avoid potential corruption or data loss in the event of a power failure.
- Metadata is replicated on two separate volumes.
- Metadata is managed through a separate caching scheme.
- Checksums protect the metadata and directory structure. A background process continuously checks and fixes incorrect checksums.

Load Balancing and High Availability

For availability and performance, client connections are load balanced across the available NAS controllers. Both NAS controllers in a NAS appliance operate simultaneously. If one NAS controller in a NAS appliance fails, clients fail over automatically to the peer controller. When failover occurs, some SMB clients will automatically reconnect to the peer NAS controller. In other cases, an SMB application might fail and you must restart it. NFS clients experience a temporary pause during failover, but client network traffic resumes automatically.

Failure Scenarios

The FluidFS cluster can tolerate a single NAS controller failure without impact to data availability and without data loss. If one NAS controller in a NAS appliance becomes unavailable (for example, because the NAS controller failed, is turned off, or is disconnected from the network), the NAS appliance status is degraded. Although the FluidFS cluster is still operational and data is available to clients, you cannot perform most configuration modifications, and performance might decrease because data is no longer cached.

The impact to data availability and data integrity of a multiple NAS controller failure depends on the circumstances of the failure scenario. Detach a failed NAS controller as soon as possible, so that it can be safely taken offline for service. Data access remains intact as long as one of the NAS controllers in each NAS appliance in a FluidFS cluster is functional.

The following table summarizes the impact to data availability and data integrity of various failure scenarios.

Scenario	System Status	Data Integrity	Comments
Single NAS controller failure	Available, degraded	Unaffected	• Peer NAS controller enters journaling mode • Failed NAS controller can be replaced while keeping the file system online
Sequential dual-NAS controller failure in single NAS appliance cluster	Unavailable	Unaffected	Sequential failure assumes enough time is available between NAS controller failures to write all data from the cache to disk (Storage Center or nonvolatile internal storage)

Scenario	System Status	Data Integrity	Comments
Simultaneous dual-NAS controller failure in single NAS appliance cluster	Unavailable	Lose data in cache	Data that has not been written to disk is lost
Sequential dual-NAS controller failure in multiple NAS appliance cluster, same NAS appliance	Unavailable	Unaffected	Sequential failure assumes enough time is available between NAS controller failures to write all data from the cache to disk (Storage Center or nonvolatile internal storage)
Simultaneous dual-NAS controller failure in multiple NAS appliance cluster, same NAS appliance	Unavailable	Lose data in cache	Data that has not been written to disk is lost
Dual-NAS controller failure in multiple NAS appliance cluster, separate NAS appliances	Available, degraded	Unaffected	• Peer NAS controller enters journaling mode • Failed NAS controller can be replaced while keeping the file system online

Ports Used by the FluidFS Cluster

You might need to adjust your firewall settings to allow traffic on the network ports used by the FluidFS cluster. For a list of ports used by the FluidFS cluster, see the *Dell EMC Fluid File System Support Matrix*.

FluidFS System Management for FS Series Appliances

This section contains information about basic FluidFS cluster system management. These tasks are performed using the Storage Manager Client.

NAS Access

FluidFS supports the Unicode /UTF-8 encoding, allowing concurrent access from any UTF-8 compatible client. All NAS interfaces expect UTF-8 characters for file, folder/directory, share, and other names.

Consequently, all names are internally maintained and managed in UTF-8 format. While individual file and directory names are each limited to 255 bytes, the number of characters might be further limited, due to the variable-width nature of the UTF-8 encoding.

Management Access

Management data items, such as volume names, share names, directory names, user names, description fields, and so on, are all maintained in UTF-8 format.

For CLI access, UTF-8 terminal applications, such as XTERM, should be used. Terminal applications that do not support UTF-8 characters, such as KTERM, are not recommended.

Seamless Session Failover

Seamless session failover decreases the client connection timeout. With seamless session failover, you can easily move a connection between cluster controllers. This feature sends a connection reset packet to the dropped client to immediately terminate a session with a failed controller. The client will then reestablish the session with the new controller and the connection will resume.

Using the Storage Manager Client or CLI to Connect to the FluidFS Cluster

As a storage administrator, you can use either the Storage Manager Client or command-line interface (CLI) to connect to and manage the FluidFS cluster. By default, the FluidFS cluster is accessed through the client network.

Connect to the FluidFS Cluster Using the Storage Manager Client

Log in to the Storage Manager Client to manage the FluidFS cluster.

Prerequisites

The Storage Manager user account must have the Administrator privilege to view, manage, or add FluidFS clusters in the Storage Manager Client.

Steps

1. Start the **Storage Manager Client** application. The Storage Manager Client opens.
2. If the Storage Manager Client welcome page opens, click **Log in to a Storage Center or Data Collector**.
3. In the **User Name** field, type the DSM Data Collector user name.
4. In the **Password** field, type the DSM Data Collector password.
5. In the **Host/IP** field, type the host name or IP address of the server that hosts the Data Collector. If the Data Collector and Client are installed on the same system, you can type `localhost` instead.
6. If you changed the web server port during installation, type the updated port in the **Web Server Port** field.
7. Click **Log In**. The Storage Manager Client connects to the Data Collector and displays the **Storage** view, including FluidFS clusters.

Reconnect to the FluidFS Cluster

If Storage Manager cannot communicate with or log in to a FluidFS cluster, Storage Manager marks the FluidFS cluster as down. Reconnect to the FluidFS cluster to provide the updated connectivity information or credentials.

Steps

1. Click the **Storage** button.
2. In the **Storage** view, select a FluidFS cluster.
3. Click the **Summary** tab.
4. Click **Reconnect to FluidFS Cluster**. The **Reconnect to FluidFS Cluster** dialog box opens.
5. In the **User Name** field, type the FluidFS cluster administrator user name. The default user name is **Administrator**.
6. In the **Password** field, type the FluidFS cluster administrator password. The default password is **Stor@ge!**.
7. Click **OK**.

Connect to the FluidFS Cluster CLI Using a VGA Console

Log in to the CLI using a VGA console to manage the FluidFS cluster. Connect a monitor to a NAS controller's VGA port and connect a keyboard to one of the NAS controller's USB ports.

Steps

1. From the command line, enter the following user-id at the first **login as** prompt:

   ```
   cli
   ```

2. Type the FluidFS cluster administrator user name at the next **login as** prompt. The default user name is **Administrator**.
3. Type the FluidFS cluster administrator password at the ***user_name*'s password** prompt. The default password is **Stor@ge!**. You are logged in to the CLI and a Welcome window opens. The window lists the available commands in the main menu.

Connect to the FluidFS Cluster CLI Through SSH Using a Password

Log in to the CLI through SSH to manage the FluidFS cluster.

Steps

1. Use either of the following options:
   - From Windows using an SSH client, connect to a client VIP. From the command line, enter the following command at the **login as** prompt:

     ```
     cli
     ```

   - From a UNIX/Linux system, enter the following command from a prompt:

     ```
     ssh cli@client_vip_or_name
     ```

2. Type the FluidFS cluster administrator user name at the **login as** prompt. The default user name is **Administrator**.
3. Type the FluidFS cluster administrator password at the ***user_name*'s password** prompt. The default password is **Stor@ge!**. You are logged in to the CLI and a Welcome window opens. The window lists the available commands in the main menu.

Connect to the FluidFS Cluster CLI Using SSH Key Authentication

You can grant trust to a specific machine and user by performing an SSH key exchange.

Steps

1. Generate an RSA SSH key.

   NOTE: The following example uses the **ssh-keygen** utility. The steps to generate an RSA SSH key can vary by operating system. See the documentation for the respective operating system for more information.

   a. Log in to a UNIX/Linux workstation for which you want to use SSH key authentication.
   b. From the command line, enter the following command:

      ```
      ssh-keygen -t rsa
      ```

   c. Press Enter at the **Enter file in which to save the key (/home/*user_name*/.ssh/id_rsa)** prompt.
   d. Press Enter at the **Enter passphrase (empty for no passphrase)** prompt and again at the **Enter same passphrase again** prompt. An SSH key is generated at `/home/user_name/.ssh/id_rsa.pub`.
2. Copy the SSH key to your clipboard.
3. Log in to the FluidFS cluster CLI through SSH using a password.
4. Enter the following command, pasting in the copied SSH key:

   ```
   system administrators passwordless-access add-ssh-keys Administrator add-ssh-keys ssh_key
   ```

   Now you can use the following command to log in to the FluidFS cluster from the workstation without needing a password:

   ```
   ssh fluidfs_administrator_user_name@client_vip_or_name
   ```

   You can also use the following format to run commands from the workstation without needing a password:

   ```
   ssh fluidfs_administrator_user_name@client_vip_or_name cli_command
   ```

Managing Secured Management

By default, all FluidFS cluster management ports are open on all subnets, along with the other ports needed for client access (SMB/NFS/FTP), replication, and NDMP. Secured management, when enabled, exclusively limits all management traffic to one specific subnet. The subnet on which secured management is enabled also has the necessary ports open for client access, replication, FTP, and NDMP traffic. Other subnets will not have any of the management ports listening on them, making them available only for client access, replication, and NDMP traffic. This setup prevents users on client (data) access subnets from accessing any FluidFS cluster management functions.

In FluidFS, the management ports listed in the following table do not participate in SMB/NFS communication, but are exposed on the client network by default. When you enable secured management, you can expose the management ports on a management subnet only.

Service	Port
Web Services	80
Secure Web Services	443
FTP	44421
FTP (Passive)	44430–44439
SSH	22
Storage Manager communication	35451

Secured management can be enabled only after the system is deployed. To make a subnet secure:

- It must exist prior to enabling the secured management feature.
- It can reside on the client network (subnet-level isolation of management traffic) or the LOM (Lights Out Management) Ethernet port (physical isolation of management traffic). The LOM Ethernet port is located on the lower-right side of the back panel of a NAS controller.
- It must be the subnet that you log in from.

Add a Secured Management Subnet

The subnet on which you enable secured management must exist prior to enabling the secured management feature.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**, and then click the **Management Network** tab.
4. In the Management Network panel, click **Edit Settings**.
   The **Modify Administrative Network** dialog box opens.
5. From the **State** drop-down list, select a state to be used for the management network.
   - Select **Restricted** for management functionality to be blocked on other subnets
   - Select **Unrestricted** for management functionality to be available on all subnets.
6. To change the prefix of the network, type a prefix length in the **Prefix** field.
7. In the **Network ID** field, type the ID for the network that you want to modify.
8. Add one or more management VIPs through which the administrator manages the FluidFS cluster.
   a. In the **Virtual IP** field, type a management virtual IP address.
   b. In the box for the **Controller IP Address** field, type a controller IP address and click **Add**. Repeat this step for each controller.
9. To specify a VLAN tag, type a VLAN tag in the **VLAN Tag** field. When a VLAN spans multiple switches, the VLAN tag is used to specify which ports and interfaces to send broadcast packets to.
10. From the **Interface** drop-down list, select the interface on which the secured management subnet is located.
    - Select **Admin** to use the LOM Ethernet port for physical isolation of management traffic. You must also connect a network cable to the LOM Ethernet port of each controller in the first (or only) appliance.
    - Select **Client** for subnet-level isolation of management traffic.
11. Click **OK**.

Change the Secured Management Subnet Interface

Change the interface on which the secured management subnet is located.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**, and then click the **Management Network** tab.
4. In the Management Network panel, click **Edit Settings**. The **Modify Administrative Network** dialog box opens.
5. From the **Interface** drop-down list, select the interface on which the secured management subnet is located.
   - Select **Admin** to use the LOM Ethernet port for physical isolation of management traffic. You must also connect a network cable to the LOM Ethernet port of each controller in the first (or only) appliance..
   - Select **Client** for subnet-level isolation of management traffic.
6. Click **OK**.

Change the Prefix for the Secured Management Subnet

Change the prefix for the secured management subnet.

Steps

1. the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**, and then click the **Management Network** tab.
4. In the Management Network panel, click **Edit Settings**. The **Modify Administrative Network** dialog box opens.
5. In the **Prefix** field, type a prefix for the secured management subnet.
6. Click **OK**.

Change the VLAN Tag for the Secured Management Subnet

When a VLAN spans multiple switches, the VLAN tag is used to specify which ports and interfaces to send broadcast packets to.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**, and then click the **Management Network** tab.
4. In the Management Network panel, click **Edit Settings**. The **Modify Administrative Network** dialog box opens.
5. In the **VLAN Tag** field, type a VLAN tag for the secured management subnet.
6. Click **OK**.

Change the VIP for the Secured Management Subnet

Change the secured management subnet VIP through which an administrator manages the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**, and then click the **Management Network** tab.
4. In the Management Network panel, click **Edit Settings**. The **Modify Administrative Network** dialog box opens.
5. To change a management VIP:
   a. In the **Virtual IP Address** field, type a management virtual IP address.

NOTE: A secured management subnet has a single management VIP.

6. Click **OK**.

Change the NAS Controller IP Addresses for the Secured Management Subnet

To change the NAS controller IP addresses for the secured management subnet when, for example, you go from an unsecured to a secured environment or you physically relocate your equipment:

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**, and then click the **Management Network** tab.
4. In the Management Network panel, click **Edit Settings**. The **Modify Administrative Network** dialog box opens.
5. The Controller IP Addresses are displayed.
6. You can add or remove controller IP addresses by clicking **Add** or **Remove**.
7. Click **OK**.

Enable or Disable Secured Management

Enable secured management to exclusively limit management traffic to one specific subnet.

Prerequisites

- The subnet on which you enable secured management must exist before you enable the secured management feature.
- The FluidFS cluster must be managed by Storage Manager using the subnet on which secured management will be enabled. To manage the FluidFS cluster on the secured management subnet, remove the FluidFS cluster from Storage Manager and then re-add the FluidFS cluster to Storage Manager using the secured management subnet management VIP.

About this task

After enabling secured management, if you are connected to Storage Manager through the secured management subnet, your management session is temporarily interrupted while the change takes effect. During this time, the following message is displayed in Storage Manager:

```
Communication with the cluster was interrupted in process of issuing a command that performs modification to the cluster.
```

After the change takes effect, your management session will resume automatically. Management sessions on all other subnets are disconnected.

Disable secured management to allow management traffic from any subnet.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity** and then click the **Management Network** tab.
4. In the Management Network panel, click **Edit Settings**.
   The **Modify Administrative Network** dialog box opens.
5. Enable or disable secured management.

   From the **State** drop-down list:
   - To enable secured management, select **Restricted** or **Unrestricted**.
   - To disable secured management, select **Disabled**.
6. Click **OK**.

Managing the FluidFS Cluster Name

The FluidFS cluster name is a unique name used to identify the FluidFS cluster in Storage Manager and the name that clients use to access the FluidFS cluster. This name is also the FluidFS cluster NetBIOS name.

If clients access the FluidFS cluster by name (instead of IP address), you must add an entry in the DNS server that associates the FluidFS cluster name to the FluidFS cluster client VIPs. If you are using multiple client VIPs, add all client VIPs to the DNS server and associate them with the same FluidFS cluster name (known as round-robin DNS). This association enables client load balancing between client VIPs.

View the FluidFS Cluster Name

View the current FluidFS cluster name that is displayed in Storage Manager and the name that clients use to access the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab. The FluidFS cluster name is displayed below the tab.

Rename the FluidFS Cluster

Changing the FluidFS cluster name changes the FluidFS cluster name that is displayed in Storage Manager and the name that clients use to access the FluidFS cluster.

Prerequisites

After changing the FluidFS cluster name, you must also make the following adjustments:

- Change the FluidFS cluster name on the DNS server.
- If the FluidFS cluster is joined to an Active Directory domain, leave and then rejoin the FluidFS cluster to the Active Directory domain. If the FluidFS cluster is joined to Active Directory using the old FluidFS cluster name, it might affect the ability of Active Directory users to access the system.

Steps

1. Click the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab.
3. In the FluidFS Cluster Status panel, click **Edit FluidFS Cluster Settings**. The **Edit FluidFS Cluster Settings** dialog box opens.
4. In the **Name** field, type the new name for the FluidFS cluster.
5. Click **OK**.

Accept the End-User License Agreement

You must accept the end-user license agreement (EULA) before using the system. The EULA is initially accepted during deployment, and the EULA approver name and title can be changed at any time.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **License** tab.
5. In the License panel, click **Accept License Agreement**. The **Accept License Agreement** dialog box opens.
6. Read the EULA.
7. In the **Approver Name** field, type your name.
8. In the **Approver Title** field, type your title.

9. Click **OK**.

Managing the System Time

Setting the system time accurately is critical for the proper functioning of the system. Setting the system time enables:

- Windows clients to mount the file system
- Scheduled activities, such as snapshot and replication tasks, to occur at the appropriate time
- The correct time to be recorded in the Event Log
- Time synchronization between the Active Directory authentication server and the FluidFS cluster, which is necessary for Active Directory authentication

You can set the system time using either of the following options:

- **Manually set the time** – Manually set the time for the FluidFS cluster.
- **Automatically synchronize the time with an NTP server** – Network Time Protocol (NTP) synchronizes clocks over a network. If the FluidFS cluster is part of a Windows network, the Active Directory server should serve as the NTP server. If the FluidFS cluster is not part of a Windows network, configure it to synchronize with a local NTP server (if such a server exists) or with an NTP server on the Internet.

View and Configure Time Settings

Provide the correct time information for the FluidFS system. An NTP server is mandatory for working with Active Directory. An NTP server is recommended for accurate snapshot and replication scheduling and for event logging. For this procedure, the time information is copied from the Storage Center setup.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**, and then click the **General** tab.
4. In the Time panel, click **Edit Settings**.
5. Select a time zone from the **Time Zone** drop-down list.
6. Add or remove NTP servers. In the **NTP Servers** field:
   - To add an NTP server, type the host name or IP address of an NTP server in the **NTP Servers** field and then click **Add**.
   - To remove an NTP server, select an NTP server from the **NTP Servers** list and then click **Remove**.
7. If the time displayed in the **Time** field is correct, click **OK**.
8. To change the current time, clear the **Set Time Using NTP Enabled** checkbox.
9. From the **Time** drop-down lists, select the date and time.
10. Click **OK**.

Managing the FTP Server

The FluidFS cluster includes an FTP server that provides a storage location for the following types of system files:

- Diagnostic results files
- License file
- SNMP MIBs and traps
- Service pack files
- Other files for technical support use

Access the FTP Server

The FTP server can be accessed at:

About this task

`ftp://fluidfs_administrator_user_name@client_vip_or_name:44421/`

Example: `ftp://Administrator@172.22.69.32:44421/`

You will be prompted for the FluidFS cluster administrator password.

Enable or Disable the FTP Server

You can enable or disable the FTP server. The FTP server must be enabled if you want to manually upload service packs without using Storage Manager.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Support** tab.
5. In the FTP Accessibility for Support panel, click **Edit Settings**. The **Modify FTP Accessibility for Support Settings** dialog box opens.
6. Enable or disable the FTP server:
   - To enable the FTP server, select the **FTP Enabled** checkbox.
   - To disable the FTP server, clear the **FTP Enabled** checkbox.
7. Click **OK**.

Managing SNMP

Simple Network Management Protocol (SNMP) is one way to monitor the health of the system and generate alert messages (SNMP traps) for system problems. To use SNMP, the FluidFS cluster-specific Management Information Bases (MIBs) and traps must be compiled into a customer-provided SNMP management station. The MIBs are databases of information that is specific to the FluidFS cluster.

FluidFS supports SNMP v3 (read requests) and v2, but does not support using both versions at the same time. SNMP v3 requires user authentication.

Obtain SNMP MIBs and Traps

The SNMP MIBs and traps for the FluidFS cluster are available for download from the FluidFS cluster FTP server.

Prerequisites

The FTP server must be enabled.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **SNMP** tab, and click the **Download MIB File** link.
5. Use the browser dialog box to begin the download process.
6. Click .

   Optionally, you can also download the SNMP MIBs and traps from:

   `ftp://`*`fluidfs_administrator_user_name`*`@`*`client_vip_or_name`*`:44421/mibs/`

Enable or Disable SNMP Traps

Enable or disable SNMP traps by category (NAS Volumes, Access Control, Performance & Connectivity, Hardware, System, or Auditing). For enabled SNMP traps, specify the severity of events for which to send SNMP traps.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **SNMP** tab.
5. In the **Events to Send SNMP Traps** panel, click **Edit Settings**. The **Modify Events Filtering** dialog box opens.
6. In the dialog box, select all checkboxes that apply to enable those traps.
7. To disable any SNMP traps, clear the appropriate checkbox.
8. Select the severity of the events (**Major** or **All**) from the drop-down lists.
9. Click **OK**.

Change the SNMP Version

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **SNMP** tab.
5. In the **SNMP MIB Access** panel, click **Edit Settings**. The **Modify SNMP MIB Access** dialog box opens.
6. In the **Read Version** field, type the version you want to change SNMP to.
7. In the **Trap Version** field, type the version you want to change SNMP to.
8. Click **OK**.

Change the SNMP Read-Only Community

Change the read-only community for devices reading SNMP variables from the FluidFS cluster. By default, the read-only community is **FluidFS**.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **SNMP** tab.
5. In the **SNMP MIB Access** panel, click **Edit Settings**. The **Modify SNMP MIB Access** dialog box opens.
6. In the **Read Only Community** field, type a read-only community name.
7. Click **OK**.

Change the SNMP Trap System Location or Contact

Change the system location or contact person for FluidFS cluster-generated SNMP traps. By default, the SNMP trap system location and contact person are **unknown**.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.

4. Click the **SNMP** tab.
5. In the **SNMP Trap** panel, click **Modify SNMP Trap**. The **Modify SNMP Trap Settings** dialog box opens.
6. Change the SNMP trap system location or contact:
   - To specify a description for the location of the FluidFS cluster, type a location in the **System Location** field.
   - To specify the name of the SNMP contact person, type a contact name in the **System Contact** field.
7. Click **OK**.

Add or Remove SNMP Trap Recipients

Add or remove hosts that receive the FluidFS cluster-generated SNMP traps.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **SNMP** tab.
5. In the **SNMP Trap** panel, click **Modify SNMP Trap**. The **Modify SNMP Trap Settings** dialog box opens.
6. Add or remove SNMP trap recipients:
   - To add an SNMP trap recipient, type a host name or IP address in the **Trap Recipients** field and click **Add**.
   - To remove an SNMP trap recipient, select an SNMP trap recipient and click **Remove**.
7. Click **OK**.

Managing the Health Scan Throttling Mode

Health scan throttling has three modes:

- **Normal** (default mode) – Health scan is running and scanning the file system to identify potential errors.
- **Maintenance** – Health scan is running in high priority and scanning the file system to identify potential errors.
- **Off** – Health scan is off and will not run.

NOTE: Keep the health scan throttling mode set to Normal unless specifically directed otherwise by Dell Technical Support.

Change the Health Scan Settings

If enabled, the Health Scan background process will scan the file system to identify potential errors..

Steps

1. In the **Storage** view, select a FluidFS cluster
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Internal** tab.
5. In the Advanced panel, click **Modify Health Scan Settings**. The **Modify Health Scan Settings** dialog box opens.
6. To enable health scan, select the **Enabled** checkbox.
7. To disable health scan, clear the **Enabled** checkbox.
8. From the **Scanning Mode** drop-down list, select Normal or Intensive.
9. Click **OK**.

Managing the Operation Mode

The FluidFS cluster has three operation modes:

- **Normal** – System is serving clients using SMB and NFS protocols and operating in mirroring mode.

- **Write-Through** – System is serving clients using SMB and NFS protocols, but is forced to operate in journaling mode. This mode of operation might have an impact on write performance. It is recommended when, for example, you have repeated electric power failures.
- **No Service** – System is not serving clients using SMB or NFS protocols and allows limited management capabilities. This mode must be selected before replacing a NAS appliance.

View or Change the Operation Mode

Changing the operation mode might affect the accessibility and performance of SMB shares and NFS exports.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Internal** tab.
5. In the Advanced panel, click **Modify Operation Mode**. The **Modify Operation Mode** dialog box opens.
6. Select a new operation mode (Normal, Write-Through, or No Service).
7. Click **OK**.

Managing Client Connections

The following options are available for managing client connections:

- Display the distribution of clients between NAS controllers
- Assign a client to a NAS controller
- Manually migrate clients to another NAS controller
- Fail back clients to their assigned NAS controller
- Rebalance client connections across NAS controllers

Display the Distribution of Clients Between NAS Controllers

Display the current distribution of clients between NAS controllers.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Clients and Routers** tab. The Filters panel displays the NAS controller and interface to which each client is connected.

View Clients Assigned to a NAS Controller

View clients that are currently assigned to a particular NAS controller.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Clients and Routers** tab. The panel displays the NAS controller and interface to which each client is connected.

Assign or Unassign a Client to a NAS Controller

You can permanently assign one or more clients to a particular NAS controller. For effective load balancing, do not manually assign clients to NAS controllers, unless specifically directed to do so by Dell Technical Support. Assigning a client to a NAS controller disconnects the client's connection. Clients will then automatically reconnect to the assigned NAS controller.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Clients and Routers** tab and select a client or router IP.
5. In the Filters panel, click **Pin**. The **Pin Client to NAS Controller** dialog box opens.
6. To assign a client to a NAS controller:
   a. From the **Pin Client to** drop-down list, select the NAS controller to which to assign the client.
   b. From the **Use Client Interface** drop-down list, select the client interface on the NAS controller to which to assign the client.
7. Click **OK**.

Manually Migrate Clients to Another NAS Controller

You can manually migrate clients between NAS controllers if, for example, the network load on the NAS controllers is not balanced. Migrating a client to another NAS controller disconnects the client's connection. Clients will then automatically reconnect to the NAS controller to which they were migrated.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. In the Filters panel, select a client and then click **Move**. The **Move Client to NAS Controller** dialog box opens.
5. From the **Move Client to** drop-down list, select the NAS controller to which to migrate the client.
6. Click **OK**.

Fail Back Clients to Their Assigned NAS Controller

You must fail back client connections to their original NAS controller when a NAS controller that was down becomes available. Failing back client connections disconnects only the client connections that failed over due to the original NAS controller failure. Those clients will then automatically reconnect to the assigned NAS controller.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. In the Filters panel, click **Failback**. The **Failback Clients** dialog box opens.
5. Click **OK**.

Rebalance Client Connections Across NAS Controllers

Rebalancing client connections evenly distributes connections across all the available NAS controllers.

About this task

You must rebalance client connections in the following situations:

- After FluidFS cluster hardware changes (for example, adding a NAS appliance)

- When a NAS controller that was down becomes available

Rebalancing client connections disconnects all client connections. Clients will then automatically reconnect to the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. In the Filters panel, click **Rebalance**. The **Rebalance Clients** dialog box opens.
5. Click **OK**.

Shutting Down and Restarting NAS Controllers

In some cases, you must temporarily shut down a FluidFS cluster or reboot a NAS controller.

Shut Down the FluidFS Cluster

In some cases, you might need to temporarily shut down all NAS controllers in a FluidFS cluster. For example, you might need to shut down the controllers if you are moving the NAS hardware to a different location. When a FluidFS cluster is shut down, NAS volume data is no longer available to clients, and clients are disconnected.

Prerequisites

Schedule a maintenance window and inform clients that the resources hosted by the FluidFS cluster will be unavailable.

CAUTION: Follow the procedure exactly to prevent data inconsistency.

Steps

1. Change the FluidFS cluster operation mode to **No Service**:
   a. In the File System view, select **Cluster Maintenance**.
   b. Click the **Internal** tab
   c. In the Advanced panel, click **Modify Operation Mode**. The **Modify Operation Mode** dialog box opens.
   d. Select **No Service** and click **OK**.
2. Press and release the recessed power button at the back of each NAS controller to shut down the controllers.

   NOTE: Do not hold the power button down.

Start Up the FluidFS Cluster

Start up a FluidFS cluster to resume operation after shutting down all NAS controllers in a FluidFS cluster.

Prerequisites

Before turning on the system, ensure that all cables are connected and all components are connected to a power source.

Steps

1. If previously shut down, turn the Storage Centers back on before starting the FluidFS cluster.
2. Press and release the recessed power button at the back of each NAS controller to turn on the controllers. Wait about 15 minutes for the cluster to come up and be manageable.
3. Change the FluidFS cluster operation mode to **Normal**:
   a. In the File System view, select **Cluster Management**.
   b. Click the **Internal** tab.
   c. In the Advanced panel, click **Modify Operation Mode**. The **Modify Operation Mode** dialog box opens.
   d. Select **Normal** and then click **OK**.

Reboot a NAS Controller

Only one NAS controller can be rebooted in a NAS appliance at a time. Rebooting a NAS controller disconnects client connections while clients are being transferred to other NAS controllers. Clients will then automatically reconnect to the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Appliances** panel, select a controller.
4. Click **Reboot**. The **Reboot** dialog box opens.
5. Click **OK**.

Managing NAS Appliance and NAS Controller Blinking

You can make the system identification button on a NAS appliance or NAS controller blink to easily locate that particular NAS appliance or NAS controller within a rack. The system identification button for a NAS appliance is located on the front panel and is labeled . The system identification button for a NAS controller is located on the back panel and is labeled .

Enable or Disable NAS Appliance Blinking

When NAS appliance blinking is enabled, the system identification button blinks so you can easily locate the NAS appliance within a rack.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Appliances** panel, select a NAS appliance.
4. Right-click on the appliance name and select **Blink** from the list box. The **Blink** dialog box opens.
5. Enable or disable NAS appliance blinking:
   - To enable NAS appliance blinking, select **Blink this appliance**.
   - To disable NAS appliance blinking, select **Stop blinking this appliance**.
6. Click **OK**.

Enable or Disable NAS Controller Blinking

When NAS controller blinking is enabled, the system identification button blinks so you can easily locate the NAS controller within a rack.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Controllers** panel, select a NAS controller.
4. Right-click on the controller and select **Blink** from the list box. The **Blink** dialog box opens.
5. Enable or disable NAS controller blinking:
   - To enable NAS controller blinking, select **Blink controller in slot 1** or **Blink controller in slot 2**.
   - To disable NAS controller blinking, clear **Blink controller in slot 1** or **Blink controller in slot 2**.
6. Click **OK**.

Validate Storage Connections

Validating storage connections gathers the latest server definitions on the FluidFS cluster and makes sure that matching server objects are defined on the Storage Centers providing the storage for the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the toolbar, click **Actions**→ **Storage Centers**→ **Validate Storage Connections**. The **Validate Storage Connections** dialog box opens.
4. Click **OK**.

FluidFS Networking

This section contains information about managing the FluidFS cluster networking configuration. These tasks are performed using the Storage Manager Client.

Managing the Default Gateway

The default gateway enables client access across subnets. Only one default gateway can be defined for each type of IP address (IPv4 or IPv6). If client access is not through a router (a flat network), a default gateway does not need to be defined.

View the Default Gateway

View the current default gateway.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab. The Static Route panel displays the default gateway.

Change the Default Gateway

Change the default gateway if it changes for the network.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**, and click the **Client Network** tab.
4. In the Static Route panel, click **Configure Default Gateway**. The **Configure Default Gateway** dialog box opens.
5. In the **Default IPv*n* Gateway** field, type a new default gateway IP address.

   To provide a default gateway for IPv4 and IPv6 addresses, you need a client subnet of the appropriate type that contains the default gateway.
6. Click **OK**.

Managing DNS Servers and Suffixes

Domain Name Service (DNS) is a networking service that enables users to locate computers by providing name-to-IP address and IP address-to-name resolution services. You can configure one or more external DNS servers (external to the FluidFS

cluster but within the site) to be used for name resolution. A DNS suffix specifies a DNS domain name without the host part of the name (for example, west.example.com rather than computer1.west.example.com).

If clients access the FluidFS cluster by name, you must add an entry in the DNS server that associates the FluidFS cluster name to the FluidFS cluster client VIPs. If you are using multiple client VIPs, add all client VIPs to the DNS server and associate them with the same FluidFS cluster name (known as round-robin DNS). This association enables client load balancing between client VIPs. In addition, you must configure DNS if you are using Active Directory, and the DNS servers must be the same DNS servers that your Active Directory domain controllers use.

View DNS Servers and Suffixes

View the current DNS servers providing name resolution services for the FluidFS cluster and the associated DNS suffixes.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**. The **DNS** panel displays the DNS servers and suffixes.

Add or Remove DNS Servers and Suffixes

Add one or more DNS servers to provide name resolution services for the FluidFS cluster and add associated DNS suffixes. Adding multiple DNS servers and suffixes ensures continued name resolution services in the event of a DNS server failure. If the FluidFS cluster cannot establish contact with the preferred server, it will attempt to connect to the remaining servers in order. Remove a DNS server or DNS suffix if it is no longer available or used.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. In the DNS panel, click **Edit Settings**. The **Edit DNS Settings** dialog box opens.
5. To add a DNS server, type the IP address of a DNS server in the **DNS Servers IP Addresses** field and then click **Add**.
6. To remove a DNS server, select it from the **DNS Server IP Addresses** field and click **Remove**.
7. To add a DNS suffix, type the DNS suffix in the **DNS Suffixes** field and then click **Add**.
8. To remove a DNS suffix, select it from the **DNS Suffixes** field and click **Remove**.
9. Click **OK**.

Change the Order of Preference for DNS Servers and Suffixes

Change the order of preference for a DNS server or DNS suffix. If the FluidFS cluster cannot establish contact with the preferred server, it will attempt to connect to the remaining servers in order.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. In the DNS panel, click **Edit Settings**. The **Edit DNS Settings** dialog box opens.
5. DNS servers are listed in descending order of preference.
   - To increase the order of preference for a DNS server, select a DNS server and click **Up**.
   - To decrease the order of preference for a DNS server, select a DNS server and click **Down**.
6. DNS suffixes are listed in descending order of preference.
   - To increase the order of preference for a DNS suffix, select a DNS suffix and click **Up**.
   - To decrease the order of preference for a DNS suffix, select a DNS suffix and click **Down**.
7. Click **OK**.

Managing Static Routes

To minimize hops between routers, static routes are recommended in routed networks when the FluidFS cluster has multiple direct paths to various routers. Static routes allow you to configure the exact paths through which the system communicates with various clients on a routed network.

Consider the network shown in the following figure. The system can have only one default gateway. Assume that router X is designated as the default gateway. Packets that are sent to clients in subnet Y are routed to router X, and are then sent back (through the switch) to router Y. These packets travel through router X needlessly, reducing the throughput to all subnets in the network.

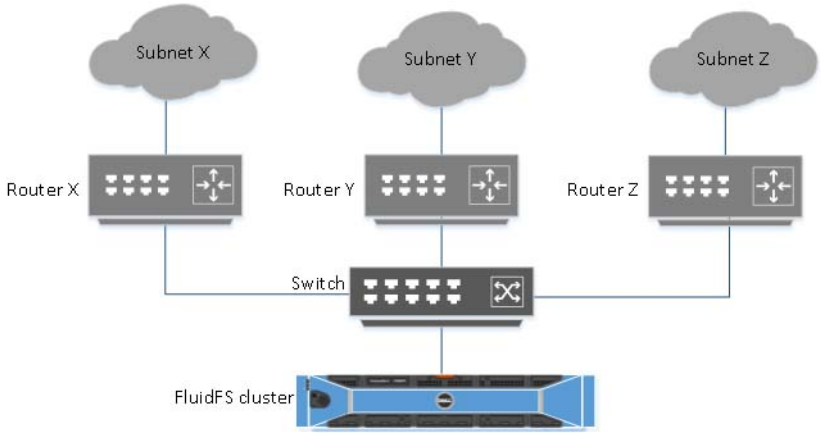


Figure 40. Routed Network

The solution is to define, in addition to a default gateway, a specific gateway for certain subnets by configuring static routes. To configure these routes, you must describe each subnet in your network and identify the most suitable gateway to access that subnet.

Static routes do not have to be designated for the entire network—a default gateway is most suitable when performance is not an issue. You can select when and where to use static routes to best meet performance needs.

View the Static Routes

View the current static routes.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab. The **Static Route** panel displays the static routes.

Add a Static Route

When adding a static route, you must specify the subnet properties and the gateway through which to access this subnet.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab.
5. In the Static Route panel, click **Create Static Route**. The **Create Static Route** dialog box opens.
6. In the **Target Network IP Address** field, type a network IP address (for example, 192.0.2.27).
7. In the **Netmask or Prefix Length** field, type a netmask (for example, 255.255.255.0).

8. In the **Gateway IP Address** field, type the gateway IP address through which to access the subnet (for example, 192.0.2.30).
9. Click **OK**.

Change the Gateway for a Static Route

Change the gateway through which to access the subnet for a static route.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab.
5. In the Static Route panel, click **Configure Default Gateway**. The **Configure Default Gateway** dialog box opens.
6. In the **Default Gateway IPv*n* Address** field, type the gateway IP address through which to access the subnet (for example, 192.0.2.25).
7. Click **OK**.

Delete a Static Route

Delete a static route to send traffic for a subnet through the default gateway instead of a specific gateway.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab.
5. In the Static Route panel, click **Delete Default Gateway**. The **Delete Default Gateway** dialog box opens.
6. Click **OK**.

Managing the Client Networks

The client networks define the client VIPs through which clients access SMB shares and NFS exports. To ensure effective load balancing, use the following recommendations to determine the number of client VIPs to define:

- If client access to the FluidFS cluster is not through a router (in other words, a flat network), define one client VIP per FluidFS cluster.
- If clients access the FluidFS cluster through a router, define a client VIP for each client interface port per NAS controller.

View the Client Networks

View the current client networks.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab. The **Client Network** panel displays the client networks.

Create a Client Network

Create a client network on which clients will access SMB shares and NFS exports.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab.
5. In the Client Network panel, click **Create Client Network**. The **Create Client Network** dialog box opens.
6. In the **Netmask or Prefix Length** field, type a netmask or prefix for the client network.
7. In the **VLAN Tag** field, type a VLAN tag.
   When a VLAN spans multiple switches, the VLAN tag specifies which ports and interfaces to send broadcast packets to.
8. Add an IP address for each NAS controller:
   a. Select a NAS controller and click **Edit Settings**. The **Edit Controller IP Address** dialog box opens.
   b. In the **IP Address** field, type an IP address for the NAS controller.
   c. Click **OK**.
   d. Repeat these steps for each NAS controller.
9. In the **Comment** field, type any additional information.
10. Click **OK**.

Change the Prefix for a Client Network

Change the prefix for a client network.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab.
5. In the Client Network panel, select a client network and then click **Edit Settings**. The **Edit Client Network Settings** dialog box opens.
6. In the **Prefix Length** field, type a prefix for the client network.
7. Click **OK**.

Change the VLAN Tag for a Client Network

Change the VLAN tag for a client network. When a VLAN spans multiple switches, the VLAN tag is used to specify which ports and interfaces to send broadcast packets to.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. Click the **Client Network** tab.
4. In the Client Network panel, select a client network and then click **Edit Settings**. The **Edit Client Network Settings** dialog box opens.
5. In the **VLAN Tag** field, type a VLAN tag for the client network.
6. Click **OK**.

Change the Client VIPs for a Client Network

Change the client VIPs through which clients will access SMB shares and NFS exports.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, expand **Tenants** and select a tenant.
4. Select **Client Accessibility**.
5. In the right pane, select the **DNS and Public IPs** tab. In the Public IPs pane, click **Edit Settings**. The **Edit Public IPs Settings** dialog box appears.
6. To add a client VIP:
   a. In the **VIP** area, enter a client virtual IP address in the box next to Add, and then click **Add**.
   b. Click **OK**.
7. To remove a client VIP:
   a. Select a client VIP.
   b. Click **Remove**.

   NOTE: A client network must have at least one client VIP.
8. Click **OK**.

Change the NAS Controller IP Addresses for a Client Network

Change the NAS controller IP addresses for a client network.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab.
5. In the Client Network panel, click **Edit Settings**. The **Edit Client Network Settings** dialog box opens.
6. In the NAS Controllers IP Addresses field, select a NAS controller and then click **Edit Settings**. The **Edit Controller IP Address** dialog box opens.
7. In the **IP Address** field, type an IP address for the NAS controller.
8. Click **OK**.

Delete a Client Network

Delete a client network if clients no longer need to access SMB shares and NFS exports on that network. You cannot delete the Primary subnet.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Client Network** tab.
5. In the Client Network panel, select a client network and then click **Delete**. The **Delete** dialog box opens.
6. Click **OK**.

View the Client Network MTU

View the current maximum transmission unit (MTU) of the client network.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Network Interfaces** tab. The **Client Interface** panel displays the MTU.

Change the Client Network MTU

Change the maximum transmission unit (MTU) of the client network to match your environment.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Network Interfaces** tab.
5. In the Client Interfaces panel, click **Edit Settings**. The **Modify Client Interface Settings** dialog box opens.
6. In the **MTU** field, type a new MTU. If your network hardware supports jumbo frames, use 9000; otherwise, use 1500.
7. Click **OK**.

View the Client Network Bonding Mode

View the current bonding mode (Adaptive Load Balancing or Link Aggregation Control Protocol) of the client network interface.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Network Interfaces** tab.
5. The **Client Interface** panel displays the bonding mode.

Change the Client Network Bonding Mode

Change the bonding mode (Adaptive Load Balancing or Link Aggregation Control Protocol) of the client network interface to match your environment.

Prerequisites

- If you have ALB, use one client VIP per client port in the FluidFS cluster.
- If you have LACP, use one client VIP per NAS controller in the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. Click the **Network Interfaces** tab.
5. In the Client Interface panel, click **Edit Settings**. The **Modify Client Interface Settings** dialog box opens.
6. From the **Mode** drop-down list, select a bonding mode (ALB or LACP).
7. Click **OK**.

About Multichannel

Multichannel is a feature of the SMB 3.0 protocol which allows the client to bind a single session to multiple connections. Multichannel provides the following benefits:

Increased Throughput – The file server can simultaneously transmit more data using multiple connections for high speed network adapters or multiple network adapters.

Network Fault Tolerance – When using multiple network connections at the same time, the clients can continue to work uninterrupted despite the loss of a network connection.

Automatic Configuration – SMB Multichannel automatically discovers the existence of multiple available network interfaces and dynamically adds connections as required.

Multichannel can be enabled and disabled from the CLI using the command `CLI > (tenant) internal protocols-settings SMB-settings edit`.

Multichannel Requirements

Multichannel requires the following:

Hardware – On both the client and the server, multichannel requires multiple NICs or a NIC configured with RSS (Receive Side Scaling).

Operating System – FluidFS supports multichannel on Windows 8 or Windows Server 2012 and 2016.

By default, the Windows client opens one connection per non-RSS NIC and up to four connections per RSS capable NIC.

Enable or Disable SMB Multichannel

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Protocols** tab.
5. In the SMB Protocol panel, click **Edit Settings**.
   The **Edit Settings** dialog box opens.
6. Click the **Advanced** tab.
7. Enable or disable SMB multichannel:
   - To enable SMB multichannel, select the **SMB Multichannel Enabled** checkbox.
   - To disable SMB multichannel, clear the **SMB Multichannel Enabled** checkbox.
8. Click **OK**.

Viewing the Fibre Channel WWNs

Storage Manager displays the NAS controller World Wide Names (WWNs) needed for updating fabric zoning on your Fibre Channel switch.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Hardware** view, expand **Appliances** → **NAS appliance ID** → **NAS controller ID**, then select **Interfaces**. The WWNs for the NAS controller are displayed in the right pane in the **Fibre Channel** list.

Managing iSCSI SAN Connectivity

iSCSI SAN subnets (Storage Center fault domains) or "fabrics" are the network connections between the FluidFS cluster and the Storage Center. The SAN network consists of two subnets, named SAN and SANb. The FluidFS cluster iSCSI SAN configuration can be changed after deployment if your network changes.

Add or Remove an iSCSI Port

Add a Storage Center iSCSI control port for each connected subnet (Storage Center fault domain).At least one iSCSI port must remain configured. If only one iSCSI port is configured, you will not be able to remove it.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **NAS Pool** tab.
3. Click the **Network** tab.
4. To add an iSCSI port:
   a. Click **Add iSCSI Ports**. The **Add iSCSI Portal** dialog box opens.
   b. Fill in the **IP Address** and **Description** fields.
   c. Click **OK**.
5. To remove a port:
   a. Select the port in the iSCSI Portals panel and then click **Delete**. The **Remove iSCSI Portal** dialog box opens.
   b. Click **OK**.
6. Click **OK**.

Add or Remove an iSCSI Fabric

The FluidFS cluster requires two iSCSI subnets (Storage Center fault domains) or "fabrics."

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **NAS Pool** tab.
3. Click the **Network** tab.
4. To add an iSCSI fabric:
   a. In the iSCSI Fabrics panel, click **Add iSCSI Fabric**. The **Add iSCSI Fabric** dialog box opens.
   b. In the **Appliance ID** field, select an ID from the drop-down list.
   c. In the **Interface** field, select an interface from the drop-down list.
   d. Type in the appropriate information in the **Netmask** and **VLAN Tag** fields.
   e. To add the controller IP addresses, select a controller from the list of controllers and then click **Edit Settings**. The **Edit Controller IP Address** dialog box opens.
   f. In the **IP Address** field, type in the address for the controller and then click **OK**.
   g. Repeat these steps for each controller.
   h. Click **OK** to close the Edit dialog box.
5. Click **OK**.
6. To remove a fabric:
   a. In the iSCSI Fabrics panel, select the appliance and then click **Delete**. The **Delete** dialog box opens.
   b. Click **OK**.

Change the VLAN Tag for an iSCSI Fabric

Change the VLAN tag for an iSCSI fabric. When a VLAN spans multiple switches, the VLAN tag specifies which ports and interfaces to send broadcast packets to.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **NAS Pool** tab.
3. Click the **Network** tab.
4. In the iSCSI Fabrics panel, select an appliance and then click **Edit Settings**. The **Modify Settings for Fabric SAN** dialog box opens.
5. In the **VLAN Tag** field, type the new VLAN tag for the iSCSI fabric.
6. Click **OK**.

Change the NAS Controller IP Addresses for an iSCSI Fabric

Change the NAS controller IP addresses for an iSCSI fabric.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Network** tab.
3. In the iSCSI Fabrics panel, select an appliance and then click **Edit Settings**. The **Modify Settings for Fabric SAN** dialog box opens.
4. Select a controller from the list of controllers and then click **Edit Settings**. The **Edit Controller IP Address** dialog box opens.
5. In the **IP Address** field, type in the address for the controller and then click **OK** to close the Edit dialog box.
6. Click **OK**.

FluidFS Account Management and Authentication

This section contains information about managing FluidFS cluster accounts and authentication. These tasks are performed using the Storage Manager Client.

Account Management and Authentication

FluidFS clusters include two types of access:

- Administrator-level access for FluidFS cluster management
- Client-level access to SMB shares, NFS exports, and FTP folder

Administrator accounts control administrator-level access. Users and groups control client-level access to SMB shares and NFS exports.

The FluidFS cluster supports administrator-level and client-level authentication for both local and remote users and groups:

- **Local users and groups** – User and group identities defined and managed on and by the FluidFS system. Local management is useful when you have only a limited number of users and groups. In addition, authentication does not depend on external servers.
- **External users and groups** – User and group identities defined and managed on and by an external repository. External management is useful when managing access of many users and groups to many different resources, but depends on the availability of the external database. FluidFS supports the following external identity repositories:
  - **Active Directory** – Configure the FluidFS cluster to access an Active Directory database to authenticate Windows users.

    NOTE: Active Directory can also be used as an LDAP database for UNIX/Linux users.
  - **NIS or LDAP** – Configure the FluidFS cluster to access an NIS or LDAP database to authenticate UNIX and Linux users.

NOTE:

- Local and external users can be used simultaneously.
- If you configure Active Directory and either NIS or LDAP, you can set up mappings between the Windows users in Active Directory and the UNIX and Linux users in LDAP or NIS to allow one set of credentials to be used for both types of data access.

Default Administrative Accounts

The FluidFS cluster has the following built-in administrative accounts, each of which serves a particular purpose.

Login Name	Purpose	SSH Access Enabled by Default	SSH Access Allowed	VGA Console Access Enabled by Default	VGA Console Access Allowed	Default Password
Administrator	FluidFS cluster management (not a UNIX or Linux user)	Yes	Yes	Yes	Yes	Stor@ge!
support	FluidFS cluster troubleshooting (regular UNIX or Linux user)	No	Yes	No	Yes	None (must be set by Administrator)
enableescalationaccess	Enable escalation account	No	No	Yes	Yes	
escalation	FluidFS cluster troubleshooting when unable to log in with support account	No	Yes	No	Yes	
cli	Gateway to command– line interface access	Yes (can bypass password using SSH key)	Yes (can bypass password using SSH key)	N/A	N/A	N/A

Administrator Account

The Administrator account is used for FluidFS cluster management and provides access to Storage Manager and the FluidFS CLI. This account cannot be removed or renamed, and has write permissions on all NAS volumes, folders, and files.

Support Account

The support account is used by technical support when accessing the FluidFS system. The support account and password are managed by the system administrator.

CAUTION: Operations performed as the support user are for advanced remote troubleshooting to resolve critical system issues only. Misuse of this account can damage the FluidFS cluster and its data.

NOTE: For strict security, enable the support account just before a remote troubleshooting session and disable it immediately after the troubleshooting session.

Enable or Disable the Support Account

Enable the support account to allow remote troubleshooting. When troubleshooting is complete, disable the support account.

Steps

1. In the **Storage** view, select a FluidFS cluster.

2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Support** tab.
5. In the **Local Support Access** panel, click **Modify Local Support Access Settings**. The **Modify Local Support Access Settings** dialog box opens.
6. Enable or disable SupportAssist:
   - To enable SupportAssist, select the **Support Account ("support")** checkbox.
   - To disable SupportAssist, clear the **Support Account ("support")** checkbox.
7. Click **OK**.

Change the Support Account Password

Change the support account password to a new, strong password after each troubleshooting session is concluded.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Support** tab.
5. In the **Local Support Access** panel, click **Change Local Support Access Password**. The **Change Local Support Access Password** dialog box opens.
6. In the **Password** field, type a password. The password must be between 8 and 14 characters long and contain three of the following elements: a lowercase character, an uppercase character, a digit, or a special character (such as +, ?, or *).
7. In the **Confirm Password** field, retype the password.
8. Click **OK**.

Enable or Disable SupportAssist

You can enable Storage Client to send the FluidFS cluster diagnostics using SupportAssist.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Support** tab.
5. In the **SupportAssist** panel, click **Modify SupportAssist Settings**. The **Modify SupportAssist Settings** dialog box opens.
6. Enable or disable SupportAssist:
   - To enable SupportAssist, select the **SupportAssist Enabled** checkbox.
   - To disable SupportAssist, clear the **SupportAssist Enabled** checkbox.
7. Click **OK**.

CLI Account

The cli account is used with an administrator account to access the command-line interface of the FluidFS cluster.

Default Local User and Local Group Accounts

The FluidFS cluster has the following built-in local user and local group accounts, each of which serves a particular purpose.

Account Type	Account Name	Purpose
Local User	Administrator	Account used for FluidFS cluster management
Local User	nobody	Account used for guest users
Local Group	Administrators	• Accommodates the Administrator account, and all other (local and remote) administrator users • BUILTIN domain group fully compatible with the Windows Administrators group
Local Group	nobody_group	Accommodates the nobody account
Local Group	Local Users	Accommodates local user accounts
Local Group	Users	BUILTIN domain group fully compatible with the Windows Users group
Local Group	Backup Operators	BUILTIN domain group fully compatible with the Windows Backup Operators group

Managing Administrator Accounts

You can create both local FluidFS administrators and make remote users (AD/LDAP/NIS) FluidFS administrators. System alerts will be sent to the email address specified for the administrator.

When creating an administrator, you specify an administrator permission level. The permission level defines the set of actions that are allowed by the administrator. Permission levels are predefined in the system as follows:

- **NAS Cluster Administrator** – The administrator can manage any aspect of the FluidFS cluster.
- **NAS Volume Administrator** – The volume administrator can change the following settings for the NAS volumes to which they are assigned:
  - NAS volume name
  - NAS volume folder to which the NAS volume is assigned
  - Access time granularity
  - Permissions interoperability
  - Report zero disk usage
  - Data reduction
  - NAS volume space settings and alert thresholds
  - SMB shares and NFS exports
  - Snapshots and snapshot schedules
  - Restore NAS volume from snapshot
  - Restore NAS volume configuration
  - Quotas
- The volume administrator can view, but not change, the rest of the FluidFS cluster configuration.
  - NAS volume clones
  - Replication

View Administrators

View the current list of administrator accounts.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Mail & Administrators** tab. The **Administrators** panel displays the current list of administrators.

Add an Administrator

Add an administrator account to manage the FluidFS cluster using the Storage Manager Client and CLI. You can define only those administrators with permission levels that are hierarchically lower than your own.

Prerequisites

Before you can create a local administrator, you must create a local user who will become an administrator.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. In the **Local Users** panel, click **Create**. The **Create Local User** dialog box opens.
6. Select a user to become an administrator:
   a. In the **File System** view, select **Cluster Maintenance**.
   b. Click the **Mail & Administrators** tab.
   c. In the **Administrators** panel, click **Grant Administration Privilege**. The **Grant Administration Privilege** dialog box opens.
   d. Click **Select User**. The **Select User** dialog box opens.
   e. From the **Domain** drop-down list, select the domain to which the user belongs.
   f. In the **User** field, type either the full name of the user or the beginning of the user name.
   g. To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list
   h. Click **Search**.
   i. Select a user from the search results and click **OK**.
   j. Click **OK**.
7. Select the **Global Administration Permission Enabled** checkbox.
8. In the **Email Address** field, type an email address for the administrator.
9. Click **OK**.

Assign NAS Volumes to a Volume Administrator

By default, new volume administrators cannot manage any NAS volumes. After a volume administrator is created, you can change the NAS volumes that can be managed by the volume administrator.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select a NAS volume.
4. In the toolbar, click **Edit Settings**. The **Edit NAS Volume Settings** dialog box opens.
5. Click **Administrators**. A list of all administrators displays.

6. Select a volume administrator from the list and click **Add**.
7. In a system with multitenancy enabled, if the tenant administrators should not be allowed to access the NAS volume, clear the **Tenant Administrators Access Enabled** checkbox.
8. Click **OK**.

Change the Permission Level of a Cluster Administrator

NAS cluster administrators can manage any aspect of the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Mail & Administrators** tab. The **Administrators** panel displays the current list of administrators.
5. In the **Administrators** panel, select an administrator and click **Edit Settings**. The **Edit Settings** dialog box opens.
6. Select or clear the **Global Administration Permission** field.
7. Type the administrator's email address.
8. Click **OK**.

Change the Email Address of an Administrator

Change the email address to which system alerts are sent for an administrator account.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Mail & Administrators** tab.
5. In the **Administrators** panel, select an administrator and click **Edit Settings**. The **Modify Mail Settings** dialog box opens.
6. In the **Email Address** field, type an email address for the administrator.
7. Click **OK**.

Change an Administrator Password

You can change the password for a local administrator account only. The password for remote administrators is maintained in the external database.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. Select an administrator and click **Change Password**. The **Change Password** dialog box opens.
6. In the **Password** field, type a password for the administrator.
7. In the **Confirm Password** field, retype the password for the administrator.
8. Click **OK**.

Delete an Administrator

Delete an administrator account when it is no longer used for FluidFS cluster management. The built-in Administrator account cannot be deleted.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. Select an administrator and click **Delete**. The **Delete** dialog box opens.
6. Click **OK**.

Managing Local Users and Groups Using MMC

You can manage local users and groups using the Microsoft Management Console (MMC) with the Local Users and Groups snap-in. To gain administrative access to the cluster, log in to Windows as a member of Domain Admins or as a member of Administrators group on the cluster.

Prerequisites

The following limitations apply when managing FluidFS local users and groups using MMC:

- Renaming users and groups is not supported.
- The primary group cannot be deleted from the membership list.
- A local group cannot be deleted if it contains member users.
- Saving the following fields of user accounts is not supported:
  - User profile settings
  - Home folder settings
  - **User must change password at next logon** checkbox
  - **User cannot change password** checkbox

About this task

To manage local users and groups, connect to the FluidFS cluster by using the client VIP address in the address bar of Windows Explorer. Log in with the administrator account and then connect to MMC.

Steps

1. Select **Start** → **Run**.
2. Type `mmc` and click **OK**. The **Console 1 - [Console Root]** window opens.
3. Select **File** → **Add/Remove Snap-in**.
4. Select **Local Users and Groups** and click **Add**.
5. In the **Local Users and Groups** window, select **Another computer** and type the FluidFS cluster name (as configured in the DNS). Alternatively, you can use the client VIP.
6. Click **Finish**. The new local users and groups tree is displayed in the **Console Root** window.
7. Select **Users** or **Groups**.
8. Select a local user or group, and select an action from the **Actions** pane.

Managing Local Users

You can create local users that can access SMB shares and NFS exports, or that will become a FluidFS cluster administrator. You might want to create local users in the following cases:

- You do not have remote users (AD/LDAP/NIS)
- Both SMB/NFS will be used, but you have a remote user repository (AD/LDAP/NIS) relevant for only one protocol and a small number of users using the other protocol

When prompted to authenticate to access an SMB share, local users must use the following format for the user name: *client_vip_or_name\local_user_name*.

Add a Local User

Add a local user account.

Prerequisites

The local group to which the local user will be assigned must have been created already.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. In the **Local Users** pane, click **Create** . The **Create Local User** dialog box opens.
6. In the **Local User** field, type a name for the local user. The user name can contain only the following characters: letters, numbers, underscores, hyphens, spaces, and periods. Also, a period cannot be used as the last character.
7. From the **Primary Local Group** drop-down list, select the primary group to which the local user is assigned.
8. In the **Password** field, type a password for the local user.
9. In the **Confirm Password** field, retype the password for the local user.
10. (Optional) Configure the remaining local user attributes as needed. These options are described in the online help.
    - To enable the local user, select the **Allow Access Enabled** checkbox.
    - To add or remove secondary groups for the local user, use the **Add** and **Remove** buttons.
    - To choose a User ID, uncheck the Automatically Generate User ID box, and enter a value in the User ID field. This value should be between 1001 and 100,000.
11. Click **OK**.

Change the Primary Local Group to Which a Local User Is Assigned

The primary group to which a local user belongs determines the quota for the user.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. Select a local user and click **Edit Settings**. The **Edit Settings** dialog box opens.
6. From the **Primary Local Group** drop-down list, select the group to assign the local user to.
7. Click **OK**.

Change the Secondary Local Groups to Which a Local User Is Assigned

Secondary groups determine Windows (SMB share) permissions.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. Select a local user and click **Edit Settings**. The **Edit Settings** dialog box opens.

6. To add a secondary local group to assign the local user to:
   a. In the **Additional Groups** area, click **Add**. The **Select Group** dialog box opens.
   b. From the **Domain** drop-down list, select the domain to assign the local group to.
   c. In the **Group** field, type either the full name of the local group or the beginning of the local group name.
   d. (Optional) Configure the remaining local group search options as needed. These options are described in the online help.

      To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

   e. Click **Search**.
   f. Select a local group from the search results.
   g. Click **OK**.
7. To remove a secondary local group to which the local user is assigned, select the local group in the **Additional Groups** area and click **Remove**.
8. Click **OK**.

Enable or Disable a Local User

Disabling a local user prevents the local user from accessing SMB shares and NFS exports.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. Select a local user and click **Edit Settings**. The **Edit Local User Settings** dialog box opens.
6. Enable or disable the local user:
   - To enable the local user, select the **Allow Access Enabled** checkbox.
   - To disable the local user, clear the **Allow Access Enabled** checkbox.
7. Click **OK**.

Set the Password Policy for a Local User

When password expiration is enabled, local users are forced to change their passwords after the specified number of days.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. Select a user in the Local Users area, and then click **Edit Settigns**. The **Edit Local User Settings** dialog box opens.
6. Enable or disable local user password expiration:
   - To enable local user and administrator password expiration, clear the **Password Never Expires** checkbox.
   - To disable local user and administrator password expiration, select the **Password Never Expires** checkbox.
7. If password expiration is enabled, in the **Time for password expiration (days)** field, type the number of days after which the password will expire.
8. Click **OK**.

Change a Local User Password

Change the password for a local user account.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab, expand **Environment** and select **Authentication**.
3. Select a local user and click **Change Password**. The **Change Password** dialog box appears.
4. In the **Password** field, type a new password for the local user. The password must be at least seven characters long and contain three of the following elements: a lowercase character, an uppercase character, a digit, or a special character (such as +, ?, or *).
5. In the **Confirm Password** field, retype the password for the local user.
6. Click **OK**.

Delete a Local User

Delete a local user account when the user no longer needs to access SMB shares and NFS exports, or manage the FluidFS cluster (in the case of an administrator based on a local user).

Prerequisites

If the local user has an associated administrator account, you must delete the administrator account before deleting the local user account.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. Select a local user and click **Delete**. The **Delete** dialog box opens.
6. Click **OK**.

Managing Local Groups

Create local groups to apply quota rules to multiple users. You can assign local users, remote users, remote user groups, and external computers to one or more local groups. The primary group to which a user belongs determines the quota for the user.

View Local Groups

View the current local groups.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
   The **Local Groups** list displays the local groups.

Add a Local Group

Add a local group containing local users, remote users, or remote user groups.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. In the **Local Group** area, click **Create**. The **Create Local Group** dialog box opens.
6. In the **Local Group** field, type a name for the local group.
7. In the **Local Users** area, select the local users that should be assigned to the local group:
   a. Click **Add**. The **Select User** dialog box opens.
   b. From the **Domain** drop-down list, select the domain to which the local user is assigned.
   c. In the **User** field, type either the full name of the local user or the beginning of the local user name.
   d. (Optional) Configure the remaining local user search options as needed. These options are described in the online help.

      To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

   e. Click **Search**.
   f. Select a local user from the search results.
   g. Click **OK**.
8. In the **External Users** area, select the individual remote users that should be assigned to the local group:
   a. Click **Add**. The **Select User** dialog box opens.
   b. From the **Domain** drop-down list, select the domain to which the remote user is assigned.
   c. In the **User** field, type either the full name of the remote user or the beginning of the remote user name.
   d. (Optional) Configure the remaining remote user search options as needed. These options are described in the online help.

      To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

   e. Click **Search**.
   f. Select a remote user from the search results.
   g. Click **OK**.
9. In the **External Groups** area, select the remote user groups that should be assigned to the local group:
   a. Click **Add**. The **Select Group** dialog box opens.
   b. From the **Domain** drop-down list, select the domain to which the remote user group is assigned.
   c. In the **Group** field, type either the full name of the remote user group or the beginning of the remote user group name.
   d. (Optional) Configure the remaining remote user group search options as needed. These options are described in the online help.

      To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

   e. Click **Search**.
   f. Select a remote user group from the search results.
   g. Click **OK**.
10. In the **External Computers** area, select the external computer account that should be assigned to the local group:
    a. Click **Add**. The **Select Computer Accounts** dialog box opens.
    b. From the **Domain** drop-down list, select the domain to which the external computer account is assigned.
    c. In the **Computer Account** field, type either the full name of the external computer account or the beginning of the external computer account name.
    d. (Optional) Configure the remaining remote user group search options as needed. These options are described in the online help.

       To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

    e. Click **Search**.
    f. Select an external computer account from the search results.

g. Click **OK**.

Change the Users Assigned to a Local Group

Modify which local users, remote users, or remote user groups are assigned to a local group.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. Select a group and click **Edit Settings**. The **Edit Local User Group Settings** dialog box opens.
6. To assign local users to the local group:
   a. In the **Local Users** area, click **Add**. The **Select User** dialog box opens.
   b. From the **Domain** drop-down list, select the domain to which the local user is assigned.
   c. In the **User** field, type either the full name of the local user or the beginning of the local user name.
   d. (Optional) Configure the remaining local user search options as needed. These options are described in the online help.

      To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

   e. Click **Search**.
   f. Select a local user from the search results.
   g. Click **OK**.
7. To assign individual remote users to the local group:
   a. In the **External Users** area, click **Add**. The **Select User** dialog box opens.
   b. From the **Domain** drop-down list, select the domain to which the remote user is assigned.
   c. In the **User** field, type either the full name of the remote user or the beginning of the remote user name.
   d. (Optional) Configure the remaining remote user search options as needed. These options are described in the online help.

      To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

   e. Click **Search**.
   f. Select a remote user from the search results.
   g. Click **OK**.
8. To assign remote user groups to the local group:
   a. In the **External Groups** area, click **Add**. The **Select Group** dialog box opens.
   b. From the **Domain** drop-down list, select the domain to which the remote user group is assigned.
   c. In the **Group** field, type either the full name of the remote user group or the beginning of the remote user group name.
   d. (Optional) Configure the remaining remote user group search options as needed. These options are described in the online help.

      To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

   e. Click **Search**.
   f. Select a remote user group from the search results.
   g. Click **OK**.
9. To remove users or groups from the local group, select a user or group in the relevant area (**Local Users**, **External Users**, or **External Groups**) and click **Remove**.
10. To assign external computers to the local group:
    a. In the **External Computers** area, select the external computer that should be assigned to the local group.
    b. Click **Add**. The **Select Computer Accounts** dialog box opens.
    c. From the **Domain** drop-down list, select the domain to which the remote user group is assigned.
    d. In the **User** field, type either the full name of the remote user or the beginning of the remote user name.
    e. (Optional) Configure the remaining remote user group search options as needed. These options are described in the online help.

To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

11. Click **OK**.

Delete a Local Group

Delete a local group if it is no longer used.

Prerequisites

Before a local group can be deleted, you must remove its members.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Local Users and Groups** tab.
5. Select a group and click **Delete**. The **Delete** dialog box opens.
6. Click **OK**.

Managing Active Directory

In environments that use Active Directory (AD), you can configure the FluidFS cluster to join the Active Directory domain and authenticate Windows clients using Active Directory for access to SMB shares. The FluidFS cluster supports mixed mode and native mode Active Directory configurations.

Enable Active Directory Authentication

Join the FluidFS cluster to an Active Directory domain to allow it to communicate with the directory service. By default, the FluidFS cluster uses the domain controller returned by Active Directory. Alternatively, you can designate a domain controller if you want to ensure that the FluidFS cluster uses a specific domain controller. Adding multiple domain controllers ensures continued authentication of users in the event of a domain controller failure. If the FluidFS cluster cannot establish contact with the preferred server, it will attempt to connect to the remaining servers in order.

Prerequisites

NAS administrators can join the FluidFS cluster to any organizational units inside an Active Directory domain.

- An Active Directory directory service must be deployed in your environment.
- The FluidFS cluster must have network connectivity to the directory service.
- You must be familiar with the Active Directory configuration.
- The FluidFS cluster requires credentials from an Active Directory account for the join operation. The join operation is the only time these credentials are required. They are not stored or cached by the FluidFS cluster.

  Use one of the following options for the account used to join the FluidFS cluster to the domain:

  - Use a Domain Admin account (preferred method).
  - Use an account that has been delegated the "join a computer to the domain" privilege, as well as being delegated full control over all computer objects in the domain.
  - If both of the previous options are unavailable, the minimum requirements for an account are as follows:
    - An Organizational Unit (OU) admin that has been delegated the "join a computer to the domain" privilege, as well as being delegated full control over objects within that OU, including computer objects.
    - Before joining the FluidFS cluster to the domain, a computer object must be created by the OU admin for the FluidFS cluster; privileges to administer are provided in the OU. The FluidFS cluster computer object name, and the NetBIOS name used when joining it, must match. When creating the FluidFS cluster computer object, in the User or Group field under permissions to join it to the domain, select the OU admin account. Then, the FluidFS cluster can be joined using the OU admin credentials.
- FluidFS clusters need read access for the **tokenGroups** attribute for all users. The default configuration of Active Directory for all domain computers is to allow read access to the **tokenGroups** attribute. If the permission is not given, Active

Directory domain users that are in nested groups or OUs encounter `Access Denied` errors, and users that are not in nested OUs or groups are permitted access.

- The Active Directory server and the FluidFS cluster must use a common source of time.
- You must configure the FluidFS cluster to use DNS. The DNS servers you specify must be the same DNS servers that your Active Directory domain controllers use.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings**. The **Edit Active Directory Settings** dialog box opens.
6. Select a domain controller from the **Preferred Domain Controllers** list, or enter a domain controller IP Address and click **Add**.
7. Click **OK**.

Modify Active Directory Authentication Settings

You cannot directly modify the settings for Active Directory authentication. You must remove the FluidFS cluster from the Active Directory domain and then re-add it to the Active Directory domain.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Leave**. The **Leave Domain** dialog box opens.
6. Click **OK**.
7. Click **Join**. The **Join Domain** dialog box opens.
8. Configure the options as needed.
9. Click **OK**.

Modify Active Directory Controller Settings

The system selects which domain controllers to use automatically, based on the sites defined in Active Directory. You can override this automatic selection and specify a list of preferred domain controllers.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings**. The **Edit Active Directory Settings** dialog box opens.
6. Type a domain controller in the box below **Preferred Domain Controller** and click **Add** or **Remove**.
7. Click **OK**.

Disable Active Directory Authentication

Remove the FluidFS cluster from an Active Directory domain if you no longer need the FluidFS cluster to communicate with the directory service.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Leave** . The **Leave Active Directory Domain** dialog box opens.
6. Click **OK**.

View Open Files

You can view up to 1,000 open files.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Activity**.
4. Click **Open Files**. The **Open Files** dialog box opens.
   The bottom portion of the dialog box displays a list of the currently open files.

Filter Open Files

You can filter open files by file name, user, protocol, or maximum number of open files to display.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Activity**.
4. Click **Open Files**. The **Open Files** dialog box opens.
5. In the top portion of the dialog box, fill in one or more of the fields (File name, User, Protocol, Number of Files to Display).
6. Click **Apply Filter/Refresh**.
   The dialog box displays a list of the currently open files that match the filters.

Managing LDAP

In environments that use Lightweight Directory Access Protocol (LDAP), you can configure the FluidFS cluster to authenticate UNIX and Linux clients using LDAP for access to NFS exports. The LDAP database can be provided by either an LDAP server or Active Directory.

The FluidFS clusters supports the following LDAP configurations:

- **Anonymous LDAP** – The connection from the FluidFS cluster to the LDAP servers is not authenticated. The data is sent in plain text.
- **Authenticated LDAP** – The connection from the FluidFS cluster to the LDAP servers is authenticated using a user name and password. The data is sent in plain text.
- **LDAP over TLS/SSL** – The connection from the FluidFS cluster to the LDAP servers is authenticated and encrypted. To validate the certificate used by the LDAP server, you must export the SSL certificate from the LDAP server and upload it to the FluidFS cluster.

Reduce the Number of Subtrees for Searches

FluidFS allows you to narrow the number of subtrees in an LDAP tree used for searching.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. In the NFS USer Repository (NIS or LDAP) area, click **Edit Settings**. The **Edit Active Directory Settings** dialog box opens.
6. Select the **LDAP** radio button.
7. In the Filtered Branches field, type the LDAP name to be used for searching and then click **Add**.
8. To use LDAP on Active Directory extended schema:
   a. fFor the Extended Schema field, select **Enabled**.
9. To use LDAP over TLS to encrypt all communications with the LDAP server:
   a. For the LDAP over TLS field, select **Enabled**.
10. To install an LDAP certificate:
    a. For the Install LDAP Certificate field, select **Enabled**.
    b. In the **LDAP certificate** field, specify a certificate.
    c. Click **Upload Certificate**.
11. To use non-anonymous LDAP bind:
    a. For the Non-Anonymous LDAP bind field, select **Enabled**.
    b. In the **Bind DN** and **Bind Password** fields, type the appropriate information.
12. Click **OK**.

Enable LDAP Authentication

Configure the FluidFS cluster to communicate with the LDAP directory service. Adding multiple LDAP servers ensures continued authentication of users in the event of an LDAP server failure. If the FluidFS cluster cannot establish contact with the preferred server, it will attempt to connect to the remaining servers in order.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. Select **LDAP**.
7. In the **Base DN** field, type an LDAP base distinguished name to represent where in the directory to begin searching for users. The name is usually in this format: `dc=domain, dc=com`.
8. In the **LDAP Servers** text field, type the host name or IP address of an LDAP server and click **Add**. Repeat this step for any additional LDAP servers.
9. (Optional) Configure the remaining LDAP attributes as needed. These options are described in the online help.
   - To indicate that Active Directory provides the LDAP database, select the **Extended Schema** checkbox.
   - To authenticate the connection from the FluidFS cluster to the LDAP server, select the **Non-Anonymous LDAP bind** checkbox. Then, type the LDAP bind distinguished name used to authenticate the connection in the **Bind DN** field and type the LDAP bind password in the **Bind Password** field.
   - To encrypt the connection from the FluidFS cluster to the LDAP server using TLS, select the **LDAP over TLS** checkbox.
   - To validate the certificate used by the LDAP server, select the **Install LDAP Certificate** checkbox. Then, click **Upload Certificate** and select the LDAP SSL certificate to upload to the FluidFS cluster.
10. Click **OK**.

Change the LDAP Base DN

The LDAP base distinguished name represents where in the directory to begin searching for users.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. In the **Base DN** field, type an LDAP base distinguished name. The name is usually in this format: `dc=domain, dc=com`.
7. Click **OK**.

Add or Remove LDAP Servers

At least one LDAP server must be configured.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. Add or remove LDAP servers:
   - To add an LDAP server, type the host name or IP address of an LDAP server in the **LDAP Servers** text field and click **Add**.
   - To remove an LDAP server, select an LDAP server and click **Remove**.
7. Click **OK**.

Enable or Disable LDAP on Active Directory Extended Schema

Enable the extended schema option if Active Directory provides the LDAP database.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. Enable or disable LDAP on Active Directory extended schema:
   - To have Active Directory provide the LDAP database, select the **Use LDAP on Active Directory Extended Schema** checkbox.
   - To have an LDAP server provide the LDAP database, clear the **Use LDAP on Active Directory Extended Schema** checkbox.
7. Click **OK**.

Enable or Disable Authentication for the LDAP Connection

Enable authentication for the connection from the FluidFS cluster to the LDAP server if the LDAP server requires authentication.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. Enable or disable authentication for the LDAP connection:
   - To enable authentication for the LDAP connection, select the **Non-Anonymous LDAP bind** checkbox. Then, type the LDAP bind distinguished name used to authenticate the connection in the **Bind DN** field and type the LDAP bind password in the **Bind Password** field.
   - To disable authentication for the LDAP connection, clear the **Use Non-Anonymous LDAP bind** checkbox.
7. Click **OK**.

Enable or Disable TLS Encryption for the LDAP Connection

Enable TLS encryption for the connection from the FluidFS cluster to the LDAP server to avoid sending data in plain text. To validate the certificate used by the LDAP server, you must export the LDAP SSL certificate and upload it to the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. Enable or disable TLS encryption for the LDAP connection:
   - To enable TLS encryption for the LDAP connection, select the **LDAP over TLS** checkbox.
   - To disable TLS encryption for the LDAP connection, clear the **LDAP over TLS** checkbox.
7. If TLS encryption is enabled, enable or disable LDAP certificate validation.
   - To enable LDAP certificate validation, select the **Install LDAP Certificate** checkbox. Then, click **Upload Certificate** and browse to and select the LDAP SSL certificate to upload to the FluidFS cluster.
   - To disable LDAP certificate validation, clear the **Install LDAP Certificate** checkbox.
8. Click **OK**.

Disable LDAP Authentication

Disable LDAP authentication if you no longer need the FluidFS cluster to communicate with the directory service.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. Select **None**.
7. Click **OK**.

Managing NIS

In environments that use Network Information Service (NIS), you can configure the FluidFS cluster to authenticate clients using NIS for access to NFS exports.

Enable or Disable NIS Authentication

Configure the FluidFS cluster to communicate with the NIS directory service. Adding multiple NIS servers ensures continued authentication of users in the event of a NIS server failure. If the FluidFS cluster cannot establish contact with the preferred server, it will attempt to connect to the remaining servers in order.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. Enable or disable NIS:
   - To disable NIS, select the **None** checkbox.
   - To enable NIS, select the **NIS** checkbox.
7. In the **NIS Domain Name** field, type a NIS domain name.
8. In the **NIS Servers** text field, type the host name or IP address of a NIS server and click **Add**. Repeat this step for any additional NIS servers.
9. NIS servers are listed in descending order of preference:
   - To increase the order of preference for a NIS server, select a NIS server and click **Up**.
   - To decrease the order of preference for a NIS server, select a NIS server and click **Down**.
10. Click **OK**.

Change the NIS Domain Name

The NIS domain name specifies which domain to query in the NIS directory service.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. In the **NIS Domain Name** field, type a NIS domain name.
7. Click **OK**.

Add or Remove NIS Servers

At least one NIS server must be configured.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. Add or remove NIS servers:

- To add a NIS server, type the host name or IP address of a NIS server in the **NIS Servers** text field and click **Add**.
- To remove a NIS server, select an NIS server and click **Remove**.

7. Click **OK**.

Change the Order of Preference for NIS Servers

If the FluidFS cluster cannot establish contact with the preferred server, it will attempt to connect to the remaining servers in order.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Directory Services** tab.
5. Click **Edit Settings** in the NFS User Repository section. The **Edit External User Database** dialog box opens.
6. NIS servers are listed in descending order of preference:
   - To increase the order of preference for a NIS server, select a NIS server and click **Up**.
   - To decrease the order of preference for a NIS server, select a NIS server and click **Down**.
7. Click **OK**.

Managing User Mappings Between Windows and UNIX/Linux Users

You can define mappings between Windows users in Active Directory and UNIX/Linux users in LDAP or NIS. The mapping ensures that a Windows user inherits the UNIX/Linux user permissions and a UNIX/Linux user inherits the Windows user permissions, depending on the direction of the mapping and the NAS volume security style.

User Mapping Policies

The user mapping policies include automatic mapping and mapping rules.

- **Automatic mapping** – Automatically map all Windows users in Active Directory to the identical UNIX/Linux users in LDAP or NIS, and map all UNIX/Linux users to the identical Windows users. Automatic mapping is disabled by default.
- **Mapping rules** – Define mappings between specific Windows users in Active Directory and the identical UNIX/Linux users in LDAP or NIS. These specific mapping rules take precedence over automatic mapping. You can select the direction of the mapping, which can go in one direction or both.
  - Mapping is allowed in one direction:
    - Windows user to a UNIX/Linux user
    - UNIX/Linux user to a Windows user
  - Mapping is allowed in both directions between a Windows user and a UNIX/Linux user.

User Mapping Policy and NAS Volume Security Style

User mapping permissions depend on the file security style for the NAS volume:

- **NTFS security style** – Permissions are controlled by Windows and NTFS. The UNIX/Linux user will adhere to the permissions of the corresponding Windows user, regardless of the UNIX/Linux permission settings.
- **UNIX security style** – Permissions are based on the UNIX/Linux permissions. The Windows user will adhere to the permissions of the corresponding UNIX/Linux user.
- **Mixed security style** – Both UNIX/Linux and Windows permissions are used. Each user can override the other user's permission settings; therefore, be careful when using the Mixed security style.

Managing the User Mapping Policy

Configure the FluidFS cluster mapping policy to automatically map all users or to allow mappings between specific users only.

Automatically Map Windows and UNIX/Linux Users

Automatically map all Windows users in Active Directory to the identical UNIX/Linux users in LDAP or NIS, and map all UNIX/Linux users to the identical Windows users. Mapping rules will override automatic mapping.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Mapping Policy** tab.
5. Click **Edit Settings**. The **Edit Mapping Policy Settings** dialog box opens.
6. Select **Automatic mapping policy of SMB and NFS users with the same name**.
7. Click **OK**.

Map Windows and UNIX/Linux Users by Mapping Rules Only

Only allow mappings between specific Windows users in Active Directory and the identical UNIX/Linux users in LDAP or NIS.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Mapping Policy** tab.
5. Click **Edit Settings**. The **Create Manual Mapping** dialog box opens.
6. Select a mapping rule.
7. Click **OK**.

Managing User Mapping Rules

Manage mapping rules between specific users. Mapping rules override automatic mapping.

Create a User Mapping Rule

Create a mapping rule between a specific Windows user in Active Directory and the identical UNIX/Linux user in LDAP or NIS. Mapping rules override automatic mapping.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Mapping Policy** tab.
5. Click **Create**. The **Create Manual Mapping** dialog box opens.
6. In the **SMB User** area, click **Select User**. The **Select User** dialog box opens.
7. Select a Windows user:
   a. From the **Domain** drop-down list, select the domain to which the user is assigned.
   b. In the **User** field, type either the full name of the user or the beginning of the user name.
   c. (Optional) Configure the remaining user search options as needed. These options are described in the online help.

To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

d. Click **Search**.
e. Select a user from the search results.
f. Click **OK**.

8. In the **NFS User** area, click **Select User**. The **Select User** dialog box opens.
9. Select a UNIX/Linux user:
   a. From the **Domain** drop-down list, select the domain to which the user is assigned.
   b. In the **User** field, type either the full name of the user or the beginning of the user name.
   c. (Optional) Configure the remaining user search options as needed. These options are described in the online help.

      To change the maximum number of search results to return, select the maximum number of search results from the **Max Results** drop-down list.

   d. Click **Search**.
   e. Select a user from the search results.
   f. Click **OK**.
10. Select the direction of the user mapping:
    - The two users will have identical file access permissions (via any protocol)
    - Enable Unix To Windows Mapping
    - Enable Windows To Unix Mapping
11. Click **OK**.

Change the Direction of Mapping for a User Mapping Rule

Change the direction of mapping between a specific Windows user in Active Directory and the identical UNIX/Linux user in LDAP or NIS.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Mapping Policy** tab.
5. Click **Edit Settings**. The **Create Manual Mapping** dialog box opens.
6. Select the direction of the user mapping:
   - The two users will have identical file access permissions (via any protocol)
   - Map NFS user to SMB user
   - Map SMB user to NFS user
7. Click **OK**.

Delete a User Mapping Rule

Delete a mapping rule between a specific Windows user in Active Directory and the identical UNIX/Linux user in LDAP or NIS.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Mapping Policy** tab.
5. Click **Edit Setttings**. The **Create Manual Mapping** dialog box opens.
6. Select a user mapping rule and click **Delete**. The **Delete** dialog box opens.
7. Click **OK**.

FluidFS NAS Volumes, Shares, and Exports

This section contains information about managing the FluidFS cluster from the client perspective. These tasks are performed using the Storage Manager Client.

Managing the NAS Pool

When configuring a FluidFS cluster, you specify the amount of raw Storage Center space to allocate to the FluidFS cluster (NAS pool). The maximum size of the NAS pool is:

- 2 PB with one Storage Center.
- 4 PB with eight Storage Centers

The usable size of the NAS pool depends on how much space the system deducts from the NAS pool for internal use. On average, the system deducts approximately 400 GB per NAS appliance for internal use. The exact amount of internal space varies by configuration, but it is roughly calculated as follows per FluidFS cluster:

(256 GB * number of NAS appliances) + (4 GB * number of Storage Center volumes) + 20 GB + 0.5% of the total NAS pool + (100 GB * number of NAS appliances, if data reduction is enabled)

View Internal Storage Reservations

View information about the space that the system deducts from the NAS pool for internal use.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Internal** tab.
   The **Internal Storage Reservations** panel displays the internal storage reservations.

View the Size of the NAS Pool

View the current configured size of the NAS pool.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab.
   The **NAS Pool Status** panel displays the configured size of the NAS pool.

Expand the Size of the NAS Pool

You can increase the size of the NAS pool as your NAS storage space requirements increase, without affecting the services to the clients. However, you cannot decrease the size of the NAS pool.

Prerequisites

The Storage Centers must have enough capacity to allocate more storage space to the FluidFS cluster.

The maximum size of the NAS pool is:

- 2 PB with one Storage Center
- 4 PB with two Storage Centers

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab.

3. In the right pane, click **Actions** → **Storage Centers** → **Expand NAS Pool**. The **Expand NAS Pool** dialog box opens.
4. In the **NAS Pool Size** field, type a new size for the NAS pool in gigabytes (GB) or terabytes (TB).

   NOTE: The new size is bound by the size displayed in the **Minimum New Size** field and the **Maximum New Size** field.

5. Click **OK**. If the container has more than one storage type, a drop-down list will appear.
6. From the **Storage Type** drop-down list, select the type of storage pool, which includes a single data page size and a specified redundancy level.
7. Click **OK**.
   The **Expand NAS Pool** dialog box displays the status of the process.

Set the Metadata Tier

Metadata tiering provides the ability to store data and metadata in different storage tiers or LUNs. Metadata tiering allows storing of metadata items on faster disks, benefiting workloads which are metadata-oriented but require low-cost disks for most of their data. This feature is disabled by default, and can be enabled at any time during system operation. Metadata tiering is disabled when the system is updated from an older version of the firmware.

About this task

When creating or expanding a NAS pool, administrators can select the percentage of the FluidFS NAS pool capacity to be allocated for the metadata tier. For example, High Priority (Tier 1) stores approximately 12.5 percent of the storage for FluidFS in the metadata tier whereas Low Priority (Tier 3) stores approximately 3 percent of the storage for FluidFS in the metadata tier.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **NAS Pool** tab.
3. In the **Storage Subsystems** panel, click **Change Storage Profile**.
   The **Select Storage Profile** window opens.
4. Select a storage profile and NAS pool percentage to allocate for metadata.
5. Click **OK**.

Enable or Disable the NAS Pool Used Space Alert

You can enable or disable an alert that is triggered when a specified percentage of the NAS pool space has been used.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab.
3. In the **Summary** panel, click **Edit NAS Pool Settings**.
   The **Edit NAS Pool Settings** dialog box opens.
4. Enable or disable the NAS pool used space alert:
   - To enable the NAS pool used space alert, select the **Used Space Alert** checkbox.
   - To disable the NAS pool used space alert, clear the **Used Space Alert** checkbox.
5. If the **Used Space Alert** checkbox is enabled, in the **Used Space Threshold** field, type a number (from 0 to 100) to specify the percentage of used NAS pool space that triggers an alert.
6. Click **OK**.

Enable or Disable the NAS Pool Unused Space Alert

You can enable or disable an alert that is triggered when the remaining unused NAS pool space is below a specified size.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab.
3. In the **Summary** panel, click **Edit NAS Pool Settings**.
   The **Set NAS Pool Space Settings** dialog box opens.
4. Enable or disable the NAS pool unused space alert:
   - To enable the NAS pool used space alert, select the **Unused Space Alert** checkbox.
   - To disable the NAS pool used space alert, clear the **Unused Space Alert** checkbox.
5. If the **Unused Space Alert** checkbox is enabled, in the **Unused Space Threshold** field, type a number (from 0 to 100) to specify the percentage of unused NAS pool space that triggers an alert.
6. Click **OK**.

About Multitenancy

Multitenancy enables a single physical FluidFS cluster to be partitioned into several separate service entities (tenants) and manage each one individually. FluidFS supports up to 100 tenants. When multitenancy is enabled, the user interface is optimized and includes the tenants view.

Network connections – Each tenant utilizes exclusive IP addresses (virtual IPs). Users who have access to the tenant's VIP can only see that tenant's NFS exports, SMB shares, and so on.

Authentication and user repositories – Each tenant utilizes its own authentication and user repositories. Each tenant can define and use the following settings:

- DNS configuration – The DNS configuration of the default tenant serves the cluster services (such as NTP).
- Active Directory – Each tenant can join a different Active Directory. Two tenants can also join the same Active Directory (with separate tenant computer objects in Active Directory).
- LDAP or NIS
- Local users and groups
- User mapping

Reusing of same name in different tenants – Multitenancy supports using the same SMB share name and the same local user or group name.

Volume Replication – Administrators can define between which tenants volume replication is allowed.

Managing tenants – FluidFS v6 added a new type of administrator called tenant administrators. A tenant administrator has the ability to:

- See (but not update) all of the general cluster settings
- Manage tenants they have been granted Tenant Administrator access to, including all the NAS volumes that belong to those tenants
- Receive email events that are relevant to the entire cluster and to the tenants they have been granted Tenant Administrator access to, such as power-down events

Using Multitenancy With Existing Features

Multitenancy interoperates with the following existing FluidFS features:

Antivirus – SMB shares are isolated to their tenant. If any shares have antivirus enabled, they utilize the virus scanners that are defined at the clusterwide level.

File Access Notifications – File access notifications are set at a clusterwide level in FluidFS. If multitenancy is in use, only one tenant can utilize the external audit server feature. Separation of file access notifications between different tenants requires multiple FluidFS clusters. Alternatively, you can use SACL auditing, which is separated between tenants for file access notifications.

NDMP Backup – You can back up any of the volumes using any of the VIPs (or physical controller IPs), regardless of multitenancy. Separation of NDMP between different tenants requires multiple FluidFS clusters.

Replication and Disaster Recovery – The cluster administrator has the ability to create a partner relationship between the tenants on the source system and the tenants on the remote system.

Enable Multitenancy

System administrators can enable multitenancy using Dell Storage Manager or the CLI. When multitenancy is enabled, the system administrator can no longer see or control tenants' contents. A tenant's content can be managed only by the tenant administrator.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. In the FluidFS cluster status section of the **Summary** panel, click **Edit FluidFS Cluster Settings**.
   The **Edit FluidFS Cluster Settings** dialog box opens.
3. Select the **Multitenancy Enabled** checkbox.
4. Click **OK**.

Disable Multitenancy

Tenant administrators can disable multitenancy using Dell Storage Manager or the CLI.

Prerequisites

Multitenancy can be disabled when only the default tenant exists; that is, to disable multitenancy, all tenants except for the default tenant must be deleted. A tenant can be deleted only when all NAS volumes on that tenant have been deleted. NAS volumes can be deleted only when all SMB shares and NFS exports have been deleted from the volume.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. In the FluidFS cluster status section of the **Summary** panel, click **Edit FluidFS Cluster Settings**.
   The **Edit FluidFS Cluster Settings** dialog box opens.
3. Clear the **Multitenancy Enabled** checkbox.
4. Click **OK**.

Multitenancy – System Administration Access

About this task

This procedure grants cluster administrator access to a user.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Mail & Administrators** tab.
5. Click **Grant Administration Privilege**.
   The **Grant Administration Privilege** dialog box opens.
6. Select the **Global Administration Permission Enabled** checkbox.
   When this checkbox is enabled, the user that you select has permission to manage anything on the cluster.
7. Click **Next**.
   The **Select User** dialog box opens.
8. Select a user and domain from the **User** and **Domain** drop-down lists.
9. Click **OK**.

Multitenancy – Tenant Administration Access

A tenant administrator manages his or her tenants' content. Tenant can be managed by multiple tenant administrators, and tenant administrators can manage multiple tenants. A tenant administrator can create or delete tenants, delegate administration per tenant, and view space consumption of all tenants.

About this task

This procedure grants tenant administrator access to a user.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Maintenance**.
4. Click the **Mail & Administrators** tab.
5. In the Administrators panel, select an Administrator, and then click **Edit Settings**.
   The **Modify Mail Settings** dialog box opens.
6. Select a user and clear the **Global Administration Permissions** checkbox.
7. Click **OK**.

Next steps

NOTE:

- Users must be added to the administrators list before they can be made a tenant administrator or a volume administrator.
- Only the following users can be administrators:
  - Users in the Active Directory domain or UNIX domain of the default tenant
  - Local users of the default tenant or any other tenant

Adding a User to the Administrator's List

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select the tenant you want to delegate as Tenant Administrator, and click **Edit Settings**.
4. In the **Edit Settings** dialog box, select the **Administrators** tab.
5. Select the user that you want to designate as Tenant Administrator for the selected tenant, and click the **Add** button.
6. Click **OK**.

Multitenancy – NAS Volume Administration Access

You must have cluster administrator permissions to define new volume administrators.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **NAS Volumes**.
4. In the **NAS Volumes** panel, select a NAS volume.
5. Click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
6. Select an administrator from the list and click **Add**.
7. Click **OK**.

NOTE: Users must be added to the administrators list before they can be made a tenant administrator or a volume administrator. Only the following users can be administrators:

-
- Users in the Active Directory domain or UNIX domain of the default tenant
- Local users of the default tenant or any other tenant

Create a New Tenant

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Tenants**.
4. Click **Create Tenant**.
   The **Create Tenant** wizard opens and guides you through the following steps:
   a. Create Tenant
   b. Public IPs
   c. DNS
   d. Limits
   e. Active Directory
   f. NFS User Repository

Create Tenant – Step 1

The tenant value must be a valid tenant name The name can contain letters, numbers, underscores, and hyphens.

Steps

1. In the Create Tenant window, type a tenant name in the **Tenant** field.
2. Click **Next**.

Create Tenant – Step 2

Steps

1. In the Create Tenant window, click **Public IPs**.

   NOTE: For FluidFS, a Public IP is the same thing as a VIP, the terms are used interchangeably.

2. Type one or more virtual IP addresses for file access in the **VIP** field. If you have clients coming from behind a router, you should define one VIP for each physical network port. if the clients are not coming from behind a router, you can use only one VIP.
3. Click **Add** or **Remove**.
4. Click **Next**.

Create Tenant – Step 3

Steps

1. In the Create Tenant window, click **DNS**.
2. Type one or more DNS Server IP addresses in the **DNS Server IP Addresses** field.
3. Click **Next**.
4. Type DNS suffixes in the **DNS Suffix** field.
5. Click **Add** or **Remove**.
6. Click **Next**.

Create Tenant – Step 4

Steps

1. In the Create Tenant window, click **Limits**.

   NOTE: Setting any of these limits is optional.

2. Select the **Restrict Tenant Capacity Enabled** checkbox.
3. Type a tenant capacity limit in gigabytes (GB).
4. Select the **Restrict Number of NAS Volumes in Tenant Enabled** checkbox.
5. Type the maximum number of NAS volumes for this tenant.
6. Select the **Restrict Number of NFS Exports in Tenant Enabled** checkbox.
7. Type the maximum number of NFS exports for this tenant.
8. Select the **Restrict Number of SMB Shares in Tenant Enabled** checkbox.
9. Type the maximum number of SMB shares for this tenant.
10. Click **Next**.

Create Tenant – Step 5

Steps

1. In the Create Tenant window, click **Active Directory**.
2. Specify the Active Directory fully qualified domain name to be used for authentication of SMB and NFS users.
3. Type a domain name in the **Domain** field.
4. (Optional) Specify the organizational unit in the AD domain where the computer account for this tenant should be created.
5. (Optional) Type the organizational unit in the **Organizational Unit** field.
6. Provide credentials to perform this operation:
   a. Type your user name.
   b. Type your password.
7. Click **Next**.

Create Tenant – Step 6

Steps

1. In the Create Tenant window, click **NFS User Repository**.
2. Specify the type of NFS user repository to use for searching UIDs and GIDs by enabling one of the following choices: **None**, **NIS**, or **LDAP**.
3. Click **Finish**.

Moving a NAS Volume Between Tenants

Steps

1. In the **Storage** view, select a FluidFS cluster
2. Click the **File System** tab.
3. In the **File System** view, expand **Volumes**, and select a volume.
4. Click **Move to Tenant**.
5. Click **OK**.

Managing NAS Volumes

A NAS volume is a subset of the NAS pool in which you create SMB shares and/or NFS exports to make storage space available to clients. NAS volumes have specific management policies controlling their space allocation, data protection, security style, and so on.

You can either create one large NAS volume consuming the entire NAS pool or divide the NAS pool into multiple NAS volumes. In either case you can create, resize, or delete these NAS volumes.

NAS volume availability depends on the availability of the Storage Centers. If a Storage Center is offline, storage center LUNs will not be available for the FluidFS cluster, and access to the shares and/or exports will be lost. Correct the Storage Center problem to resume service.

The following NAS features can be configured on each NAS volume:

- File security styles
- Quota rules
- Data reduction
- Snapshots
- NDMP backup
- Replication

File Security Styles

The Windows and UNIX/Linux operating systems use different mechanisms for resource access control. Therefore, you assign each NAS volume a file security style (NTFS, UNIX, or Mixed) that controls the type of access controls (permission and ownership) for the files and directories that clients create in the NAS volume.

A NAS volume supports the following security styles:

- **UNIX** – Controls file access using UNIX permissions. A client can change permissions only by using the `chmod` and `chown` commands on the NFS mount point.
- **NTFS** – Controls file access by Windows permissions. A client can change the permission and ownership using Windows (**File Properties** → **Security** tab).
- **Mixed** – Supports both NTFS and UNIX security styles. If you choose this option, the default security of a file or directory is the last one set. Permissions and access rights from one method to another are automatically translated. (For example, if a Windows administrator sets up file access permissions on a file through an SMB share, a Linux user can access the file system through NFS and change all the file permissions.) Therefore, this option is not recommended in production environments, except where you are not concerned about file access security and just need some NAS volume space to store files temporarily.

Both NTFS and UNIX security styles allow multiprotocol file access. The security style determines only the method of storing and managing the file access permissions information within the NAS volume.

If you need to access the same set of files from both Windows and UNIX or Linux, the best way to implement multiprotocol access is by setting up individual user mapping rules or by enabling automatic user mapping. Ownership and access permissions are automatically translated based on user mapping settings and file access credentials.

Modifying the file security style of a NAS volume affects only those files and directories created after the modification.

Thin and Thick Provisioning for NAS Volumes

In addition to the thin provisioning applied to the NAS pool, NAS volumes can be thin-provisioned. With thin provisioning (the default), storage space is consumed on the Storage Centers only when data is physically written to the NAS volume, not when the NAS volume is initially allocated. Thin provisioning offers the flexibility to modify NAS volumes to account for future increases in usage. However, because it is possible for the storage space used by the NAS volumes to exceed the Storage Center space allocated to the NAS pool, you must monitor available capacity on the Storage Centers to ensure that the FluidFS cluster always has sufficient free space available. You can also specify a portion of the NAS volume (reserved space) that is dedicated to the NAS volume (no other volumes can take the space). The total reserved space of all NAS volumes cannot exceed the available capacity of the NAS pool.

If a file is deleted from a thin-provisioned NAS volume, the free space as seen in Storage Manager increases. The freed-up capacity is also visible and available to clients in the SMB shares or NFS exports. However, the Storage Center does not report any capacity freed up in the NAS pool unless you enable the SCSI Unmap feature.

Thick provisioning allows you to allocate storage space on the Storage Centers statically to a NAS volume (no other volumes can take the space). Thick provisioning is appropriate if your environment requires guaranteed space for a NAS volume.

Managing NAS Volume Space

FluidFS maintains file metadata in i-node objects. FluidFS i-nodes are 4 KB in size (before metadata replication) and can contain up to 3.5 KB of file data.

When a new virtual volume is created, a portion of it is allocated as i-node area. When a new file is created and there are no free i-nodes left, an additional portion of the volume is allocated to the i-node area. When a file is deleted, however, the i-node is marked as free (to make the allocation of new file i-nodes efficient) rather than returned to the free-space pool.

Free i-nodes are returned to the free-space of a volume only when the ratio between the free-space and the number of free i-nodes becomes very low. When this situation occurs, a special background process is invoked which runs only until the ratio crosses an internal threshold. The process does not run until all free i-nodes are returned to the free-space.

In deployment environments characterized by large amounts of small files, a massive deletion of small files does not fully reflect in the amount of free-space in the volume. For example, if you filled a 100 TB volume with 70 TB of small files (leaving 30 TB free-space) and then deleted 50 TB of them, the amount of free-space would likely not increase much. However, as long as the workload remains small-file oriented, the system reuses the free i-nodes and does not consume from the free-space. Creating some large files requires more space and eventually return a good portion of the free i-nodes to the free space.

Choosing a Strategy for NAS Volume Creation

When you define multiple NAS volumes, you can apply different management policies — such as data reduction, data protection, file security style, and quotas — based on your needs.

Consider the following factors to help choose the right strategy based on your environment's requirements:

- **General requirements**
  - NAS volumes can be created, resized (increased or decreased), or deleted.
  - A single NAS volume can contain NFS exports, SMB shares, or a combination of NFS exports and SMB shares.
  - The minimum size of a NAS volume is 20 MB. (If the volume has already been used, the minimum size should be more than the used space or reserved space, whichever is highest.)
- **Business requirements** – A company or application requirement for separation or for using a single NAS volume must be considered. NAS volumes can be used to allocate storage for departments on demand, using the threshold mechanism to notify administrators when they approach the end of their allocated free space.
- **Data reduction** – Each NAS volume can have a dedicated data reduction policy to best suit the type of data it stores.
- **Snapshots** – Each NAS volume can have a dedicated snapshot scheduling policy to best protect the type of data it stores.
- **Security style** – In multiple-protocol environments, it might be beneficial to separate the data and define NAS volumes with UNIX security style for UNIX/Linux-based clients and NTFS security style for Windows-based clients. This separation enables the administrator to match the security style with business requirements and various data access patterns. The security style can also be set to Mixed, which supports both POSIX security and Windows ACLs on the same NAS volume. When a NAS volume is created, the default file permissions is set to Windows. The settings should be edited immediately after the NAS volume has been created.
- **Quotas** – Different quota policies can be applied to different NAS volumes, allowing the administrator to focus on managing quotas when it is appropriate.
- **Replication schedules** – Different volumes can have different replication schedules and policies.
- **Auditing SACL SMB Access** – Different volumes can have different policies for handling the auditing of SACL SMB accesses.

Examples of NAS Volume Creation

This section includes examples that show how NAS volumes can be created to meet the needs of an organization with the departments and NAS volume requirements described in the following table.

Department	Security Style	Snapshots	Replication	NDMP Backup	Number of SMB/NFS Clients	Read/Write Mix	Hourly Change % of Existing Data
Post Production	UNIX	Hourly	No	Weekly	20	20/80	1%

Department	Security Style	Snapshots	Replication	NDMP Backup	Number of SMB/NFS Clients	Read/Write Mix	Hourly Change % of Existing Data
Administration and Finance	NTFS	No	No	Weekly	10	50/50	None
Broadcast	Mixed	No	No	Weekly	10	90/10	None
Press	NTFS	Daily	No	No	5	10/90	5%
Marketing	NTFS	Daily	Yes	No	5	50/50	None

An average read/write mix is 20/80. An average hourly change rate for existing data is less than 1 percent.

Example 1

Create NAS volumes based on departments. The administrator breaks up storage and management into functional groups. In this example, the departmental requirements are different and support the design to create NAS volumes along department lines.

- **Advantages**
  - The NAS volumes are easier to manage because they are set up logically.
  - The NAS volumes are created to match the exact needs of the department.
- **Disadvantage** – The NAS volumes become harder to manage if the number of departments in the organization increases.

Example 2

Group departments that have similar security requirements into NAS volumes. The administrator creates three NAS volumes: one for UNIX, one for NTFS, and one for mixed.

- **Advantages** – The NAS volumes work separately between Windows and Linux.
- **Disadvantage** – Unwanted services could be provided to certain departments. For example, when the SMB volume is backed up weekly for the administration and finance departments, the press and marketing departments also get backups even though they do not require them.

Example 3

NAS volumes can be created based on a feature (snapshots, replication, NDMP backup, and so on).

- **Advantages** – The NAS volumes are created to match the exact needs for each feature.
- **Disadvantage** – User mapping is required. A user needs to choose one security style (either NTFS or UNIX) and then, based on the security style chosen, the correct mapping for other users is set.

NAS Volumes Storage Space Terminology

Storage Manager displays storage space details for individual NAS volumes and for all NAS volumes collectively. The following table defines terminology used in Storage Manager related to NAS volume storage space.

Term	Description
Size	Maximum size of a NAS volume defined by the storage administrator
Used space	Storage space occupied by writes to the NAS volume (user data and snapshots)
Reserved space	A portion of a thin-provisioned NAS volume that is dedicated to the NAS volume (no other volumes can take the space). The amount of reserved space is specified by the storage administrator. Reserved space is used before unreserved space.
Unreserved space	A portion of a thin-provisioned NAS volume that is not reserved (other volumes can take the space). To calculate the amount of unreserved space for a NAS volume, use: (NAS volume size) – (NAS volume reserved space)

Term	Description
Unused space	Storage space that is physically currently available for the NAS volume. To calculate the amount of available space for a NAS volume, use: (unused NAS volume reserved space) + (NAS volume unreserved space
Overcommitted space	Storage space allotted to a thin-provisioned volume over and above the actually available physical capacity of the NAS pool. To calculate the amount of overcommitted space for a NAS volume, use: (Total volume space) – (NAS pool capacity) With thin provisioning, storage space is consumed only when data is physically written to the NAS volume, not when the NAS volume is initially allocated. More storage space can be allocated to the NAS volumes than has been allocated in the NAS pool itself.
Snapshot space	Storage space occupied by snapshots of a NAS volume
Data reduction saving	Storage space reclaimed as a result of data reduction processing

Managing the Storage Profile for a NAS Cluster or Pool

Storage Center Storage Profiles control how Storage Center manages volume data. The selected Storage Profile dictates which storage tier accepts initial writes, as well as how data progression moves pages between storage tiers to balance performance and cost.

For more information about Storage Profiles, see the *Storage Manager Administrator's Guide*.

View the Storage Profile for the NAS Cluster or Pool

View the Storage Center Storage Profiles configured for the NAS cluster or pool. A unique Storage Profile can be configured for each Storage Center that provides storage for the FluidFS cluster.

Steps

In the **Storage** view, select a FluidFS cluster.
The Storage Profile for each Storage Center appears in the **Storage Subsystems** area.

Change the Storage Profile for the NAS Cluster or Pool

Change the Storage Center Storage Profiles configured for the NAS cluster or pool. A unique Storage Profile can be configured for each Storage Center that provides storage for the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **NAS Pool** tab.
3. In the Storage Subsystems panel, click **Change Storage Profile**.
4. Locate the Storage Center for which you want to change the Storage Profile.
5. From the **Storage Profile** drop-down list, select a Storage Profile.
6. Click **OK**.

Configuring NAS Volumes

Configure NAS volumes to manage the volumes and volume alerts.

Optimize NAS Volumes for Use as VMware vSphere Datastores

When you configure a NAS volume to use VM- (virtual machine) consistent snapshots, each snapshot creation (scheduled, manual, replication, NDMP and so on) automatically creates an additional snapshot on the VMware server.

About this task

When enabled, if the VMware servers are defined, the NAS volume is aware that it is being used as a repository for a VM datastore. The NAS volume creation is synchronized with relevant VM snapshot creation in order to keep VMware data stored on the NAS volume in a consistent state.

NOTE: VM application awareness cannot be used on NAS volumes that use the global namespace feature.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click the **Advanced** tab.
6. Enable or disable VM-consistent snapshots:
   - To enable VM-consistent snapshots, select the **Optimize NAS Volume for use as VMware vSphere Datastore** checkbox.
   - To disable VM-consistent snapshots, clear the **Optimize NAS Volume for use as VMware vSphere Datastore** checkbox.
7. Click **OK**.

Restrict Snapshot Access

You can restrict a user's ability to access snapshot files or folders on a NAS volume.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click the **Data Protection** tab.
6. Enable or disable a user's access to snapshot contents:
   - To enable a user's access to a NAS volume snapshot, select the **Access to Snapshot Contents** checkbox.
   - To disable a user's access to a NAS volume snapshot, clear the **Access to Snapshot Contents** checkbox.
7. Click **OK**.

Results

NOTE: Snapshot files and folders will continue to be accessible by backup operators and local administrators even if **Access to Snapshot Contents** is enabled.

View NAS Volumes

View the current NAS volumes.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
   The NAS Volumes panel displays all the current NAS volumes.

Create a NAS Volume

Create a NAS volume to allocate storage that can be shared on the network. When a NAS volume is created, default values are applied.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **NAS volume**.
4. In the NAS Volumes panel, click **Create NAS Volume**.
   The **Create NAS Volume** dialog box opens.
   NOTE: The default security style is Windows for newly created NAS volumes. To change the security style, select **Edit Settings** and then click the **Interoperability** tab.
5. In the **Name** field, type a unique name for the NAS volume.
6. In the **Size** field, type a size for the NAS volume in megabytes (MB), gigabytes (GB), or terabytes (TB).
   NOTE: A NAS volume must have a minimum size of 20 MB.
7. In the **Folder** panel, select a parent folder for the NAS volume.
8. Click **OK**.

Rename a NAS Volume

Rename a NAS volume.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. In the **Name** field, type a new name for the NAS volume.
6. Click **OK**.
   NOTE: Renaming a NAS volume impacts current NFS clients. Those clients receive stale NFS file handle error messages. You must unmount and then remount the NFS mount point with the new name of the volume.

Change Access Time Granularity for a NAS Volume

Change the access time granularity settings of a NAS volume to change the interval at which file-access timestamps are updated.

Steps

1. In the **Storage** view, select a FluidFS cluster.

2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click **Advanced Settings**.
6. In the **Update File Access Time** area, select the interval at which file-access timestamps are updated by selecting the appropriate option: `Always`, `Every Five Minutes`, `Once an Hour`, and `Once a Day`.
7. Click **OK**.

Change Permissions Interoperability for a NAS Volume

Change the permissions interoperability (file security style) settings of a NAS volume to change the file access security style for the NAS volume. Modifying the file security style of a NAS volume affects only the files and directories created after the modification.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. In the **Interoperability** area, select the file permissions interoperability for the NAS volume.
6. Click **OK**.

Change the Space Settings of a NAS Volume

Change the space settings of a NAS volume, including provisioning, size, and reserved space.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. From the **Space Provisioning** drop-down list, select the space provisioning type (`Thick` or `Thin`). These options are described in the online help.
6. In the **Size** field, type a new size for the NAS volume in megabytes (MB), gigabytes (GB), or terabytes (TB).

   NOTE: The new size must be larger than the space used by the NAS volume.

7. (For thin NAS volumes) In the **Reserved Space** field, type the size of the storage that is statically allocated to the NAS volume in megabytes (MB), gigabytes (GB), or terabytes (TB).

   NOTE: The reserved space must be smaller than the configured size of the NAS volume.

8. Click **OK**.

SCSI Unmap

When the SCSI Unmap featured is enabled, deleted pages are returned to the storage pool as block or file storage.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the NAS Pool Advanced Status area, click **Edit Space Reclaming Settings**.

4. To enable SCSI Unmap, select the **Enable SCSI Unmap (TRIM)** checkbox.
5. Click **OK**.

Enable or Disable a NAS Volume Used Space Alert

You can enable an alert that is triggered when a specified percentage of the NAS volume space has been used.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click **Space**.
6. Enable or disable a NAS volume used space alert:
   - To enable a NAS volume used space alert, select the **Used Space Alert** checkbox.
   - To disable a NAS volume used space alert, clear the **Used Space Alert** checkbox.
7. If a NAS volume used space alert is enabled, in the **Used Space Threshold** field, type a number (from 0 to 100) to specify the percentage of used NAS volume space that triggers an alert.
8. Click **OK**.

Enable or Disable a NAS Volume Unused Space Alert

You can enable an alert that is triggered when the remaining unused NAS volume space is below a specified size. This alert is for notification purposes only. The user is responsible for maintaining the space.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click **Space**.
6. Enable or disable a NAS volume unused space alert:
   - To enable a NAS volume unused space alert, select the **Unused Space Enabled** checkbox.
   - To disable a NAS volume unused space alert, clear the **Unused Space Enabled** checkbox.
7. If a NAS volume unused space alert is enabled, in the **Unused Space Alert** field, type a size in megabytes (MB), gigabytes (GB), or terabytes (TB) to specify the unused NAS volume space that triggers an alert.
8. Click **OK**.

Enable or Disable a NAS Volume Snapshot Space Consumption Threshold Alert

You can enable an alert that is triggered when a specified percentage of the NAS volume space has been used for snapshots.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click **Space**.
6. Enable or disable a NAS volume snapshot space consumption threshold alert:

- To enable a NAS volume snapshot space consumption threshold alert, select the **Snapshot Space Aler** checkbox.
- To disable a NAS volume snapshot space consumption threshold alert, clear the **Snapshot Space Aler** checkbox.

7. If a NAS volume snapshot space consumption threshold alert is enabled, in the **Snapshot Space Threshold** field, type a number (from 0 to 100) to specify the percentage of used NAS volume snapshot space that triggers an alert.
8. Click **OK**.

Results

NOTE: Snapshot space is not available for NAS volumes with files processed by data reduction.

Delete a NAS Volume

After deleting a NAS volume, the storage space used by the deleted volume is reclaimed by the NAS pool. Deleting a NAS volume deletes all the files and directories as well as its properties, that is, SMB shares and NFS exports, snapshots definitions, and so on. After it is deleted, the NAS volume cannot be restored unless it is redefined and restored from an external backup.

Prerequisites

- Before a NAS volume can be deleted, you must remove its SMB shares, NFS exports, replications, quota rules, NAS volume clones, and any other reference to the NAS volume.
- Ensure that the NAS volume is not mounted and warn affected clients that the data will be deleted.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK**.

Organizing NAS Volumes in Storage Manager Using Folders

By default, Storage Manager displays NAS volumes in alphabetical order. To customize the organization of NAS volumes in Storage Manager, you can create folders to group NAS volumes.

Create a NAS Volume Folder

Add folders to organize NAS volumes.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. In the NAS Volumes panel, click **Create NAS Volume Folder**.
   The **Create NAS Volume Folder** dialog box opens.
5. In the **Name** field, type a name for the folder.
6. In the **Parent Folder** area, select a parent folder.
7. Click **OK**.

Rename a NAS Volume Folder

Rename a NAS volume folder.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. Click **Edit Settings**.
   The **Edit NAS Volume Folder Settings** dialog box opens.
5. In the **Name** field, type a new name for the folder.
6. Click **OK**.

Change the Parent Folder for a NAS Volume Folder

Change the parent folder for a NAS volume folder.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. Click **Edit Settings**.
   The **Edit NAS Volume Folder Settings** dialog box opens.
5. In the **Parent Folder** area, select a parent folder.
6. Click **OK**.

Move a NAS Volume Into a NAS Volume Folder

To group a NAS volume with other NAS volumes, move it into a NAS volume folder.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. Click **Edit Settings**.
   The **Edit NAS Volume Folder Settings** dialog box opens.
5. In the **Folder** area, select a parent folder.
6. Click **OK**.

Delete a NAS Volume Folder

Delete a NAS volume folder if you no longer want to group NAS volumes.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. Click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK**.
   If the folder contains NAS volumes, they are moved into the (default) root parent folder of the NAS volume folder.

Cloning a NAS Volume

Cloning a NAS volume creates a writable copy of the NAS volume. This copy is useful to test against non-production data sets in a test environment without impacting the production file system environment. Most operations that can be performed on NAS volumes can also be performed on clone NAS volumes, such as resizing, deleting, and configuring SMB shares, NFS exports, snapshots, replication, NDMP, and so on.

The clone NAS volume is created from a snapshot (base snapshot) taken on the original NAS volume (base volume). No space is consumed by the clone NAS volume until new data is stored or it is modified.

NAS Volume Clone Defaults

Clone NAS volumes have the following default values:

- The volumes have the same size as their base volumes, are thin-provisioned, and have a reserved space of 0 (and therefore consume no space).
- Quota usage is copied from the base snapshot of the base volume.
- Quota rules have the default definitions (as with a new NAS volume). Directory quotas have the same definitions as the base volume at the time of the snapshot.
- The volumes have the same permissions on folders (including the root directory) as the base volumes.
- The volumes have the same security style and access time granularity definitions as the base volumes.
- No SMB shares, NFS exports, or snapshot schedules are defined.

NAS Volume Clone Restrictions

The following restrictions exist with clone NAS volumes:

- You cannot create a clone NAS volume of a clone NAS volume (nested clones) unless a clone NAS volume is replicated to another FluidFS cluster and then cloned.
- You cannot delete a base volume until all of its clone NAS volumes have been deleted.
- A snapshot cannot be deleted as long as clone NAS volumes are based on it.
- Restoring to an older snapshot fails if it would result in a base snapshot being deleted.
- You can replicate a clone NAS volume only after the base volume is replicated. If the base snapshot in the base volume is removed, and a clone NAS volume exists on the replication target FluidFS cluster, replication between NAS volumes will stop. To resume replication, the cloned NAS volume on the target FluidFS cluster must be deleted.
- You cannot create a clone NAS volume from a replication source NAS volume snapshot (a snapshot with a name starting with rep_) or NDMP snapshot. However, you can create a clone NAS volume of a replication target NAS volume.
- Before creating a clone NAS volume, data reduction and the snapshot space consumption threshold alert must be disabled on the base volume (previously deduplicated data is allowed).
- Data reduction cannot be enabled on a clone NAS volume.
- After a NAS volume is cloned, data reduction cannot be reenabled until all clone NAS volumes have been deleted.
- A clone NAS volume contains user and group recovery information, but not the NAS volume configuration.
- Clone NAS volumes count toward the total number of NAS volumes in the FluidFS cluster.

View NAS Volume Clones

View the current NAS volume clones.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. Click the **Snapshots & Clones** tab.
   The **Cloned NAS Volume** panel displays the current NAS volume clones.

Create a NAS Volume Clone

Cloning a NAS volume creates a writable copy of the NAS volume.

Prerequisites

- The snapshot from which the clone NAS volume will be created must already exist.
- Data reduction must be disabled on the base volume.
- The snapshot space consumption threshold alert must be disabled on the base volume.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. Click the **Snapshots & Clones** tab and then select a snapshot.
5. Click **Create Cloned NAS Volume** .
   The **Create Cloned NAS Volume** dialog box opens.
6. In the **NAS Volume Name** field, type a name for the NAS volume clone.
7. In the **Folder** area, select a parent folder for the NAS volume clone.
8. Click **OK**.

Delete a NAS Volume Clone

Delete a NAS volume clone if it is no longer used.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and then select a NAS volume.
4. Click the **Snapshots & Clones** tab and then select a clone.
5. Click **Delete**.
   The **Delete** dialog box opens.
6. Click **OK**.

Managing SMB Shares

Server Message Block (SMB) shares provide an effective way of sharing files across a Windows network with authorized clients. The FluidFS cluster supports SMB protocol versions 1.0, 2.0, 2.1, 3.0, and 3.1.1.

When you first create an SMB share, access is limited as follows:

- The Administrator account has full access.
- If you are using Active Directory, the AD domain administrator has full access.

To assign other users access to an SMB share, you must log in to the SMB share using one of these administrator accounts and set access permissions and ownership of the SMB share.

Share-Level Permissions

The default share-level permissions (SLP) for a new share is full control for authenticated users. This control can be modified either:

- Using the MMC tool
- In the Storage Manager **Security** tab of the **Edit Settings** panel

Configuring SMB Shares

View, add, modify, and delete SMB shares.

View All SMB Shares on the FluidFS Cluster

View all current SMB shares for the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **SMB Shares**.
   The SMB Shares panel displays the current shares.

View SMB Shares on a NAS Volume

View the current SMB shares for a NAS volume.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** , and select a NAS volume.
4. Click the **SMB Shares** tab.
   The SMB Shares panel displays the current shares.

Create an SMB Share

Create an SMB share to share a directory in a NAS volume using the SMB protocol. When an SMB share is created, default values are applied for some settings. To change the defaults, you must modify the SMB share.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **SMB Shares**.
4. In the SMB Shares panel, click **Create SMB share**.
   The **Select NAS Volume** dialog box opens.
5. Select a NAS volume on which to create an SMB share and click **OK**.
   The **Create SMB Share** dialog box opens.
6. In the **Share Name** field, type a name for the SMB share.
7. In the **Path** field, specify the directory that you want to share:

   NOTE: A share path must be less than 512 characters long. Fewer characters are accepted if the name is entered in Unicode, because Unicode characters take up a variable amount of bytes, depending on the specific character.

   - To share the root of the NAS volume, leave the **Path** field set to the default value of **/**.
   - To specify an existing directory to share, type the path to the directory in the **Path** field.
   - To browse to an existing directory to share:

     Click **Select Folder**. The **Select Folder** dialog box opens and displays the top-level folders for the NAS volume. Locate the folder to share, select the folder, and click **OK**.

     - To drill down to a particular folder and view the subfolders, double-click the folder name.
     - To view the parent folders of a particular folder, click **Up**.
   - To specify a new directory to share, type the path to the directory to create in the **Path** field and select the **Create Folder If It Does Not Exist** checkbox.
   - To browse existing directories and create a new directory to share:

Click **Select Folder**. The **Select Folder** dialog box opens and displays the top-level folders for the NAS volume. Navigate to the folder in which to create the new folder and click **Create Folder**. The **Create Folder** dialog box opens. In the **Folder Name** field, type a name for the folder, then click **OK** to close the **Create Folder** dialog box. Select the new folder and click **OK**.

   - To drill down to a particular folder and view the subfolders, double-click the folder name.
   - To view the parent folders of a particular folder, click **Up**.

8. (Optional) Configure the remaining SMB share attributes as needed. These options are described in the online help.
   - Type descriptive text for the benefit of administrators in the **Notes** field. This text is not displayed to SMB clients.
   - To prevent clients accessing the share from being able to view the names of folders and files in the share to which they do not have access, select the **Access Based Enumeration** checkbox.
9. Click **OK**.

Delete an SMB Share

If you delete an SMB share, the data in the shared directory is no longer shared but it is not removed.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **SMB Shares**.
4. In the SMB Shares panel, select an SMB share and click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK**.

Set Share-Level Permissions for an SMB Share

Administrators can set initial permissions for an SMB share without having to log in to the share using Windows and setting the folder security properties.

About this task

This procedure grants users share-level permission (full control, modify, or read) for an SMB share.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **SMB Shares**.
4. In the SMB Shares panel, select an SMB share and click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. Click **Share Security**.
   The **Edit SMB Share Settings** dialog box opens.
6. Click the **Add**, **Edit**, or **Remove** link below the permissions table.
   The **Select Account** dialog box opens.
7. Provide the required information and then click **OK**.

Enable or Disable Access-Based Share Enumeration for an SMB Share

When SLP access-based share enumeration is enabled, if a particular user or group does not have share-level permissions for a specific SMB share, the SMB share and its folders and files will not be visible to the user or group. When SLP access-based share enumeration is disabled, the SMB share and its folders and files will be visible to users and groups regardless of whether they have permissions for the SMB share.

Steps

1. In the **Storage** view, select a FluidFS cluster.

2. Click the **File System** tab.
3. In the **File System** view, select **SMB Shares**.
4. In the SMB Shares panel, select an SMB share and click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. Click **Content**.
6. Enable or disable access-based share enumeration:
   - To enable access-based share enumeration, select the **Access Based Enumeration** checkbox.
   - To disable access-based share enumeration, clear the **Access Based Enumeration** checkbox.
7. Click **OK**.

Enable or Disable AES-Based Encryption for an SMB Share

Encryption requires SMBv3 or later. If you are using SMB versions earlier than v3, access to encryption-enabled shares will be denied.

About this task

This procedure enables or disables Advanced Encryption Standard (AES)-based encryption on an SMB share.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **SMB Shares**.
4. In the SMB Shares panel, select an SMB share and click **Edit Settings**.
   The **Edit Settings** dialog box opens.
5. Click **Advanced**.
6. In the **AES-based Encryption** field, select or clear the **Enable** checkbox.
7. Click **OK**.

Enable or Disable SMB Message Signing

To help prevent attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets. SMB2 protocol 3.1.1 dialect adds pre-authentication integrity, cipher negotiation, AES-128-GCM cipher, and cluster dialect fencing. Pre-authentication integrity improves protection from an attacker in tampering with SMB2's connection establishment and authentication of messages. The cipher can be negotiated during connection establishment. In addition to AES-128-CCM cipher used at SMB 3.0.x, Windows 10 (and Windows Server 2016) added AES-128-GCM cipher in SMB 3.1.1. The GCM mode offers a significant performance gain.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Protocols** tab.
5. In the SMB Protocol panel, click **Edit Settings**.
   The **Edit Settings** dialog box opens.
6. Enable or disable required message signing:
   - To enable required message signing, select the **SMB Signing Enforcement** checkbox.
   - To disable required message signing, clear the **SMB Signing Enforcement** checkbox.
7. Click **OK**.

Enable or Disable SMB Message Encryption

SMBv3 adds the capability to make data transfers secure by encrypting data in flight. This encryption protects against tampering and eavesdropping attacks.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Protocols** tab.
5. In the SMB Protocol panel, click **Edit Settings**.
   The **Edit Settings** dialog box opens.
6. Enable or disable message encryption:
   - To enable message encryption, select the **SMB Encryption Enforcement** checkbox.
   - To disable message encryption, clear the **SMB Encryption Enforcement** checkbox.
7. Click **OK**.

Viewing and Disconnecting SMB Connections

You can view active and idle SMB client connections and disconnect individual SMB connections.

Display SMB Connections

To display active and idle SMB connections:

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Activity**.
4. Click the **Sessions** tab.
5. In the Sessions Display Filter panel, use the **All Protocols** drop-down list to display the SMB and NFS connections.
6. Display the SMB connections:
   - To limit the display to SMB connections, select **SMB** from the drop-down list in the Protocol filter.
   - To limit the display to active SMB connections, select **None** from the drop-down list in the Session idle more than filter.
   - To limit the display to idle SMB connections, select a value from the drop-down list in the Session idle more than filter.
7. Click **Apply Filter/Refresh**.

Disconnect an SMB Connection

To disconnect a particular SMB connection:

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Activity**.
4. Click the **Sessions** tab.
5. In the Sessions Display Filter panel, use the **All Protocols** drop-down list to display the SMB and NFS connections.
6. Right-click on a connection and click **Disconnect**.
   The **Disconnect** dialog box opens.
7. Click **OK**.

Using SMB Home Shares

The FluidFS cluster enables you to create a share for a user that is limited to that user. For example, when a user "jsmith" connects to the FluidFS cluster, jsmith will be presented with any available general shares, as well as a share labeled "jsmith" that is visible only to jsmith.

Automatic Creation of Home Share Folders

Automatic creation of home share folders automatically creates folders for users when they log in for the first time. The ownership of the home share is automatically assigned to the user, and the domain administrator is automatically granted full access to the share.

About this task

This procedure enables the automatic creation of home share folders.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **SMB Shares**.
4. In the SMB Shares panel, click **Edit SMB Home Share Settings**.
   The **Set SMB Home Share** dialog box opens.
5. Select the **Enabled** checkbox for the **SMB Home Share** option.
6. Select the **Enabled** checkbox for **Create Folder**.
7. Click **OK**.

Manual Creation of Home Share Folders

Manual creation of home share folders can be accomplished with a script (user-created), batch file, or PowerShell cmdlet that is written by the storage administrator. Alternatively, the storage administrator can manually create these folders to provide stronger access controls to the storage administrator. The storage administrator can decide whether some or all of the users will be given a home share.

Managing ACLs on an SMB Share Folder

When a new share root folder is created from Storage Manager on NTFS and mixed security styles, the folder is assigned the default ACL. You can view and modify the owner, SACL, and DACL for root folders of SMB shares using Storage Manager.

Configure SMB Home Shares

Enable SMB home shares to create a share for a client that is limited to that particular client.

Steps

1. Create an SMB share containing a user-based directory tree:
   a. In the **Storage** view, select a FluidFS cluster.
   b. Click the **File System** tab.
   c. In the **File System** view, select **SMB Shares**.
   d. In the SMB Shares panel, click **Edit SMB Home Share Settings**.
      The **Set SMB Home Share** dialog box opens.
   e. Select the **Enabled** checkbox for the **SMB Home Share** option.
   f. Click **Change** in the NAS Volume area.
      The **Select NAS Volume** dialog box opens.
   g. Select the NAS volume on which the SMB home shares are located and click **OK**.
   h. In the **Initial path** field, specify a folder that is the root of all the users' folders (for example, `/users`).

NOTE: A folder name must be less than 100 characters long and cannot contain the following characters: >, ", \, |, ?, and *

- To specify an existing folder, type the path to the folder in the **Initial path** field.
- To browse for an existing folder:

  Click **Select Folder**. The **Select Folder** dialog box opens and displays the top-level folders for the NAS volume. Locate and select the folder, and then click **OK**.

  - To drill down to a particular folder and view the subfolders, double-click the folder name.
  - To view the parent folders of a particular folder, click **Up**.
- To browse existing directories and create a new folder:

  Click **Select Folder**. The **Select Folder** dialog box opens and displays the top-level folders for the NAS volume. Navigate to the folder in which to create the new folder and click **Create Folder**. The **Create Folder** dialog box opens. In the **Folder Name** field, type a name for the folder, then click **OK** to close the **Create Folder** dialog box. Select the new folder and click **OK**.
  - To drill down to a particular folder and view the subfolders, double-click the folder name.
  - To view the parent folders of a particular folder, click **Up**.

i. From the **Folder template** drop-down list, select the form that the user's folders should take:
   - Select **/Domain/User** if you want the user's folders to take the form *initial_path / domain / user_name*.
   - Select **/User** if you want the user's folders to take the form *initial_path / user_name*.

j. (Optional) Configure the remaining SMB home shares attributes as needed. These options are described in the online help.
   - To prevent clients accessing the share from being able to view the names of folders and files in the share to which they do not have access, click the **Content** tab and select the **Access Based Enumeration** checkbox.
   - To enable virus scanning for SMB home shares, click the **Antivirus Scanners** tab and select the **Virus Scan** checkbox.
   - To exempt directories from antivirus scanning, select the **Folders Filtering Enabled** checkbox and specify the directories in the **Directories excluded from scan** list.
   - To exempt file extensions from antivirus scanning, select the **File Extension Filtering Enabled** checkbox and specify the extensions in the **Extensions excluded from scan** list.
   - To deny access to files larger than the specified antivirus scanning file size threshold, select the **Deny un-scanned large files** checkbox.
   - To change the maximum size of files that are included in antivirus scanning, type a size in the **Virus scan file size threshold** field in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).

k. Click **OK**.

If you did not enable automatic folder creation, perform steps 2 and 3.

2. Give ownership of the SMB home shares to the account that will create the folders (either using a user-created script or manually) for each user's home share.
   a. Using Windows Explorer, connect to the SMB home share initial path.
   b. In the security setting of the SMB share, click **Advanced** and change the owner to **Domain Admins**, a specific domain administrator, or a FluidFS cluster administrator account.
   c. Disconnect from the SMB home share and reconnect to it as the account that has ownership of it.
3. Using Windows Explorer, for each user that you want to be given a home share, create a folder for them that conforms to the folder template you selected previously.

Changing the Owner of an SMB Share

When an SMB share is created, the owner of the SMB share must be changed before setting any access control lists (ACLs) or share-level permissions (SLP), or attempting to access the SMB share. The following methods can be used to initially change the owner of an SMB share:

- Use an Active Directory domain account that has its primary group set as the **Domain Admins** group.
- Use the FluidFS cluster Administrator account (used if not joined to Active Directory or Domain Admin credentials are not available).

Change the Owner of an SMB Share Using an Active Directory Domain Account

The Active Directory domain account must have its primary group set as the **Domain Admins** group to change the owner of an SMB share. These steps might vary slightly depending on which version of Windows you are using.

Steps

1. Open Windows Explorer and in the address bar type: `\\client_vip_or_name`. A list of all SMB shares is displayed.
2. Right-click the required SMB share (folder) and select **Properties**. The **Properties** dialog box opens.
3. Click the **Security** tab and then click **Advanced**. The **Advanced Security Settings** dialog box opens.
4. Click the **Owner** tab and then click **Edit**. The **Advanced Security Settings** dialog box opens.
5. Click **Other users or groups**. The **Select User or Group** dialog box opens.
6. Select the domain admin user account that is used to set ACLs for this SMB share or select the **Domain Admins** group. Click **OK**.
7. Ensure that **Replace owner on subcontainers and objects** is selected and click **OK**.
8. Click the **Permissions** tab and follow Microsoft's best practices to assign ACL permissions for users and groups to the SMB share.

Change the Owner of an SMB Share Using the FluidFS Cluster Administrator Account

If the FluidFS cluster is not joined to Active Directory, use the Administrator account to change the owner of an SMB share. These steps might vary slightly depending on which version of Windows you are using.

Steps

1. Start the **Map network drive** wizard.
2. In **Folder** type: `\\client_vip_or_name\smb_share_name`
3. Select **Connect using different credentials**.
4. Click **Finish**.
5. When prompted, type the Administrator credentials and click **OK**.
6. Right-click the mapped SMB share (folder) and select **Properties**. The **Properties** dialog box opens.
7. Click the **Security** tab and then click **Advanced**. The **Advanced Security Settings** dialog box opens.
8. Click the **Owner** tab and then click **Edit**. The **Advanced Security Settings** dialog box opens.
9. Click **Other users or groups**. The **Select User or Group** dialog box opens.
10. Select the domain admin user account that is used to set ACLs for this SMB share or select the **Domain Admins** group. Alternatively, the FluidFS cluster Administrator account can be used. Click **OK**.
11. Ensure that **Replace owner on subcontainers and objects** is selected and click **OK**.
12. After the owner is set, unmap the network drive.
13. Remap the network drive as the account that has ownership of it, as set previously.
14. Click the **Permissions** tab of the **Advanced Security Settings** dialog box and follow Microsoft's best practices to assign ACL permissions for users and groups to the SMB share.

Managing ACLs or SLPs on an SMB Share

The FluidFS cluster supports two levels of access control to SMB shares, files, and folders:

- **Access control lists (ACLs)**: Govern access to specific files and folders. The administrator can control a wide range of operations that users and groups can perform.
- **Share-level permissions (SLPs):** Govern access to entire shares. The administrator controls only read, change, or full access to an entire share.

SLPs are limited because they only address full control, modify, and read rights for any given user or group at the SMB share level. ACLs control many more operations than only read/change/full access. Use the default setting for SLP (authenticated users has full control) and use ACLs to control access to the SMB share, unless a specific requirement for SLPs cannot be accomplished using ACLs.

A Windows administrator should follow the best practices defined by Microsoft for ACLs and SLPs.

NOTE: Do not attempt to create an SMB share using MMC. Use MMC only to set SLPs.

Automatic ACL to UNIX Word 777 Mapping

When files with Windows ACLs are displayed from NFS clients, the FluidFS mapping algorithm shows a translated UNIX access mode. Perfect translation is not possible, so a heuristic is used to translate from the rich Windows ACL to the 9 bits of the UNIX word. However, when some special SIDs are used inside ACL (for example, creator-owner ACE), the mapping can be inaccurate. For some applications, NFS clients must see the exact mapping or a mapping for more permissive access. Otherwise, the NFS applications might not perform denied operations.

FluidFS versions 5 or later provide an option that causes all objects with SMB ACLs to be presented with UNIX Word 777 from NFS clients (for display only). This option, which is disabled by default, can be configured under NAS Volume settings.

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select a NAS volume.
4. Click **Edit Settings**.
5. In the Edit NAS Volume Settings panel, click **Interoperability**.
6. Select the **Display ACL to UNIX 777 to NFS Clients Enabled** checkbox.

NOTE: Actual data-access checks in FluidFS are still made against the original security ACLs.

This feature applies only to NAS volumes with Windows or mixed security style (for files with Windows ACLs).

Setting ACLs on an SMB Share

To set ACLs, use Windows Explorer procedures. When defining an ACL for a local user account, you must use this format: *client_vip_or_name**local_user_name*

Setting SLPs on an SMB Share Using MMC

To set SLPs, use the Microsoft Management Console (MMC) with the Shared Folder snap-in to set permissions. Administrators can use a predefined MMC file (.msc) from the Windows Server 2008/2012/2016 Start menu and add a Shared Folder snap-in to connect to the FluidFS cluster.

About this task

The MMC does not let you chose which user to connect with a remote computer. By default, it forms the connection through the user logged in to the machine. To connect through a different user:

- If the FluidFS cluster that you are trying to manage is joined to an Active Directory, log in to the management station with *domain*\Administrator.
- Before using MMC, connect to the FluidFS cluster by using the client VIP address in the address bar of Windows Explorer. Log in with the administrator account and then connect to MMC.

  NOTE: You might need to reset the local administrator password first.

Steps

1. Click **Start** → **Run**.
2. Type **mmc** and click **OK**. The **Console 1 - [Console Root]** window opens.
3. Select **File** → **Add/Remove Snap-in**.
4. Select **Shared Folders** and click **Add**.
5. In the **Shared Folders** window, select **Another computer** and type the FluidFS cluster name (as configured in the DNS). Alternatively, you can use a client VIP.
6. Click **Finish**. The new shares tree is displayed in the **Console Root** window.
7. Right-click the required SMB share and select **Properties**.
8. In the **Share Properties** window, click the **Share Permission** tab to set SLPs.

Displaying Security Audit Events

Storage Manager displays a centralized view of the security audit events generated in volumes where SACL events are configured.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab and select **Client Activity**.
3. Click the **SACL Auditing Events** tab.
4. In the **Events** panel, select which security audit events that you want to display.

Audit SACL Access

Set Audit SACL (System Access Control List) Access to enable the type of auditing to be performed when an object (a file or directory with SACL entries) is accessed. If SACL access is not enabled for a NAS volume, then even if a file or directory has SACL entries, the access does not generate an auditing event. Generated events for a NAS volume can be limited to successes, failures, or both.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click **Data protection**.
6. In the **SACL Audit on File Access Events** area, select **On Success**, **On Failure**, or both.
7. Click **OK**.

View Audit SACL Access

You can view SACL (System Access Control List) access to ensure that an auditing event is generated when a file or directory is accessed. To view Audit SACL Access:

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click the **Data Protection** tab.
   The Auditing panel displays the SACL access settings for the volume.

Accessing an SMB Share Using Windows

Microsoft Windows offers several methods for connecting to SMB shares. To access an SMB share, the client must be a valid user (local or remote) and provide a valid password.

Option 1 - net use Command

Run the `net use` command from a command prompt:

About this task

```
net use drive_letter: \\client_vip_or_name\smb_share_name
```

Option 2 - UNC path

Use the UNC path.

Steps

1. From the **Start** menu, select **Run**. The **Run** window opens.
2. Type the path to the SMB share that you want to connect to:
   `\\client_vip_or_name\smb_share_name`
3. Click **OK**.

Option 3 - Map the Share as a Network Drive

Map the share as a network drive.

Steps

1. Open **Windows Explorer** and choose **Tools** → **Map Network Drive**. The **Map Network Drive** dialog box opens.
2. From the **Drive** drop-down list, select any available drive.
3. Either type the path to the SMB share that you want to connect to in the **Folder** field or browse to the SMB share:
   `\\client_vip_or_name\smb_share_name`
4. Click **Finish**.

Option 4 - Network

Connect to the share using the Windows Network. This option does not map the share.

Steps

1. From the **Start** menu, select **Computer**. The **Computer** window opens.
2. Click **Network**.
3. Locate the NAS appliance and double-click it.
4. From the **SMB shares** list, select the SMB share that you want to connect to.

Show Dot Files to SMB Client

You can enable or disable the show dot files setting for each SMB share. By default, the setting is enabled, which means files with names that start with a dot character (period) are shown to SMB clients. When disabled, files that start with a dot are shown with a hidden flag set to SMB clients of all versions (SMB, SMB2) that access the specific share. This setting applies to all files and folders in the system, regardless of the creation origin.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **SMB Shares**.
4. In the SMB Shares panel, select an SMB share and click **Edit Settings**.
   The **Edit SMB Share Settings** dialog box opens.
5. Click **Content**.
6. Enable or disable showing files with names starting with a dot:
   - To enable showing files with names starting with a dot, select the **Show files with name starting with a dot** checkbox.
   - To disable showing files with names starting with a dot, clear the **Show files with name starting with a dot** checkbox.
7. Click **Apply**, then click **OK**.

Branch Cache

Branch cache, when properly configured in both the client computers and the FluidFS cluster, significantly improves performance for consecutive reads from different clients on the same network communicating with FluidFS cluster over WAN.

To optimize WAN bandwidth when users access content on remote servers, branch cache reads content from the main office and caches the content at branch office locations, allowing client computers at branch offices to retrieve the data locally. When branch cache is configured, Windows branch cache clients first retrieve content from the storage system and then cache the content on a computer within the branch office. If another branch-cache-enabled client in the branch office requests the same content, the storage system first authenticates and authorizes the requesting user. The storage system then determines whether the cached content is still up to date and, if it is, sends the client metadata about the cached content. The client then uses the metadata to retrieve content directly from the local host of the cache, if such data exists locally. The client then uses the metadata to retrieve content directly from the cache of the local host.

Branch cache has the following limitations:

- FluidFs will not calculate hash for files smaller than 64 KB or larger than 256 MB.
- The hash calculation will not be performed on read-only, full, or replication destination volumes.

Configuring Branch Cache

Branch cache must be properly configured on each client that supports branch cache on the branch office site.

About this task

On Windows 7 or 8, set the appropriate group policies: **Computer Configuration** > **Policies** > **Administrative Templates** > **Network** > **Turn on BranchCache** > **Enabled**.

On Windows 8.1, you can also configure branch cache using PowerShell cmdlets such as `Enable-BCHostedClient -ServerNames` *hosted_cache_server_name*.

Branch cache is disabled by default. This procedure enables (or disables) branch cache.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **SMB Shares**.
4. In the SMB Shares panel, select an SMB share and click **Edit Settings**.
   The **Edit SMB Share Settings** dialog box opens.
5. Click **Advanced**.
6. Select or clear the **Enable branch cache** checkbox.
7. Click **Apply** > **OK**.

   For more information about branch cache configuration, refer to the technet article located at http://technet.microsoft.com/en-us/library/hh848392.aspx.

Accessing an SMB Share Using UNIX or Linux

Mount the SMB share from a UNIX or Linux operating system using one of the following commands:

```
# mount -t smbfs -o user_name=user_name,password=password//client_vip_or_name/
smb_share_name/local_folder
```

```
# smbmount //client_vip_or_name/smb_share_name/local_folder -o user_name=user_name
```

Managing NFS Exports

Network File System (NFS) exports provide an effective way of sharing files across a UNIX or Linux network with authorized clients. After creating NFS exports, NFS clients then need to mount each NFS export. The FluidFS cluster fully supports NFS protocol version 3 and all requirements of NFS protocol versions 4.0 and 4.1.

- **Supported NFSv4 features**:
  - File and byte-range locking

    NOTE: Starting with FluidFS v6, if the multitenancy feature is enabled, NAS administrators can configure NFSv4 to switch from mandatory to advisory byte-range locks at the tenant level using the CLI.
  - Kerberos v5 security using an AD server
  - AUTH_SYS legacy weak authentication
  - UID translation using an LDAP server (UNIX or AD) or a NIS server
  - UTF-8 file and directory names
- **Unsupported NFSv4 features**:
  - Delegation of file locks to clients
  - Full interoperability between NFSv3 and NFSv4 (for example, conflict resolution for locks from clients using different protocols)
  - Antivirus scanning and result caching
  - LIPKEY and SPKM-3 security (not mandatory in NFSv4.1)
  - Kerberos UNIX server

NFS v4 Implementation

Before implementing NFSv4, note the following, and refer to the respective documentation for your NFSv4 clients:

- **User and Group identification** — NFSv4 users and groups are identified by a <name>@<domain> string (rather than the traditional UID/GID numbers). The NFSv4 server (FluidFS) and clients must be configured to use the same external Network Information Service (NIS) or LDAP domain, which ensures consistent <UID/GID>-<name> mapping of identities. If the string does not map to a domain object, it defaults to the `nobody` identity.
- **Protection mode**— Configure the NAS volume with UNIX security style to allow NFSv4 ACLs. NFSv4 ACLs are supported, but POSIX ACLs are not.
- **Interoperability** —
  - You can modify permissions or ownership to NFSv4 ACL on UNIX volumes. NFSv4 clients can transparently access UNIX/POSIX or NTFS protected files. The accessing identity is translated and checked against the UNIX/POSIX or NTFS ACL metadata (permissions and ownership), to verify access authorization.
  - NFSv4 ACL-protected objects can analogously be accessed by NFSv3 and SMB clients.
- **Single port configuration** — NFSv4 communicates over TCP port 2049 only.

For detailed information about the Network File System (NFS) version 4 protocol, see RFC 7530.

Configuring NFS Exports

View, add, modify, and delete NFS exports, and control the maximum NFS protocol level that the cluster will support.

View All NFS Exports on a FluidFS Cluster

View all current NFS exports for a FluidFS cluster.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **NFS Exports**. The NFS exports are displayed in the right pane.

View NFS Exports on a NAS Volume

To view the current NFS exports for a NAS volume:

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, expand **NAS Volumes** and select a NAS volume.
4. Click the **NFS Exports** tab. The NFS exports are displayed.

Add an NFS Export

Create an NFS export to share a directory in a NAS volume using the NFS protocol. When an NFS export is added, default values are applied for some settings. To change the defaults, you must modify the NFS export.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **NFS Exports**.
4. Click **Create NFS export**. The **Create NFS export** dialog box appears.
5. Select a NAS volume on which to create an NFS export and click **OK**. The **Create NFS export** dialog box appears.
6. In the **Folder Path** field, specify the directory that you want to share:

   NOTE: A folder name must be less than 100 characters long and cannot contain the following characters: >, ", \, |, ?, and *.

   - To share the root of the NAS volume, leave the **Folder Path** field set to the default value of **/**.
   - To use an existing directory to share, type the path to the directory in the **Folder Path** field.
   - To browse to an existing directory to share:

     Click **Select Folder**. The **Select Folder** dialog box appears and displays the top-level folders for the NAS volume. Locate the folder to share, select the folder, and click **OK**.

     - To drill down to a particular folder and view the subfolders, double-click the folder name.
     - To view the parent folders of a particular folder, click **Up**.
   - To view a new directory to share, type the path to the directory to create in the **Folder Path** field and select the **Create Folder If It Does Not Exist** check box.
   - To browse existing directories and create a new directory to share:

     Click **Select Folder**. The **Select Folder** dialog box appears and displays the top-level folders for the NAS volume. Navigate into the folder in which to create the new folder and click **Create Folder**. The **Create Folder** dialog box appears. In the **Folder Name** field, type a name for the folder, then click **OK** to close the **Create Folder** dialog box. Select the new folder and click **OK**.

     - To drill down to a particular folder and view the subfolders, double-click the folder name.

- To view the parent folders of a particular folder, click **Up**.

7. (Optional) Configure the remaining NFS export attributes as needed. These options are described in the online help.
   - Type descriptive text for the benefit of administrators in the **Notes** field. This text is not displayed to NFS clients.
   - To change the client access settings for the NFS export, use the **Add**, **Remove**, and **Edit** buttons.
8. Click **OK**.

Change the Folder Path for an NFS Export

Change the path to the directory that you want to share for an NFS export.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **NFS Exports**.
4. In the right pane, select an NFS export and click **Edit Settings**. The **Edit NFS Export Settings** dialog box appears.
5. In the **Folder Path** field, specify the directory that you want to share:

   NOTE: A folder name must be less than 100 characters long and cannot contain the following characters: >, ", \, |, ?, and *

   - To share the root of the NAS volume, set the **Folder Path** field to **/**.
   - To use an existing directory to share, type the path to the directory in the **Folder Path** field.
   - To browse to an existing directory to share:

     Click **Select Folder**. The **Select Folder** dialog box appears and displays the top-level folders for the NAS volume. Locate the folder to share, select the folder, and click **OK**.

     - To drill down to a particular folder and view the subfolders, double-click the folder name.
     - To view the parent folders of a particular folder, click **Up**.
   - To browse existing directories and create a new directory to share:

     Click **Select Folder**. The **Select Folder** dialog box appears and displays the top-level folders for the NAS volume. Navigate to the folder in which to create the new folder and click **Create Folder**. The **Create Folder** dialog box appears. In the **Folder Name** field, type a name for the folder, then click **OK** to close the **Create Folder** dialog box. Select the new folder and click **OK**.

     - To drill down to a particular folder and view the subfolders, double-click the folder name.
     - To view the parent folders of a particular folder, click **Up**.
6. Click **OK**.

Change the Client Authentication Methods for an NFS Export

Change the authentication method(s) that clients use to access an NFS export.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **NFS Exports**.
4. In the right pane, select an NFS export and click **Edit Settings**. The **Edit NFS Export Settings** dialog box appears.
5. In the middle area, select the check boxes for one or more authentication methods (**UNIX Style**, **Kerberos v5**, **Kerberos v5 Integrity**, or **Kerberos v5 Privacy**) that clients are allowed to use to access an NFS export. These options are described in the online help.
6. Click **OK**.

Change the Client Access Permissions for an NFS Export

Change the permissions for clients accessing an NFS export.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **NFS Exports**.
4. In the right pane, select an NFS export and click **Edit Settings**. The **Edit NFS Exports Settings** dialog box appears.
5. To add access permissions for clients accessing the NFS export:
   a. Click **Add**. The **Add Access Permission** dialog box appears.
   b. In the **Client Machine Trust** area, select an option to specify which client machines (**All Clients**, **Single Client**, **Client Machines in a Network**, or **Client Machines in a Netgroup**) are allowed to access the NFS export. These options are described in the online help.
   c. Specify whether clients have read and write access or read-only access to the NFS export.
      - To allow read and write access, select the **Allow Access for** check box.
      - To allow read-only access, clear the **Allow Access for** check box.
   d. From the **Trust Users** drop-down menu, select which client accounts (**All but root**, **Everybody**, or **Nobody**) are allowed to access the NFS export. These options are described in the online help.
   e. Click **OK**.
6. To change access permissions for clients accessing the NFS export:
   a. Select an entry in the **Access Details** list and click **Edit**. The **Edit Access Permission** dialog box appears.
   b. In the **Client Machine Trust** area, select an option to specify which client machines (**All Clients**, **Single Client**, **Client Machines in a Network**, or **Client Machines in a Netgroup**) are allowed to access the NFS export. These options are described in the online help.
   c. Specify whether clients have read and write access or read-only access to the NFS export.
      - To allow read and write access, select the **Allow Access for** check box.
      - To allow read-only access, clear the **Allow Access for** check box.
   d. From the **Trust Users** drop-down menu, select which clients (**All but root**, **Everybody**, or **Nobody**) are allowed to access the NFS export. These options are described in the online help.
   e. Click **OK**.
7. To remove access permissions for clients accessing the NFS export, select an entry in the **Access Details** list and click **Remove**.
8. Click **OK**.

NOTE: The option *Trust everybody* is not allowed for *All Clients* and must be combined with a restriction to a single client, a network, or a netgroup.

Enable or Disable Secure Ports for an NFS Export

Requiring secure ports limits client access to an NFS export to ports lower than 1024.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **NFS Exports**.
4. In the right pane, select an NFS export and click **Edit Settings**. The **Edit NFS Export Settings** dialog box appears.
5. Enable or disable secure ports.
   - To enable secure ports, select the **Require Secure Port** check box.
   - To disable secure ports, clear the **Require Secure Port** check box.
6. Click **OK**.

Delete an NFS Export

If you delete an NFS export, the data in the shared directory is no longer shared but it is not removed.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **NFS Exports**.
4. In the right pane, select an NFS export and click **Delete**. The **Delete** dialog box appears.
5. Click **OK**.

View or Select the Latest NFS Version Supported

NFS v4 is enabled or disabled on a systemwide basis. By default, NFS v4 is disabled, which forces clients to use NFS v3 and earlier. You might want to use earlier versions if you have clients that are incompatible with NFSv4.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab, and select **Client Accessibility**.
3. In the right pane, click the **Protocols** tab, and then click **Edit Settings**. The **Edit NFS Protocol Settings** dialog box appears.
4. For the **Maximum NFS Protocol Supported** field, click the down-arrow and select the version of NFS that you want to use. The options are NFSv3, NFSv4.0, and NFS v4.1.
5. Click **OK**.

Setting Permissions for an NFS Export

To assign users access to an NFS export, you must log in to the NFS export using a trusted client machine account and set access permissions and ownership of the NFS export using the `chmod` and `chown` commands on the NFS mount point.

Accessing an NFS Export

Clients use the `mount` command to connect to NFS exports on UNIX or Linux systems.

NOTE: The parameters shown in the command lines are recommended parameters. See the `mount` command manual page in the respective operating system for more information and other options.

Global Namespace

Global namespace is a virtual view of shared folders in an organization. This feature allows the Administrator to provide a single point of access for data that is hosted on two or more separate servers.

Global namespace is enabled by default, and can be configured using the CLI. See the white paper *Dell FluidFS FS8600 Appliance CLI Reference Guide* for more information about global namespace commands.

Global Namespace Limitations

- Global namespace is supported on SMB2.x, SMB3.x, and NFSv4.x clients only.
- Global namespace cannot be configured on these volumes:
  - NAS volume that reached full capacity
  - Replication destination NAS volume (or by any other read-only NAS volume)
- NFSv4 redirection targets support NFSv4 protocol (the remote NAS server supports NFSv4, enabling NFSv4 redirections).
- SMB shares cannot be defined on the redirection folder directly. An SMB share is defined on a local folder that contains the redirection folder. The redirection folder cannot be defined on SMB shared folder (even when empty).
- Redirection folders cannot be set on non-empty directories.

- NAS virtual volume backup, restore, replication, and snapshot operations are not supported on the remote target data. It is supported only on the redirection folders (including the redirection data information) that reside inside the local volume data.
- After the NFSv4 or SMB client is redirected to the remote server and establishes the remote connection, the client continues further communication with the remote server.

Additional Documentation

For more information about configuring namespace aggregation, see: Using Dell FluidFS Global Namespace

Using FTP

File Transfer Protocol (FTP) is used to exchange files between computer accounts, transfer files between an account and a desktop computer, or to access online software archives. FTP is disabled by default. Administrators can enable or disable FTP support, and specify the landing directory (volume, path) on a per-system basis.

FTP user access to a file is defined by file permissions. FTP anonymous users are treated as nobody. Access permission is denied or granted, depending on the file's ACLs or UNIX access mode. FTP access respects and interoperates with SMB/NFS file permissions: ACLs, NFSv4 ACLs, UNIX word, SID owner, and UID ownership. FTP access to a file also considers SMB/NFSv4 open file state and byte-range locks. It breaks oplocks when needed.

FTP User Authentication

FTP users can authenticate themselves when connecting to the FTP site or to use anonymous access (if allowed by the FTP site). When authenticated using a user name and password, the connection is encrypted. Anonymous users authenticate using `anonymous` as the user name and a valid email address as the password.

FTP Limitations

- The number of concurrent FTP sessions is limited to 800 sessions per NAS appliance.
- Idle FTP connections time out and close after 900 seconds (15 minutes).
- The FTP client does not follow symbolic links, NFS referrals, or SMB wide-links.
- FTP changes in directory structure (create new file, delete, rename) trigger SMB change notifications.
- FTP access triggers file-access notification events (the File Access Notification feature).
- FTP presents the underlying file system as case sensitive.
- File names have the following limitations:
  - Are case sensitive
  - Cannot be longer than 255 characters
  - Cannot contain any of the following characters:
    - . and ..
    - @Internal&Volume!%File
  - Cannot have a suffix of four, or multiple of three, characters between two ~ signs (for example, ~1234~ and ~123123~)

Enable or Disable FTP

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Client Accessibility**.
4. Click the **Protocols** tab.
5. Scroll down to **FTP Protocol** and click **Edit Settings**. The **Modify FTP Settings** dialog box opens
6. Enable or disable FTP:
   - To enable FTP, select the **Enable FTP** checkbox.
   - To disable FTP, clear the **Enable FTP** checkbox.
7. This dialog box also displays Landing Volume and Landing Directory fields. To change the landing volume or landing directory, click **Select** next to each field.
8. Click **OK**.

Using Symbolic Links

A symbolic link is a special type of file that contains a reference to another file or directory in the form of an absolute or relative path and that affects path name resolution. Symbolic links operate transparently for most operations: programs that read or write to files named by a symbolic link behave as if operating directly on the target file. The symbolic link contains a text string that is automatically interpreted and followed by the operating system as a path to another file or directory.

Local file system symbolic links are available in NTFS starting with Windows Vista and Windows Server 2008, but the symbolic links over SMB are available only with SMB2.

Limitations on Using Symbolic Links

When using symbolic links, note the following limitations:

- SMB1, FTP, and NFS do not support symbolic links.
- Symbolic links are limited to 2,000 bytes.
- User and directory quotas do not apply to symbolic links.
- FluidFS space counting does not count symbolic link data as regular file data.
- Symbolic links are not followed when accessed from snapshot view. They appear as regular files or folders.
- If a relative symbolic link was moved to another location, it might become invalid.
- Cloning SMB symbolic links is not supported.

File Access

Symbolic links are enabled by default. You cannot configure symbolic links in FluidFS, but you can access them using the following Microsoft tools:

- **mklink** – Basic utility used to create both symbolic and hard links (hard links are not supported over SMB, but locally only)
- **fsutil** – File system utility that enables working with reparse points and modifying symbolic links policy

For more information about symbolic links, go to https://msdn.microsoft.com/en-us/library/windows/desktop/aa365680%28v=vs.85%29.aspx.

Managing Quota Rules

Quota rules allow you to control the amount of NAS volume space that a user or group can utilize. Quotas are configured on a per NAS volume basis.

When a user reaches a specified portion of the quota size (soft quota limit), an alert is sent to the storage administrator. When the maximum quota size (hard quota limit) is reached, users cannot write data to the SMB shares and NFS exports on the NAS volume, but no alert is generated.

About Data Reduction

The FluidFS cluster supports two types of data reduction:

- **Data deduplication** – Uses algorithms to eliminate redundant data, leaving only one copy of the data to be stored. The FluidFS cluster uses variable-size block level deduplication as opposed to file level deduplication or fixed-size block level deduplication.
- **Data compression** – Uses algorithms to reduce the size of stored data.

When using data reduction, note the following limitations:

- The minimum file size to be considered for data reduction processing is 65 KB.
- Because quotas are based on logical rather than physical space consumption, data reduction does not affect quota calculations.
- If you disable data reduction, data remains in its reduced state during subsequent read operations by default. You can enable rehydrate-on-read when disabling data reduction, which causes a rehydration (the reversal of data reduction) of data on subsequent read operations. You cannot rehydrate an entire NAS volume in the background, although you could accomplish this task by reading the entire NAS volume.
- Cross-volume deduplication is not supported at this time.

- Data reduction does not support base clone and cloned volumes.

Table 17. Data Reduction Enhancements in FluidFS v6.0 or later

FluidFS v6.0 or later	FluidFS v5.0 or earlier
Data reduction is enabled on a per-NAS-cluster basis.	Data reduction is enabled on a per-NAS-volume basis.
Data reduction supports deduplication of files that are created or reside on different domains.	Data reduction is applied per NAS controller, that is, the same chunks of data that are owned by the different NAS controllers are not considered duplicates.
The distributed dictionary service detects when it reaches almost full capacity and doubles in size (depending on available system storage).	The dictionary size is static and limits the amount of unique data referenced by the optimization engine.

Date Reduction Age-Based Policies and Archive Mode

By default, data reduction is applied only to files that have not been accessed or modified for 30 days to minimize the impact of data reduction processing on performance. The number of days after which data reduction is applied to files is configurable using Storage Manager.

The default number of days is set to 30. When using FluidFS v5 or earlier, you can change the default to as low as 5 days, and you can start data reduction processing immediately (archive mode). Starting with FluidFS v6, there is no archive mode available. You can set the **Exclude Files Accessed in the Last** and **Exclude Files Modified in the Last** defaults to 1 day instead of using archive mode.

For more information about enabling and disabling archive mode, see the *Dell FluidFS FS8600 Appliance CLI Reference Guide*.

Data Reduction Considerations

Consider the following factors when enabling data reduction:

- Data reduction processing has a 5-20% impact on the performance of read operations on reduced data. It does not have any impact on write operations or read operations on normal data.
- The new (reduced) data and metadata is written to the highest tier in the respective Storage Profile of the FluidFS LUNs. Standard data progression process is then applied.
- Increased internal traffic during data reduction processing.
- Data is rehydrated for antivirus scanning.
- Data is rehydrated before being replicated to a target NAS volume. If replication is already configured, the data being reduced was already replicated
- You cannot enable data reduction on a clone NAS volume.
- Data reduction stops automatically when a NAS volume has less than 5 GB of unused space. Therefore, a NAS volume resize can inadvertently stop data reduction.

Configuring Data Reduction

Data reduction must be enabled at the system level and configured on a per NAS volume basis.

Enable or Disable Data Reduction on the FluidFS Cluster

Data reduction must be enabled at the system level before it will run on NAS volumes on which data reduction is enabled. To minimize the impact of data reduction processing on system performance, schedule data reduction to run during off-peak times.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, NAS Pool Advanced Status area, click **Edit Data Reduction Settings**.
   The **Edit Data Reduction Settings** dialog box opens.
4. Enable or disable data reduction on the FluidFS cluster:

- To enable data reduction on the FluidFS cluster, select the **Enable Data Reduction Optimization** checkbox.
- To disable data reduction on the FluidFS cluster, clear the **Enable Data Reduction Optimization** checkbox.

5. Enter the **Data Reduction Optimization Start Time**.
6. Enter the number of hours to run data reduction in the **Data Reduction Optimization Runtime**field.
7. Click **OK**.

Enable Data Reduction on a NAS Volume

Data reduction is enabled on a per NAS volume basis.

Prerequisites

Data reduction must be enabled at the system level before it can run on individual NAS volumes.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the NAS Volume panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click **Data Reduction**.
6. Select the **Data Reduction Enabled** checkbox.
7. For the **Data Reduction Method** field, select the type of data reduction (**Deduplication** or **Deduplication and Compression**) to perform.

   Deduplication and compression will usually save more space, but more resources will be used during data reduction and during reads of data that was compressed, possibly reducing performance.
8. (Optional) Configure the remaining data reduction attributes as needed. These options are described in the online help.
   - To change the number of days after which data reduction is applied to files that have not been accessed, type the number of days in the **Exclude Files Accessed in the Last** field. The number of days must be at least 1.
   - To change the number of days after which data reduction is applied to files that have not been modified, type the number of days in the **Exclude Files Modified in the Last** field. The number of days must be at least 1.
9. Click **OK**.

Change the Data Reduction Type for a NAS Volume

Change the data reduction type (Deduplication or Deduplication and Compression) for a NAS volume.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the NAS Volume panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click **Data Reduction**.
6. For the **Data Reduction Method** field, select the type of data reduction (**Deduplication** or **Deduplication and Compression**) to perform.

   Deduplication and compression will usually save more space, but more resources will be used during data reduction and during reads of data that was compressed, possibly reducing performance.
7. Click **OK**.

Change the Candidates for Data Reduction for a NAS Volume

Change the number of days after which data reduction is applied to files that have not been accessed or modified for a NAS volume.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the NAS Volume panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Specify when to apply data reduction for files:
   - To change the number of days after which data reduction is applied to files that have not been accessed, type the number of days in the **Exclude Files Accessed in the Last** field. The number of days must be at least 1.
   - To change the number of days after which data reduction is applied to files that have not been modified, type the number of days in the **Exclude Files Modified in the Last** field. The number of days must be at least 1.
6. Click **OK**.

Disable Data Reduction on a NAS Volume

By default, after disabling data reduction on a NAS volume, data remains in its reduced state during subsequent read operations. You have the option to enable rehydrate-on-read when disabling data reduction, which causes a rehydration (the reversal of data reduction) of data on subsequent read operations.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the NAS Volumes panel, click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Clear the **Data Reduction** checkbox.
6. Click **OK**.

Viewing Data Reduction Savings

Storage Manager displays data reduction savings for individual NAS volumes and for the FluidFS cluster.

View Data Reduction Savings for a FluidFS Cluster

View the amount (in megabytes) and percentage of storage space reclaimed for a FluidFS cluster as a result of data reduction processing.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
   The **FluidFS NAS Pool Status** panel displays the data reduction savings.

View Data Reduction Savings for a NAS Volume

View the amount (in megabytes) of storage space reclaimed for a NAS volume as a result of data reduction processing.

Steps

1. In the **Storage** view, select a FluidFS cluster.

2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
   The **NAS Volume Status** panel displays the data reduction savings.

FluidFS Data Protection

This section contains information about protecting FluidFS cluster data. Data protection is an important and integral part of any storage infrastructure. These tasks are performed using the Storage Manager Client.

Managing Antivirus

The FluidFS cluster antivirus service provides real-time antivirus scanning of files stored in SMB shares. The antivirus service applies only to SMB shares; NFS is not supported. The scan operation is transparent to the client, subject to the availability of an antivirus server.

Files are scanned when a client tries to read or execute the file.

The antivirus service consists of two components:

- Antivirus servers — one or more network-accessible computers running a supported third-party, ICAP-enabled antivirus application to provide the antivirus scanning service to the FluidFS cluster.
- A FluidFS cluster antivirus scanning policy specifies file extensions and directories to exclude from scans, an antivirus scanning file size threshold, and whether to allow or deny access to files larger than the file size threshold.

When an SMB share client requests a file from the FluidFS cluster, the cluster passes the file to an antivirus server for scanning and then takes one of the following actions:

- If the file is virus-free, the FluidFS cluster permits client access. The FluidFS cluster does not scan that file again, providing it remains unmodified since the last check.
- If the file is infected, the FluidFS cluster denies client access. The client does not know that the file is infected. Therefore:
  - A file access returns a system-specific `file not found` state for a missing file, depending on the client's computer.
  - An access denial might be interpreted as a file permissions problem.

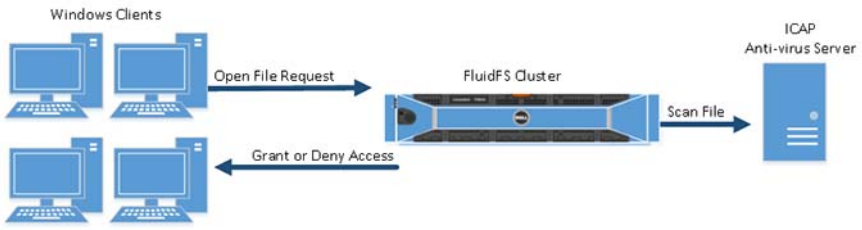


Figure 41. Antivirus Scanning

Only storage administrators can recover an uninfected version of the file, or access and process the infected file. To gain access to an infected file, you must connect to the SMB share through another SMB share on which the antivirus service is disabled. Otherwise, the FluidFS cluster recognizes the file as infected, and denies access. You can also access the file through an NFS export, because NFS does not support antivirus scanning.

File transfers between the FluidFS cluster and the anti-virus server are not encrypted, so communication should be protected or restricted.

Supported Antivirus Applications

For the latest list of supported antivirus applications, see the *Dell Fluid File System Support Matrix*.

Configuring Antivirus Scanning

To perform antivirus scanning, you must add an antivirus server and then enable antivirus scanning for each SMB share.

NOTE: If any of the external services are configured with IPv6 link-local addresses, the monitor will always show these services as `Unavailable`.

Managing Snapshots

Snapshots are read-only, point-in-time copies of NAS volume data. Storage administrators can restore a NAS volume from a snapshot if needed. In addition, clients can easily retrieve files in a snapshot, without storage administrator intervention.

Snapshots use a redirect-on-write method to track NAS volume changes. That is, snapshots are based on a change set. When the first snapshot of a NAS volume is created, all snapshots created after the baseline snapshot contain changes from the previous snapshot.

Various policies can be set for creating a snapshot, including when a snapshot is to be taken and how long to keep snapshots. For example, mission-critical files with high churn rates might need to be backed up every 30 minutes, whereas archival shares might only need to be backed up daily.

If you configure a NAS volume to use VM-consistent snapshots, each snapshot creation operation such as scheduled, manual, replication, or NDMP automatically creates a snapshot on the VMware server. This feature enables you to restore the VMs to the state they were in before the NAS volume snapshot was taken.

Because snapshots consume space on the NAS volume, ensure that you monitor available capacity on the NAS volume and schedule and retain snapshots in a manner that ensures that the NAS volume always has sufficient free space available for both user data and snapshots. Also, to be informed when snapshots are consuming significant NAS volume space, enable a snapshot consumption alert.

The FluidFS cluster automatically deletes one or more snapshots for a NAS volume in the following cases:

- If you delete a NAS volume, the FluidFS cluster deletes all of the snapshots for the NAS volume.
- If you restore a NAS volume from a snapshot, the FluidFS cluster deletes all the snapshots created after the snapshot from which you restored the NAS volume.

Dedicated FluidFS Snapshot Profiles

For FluidFS deployments, Storage Manager creates a dedicated FluidFS snapshot that is automatically assigned to FluidFS LUNs (storage volumes). The profile setting defaults to Daily, and the retention policy is to delete after 25 hours.

Creating On-Demand Snapshots

Create a NAS volume snapshot to take an immediate point-in-time copy of the data.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the **NAS Volume Status** panel, click the **Snapshots & Clones** tab.
5. In the **Snapshot** area, click **Create**.
   The **Create Snapshot** dialog box opens.
6. In the **Snapshot** field, type a name for the snapshot.
7. (Optional) Configure the remaining snapshot attributes as needed. These options are described in the online help.
   - To retain the snapshot indefinitely, clear the **Snapshot Expiration Enabled** checkbox.
   - To expire the snapshot in the future, select the **Snapshot Expiration Enabled** checkbox and specify a day and time on which to expire the snapshot.
8. Click **OK**.

Managing Scheduled Snapshots

You can create a schedule to generate snapshots regularly. To minimize the impact of snapshot processing on system performance, schedule snapshots during off-peak times. Snapshots created by a snapshot schedule are named using this format *<snapshot_schedule_name>_YYYY_MM_DD__HH_MM*

Create a Snapshot Schedule for a NAS Volume

Create a NAS volume snapshot schedule to take a scheduled point-in-time copy of the data.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Snapshot & Clones** tab.
5. In the **Snapshot Schedules** area, click **Create**.
   The **Create Snapshot Schedule** dialog box opens.
6. In the **Snapshot Schedule** field, type a name for the snapshot schedule.
7. Specify when to create snapshots:
   - To create a snapshot based on a period of time, select the **Take snapshot every** option and type the frequency in minutes, hours, days, or weeks.
   - To create a snapshot based on day and time, select the **Take snapshot on** option and select the days and times.
8. (Optional) Configure the remaining snapshot schedule attributes as needed. Replication provides three different snapshot retention policies: Identical (default), Minimum, and Archive with Retention Period in Days. These options are described in the online help.
   - To retain all snapshots that are created by the snapshot schedule indefinitely, clear the **Take snapshot every** option.
   - To expire the snapshots that are created by the snapshot schedule in the future, select the **Retain each snapshot for** option and specify the retention period for snapshots in minutes, hours, days, or weeks in the adjacent fields.
9. Click **OK**.

Change the Snapshot Frequency for a Snapshot Schedule

Change how often to create snapshots for a snapshot schedule.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the **NAS Volume Status** panel, click the **Snapshots & Clones** tab.
5. Select a snapshot schedule and click **Edit Settings**.
   The **Edit Snapshot Schedule** dialog box opens.
6. Specify when to create snapshots:
   - To create a snapshot based on a period of time, select the **Take snapshot every** option and type the frequency in minutes, hours, days, or weeks.
   - To create a snapshot based on day and time, select the **Take snapshot on** option and select the days and times.
7. Click **OK**.

Change the Retention Policy for a Snapshot Schedule

Specify whether to retain all snapshots that are created by a snapshot schedule or expire the snapshots after a period of time.

Steps

1. In the **Storage** view, select a FluidFS cluster.

2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the **NAS Volume Status** panel, click the **Snapshots & Clones** tab.
5. Select a snapshot schedule and click **Edit Settings**.
   The **Edit Settings** dialog box opens.
6. Specify the retention policy.

   NOTE: Replication using current snapshot – This option of the "archive" retention policy affects setting up a new replication of a volume. You can replicate using the current snapshot, rather than replicating from all the previous snapshots.

7. Click **OK**.

Delete a Snapshot Schedule

Delete a snapshot schedule if you no longer want to take a scheduled point-in-time copy of the data.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the **NAS Volume Status** panel, click the **Snapshots & Clones** tab and then select a snapshot schedule.
5. Select a snapshot schedule and click **Delete**.
   The **Delete** dialog box opens.
6. Click **OK**.

Modifying and Deleting Snapshots

Manage snapshots that were created on demand or by a schedule.

Rename a Snapshot

To rename a snapshot:

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the **NAS Volume Status** panel, click the **Snapshots & Clones** tab.
5. Select a snapshot and click **Edit Settings**.
   The **Edit Snapshot Settings** dialog box opens.
6. In the **Name** field, type a new name for the snapshot.
7. Click **OK**.

Change the Retention Policy for a Snapshot

Specify whether to retain the snapshot indefinitely or expire the snapshot after a period of time.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the **NAS Volume Status** panel, click the **Snapshots & Clones** tab.

5. Select a snapshot and click **Edit Settings**.
   The **Edit Snapshot Settings** dialog box opens.
6. Specify the retention policy:
   - To retain the snapshot indefinitely, clear the **Snapshot Expiration Enable** checkbox.
   - To expire the snapshot in the future, select the **Snapshot Expiration Enable** checkbox and specify a day and time on which to expire the snapshot.
7. Click **OK**.

Delete a Snapshot

Delete a snapshot if you no longer need the point-in-time copy of the data.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the **NAS Volume Status** panel, click the **Snapshots & Clones** tab.
5. Select a snapshot and click **Delete**.
   The **Delete** dialog box opens.
6. Click **OK**.

Restoring Data from a Snapshot

You can restore data in two ways:

- **Restore individual files**: After a snapshot is created, the FluidFS cluster creates a client-accessible snapshots directory containing a copy of the files included in the snapshot. Clients can easily restore individual files from a snapshot using copy and paste, without storage administrator intervention. This method is useful for the day-to-day restore activities of individual files.
- **Restore a NAS volume from a snapshot:** The storage administrator can restore an entire NAS volume by rolling the state back to the time of an existing snapshot. This method is useful in the case of an application error or virus attacks.

Snapshots retain the same security style as the active file system. Therefore, even when using snapshots, clients can access only their own files based on existing permissions. The data available when accessing a specific snapshot is at the level of the specific share and its subdirectories, ensuring that users cannot access other parts of the file system.

View Available Snapshots

View snaphots available for restoring data.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the **NAS Volume Status** panel, click the **Snapshots & Clones** tab.
   The **Snapshots** list displays the snapshots.

Restore a NAS Volume From a Snapshot

The storage administrator can restore an entire NAS volume from a snapshot. The restored NAS volume will contain all the NAS volume data that existed at the time the snapshot was created. Each file in the restored NAS volume will have the properties, such as permission and time, that existed when you (or a schedule) created the snapshot.

Prerequisites

After you restore a NAS volume from a snapshot:

- The FluidFS cluster deletes any snapshots that were created after the snapshot from which you restored the NAS volume. Snapshots created before the snapshot from which you restored the NAS volume are not affected.
- Current SMB clients of the NAS volume are automatically disconnected.
- Current NFS clients of the NAS volume receive `stale NFS file handle` error messages. You must unmount and then remount the NFS exports.

CAUTION: The restore operation cannot be undone. Any data created or changed between the time of the snapshot and when the restore operation is completed is permanently erased. You should restore a NAS volume from a snapshot only if you first understand all the repercussions of the restore operation.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. In the **NAS Volume Status** panel, click the **Snapshots & Clones** tab.
5. Select a snapshot and click **Restore NAS Volume**.
   The **Restore NAS Volume** dialog box opens.
6. Click **OK**.

Option 1 – Restore Files Using UNIX, Linux, or Windows

This restore option allows clients to restore a file from a snapshot using copy and paste.

Steps

1. Access the NFS export or SMB share.
2. Access the `.snapshots` directory.
3. Find the snapshot according to its time of creation.
4. Copy the file to its original location.

Option 2 – Restore Files Using Windows Only

Snapshots integrate into the Shadow Copies and previous versions features of Windows. This restore option allows clients to restore a file using previous versions.

Steps

1. Right-click the file and then select **Properties**.
2. Click the **Previous Versions** tab.
   A list displays the available previous versions of the file.
3. Select the version to restore and then click **Restore**.

Disabling Self-Restore

Steps

1. In the **Storage view**, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click **Edit Settings**.
   The **Edit NAS Volume Settings** dialog box opens.
5. Click **Data Protection**.
6. To allow or prevent user access to snapshot content:
   - To allow user access to snapshot content, select the **Access to Snapshot Contents** checkbox.
   - To prevent user access to snapshot content, clear the **Access to Snapshot Content** checkbox.
7. Click **OK**.

Managing NDMP

The FluidFS cluster supports Network Data Management Protocol (NDMP), which is an open standard protocol that facilitates backup operations for network attached storage, including FluidFS cluster NAS volumes. NDMP should be used for longer-term data protection, such as weekly backups with long retention periods.

The FluidFS cluster supports remote and three-way backup architecture implementations, wherein a supported, external Data Management Application (DMA) server mediates the data transfer between the FluidFS cluster and the storage device. The FluidFS cluster supports full, differential, and incremental NDMP Level Based Backup (levels 0-9), Full, Incremental/Differential Token Based Backup, and Direct Access Recovery (DAR). The FluidFS cluster supports NDMP versions 3 and 4 (default mode).

The FluidFS cluster includes an NDMP server that is responsible for the following operations:

- Processing all NDMP backup and restore requests sent from DMA servers
- Sending all NDMP replies and notification messages to DMA servers
- Transferring data over the network to or from remote NDMP tape or data servers

The NDMP server handles all communications with the DMA servers and other NDMP devices through an XDR encoded TCP (Transmission Control Protocol) data stream.

The NDMP server supports two backup types:

- **dump**: Generates inode-based NDMP file history
- **tar**: Generates path-based NDMP file history

The backup type is controlled by the NDMP environment variable **TYPE**. Both backup types support the same functionalities, but the **tar** backup type might be able to process the information more efficiently for certain DMA servers.

Backup and Restore – NDMP

Backup and Restore Applications on page 434 lists the supported backup and restore applications. See the *Dell Fluid File System Support Matrix* for the latest information.

Table 18. Backup and Restore Applications

Application	Supported Version
CommVault Simpana	11.x
Dell Quest NetVault	10.x, 11.x
EMC Networker	9.x
IBM Tivoli Storage Manager	6.3
Symantec BackupExec	2014, 2015
Symantec NetBackup	7.x

Refer to the application documentation for the minimal revision/service pack supporting Dell FluidFS systems.

Supported Tape Libraries on page 434 lists the supported tape libraries for 2–way NDMP backup (Fibre Channel connections only).

Table 19. Supported Tape Libraries

Supplier	Models
Dell	TL-2000, TL-4000, ML-6000

NDMP Agent Characteristics on page 434 lists the supported range for each of the NDMP characteristics.

Table 20. NDMP Agent Characteristics

Functionality	Supported Range
NDMP version	v2, v3, v4
DMA address type	IPv4 only
DMA servers configured	Up to 10

Table 20. NDMP Agent Characteristics (continued)

Functionality	Supported Range
Concurrent NDMP sessions	Up to 10
DMA user-name length	1–63 bytes (accepts Unicode)
DMA password length	1–32 characters
Maximum number of *include* paths for an NDMP job	32
Maximum number of *exclude* paths for an NDMP job	32

NOTE: Your environment should allow ICMP (ping) traffic between the FluidFS controllers' private IP addresses (not the access VIPs) and the backup server.

Supported NDMP Environment Variables on page 435 describes the NDMP environmental variables that are supported by FluidFS. Refer to the Data Management Application (DMA) documentation for a listing of the variables supported by DMA. If DMA does not set any of the variables, the NDMP server operates with the default value.

Table 21. Supported NDMP Environment Variables

Variable Name	Description	Default
TYPE	Specifies the type of backup/restore application. Valid values are `dump` and `tar`, and are case sensitive. `dump` – NDMP server generates inode-based file history. `tar` – NDMP server generates file-based file history.	dump
FILESYSTEM	Specifies the path to be used for backup. The path must be a directory.	Not applicable
LEVEL	Specifies the dump level for the backup operation. Valid values are `0` to `9`.	`0`
HIST	Specifies how file history is to be generated. The supported values are `d`, `f`, `y`, and `n`. `d` specifies that node/dir format file history will be generated. `f` specifies that file-based file history will be generated. `y` specifies that the default file history type (which is the node/dir format) will be generated. `n` specifies that no file history will be generated.	`Y`
DIRECT	Specifies whether the restore is a Direct Access Retrieval. Valid values are `Y` and `N`.	`Y`
UPDATE	Specifies whether the dump level and dump time for a backup operation should be updated on the NDMP server so that subsequent backups can reference the dump level from previous backups. Valid values `Y` and `N`.	`Y`
EXCLUDE	Specifies a pattern for file or directory names that are not to be backed up. The pattern is a comma-separated list of file or directory names, up to 32. Each name will be used to match to nodes encountered during backup. A name can contain an asterisk (*)as the wildcard character. The comma (,) or backslash (\ )characters in a name should be escaped with a backslash.	No default
RECURSIVE	Specifies whether the restore should be recursive or not. Valid values are `Y` and `N`. If this variable is set to `N`, only the files that are the immediate children of the restore target are restored.	`Y`
RESTORE_OVERWRITE	Specifies whether the restore operation should overwrite existing files with the backup data. Valid values are `Y` and `N`.	`Y`
LISTED_INCREMENTAL	Controls behavior similar to the `listed incremental` option of the tar application. This variable specifies whether an additional directory listing	`N`

Table 21. Supported NDMP Environment Variables (continued)

Variable Name	Description	Default
	is added to the backup stream during incremental backup so that the recovery operation can handle files and directories deleted between the incremental backups. During backup, if this variable is set, an additional directory listing is added to the backup data stream. Because of the additional process required, this addition could affect the backup data stream size and performance. During recovery, if this variable is set and if the backup data stream was generated with this variable turned on, the NDMP server handles deleting files and directories that are deleted between incremental backups. Setting this variable requires additional processing time and enlarges the backup data stream size (how much it changes depends on the number of elements in the backup data set). If this feature is not important to the end user, it should not be set.	
BASE_DATE	Used by TSM for token-based backup, as an alternative to using the LEVEL environment variable. When BASE_DATE is set to `0`, a full backup is performed. After a full backup completes, a token can be retrieved by retrieving the DUMP_DATE environment variable. This token can then be passed in later backups as the value of BASE_DATE. The backup performed in this case is an incremental backup relative to the time when the token was generated. When BASE_DATE is set to `-1`, token-based backup is disabled.	`-1`
DEREF_HARD_LINK	Controls whether hard link files data content are backed up for all instances of the same file. Valid values are `Y` and `N`.	`N`

Incremental Backups

Each time a backup is performed, the NDMP server stores the timestamp for the backup. When the NDMP server performs an incremental backup, it uses the timestamp stored for the previous full or incremental backup to determine if a directory or file needs to be included.

Both supported backup types (dump and tar) support incremental backup. The algorithm for traversing the backup target directory is the same. However, because inode-based file history generation has different requirements to support DAR, the backup data stream generated is different:

- **dump**: Each directory visited will be backed up and a file history entry will be generated. It does not matter whether the directory has changed.
- **tar**: Backs up and generates a file history entry only for the directories that have changed.

Therefore, the amount of data backed up using a tar backup will be less than that of a dump backup. The size difference depends on the number of directories in the backup data set.

Handling Hard Links

NDMP backup handles hard link files in the most efficient way by default. That is, the hard link files' data content will be backed up only once. After the backup operation encounters the first hard link file and backs up its content, the backup process remembers the inode number of that file. Subsequently, when the backup operation encounters files with the same inode number, only the header is backed up. When this backup data stream is restored, the hard link files will be recovered as hard link files.

This mode of backup could create a problem in the case of a selective restore when the selected files or directories to be restored contain hard link files that are not the first instance encountered during backup. In this case, the restore fails and an NDMP message is sent to the DMA server indicating the first instance of the file that should also be included in the selective restore.

To work around this problem, change the behavior during backup. If a backup is started with the **DEREF_HARD_LINK** environment variable set to **Y**, the backup will back up all instances of the hard link files as if they were regular files, rather

than just backing up the first instance of the hard link files. In this case, a selective restore will always have the file data. The disadvantage of this option is that backups might take longer and more space is required to back up a data set with hard link files.

Backing Up NAS Volume Data Using NDMP

The FluidFS cluster does not use a dedicated IP address for backup operations; any configured client network address can be used. Data is sent over Ethernet. Multiple NDMP backup and restore sessions can run at the same time with a maximum of 48 sessions per NAS controller. To minimize the impact of NDMP backup processing on system performance, schedule NDMP operations during off-peak times.

About this task

After you configure NDMP in a FluidFS cluster, the NDMP server monitors the client network for backup requests from the DMA servers. The DMA server then accesses (mounts) the NAS volumes that it intends to back up and initiates the backup operations.

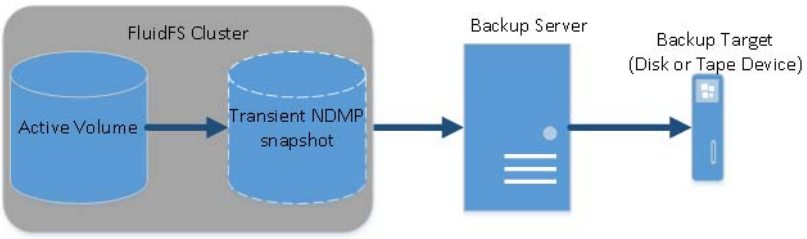


Figure 42. NDMP Backups

Keep the following considerations in mind when backing up NAS volume data using NDMP:

- NDMP does not provide high availability (HA). If a backup session is interrupted due to connection loss, the session is terminated.
- Manually deleting the temporary snapshot for the current backup session is not allowed and will immediately terminate the session.
- If a backup session is terminated with an error, the temporary snapshot might be left in place, and the system will delete the snapshot automatically.

The following steps outline the process for backing up NAS volume data with NDMP:

Steps

1. The DMA server creates a connection to the FluidFS cluster IP address.
2. The NDMP server on the FluidFS cluster creates a temporary snapshot of each NAS volume that the DMA server designated for backup. Alternatively, when performing a backup of replication target NAS volumes, the FluidFS cluster does not create a dedicated NDMP snapshot. Instead, it uses the base replica snapshot from the last successful replication.

   Temporary NDMP snapshots are named using the following format: `ndmp_backup_session_id_controller_number`
3. The NDMP server copies the NAS volume data to the DMA server.
4. After receiving the data, the DMA server moves the data to a storage device, such as a local disk or tape device.
5. After the backup completes, the NDMP server deletes the temporary snapshots.

NDMP Environment Variables

NDMP environment variables control the behavior of the NDMP server for each backup and restore session.

To determine whether the DMA server supports setting these environment variables, refer to the documentation for your DMA server. If the DMA server cannot set a particular environment variable, the NDMP server operates with the default value.

The following table summarizes the supported environment variables.

Environment Variable	Description	Used In	Default Value
TYPE	Specifies the type of backup and restore application. The valid values are: ● **dump** – NDMP server generates inode-based file history ● **tar** – NDMP server generates file-based file history	Backup and Restore	dump
FILESYSTEM	Specifies the path to be used for the backup. The path must be a directory.	Backup	None
LEVEL	Specifies the dump level for the backup operation. The valid values are **0** to **9**.	Backup	0
HIST	Specifies how file history is to be generated. The valid values are: ● **d** – Specifies that node/dir-format file history will be generated ● **f** – Specifies that file-based file history will be generated ● **y** – Specifies that the default file history type (which is the node/dir format) will be generated ● **n** – Specifies that no file history will be generated	Backup	y
DIRECT	Specifies whether the restore is a Direct Access Retrieval. The valid values are **Y** and **N**.	Backup and Restore	Y
UPDATE	Specifies whether the dump level and dump time for a backup operation should be updated on the NDMP server so that subsequent backups can reference the dump level from previous backups. The valid values are **Y** and **N**.	Backup	Y
EXCLUDE	Specifies a pattern for matching to directory and file names that are not to be backed up. This environment variable is a list of strings separated by commas. Each entry is matched against nodes encountered during backup. The string can contain an asterisk (*) as the wildcard character, but the asterisk must be the first or last character of the pattern. A maximum of 32 comma-separated strings are supported.	Backup	No exclude pattern is specified by default
RECURSIVE	Specifies whether the restore should be recursive. The valid values are **Y** and **N**. If this environment variable is set to **N**, only files that are the immediate children of the restore target are restored.	Restore	Y
RESTORE_OVERWRITE	Specifies whether the restore operation should overwrite existing files with the backup data. The valid values are **Y** and **N**.	Restore	Y
LISTED_INCREMENTAL	Specifies whether an additional directory listing is added to the backup stream during incremental backup so that the restore operation can handle files and directories deleted between the incremental backups. This environment variable controls behavior similar to the `listed incremental` option of the tar application. The valid values are **Y** and **N**. During backup, if this variable is set to **Y**, an additional directory listing is added to the backup data stream. Because of the additional processing required, this option could impact the backup data stream size and performance. During restore, if this variable is set to **Y** and the backup data stream was generated with this variable set to **Y**, the NDMP server will handle deleting files and directories that are deleted between incremental backups. Setting this variable to **Y** requires additional processing time and increases the backup data stream size (the size of the increase depends on the number of elements in the backup data set). If this feature is not important in your environment, this variable should not be set.	Backup and Restore	N
BASE_DATE	Specifies whether a token-based backup is performed. Token-based backup is used by Tivoli Storage Manager as an alternative	Backup	-1

Environment Variable	Description	Used In	Default Value
	to backups using the LEVEL environment variable. The valid values are: • **-1** – Specifies that token-based backup is disabled • **0** – Specifies that a token-based backup is performed. After the backup completes, a token can be retrieved by using the DUMP_DATE environment variable. This token can then be passed in a subsequent backup as the value of BASE_DATE. The backup performed in this case will be an incremental backup relative to the time when the token was generated.		
DEREF_HARD_LINK	Specifies whether hard link files' data content is backed up for all instances of the same file. The valid values are **Y** and **N**.	Backup	N

Supported DMA Servers

For the latest list of supported DMA servers, see the *Dell Fluid File System Support Matrix*.

Configuring NDMP

Before you can begin an NDMP backup, you must add a DMA server and configure the NDMP user name, password, and client port.

Add or Remove a DMA Server

Configure one or more DMA servers from which the NDMP server can service NAS volume backup requests. Any number of DMA servers can perform backups at any point in time.

Prerequisites

- The DMA server must be network accessible.
- The DMA server must run a supported NDMP backup application.

Remove a DMA server if it is no longer needed for NDMP backups.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Cluster Connectivity**.
4. Click the **Backup** tab.
5. In the **NDMP** pane, click **Edit Settings**.
   The **Edit NDMP Settings** dialog box opens.
6. In the **DMA Servers Hosts** field, type the IP address of a DMA server.
   - To add a DMA server, click **Add**.
   - To remove a DMA server, click **Remove**.

   Repeat this step for any additional DMA servers.
7. Click **OK**.

Change the NDMP Password

A user name and password are required when configuring an NDMP server in the DMA. The default password is randomized and must be changed prior to using NDMP.

Steps

1. In the **Storage** view, select a FluidFS cluster.

2. Click the **File System** tab.
3. In the **File System** view, click **Cluster Connectivity**.
4. Click the **Backup** tab.
5. In the **NDMP** pane, click **Change Backup User Password**.
   The **Change Backup User Password** dialog box opens.
6. In the **Password** field, type an NDMP password. The password must be at least seven characters long and contain three of the following elements: a lowercase character, an uppercase character, a digit, or a special character (such as +, ?, or *).
7. In the **Confirm Password** field, retype the NDMP password.
8. Click **OK**.

Change the NDMP User Name

A user name and password are required when configuring an NDMP server in the DMA. By default, the user name is backup_user. You can change this user name if needed.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Cluster Connectivity**.
4. Click the **Backups** tab.
5. In the **NDMP** pane, click **Edit Settings**.
   The **Edit NDMP Settings** dialog box opens.
6. In the **Backup User** field, type a new NDMP user name.
7. Click **OK**.

Change the NDMP Client Port

By default, the NDMP server monitors port 10000 for incoming connections. You can change the client port to match the port used by the DMA.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Cluster Connectivity**.
4. Click the **Backup** tab.
5. In the **NDMP** pane, click **Edit Settings**.
   The **Edit NDMP Settings** dialog box opens.
6. In the **NDMP Port** field, type a new client port.
7. Click **OK**.

Specifying NAS Volumes Using the DMA

To perform backup and restore operations, the DMA server must be configured to be able to access the FluidFS cluster.

On each DMA server, you must configure the following components:

- Client VIP (or a DNS name) that the DMA server accesses. If you change the client VIP, you must also make the appropriate change on the DMA servers.
  NOTE: NDMP has no load balancing built in. A single DMA backing up 10 NAS volumes from a single client VIP forces all 10 sessions on the same NAS controller. Therefore, use DNS round-robin to provide load balancing by specifying the DNS name of the FluidFS cluster in the DMA.
- NDMP user name and password (default user name is backup_user)
- Port that the NDMP server monitors for incoming connections (default port is 10000)

(Optional) In addition, some DMA servers require more information, such as the host name of the FluidFS cluster, OS type, product name , and vendor name.

- Host name of the FluidFS cluster, which uses the following format:*controller_number.FluidFS_cluster_name*
- OS type – DellFluid File System
- Product – Compellent FS8600
- Vendor – Dell

Most backup applications automatically list the available NAS volumes to back up. Otherwise, you can manually type in the NAS volume path. The FluidFS cluster exposes backup NAS volumes at the following path:

```
/NAS_volume_name
```

To improve data transfer speed, increase the number of concurrent backup jobs to more than one per NAS controller, distributing the load across the available NAS controllers.

NDMP Exclude File Under Paths Using FluidFS

When you define a backup using DMA, you can select specific directories from the virtual NAS volume to include in, or exclude from, backup jobs.

Requirements

The following requirements must be met to include or exclude NDMP paths:

- The path specified can be a directory or a file. If the path is a directory, all child elements of that directory will be included in (or excluded from) the backup.

  Each path specified is a child of the backup root directory and must start with a forward slash (/).

- The maximum number of paths that you can include or exclude is 32.
- Each path can be a maximum of 128 bytes long.
- The first or the last element of the path can contain a wildcard character (*).
- If both include and exclude paths are defined, the NDMP server will first check for include, then check for exclude.

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click **Edit Settings**.

   The **Edit NAS Volume Settings** dialog box opens.

5. Select **Data Protection**.
6. Select or clear the **NDMP Exclude Files Under Paths** checkbox.
7. Specify a path to exclude and click **Add**.

NDMP Exclude Files Matching the Patterns Using FluidFS

Configuring DMA clients with data-exclusion patterns might not work with a few backup vendors such as BackupExec and Netbackup. FluidFS has an option for handling exclude paths and patterns, which will be skipped when executing NDMP backup on the NAS volume.

This option can be configured at the NAS volume level, and is available under NAS Volume Settings.

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. Select a NAS volume and click **Edit Settings**.
4. In the **Edit NAS Volume Settings** panel, click **Data Protection**.
5. Select the **NDMP Exclude Files Matching the Patterns Enabled** checkbox.
6. Specify a pattern to exclude and click **Add**.

Viewing NDMP Jobs and Events

All NDMP jobs and events can be viewed using Storage Manager.

View Active NDMP Jobs

View all NDMP backup and restore operations being processed by the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Cluster Connectivity**.
4. Select **Backup**.
   The **NDMP Sessions** area displays the NDMP jobs.

Managing Replication

Replication copies NAS volume data from the local (source) FluidFS cluster to a different NAS volume on the local FluidFS cluster or to a remote (target) FluidFS cluster.

The following figure shows an overview of remote replication between NAS volumes on different FluidFS clusters.

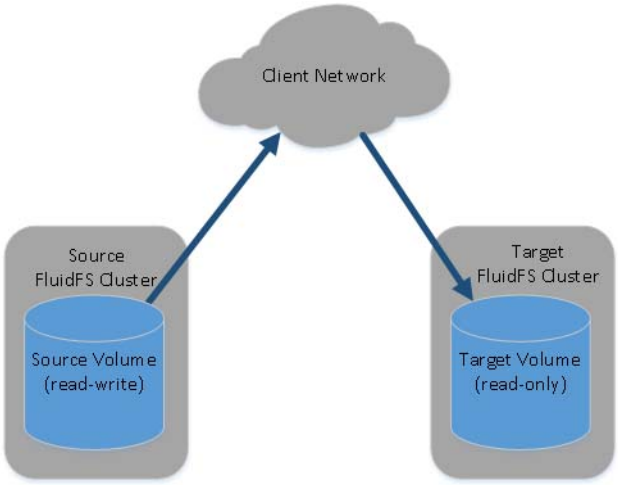


Figure 43. Remote Replication

The following figure shows an overview of local replication between NAS volumes on a single FluidFS cluster or to a different NAS volume on the local FluidFS cluster.

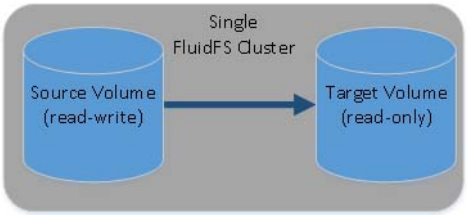


Figure 44. Local Replication

Replication can be used in various scenarios to achieve different levels of data protection.

Replication Scenarios	Description
Fast backup and restore	Maintains full copies of data for protection against data loss, corruption, or user mistakes
Remote data access	Applications can access mirrored data in read-only mode, or in read-write mode if NAS volumes are promoted or cloned
Online data migration	Minimizes downtime associated with data migration
Disaster recovery	Mirrors data to remote locations for failover during a disaster

Configuring replication is a three-step process:

- Add a replication partnership between two FluidFS clusters.
- Add replication for a NAS volume.
- Run replication on demand or schedule replication.

How Replication Works

Replication leverages snapshots. The first time you replicate a NAS volume, the FluidFS cluster copies the entire contents of the NAS volume. For subsequent replication operations, the FluidFS cluster copies only the data that changed since the previous replication operation started. This design allows for faster replication, efficient use of system resources, and saves storage space while keeping data consistent. Replication is asynchronous, meaning that each source NAS volume can have a unique schedule for replicating data to the target NAS volume.

The amount of time replication takes depends on the amount of data in the NAS volume and the amount of data that has changed since the previous replication operation.

When replicating a NAS volume to another FluidFS cluster, the other FluidFS cluster must be set up as a replication partner. Each FluidFS cluster can have multiple replication partners, enabling you to replicate different NAS volumes to different partners, depending on operational requirements. However, each individual NAS volume can be replicated to only one target NAS volume on one replication partner. The following figure summarizes which replication scenarios are supported.

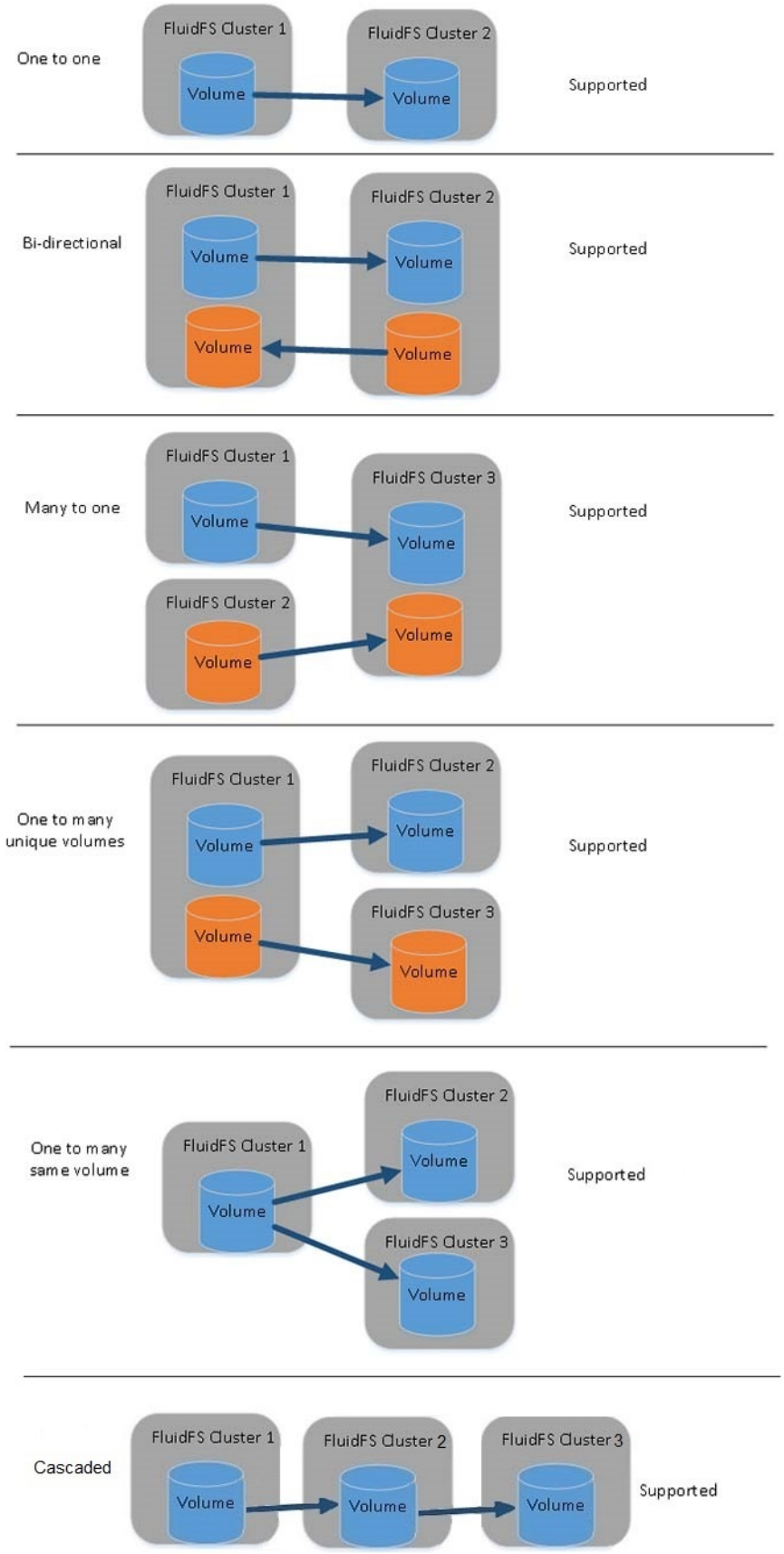


Figure 45. Replication Scenarios

After a partner relationship is established, replication between the partners can be bidirectional. One system could hold target NAS volumes for the other system as well as source NAS volumes to replicate to that other system.

A replication policy can be set up to run according to a set schedule or on demand. Replication management flows through a secure SSH tunnel from system to system over the client network.

To access or recover data, you can promote a target NAS volume to a recovery NAS volume and grant clients access to the recovery NAS volume data. The recovery NAS volume will appear as if it is a local NAS volume.

Target NAS Volumes

A target NAS volume is a read-only copy of the source NAS volume that resides on the target FluidFS cluster. The target NAS volume holds identical system configuration information (quota rules, snapshot policy, security style, and so on) as the source NAS volume. You can promote target NAS volumes to recovery NAS volumes temporarily or permanently and grant clients access to recovery NAS volume data.

The following considerations apply to target NAS volumes:

- Unlike source NAS volumes, you cannot create snapshots of target NAS volumes.
- The target FluidFS cluster must have enough free space to store the target NAS volumes.
- The system retains only the current replica of the source NAS volumes. To roll back to a previous point in time, you must use snapshots.
- You can either replicate the source NAS volume to an existing NAS volume or to a new target NAS volume. If you replicate to an existing NAS volume, the NAS volume must not contain any data you want to retain. Any data residing on the NAS volume will be overwritten and cannot be recovered.
- Target NAS volumes count toward the total number of NAS volumes in the FluidFS cluster.

Managing Replication Partnerships

When replicating a NAS volume to another FluidFS cluster, the other FluidFS cluster must be set up as a replication partner. This setup is a bidirectional replication trust; source NAS volumes and target NAS volumes can be located on either system.

Add a Replication Partnership

Add a replication partner before configuring replication.

Prerequisites

- Both the source and target FluidFS clusters must be managed by the same Storage Manager Data Collector.
- The target FluidFS cluster should be at the same or later FluidFS version than the source FluidFS cluster.
- The source and target FluidFS clusters must be able to communicate with each other so that replication operations can occur.
- Verify that the FluidFS replication ports are open on your firewall to allow replication between the source and target FluidFS clusters. The list of required ports can be found in the*Dell Fluid File System Support Matrix*. FluidFS supports using a single port for replication if both replication partners are running FluidFS v5 or later.
- The target FluidFS cluster has enough space to replicate the data from the source FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Replications**.
4. Cick the **Remote Clusters** tab, then click **Add Remote Cluster**.
   The **Add Remote Cluster** wizard starts.
5. Select the remote FluidFS cluster and click **OK**.

   Valid port numbers are 10560 or 3260.

Change the Local or Remote Networks for a Replication Partnership

Change the local or remote replication network or IP address for a replication partnership. NAS volumes can be replicated only between tenants that are mapped on the local and remote FluidFS clusters.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Replications**.
4. Click the **Remote Clusters** tab, select a remote cluster, and then click **Edit Settings**.
   The **Edit Remote NAS Cluster Settings** dialog box opens.
5. Click **Add**.
   The **Add Tenants Mapping for Replication** dialog box opens.
6. Select a tenant from the **Local FluidFS Cluster** drop-down list.
7. Select a tenant from the **Remote FluidFS Cluster** drop-down list.
8. Click **OK**.

Delete a Replication Partnership

When you delete a replication partnership, the replication relationship between the source and target FluidFS clusters is discontinued. When deleting a replication partnership, ensure that both systems are up and running. If both systems are up, the replication partnership is deleted on both systems. If one of the systems is down or unreachable, the partnership is deleted only on the system that is up. After the other system comes back up, the partnership must be deleted on that system as well.

Prerequisites

Replications between the replication partners must be deleted.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Replications**.
4. Click the **Remote Clusters** tab.
5. Select a remote FluidFS cluster and click **Delete**.
   The **Delete** dialog box opens.
6. Click **OK**.

Replication Throttling

Replication throttling can fine-tune network bandwidth usage for replication of a pair of NAS volumes between two clusters.

Users can limit FluidFS replication bandwidth usage by:

- Lowering bandwidth usage during work hours and increasing bandwidth consumption during nighttime
- Increasing bandwidth usage during weekends

How Replication Throttling Works

Replication throttling:

- Creates a new system entity named **QoS node** and defines bandwidth allocation in KBps
- Defines usage percentage per hour of the week
- Binds a QoS (Quality of Service) node (network level) of outgoing traffic to a replication. The average network usage should not exceed the bandwidth allocation in a minute timeframe. The default is not to limit the bandwidth for replication.

Limitations

The following limitations apply to replication throttling:

- The maximum number of active outgoing replications is 10. If more than 10 replications are active, they are queued.
- The maximum number of active incoming replications is 100. If more than 100 replications are active, they are queued.
- The maximum number of replication partners is 100.
- The maximum number of replicated NAS volumes or containers (source and target) on a cluster is 1024.
- The maximum number of replication schedules per system is 1024.

Define a QoS Node

Create a QoS (Quality of Service) definition to bind a QoS node (network level) of outgoing traffic to a replication.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Replications**.
4. Click the **Replication QoS Nodes** tab.
5. Click **Create QoS Node**.
   The **Create Replication QoS Node** dialog box opens.
6. Type a name and choose the bandwidth limit for the node in KB/s.
7. Click **OK**.
   The **Edit Replication QoS Schedule** dialog box opens.
8. Drag the mouse to select an area, right-click on it, and choose the percentage of the bandwidth limit to allow in these day and hour combinations.
9. Click **OK**.

Change a QoS Node

Change a QoS (Quality of Service) node (network level) of outgoing traffic bound to a replication.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Replications**.
4. Click the **Replication QoS Nodes** tab.
5. Right-click on a QoS and select **Edit Settings**.
   The **Edit Replication QoS Settings** dialog box opens.
6. Change the name and/or the bandwidth limit for the node in KB/s.
7. Click **OK**.
   The **Edit Replication QoS Schedule** dialog box opens.
8. Drag the mouse to select an area, right-click on it, and choose the percentage of the bandwidth limit to allow in these day and hour combinations.
9. Click **OK**.

Configure Replication Throttling

Use replication throttling to fine-tune network bandwidth usage for replication of a pair of NAS volumes between two clusters.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Replications**.
4. Click the **Replication NAS Volumes** tab, select a replication, and then right-click.
5. Select **Replication Actions**.
6. From the drop-down list, select **Edit Replication QoS**.

7. Select the **Enable QoS** checkbox and then select a predefined QoS node from the drop-down list.
8. Click **OK**.

Change Replication Throttling

To disable replication throttling on a QoS node:

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Replications**.
4. Click the **Replication NAS Volumes** tab, select a replication, and then right-click.
5. Select **Replication Actions**.
6. From the drop-down list, select **Edit Replication QoS**.
7. Clear the **Enable QoS** checkbox to disable using a QoS node.
8. Click **OK**.

Single Port Replication

With single-port replication, communication for all involved components uses only one port. The single port infrastructure supports communication over IPv4 and IPv6, and is opened on all controller IPs and client VIPs.

Single port replication provides the following features:

- Trusted cluster establishment
- File system communication using a single common replication port
- Replication management communication using a single common replication port

Replicating NAS Volumes

You can perform manual and scheduled replication operations, and pause, resume, delete, and monitor replication.

One-to-Many and Cascaded Replications

FluidFS replication supports one-to-many and cascaded replications.

This feature creates more complicated replication formations. For example, this feature supports:

- Multiple disaster recoveries for the same NAS volume
- Distribution of the same data to multiple destinations around the world
- Cascading the data from the production cluster to another cluster and replicating from this cluster to reduce the load on the production cluster

One-to-Many

One-to-many replication connects a source NAS volume to multiple destination NAS volumes. A NAS volume can be connected as the source NAS volume in more than one replication pair at the same time. The destination NAS volumes can be on different clusters. One-to-many replications are independent and can be run in parallel.

Limitation

When using one-to-many replication, the destination NAS volume can consume more space than the source NAS volume because it has more snapshots.

Cascaded

A NAS volume that is the destination of one replication can serve as the source NAS volume for another replication. The replication data can be cascaded from a NAS volume to a second NAS volume and from it to a third NAS volume and so on. Multiple NAS volumes that are connected in a cascaded replication can also include one-to-many replications.

Limitation

When using cascaded replication for replications that are not alike, a replication can be limited when the different replication is not a cascaded replication.

Display One-to-Many and Cascaded Replications

About this task

A NAS administrator can determine that one-to-many and cascaded replications is configured by noticing the following change for a volumes:

- The same NAS volume is in the replication source list and replication destination list
- NAS volume status has a new possible status: `source and destination`
- A table of both replications and status for each replication instead of only one or the other

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand**Replications** and then select a cluster.
   The right pane displays the NAS volumes that are defined as the source and destination of the replication.

Add Replication for a NAS Volume

Adding replication creates a replication relationship between a source NAS volume and a target NAS volume. After adding replication, you can set up a replication policy to run according to a set schedule or on demand.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click **Create Replication**. The **Create Replication** wizard starts.

   If **Inline Data Reduction for Replication Optimization** is enabled, NAS volume replication will try to optimize network utilization by reducing the amount of data copied. Dell recommends either **Conditional Compression** or **Deduplication and Conditional Compression** as the inline data reduction method because it dynamically enables compression for in-flight data based on system utilization. This option is completely independent of normal FluidFS data reduction (dedupe and compression). Data that is already reduced is rehydrated and then reduced in-flight on its way to the remote destination.
5. Select a remoteFluidFS cluster, a policy from **Snapshot Retention Policy at the destination**, and a node from **Limit Replication Bandwidth According to QoS node** (if enabled), and then click **Next**.
   The **Select Remote NAS Volume** page opens.
6. Specify a target NAS volume using one of the following options:
   - Select an existing NAS volume on the target FluidFS cluster.
   - Create a NAS volume on the target FluidFS cluster.

     Click **Create Remote Volume**. The **Create NAS Volume** dialog box opens. In the **Name** field, type a name for the NAS volume. In the **Size** field, type a size for the NAS volume that is the same size or larger than the source NAS volume. In the **Folder** field, select a parent folder for the NAS volume. Click **OK** to close the dialog box, then select the newly created NAS volume.
7. Click **Finish**.

Delete Replication for a NAS Volume

Deleting replication for a NAS volume is similar to disabling replication for a NAS volume in that it does not disrupt replication operations for other NAS volumes or the replication partnership between the source and target FluidFS clusters. After deleting replication, the target NAS volume becomes a standalone, writable NAS volume. You can delete replication from either the source or target FluidFS cluster.

Prerequisites

- The target NAS volume must be promoted to a standalone NAS volume.
- You must remove replication schedules for the replication.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Replications** tab.
5. In the Replication Status area, click **Delete**.
   The **Delete** dialog box opens.
6. Click **OK**.

Run Replication On Demand

After a replication is created, you can replicate a NAS volume on demand. You can run replication only from the source FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Replications** tab.
5. In the Replication Status area, click **Manual Start**.
   The **Start Manual Replication** dialog box opens.
6. Click **OK**.

Schedule Replication

After a replication is created, you can schedule replication for a NAS volume to run regularly. You can schedule replication only from the source FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Replication** tab.
5. In the Replication Schedules area, click **Create**. T
   he **Create Replication Schedule** dialog box opens.
6. In the **Schedule Name** field, type a name for the replication schedule.
7. Specify when to run replication:
   - To run replication based on a period of time, select the **Replicate every** checkbox and type the frequency in minutes, hours, days, or weeks.
   - To run replication based on day and time, select the **Replicate on** checkbox and select one or more days and times.
8. Click **OK**.

Change a Replication Schedule

Change the frequency that replication runs for a replication schedule.

Steps

1. In the **Storage** view, select a FluidFS cluster.

2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Replication** tab.
5. Select a replication schedule and click **Edit Settings**.
   The **Edit Replication Schedule Settings** dialog box opens.
6. Specify when to run replication:
   - To run replication based on a period of time, select the **Replicate every** checkbox and type the frequency in minutes, hours, days, or weeks.
   - To run replication based on day and time, select the **Replicate on** checkbox and select one or more days and times.
7. Click **OK**.

Delete a Replication Schedule

Delete a replication schedule if you no longer want replication to run regularly. You can delete a replication schedule only from the source FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Replications** tab.
5. Select a replication schedule and click **Delete**.
   The **Delete** dialog box opens.
6. Click **OK**.

Pause Replication

When you pause replication, any replication operations for the NAS volume that are in progress are suspended. While replication is paused, scheduled replications do not take place. If you require multiple replications to be paused, perform the following steps for each replication. You can pause replication only from the source FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Replications** tab.
5. In the Replication Status area, click **Pause** .
   The **Pause Replication** dialog box opens.
6. Click **OK**.

Resume Replication

When you resume replication, any replication operations that were in progress at the time the operation was paused will resume. In addition, any replication schedules will resume at their next scheduled time. Replication can be resumed for individual NAS volumes. You can resume replication only from the source FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Replications** tab.
5. In the Replication Status area, click **Resume** .
   The **Resume Replication** dialog box opens.

6. Click **OK**.

Monitoring Replication Progress and Viewing Replication Events

The progress of replication operations and events related to replication can be viewed using Storage Manager.

Monitor Replication Progress

Monitor the progress of all replication operations being processed for the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Replications**.
4. Click the **Replications** tab.
   The **Replication Status** area displays the progress for each replication.

View Replication Events

Events related to replication can be viewed using Storage Manager.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Replications**.
4. Click the **Replication Events** tab.
   The replication events are displayed.

Results

You can search for specific replication events by typing search text in the box at the bottom of the **Replications** panel.

Recovering an Individual NAS Volume

You can access or restore data from a target NAS volume if needed.

Promote a Target NAS Volume

Promoting a target NAS volume to a recovery NAS volume makes the target NAS volume writable, and clients can manually fail over to it. This operation can be performed regardless of whether the source NAS volume is available. The recovery NAS volume's data will be complete up to the point in time of the most recent successful replication. When you promote a target NAS volume, any replication operations for the NAS volume that are in progress are suspended. You can promote a target NAS volume from either the source or target FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Replications** tab.
5. In the Replication Status area, click **Promote Destination**.
   The **Promote Destination** dialog box opens.
6. Click **OK**.

Demote a Target NAS Volume

Demote the target NAS volume to resume the original replication operations. When you demote a target NAS volume, all data written to the recovery NAS volume while it was temporarily promoted will be lost. You can demote a target NAS volume only from the source FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** viewe, expand **NAS Volumes** and select a NAS volume.
4. Click the **Replications** tab.
5. Select **Demote Destination**.
   The **Demote Destination** dialog box opens.
6. Click **OK**.

Using Replication for Disaster Recovery

You can create a disaster recovery configuration in which you replicate data from a primary FluidFS cluster to a target FluidFS cluster that you can fail over to if the primary FluidFS cluster stops responding because of an unexpected failure (hardware, disk, and so on). The target FluidFS cluster could either be used solely for backup for the primary site, or it could have its own NAS volumes sharing data at the target site. In a bi-directional configuration, both FluidFS clusters can act as a failover target for each other.

After you have fixed the reason that caused the original FluidFS cluster to fail, you can manually fail back to the original configuration in which clients access data on the source NAS volume, which in turn replicates to the target NAS volume. Depending on time and bandwidth considerations, failing back to the source NAS volume might take a considerable amount of time to complete.

The following considerations apply when using replication for disaster recovery:

- If the original source NAS volume is no longer available, you can configure the recovery NAS volume to replicate to another NAS volume in the original source FluidFS cluster. However, if the original source NAS volume is available, fail back to it. Failing back to the original source NAS volume usually takes less time than failing back to a new NAS volume. If the FluidFS clusters have a common snapshot, they only need to synchronize the data that changed after that snapshot was created. If no common snapshot is available, or if replicating to a new NAS volume, all data must be synchronized.
- A single FluidFS cluster cannot contain two sets of SMB home shares. Consider the example that Cluster A and Cluster B both have SMB home shares, for different sites or user bases. Cluster A and Cluster B both serve as replication destinations for each other's NAS volume that contains the SMB home shares. If the administrator tries to fail over Cluster A's NAS volume that contains SMB home shares to Cluster B, Cluster B rejects this operation because it already has SMB home shares defined on it.

Managing the DNS Configuration for Single NAS Volume Failover

For single NAS volume failover, it is important that the environment is set up to properly migrate clients of the NAS volumes you are failing over, without disrupting the clients of other NAS volumes you are not failing over.

When a NAS volume is failed over from one FluidFS cluster to another, the IP addresses that are used to access it change from Cluster A's IP addresses to Cluster B's IP addresses. You can facilitate this change using DNS. It is recommended to set up a DNS entry to correlate to each NAS volume, and change the DNS entry for single NAS volumes when they are failed over.

For example, suppose Marketing and Sales have their own NAS volumes, each with an SMB share on the NAS volumes named **marketing_share** and **sales_share** respectively. A DNS entry named **FluidFSmarketing**, is created for Marketing and another DNS entry for Sales named **FluidFSsales** is created. Both NAS volumes point to the same set of client VIPs on source Cluster A. Marketing can access the Marketing NAS volume or SMB share using **\\FluidFS marketing\marketing**, and Sales can access the Sales NAS volume or SMB share using **\\FluidFSsales\sales**.

Initially, both DNS entries **FluidFSmarketing** and **FluidFS sales** point to the same set of client VIPs. At this point, both the **marketing** and **sales** SMB shares can be accessed from either one of the DNS names, **FluidFSmarketing** or **FluidFS sales**. When you want to fail over a single NAS volume (for example **Marketing**) change the DNS entries for **FluidFSmarketing** to resolve to the client VIPs on Cluster B.

Maintain a table to track which DNS entries are used to access each NAS volume. This helps when performing failover and setting up group policies.

Setting Up and Performing Disaster Recovery

This section contains a high-level overview of setting up and performing disaster recovery. In these instructions, **Cluster A** is the source FluidFS cluster containing the data that must be backed up and **Cluster B** is the target FluidFS cluster, which backs up the data from source cluster A.

Prerequisites

Prerequisites

- Cluster B is installed, but has no NAS volumes configured.
- Cluster A and Cluster B are at the same FluidFS version.
- Cluster B has different network settings (client, SAN, internal, and so on) than source Cluster A, however, Cluster A and Cluster B must be able to communicate with each other so that replication operations can occur.
- Cluster B has enough space to replicate all data from Cluster A.

Phase 1 — Build up the replication partnership between Cluster A and Cluster B

Set up replication between Cluster A and Cluster B.

Steps

1. From Cluster A, set up a replication partnership between Cluster A and Cluster B.
2. Create a regular replication schedule so that the target volumes in Cluster B always have an up-to-date replication copy for Cluster A.

   The replication policy must be a one-to-one match on a volume basis, for example:

   Source volume A1 (Cluster A) to target volume B1 (Cluster B)

   Source volume A2 (Cluster A) to target volume B2 (Cluster B)

   NOTE: If NFS exports are used, the NAS volume names of the source and target should be the same, as the export path name includes the NAS volume name. This is not relevant for SMB shares.

   Source volume A*n* (Cluster A) to target volume B*n* (Cluster B)

3. Ensure that at least one successful replication has occurred for all the source volumes in Cluster A.

   If the replication fails, fix the problems encountered and restart the replication process.

4. Record all Cluster A settings for future use. Replication restore is not a complete BMR (bare metal restore). Settings such as network configuration (client, SAN, and internal) cannot be backed up and restored using the replication method. Note all Cluster A settings (for use when restoring Cluster A) including network configuration, cluster wide settings such as cluster name, alert settings, and so on for future use. If the system restore operation fails to restore these settings, you can manually restore the Cluster A settings back to their original values.

Phase 2 — Cluster A fails and clients request failover to target Cluster B

If Cluster A stops responding because of an unexpected failure, fail over to Cluster B.

Steps

1. From Cluster B, promote the target volumes in Cluster B. This transforms the original target volumes (B1, B2, .. B*n*) to standalone NAS volumes and makes them writable.
2. Delete the replication policies for the original source volumes (A1, A2, .., A*n*).
3. Apply the source volume configuration from the original source volumes in Cluster A to the target volumes in Cluster B.
4. Restore the users and groups configuration from Cluster A. This restores the Cluster B users and groups to Cluster A settings.
5. Ensure that Cluster B is used to temporarily serve client requests during the failover time.
   a. Choose one of the following options:
      - IP address-based failovers: Change the IP addresses for Cluster B to match the IP addresses used by Cluster A. Existing client connections might break and might need to be re-established.
      - DNS-based failovers: Point the DNS names from your DNS server to Cluster B instead of Cluster A.

Ensure that the DNS server on Cluster B is the same as the DNS server or in the same DNS farm as the DNS server of Cluster A. Existing client connections might break and might need to be re-established. You must unmount and re-mount the NFS exports on the clients.

b. (Single NAS volume failovers) Manually update the DNS entry for the NAS volume that was failed over. This redirects clients that are accessing this volume from Cluster A to Cluster B, while other clients keep accessing other volumes using the same DNS name. Client systems might need to refresh their DNS cache.

c. (Single NAS volume failovers) To force SMB and NFS clients to Cluster B, you must delete the SMB shares and NFS exports on Cluster A. This forces the SMB and NFS clients to reconnect, at such time they are connected to Cluster B. After restoring the source volume's configuration on Cluster B, all of the SMB shares and NFS exports will be present on the target volume (on Cluster B), so no SMB share/NFS export configuration information is lost.

   The failed over volume can now be accessed using the exact same DNS name and SMB share/NFS export name as it was when hosted on Cluster A, except now it is hosted on Cluster B.

d. Join Cluster B to the AD server or LDAP/NIS.

   Ensure that the AD server and LDAP server are in the same AD/LDAP farm or same server.

Phase 3—Restore Cluster A and fail back from Cluster B to Cluster A

After you have fixed the reason that caused Cluster A to fail, fail back over to Cluster A.

Steps

1. Fix the reason that caused Cluster A to fail and if required reinstall FluidFS.
2. Rebuild the FluidFS cluster:
   - IP address-based failovers: Use the settings for Cluster A that you recorded earlier, but change the IP addresses for Cluster A to match the IP addresses originally used by Cluster B.
   - DNS-based failovers: Use the settings for Cluster A that you recorded earlier.
3. From Cluster B, set up a replication partnership between Cluster B and Cluster A.
4. Configure replication for all the promoted recovery volumes in Cluster B, and specify that they replicate back to the original source volumes in Cluster A.

   The replication policy must be a one-to-one match on a volume basis, for example:

   Source volume B1 (Cluster B) to target volume A1 (Cluster A)

   Source volume B2 (Cluster B) to target volume A2 (Cluster A)

   Source volume B*n* (Cluster B) to target volume A*n* (Cluster A)

5. Manually perform replication on the promoted recovery volumes in Cluster B (B1, B2, .., B*n*). Proceed to the next step when replication completes.

   If the replication fails, fix the problems encountered and restart the replication process. Ensure that all the NAS volumes are successfully replicated to Cluster A.

6. From Cluster A, promote the original source volumes (A1, A2, .., A*n*).
7. From Cluster B, delete replication for the promoted recovery volumes (B1, B2, .., B*n*) and apply the source volume configuration from Cluster B to Cluster A. Repeat this procedure to delete all the replication policies and bring all target volumes in Cluster A to standalone NAS volumes.
8. From Cluster A, restore the users and groups configuration from Cluster B. This restores the Cluster A users and groups configuration to Cluster B settings.

   NOTE: If the system configuration restore fails, manually set the system back to the original settings (use the settings for Cluster A that you recorded earlier).

9. Start using Cluster A to serve client requests.
   a. Choose one of the following options:
      - IP address-based failovers: Change the IP addresses for Cluster A to match the IP addresses originally used by Cluster A and change the IP addresses for Cluster B to match the IP addresses originally used by Cluster B. Existing client connections might break and might need to be re-established.
      - DNS-based failovers: Point the DNS names from your DNS server to Cluster A instead of Cluster B.

Ensure that the DNS server on Cluster A is the same as the DNS server or in the same DNS farm as the DNS server of Cluster B. Existing client connections might break and might need to be re-established. You must unmount and re-mount the NFS Exports on the client.

b. (Single NAS volume failovers) Manually update the DNS entry for the NAS volume that was failed over. This redirects clients that are accessing this volume from Cluster B to Cluster A, while other clients keep accessing other volumes using the same DNS name. Client systems might need to refresh their DNS cache.
c. (Single NAS volume failovers) To force SMB and NFS clients to Cluster A, you must delete the SMB shares and NFS exports on Cluster B. This forces the SMB and NFS clients to reconnect, at such time they are connected to Cluster A. After restoring the source volume's configuration on Cluster A, all of the SMB shares and NFS exports will be present on the target volume (on Cluster A), so no SMB share/NFS export configuration information is lost.

   The failed over volume can now be accessed using the exact same DNS name and SMB share/NFS export name as it was when hosted on Cluster B, except now it is hosted on Cluster A.

d. Join Cluster A to the AD server or LDAP/NIS.
e. From Cluster A, configure replication between the original source volumes (A1, A2,.. , A*n*) and the original target volumes (B1, B2,.. , B*n*) to prepare for the next disaster recovery.

File Access Notification

File access notification occurs when both systemwide file access auditing configuration is enabled and file operation matches any active (enabled) preconfigured file access notification policy for the volume. Auditing events are generated after permissions check for the file operation and before the actual execution of the operation.

About this task

NOTE: Third-party software is required to provide auditing capabilities. The following third-party software applications are supported:

- Varonis DataAdvantage
- Dell Quest ChangeAuditor

See the FluidFS Support Matrix for the latest supported third-party software applications.

Steps

1. From the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, select **Cluster Connectivity**.
4. In the **Cluster Connectivity** panel, click the **External Servers** tab.
5. Under **External Audit**, click **Edit Settings**.
   The **External Audit Settings** dialog box opens.
6. Select the **External Audit** checkbox.
7. Provide the information for the **Subscriber Name** and **Auditing Server Hosts** fields.
8. Click **OK**.

FluidFS Monitoring

This section contains information about monitoring the FluidFS cluster. These tasks are performed using the Storage Manager Client.

Monitoring NAS Appliance Hardware

Storage Manager displays an interactive, graphical representation of the front and rear views of NAS appliances.

Storage Manager also displays the status of the following NAS appliance and NAS controller hardware components:

- Interfaces
- Disks

- Backup power supplies
- Fans
- Power supplies
- Temperature of the components

View the Status of the Interfaces

View the status of the interfaces in a NAS controller.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Hardware** view, expand **Appliances** to select an appliance ID and a controller ID.
4. Select **Interfaces**.
   The status of each interface is displayed.

View the Status of the Disks

View the status of the disks in the internal storage device in a NAS controller.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Hardware** tab navigation pane, expand **Appliances**→ ***Appliance ID***→ ***Controller ID***, then select **Disks**. The status of each disk is displayed in the right pane.

View the Status of a Backup Power Supply

View the status of a backup power supply in a NAS controller.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Hardware** view, expand **Appliances** to select an appliance ID and a controller ID.
4. Select **Backup Power Supply**.
   The status of the backup power supply is displayed.

View the Status of the Fans

View the status of the fans in a NAS appliance.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Hardware** view, expand **Appliances** and select an appliance ID.
4. Select **Fans**.
   The status of each fan is displayed.

View the Status of the Power Supplies

View the status of the power supplies in a NAS appliance.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Hardware** view, expand **Appliances** and select an appliance ID.
4. Select **Power Supply**.
   The status of each power supply is displayed.

Viewing the Status of FluidFS Cluster Services

Storage Manager displays the status of services configured on a FluidFS cluster (such as Active Directory, LDAP, DNS, and NTP).

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab.
   The **FluidFS Cluster Status** section displays the status of each service.

Results

NOTE: If any of the external services are configured with IPv6 link-local addresses, the monitor will always show these services as `Unavailable`.

Viewing the Status of Background Processes

Some operations take time to perform and do not complete immediately, such as detaching a NAS controller. In these cases, you can monitor the progress of operations in Storage Manager.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, click **Cluster Maintenance**.
4. Click the **Internal** tab.
   The status of each background process is displayed.

Viewing FluidFS Cluster NAS Pool Trends

Storage Manager displays statistics about the NAS pool for a FluidFS cluster, including total capacity, unused reserved space, unused unreserved space, and used space.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
   The **NAS Pool Trends** section displays the NAS pool trends.

Viewing FluidFS Cluster Storage Usage

Storage Manager displays a line chart that shows storage usage over time for a FluidFS cluster, including total capacity, unused reserved space, unused unreserved space, and used space.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab.
   The **Summary** view displays the FluidFS cluster storage usage.

Viewing NAS Volume Storage Usage

Storage Manager displays a line chart that shows storage usage over time for a particular NAS volume, including NAS volume size, used space, snapshot space, unused reserved space, and unused unreserved space.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** view, expand **NAS Volumes** and select a NAS volume.
4. Click the **Capacity Trends and Statistics** tab.
   The NAS volume storage usage chart is displayed.

Viewing FluidFS Cluster Traffic Statistics

Storage Manager displays line charts that show traffic statistics over time for a FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Performance** tab.
   The traffic statistics chart is displayed.
3. (Optional) Customize the display as needed. These options are described in the online help.
   - To view the statistics of a different timeframe, select one of the following time period options: **Last Day**, **Last Week**, **Last Month**, or **Last Year**.
   - To change the data metrics to display, select one or more of the following options:
     - **Total MB/Sec:** Displays all read and write traffic in megabytes per second
     - **SMB Write MB/Sec:** Displays SMB write traffic in megabytes per second
     - **SMB Read MB/Sec:** Displays SMB read traffic in megabytes per second
     - **Replication Write MB/Sec:** Displays replication write traffic in megabytes per second
     - **Replication Read MB/Sec:** Displays replication read traffic in megabytes per second
     - **NDMP Write MB/Sec:** Displays NDMP write traffic in megabytes per second
     - **NDMP Read MB/Sec:** Displays NDMP read traffic in megabytes per second
     - **NFS Write MB/Sec:** Displays NFS write traffic in megabytes per second
     - **NFS Read MB/Sec:** Displays NFS read traffic in megabytes per second
     - **NFSWrite IO/Sec:** Displays NFS write I/O operations per second
     - **NFS Read IO/Sec:** Displays NFS read I/O operations per second
     - **SMB Write IO/Sec:** Displays SMB write I/O operations per second
     - **SMB Read IO/Sec:** Displays SMB read I/O operations per second

FluidFS Maintenance

This section contains information about performing FluidFS cluster maintenance operations. These tasks are performed using the Storage Manager Client.

Connecting Multiple Data Collectors to the Same Cluster

You can have multiple data collectors connected to the same FluidFS cluster.

About this task

To designate the Primary data collector and/or whether it receives events:

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab
3. In the FluidFS Cluster Status area, click **Edit FluidFS Cluster Settings**.
4. In the **General** panel, select or clear the **Primary Data Collector Enabled** checkbox.
5. Select or clear the **Receive Events** checkbox.
6. Click **OK**.

Adding and Removing FluidFS Clusters in Storage Manager

Use Storage Manager to view, add, or remove FluidFS clusters.

View FluidFS Clusters Managed by Storage Manager

View FluidFS clusters that have been added to Storage Manager.

Steps

In the **Storage** view, select **FluidFS clusters**.
The FluidFS clusters that have been added to Storage Manager are displayed in the right pane.

Add the FluidFS Cluster to Storage Manager

Add the FluidFS cluster to manage using Storage Manager.

Prerequisites

The FluidFS cluster must be mounted in a rack, cabled, and deployed.

Steps

1. In the **Storage** view, select **Dell Storage**.
2. Click **Add FluidFS Cluster**.
   The **Add FluidFS Cluster** dialog box opens.
3. Complete the fields in the **Register FluidFS w/ Storage Manager** section:
   a. In the **Hostname** field, type the host or cluster name or a client VIP of the FluidFS cluster.
   b. In the **User Name** field, type the name of a FluidFS cluster administrator.
   c. In the **Password** field, type the password for the FluidFS cluster administrator.
   d. In the **Folder** panel, select the parent folder for the FluidFS cluster.
4. Click **Finish**.
   The FluidFS cluster is added to the list in Storage Manager.

Remove a FluidFS Cluster From Storage Manager

Remove a FluidFS cluster if you no longer want to manage it using Storage Manager. For example, you might want to move the FluidFS cluster to another Storage Manager Data Collector.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **Summary** tab.
3. In the right pane, click **Delete**. The **Delete** dialog box appears.
4. Click **OK**.

Organizing FluidFS Clusters Using Folders

By default Storage Manager displays FluidFS clusters in alphabetical order. To customize the organization of FluidFS clusters in Storage Manager, create folders to group FluidFS clusters.

Create a FluidFS Cluster Folder

Add folders to organize FluidFS clusters.

Steps

1. In the **Storage** view, select **FluidFS Clusters**.
2. Click **Create Folder**.
   The **Create Folder** dialog box opens.
3. In the **Name** field, type a name for the folder.
4. In the **Parent** panel, select a parent folder.
5. Click **OK**.

Rename a FluidFS Cluster Folder

Rename a FluidFS cluster folder.

Steps

1. In the **Storage** view, select a FluidFS cluster folder.
2. In the **Summary** tab, click **Edit Summary Settings**. The **Edit FluidFS Cluster Folder Settings** dialog box appears..
3. In the **Name** field, type a new name for the folder.
4. Click **OK**.

Change the Parent Folder for a FluidFS Cluster Folder

Change the parent folder for a FluidFS cluster folder.

Steps

1. In the **Storage** view, select a FluidFS cluster folder.
2. Click the **Summary** tab and click **Edit Settings**.
   The **Edit FluidFS Cluster Folder Settings** dialog box opens.
3. In the **Parent** field, select a parent folder.
4. Click **OK**.

Move a FluidFS Cluster into a FluidFS Cluster Folder

Move a FluidFS cluster into a folder to group it with other FluidFS clusters.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab.
3. In the right pane, click **Move**. The **Select Folder** dialog box appears.
4. Select a parent folder.
5. Click **OK**.

Delete a FluidFS Cluster Folder

Delete a FluidFS cluster folder if it is not being used.

Prerequisites

The folder must be empty.

Steps

1. In the **Storage** view, select a FluidFS cluster folder.
2. Click the **Summary** tab.
3. Click **Delete**.
   The **Delete** dialog box opens.
4. Click **OK**.

Adding a Storage Center to a FluidFS Cluster

The back-end storage for a FluidFS cluster can be provided by one or two Storage Centers.

Prerequisites

The Storage Center must be added to Storage Manager and have front-end connectivity to the FluidFS cluster.

About this task

If a FluidFS cluster uses only one Storage Center, you might want to add another Storage Center to provide storage for the FluidFS cluster if:

- The Storage Center that currently provides storage for the FluidFS cluster is running out of space.
- You want to spread out the storage load.
- You want to allocate more storage to the NAS pool than is supported by a single Storage Center.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Summary** tab.
3. Click **Actions**→ **Storage Centers**→ **Add Storage Centers**.
   The **Add Storage Center** wizard starts and opens the **Select Storage Centers (only supported Storage Centers shown)** page.
4. Select the additional Storage Center to provide storage for the FluidFS cluster and then click**Next**.
5. (iSCSI only) Select two fault domains on the **Select iSCSI Fault Domains from Storage Center** page and click **Next**.
6. (iSCSI only) To configure the IP addresses for **SAN / eth30**, use the **Configure IP Addresses for NAS Controller iSCSI HBAs** page. This page displays the existing values that were configured during deployment. To use the existing values, click **Next**. To change the values:
   a. Select a NAS controller and click **Edit Settings**.
      The **Edit Controller IP Address** dialog box opens.

b. In the **IP Address** field, type an IP address for the NAS controller.
c. Click **OK**.
d. Repeat the preceding steps for each NAS controller.
e. To specify a VLAN tag, type a VLAN tag in the **VLAN Tag** field.

   When a VLAN spans multiple switches, the VLAN tag is used to specify to which ports and interfaces to send broadcast packets.
f. Click **Next**.

7. (iSCSI only) To configure the IP addresses for **SANb / eth31**, use the **Configure IP Addresses for NAS Controller iSCSI HBAs** page. This page displays the existing values that were configured during deployment. To use the existing values, click **Next**. To change the values:
   a. Select a NAS controller and click **Edit Settings**.
      The **Edit Controller IP Address** dialog box opens.
   b. In the **IP Address** field, type an IP address for the NAS controller.
   c. Click **OK**.
   d. Repeat the preceding steps for each NAS controller.
   e. To specify a VLAN tag, type a VLAN tag in the **VLAN Tag** field.

      When a VLAN spans multiple switches, the VLAN tag is used to specify to which ports and interfaces to send broadcast packets.
   f. Click **Next**.
8. To verify connectivity between the FluidFS cluster and the Storage Center, use the **Connectivity Report** page. The NAS controller ports must show the status as `Up` before you can complete the wizard. If you click **Finish** and the NAS controller ports do not have the `Up` status, an error will be displayed.
   - (iSCSI NAS appliances) When the Connectivity Report initially appears, iSCSI logins might still be occurring in the background, causing some or all of the FluidFS cluster iSCSI initiators to show the status `Not Found/Disconnected`. If you see this status, wait 30 seconds, then click **Refresh** to update the Connectivity Report. When the iSCSI logins are complete and the Connectivity Report has been refreshed, the status for each FluidFS cluster iSCSI initiator shows as `Up`.
   - (Fibre Channel NAS appliances) When the Connectivity Report initially appears, the FluidFS cluster HBAs show the status `Not Found/Disconnected`. You must record the WWNs and manually update fabric zoning on the Fibre Channel switch. Then, click **Refresh** to update the Connectivity Report. When the zoning is configured correctly and the Connectivity Report has been refreshed, the status for each FluidFS cluster HBA shows as `Up`.
9. Click **Finish**.

   NOTE: The Storage Center that was just added is not providing storage space to the FluidFS cluster yet. After adding a Storage Center, you must expand the NAS pool to get the new Storage Center to provide block-level storage for the NAS pool.
10. Expand the NAS pool.

    When the expand NAS pool process is complete, the **Storage Center** tab will display both Storage Centers and the **Volume Status** should show as `Up`.

Adding and Deleting NAS Appliances in a FluidFS Cluster

FluidFS supports up to four NAS appliances for each FluidFS cluster.

Add NAS Appliances to a FluidFS Cluster

You can add a NAS appliance (two NAS controllers) to a FluidFS cluster to increase processing power. Adding a NAS appliance allows additional client connections and evenly redistributes client connections and FluidFS cluster operations among more NAS controllers contributing their resources.

Prerequisites

- The additional NAS appliance is mounted in a rack and cabled, and the NAS controllers are in standby mode and powered on. A NAS controller is on and in standby mode if the power LED is flashing green at around two flashes per second.
- NAS appliance service tags are recorded.
- New client VIP IP addresses are available to be added to the new NAS appliance. To ensure effective load balancing, use the following recommendations to determine the number of client VIPs to define:

- If client access to the FluidFS cluster is not through a router (in other words, a flat network), define one client VIP per FluidFS cluster.
- If clients access the FluidFS cluster through a router, define a client VIP for each client interface port per NAS controller.

- New NAS controller IP addresses are available to be added to the new NAS appliance. Verify that there are two additional IP addresses available per NAS appliance.

About this task

For high availability reasons, you must add NAS appliances as NAS controller pairs. You cannot add a single NAS controller. Only one NAS appliance can be added at a time up to a maximum of four NAS appliances (eight NAS controllers).

Adding a NAS appliance is a seamless operation that does not interrupt current FluidFS cluster operations. After the NAS appliance is successfully added, new client connections are automatically distributed to all NAS controllers, ensuring that there is efficient load balancing between all NAS controllers.

NOTE: Due to the complexity and precise timing required, schedule a maintenance window to add the NAS appliance(s).

Steps

1. (Directly cabled internal network only) If the FluidFS cluster contains a single NAS appliance, with a direct connection on the internal network, re-cable the internal network as follows.
   a. Cable the new NAS appliance(s) to the internal switch.
   b. Remove just one of the internal cables from the original NAS appliance.
   c. Connect a cable from each NAS controller port vacated in Step b to the internal switch.
   d. Remove the second internal cable from the original NAS appliance.
   e. Connect a cable from each NAS controller port vacated in Step d to the internal switch.
2. In the **Storage** view, select a FluidFS cluster.
3. Click the **Hardware** tab.
4. In the **Hardware** tab navigation pane, select **Appliances**.
5. In the right pane, click **Add Appliances**. The **Add Appliances** wizard appears and displays the **Select Appliances to Add** page.
6. Select the NAS appliance to add to the FluidFS cluster.
   a. In the top pane, select the NAS appliance.
   b. Click **Add Appliance**. The selected NAS appliance is moved to the bottom pane.
   c. Click**Next**.
7. (iSCSI only) Complete the **Configure IP Addresses for NAS Controller iSCSI HBAs** page to configure the IP addresses for **SAN / eth30**.
   a. Select a NAS controller and click **Edit Settings**. The **Edit Controller IP Address** dialog box appears.
   b. In the **IP Address** field, type an IP address for the NAS controller.
   c. Click **OK**. Repeat the preceding steps for each NAS controller.
   d. To specify a VLAN tag, type a VLAN tag in the **VLAN Tag** field. When a VLAN spans multiple switches, the VLAN tag is used to specify to which ports and interfaces to send broadcast packets.
   e. Click **Next**.
8. (iSCSI only) Complete the **Configure IP Addresses for NAS Controller iSCSI HBAs** page to configure the IP addresses for **SANb / eth31**.
   a. Select a NAS controller and click **Edit Settings**. The **Edit Controller IP Address** dialog box appears.
   b. In the **IP Address** field, type an IP address for the NAS controller.
   c. Click **OK**. Repeat the preceding steps for each NAS controller.
   d. To specify a VLAN tag, type a VLAN tag in the **VLAN Tag** field. When a VLAN spans multiple switches, the VLAN tag is used to specify to which ports and interfaces to send broadcast packets.
   e. Click **Next**. The **Configure Client Network** page displays.
9. If needed, add additional client VIPs through which the clients will access SMB shares and NFS exports.
   a. In the **Virtual IP Addresses** area, click **Add**. The **Add Client IP Address** dialog box appears.
   b. In the **IP Address** field, type a client VIP IP address.
   c. Click **OK**.
10. Add an IP address for each new NAS controller. Repeat the following steps for each NAS controller.
    a. Select a NAS controller and click **Edit Settings**. The **Edit Controller IP Address** dialog box appears.
    b. In the **IP Address** field, type an IP address for the NAS controller.

c. Click **OK**.

11. (Optional) Configure the remaining client network attributes as needed.
    - To change the netmask of the client network, type a new netmask in the **Netmask** field.
    - To specify a VLAN tag, type a VLAN tag in the **VLAN Tag** field.
12. Click **Next**. After you are finished configuring each client network, the **Connectivity Report** page displays.

    NOTE: Adding the appliance to the cluster can take approximately 15 minutes.

13. Use the **Connectivity Report** page to verify connectivity between the FluidFS cluster and the Storage Center. The NAS controller ports must show the status **Up** before you can complete the wizard. If you click **Finish** and the NAS controller ports do not have the status **Up**, an error will be displayed.
    - For iSCSI NAS appliances, when the Connectivity Report initially appears, iSCSI logins might still be occurring in the background, causing some or all of the FluidFS cluster iSCSI initiators to show the status **Not Found/Disconnected**. If this happens, wait 30 seconds, then click **Refresh** to update the Connectivity Report. When the iSCSI logins are complete and the Connectivity Report has been refreshed, the status for each FluidFS cluster iSCSI initiator shows **Up**.
    - For Fibre Channel NAS appliances, when the Connectivity Report initially appears, the FluidFS cluster HBAs show the status **Not Found/Disconnected**. You must record the WWNs and manually update fabric zoning on the Fibre Channel switch. Then, click **Refresh** to update the Connectivity Report. When the zoning is configured correctly and the Connectivity Report has been refreshed, the status for each FluidFS cluster HBA shows **Up**.
14. Click **Finish**.

Delete a NAS Appliance From the FluidFS Cluster

If an attempt to add a NAS appliance to a FluidFS cluster fails, the entry for the NAS appliance must be deleted from the FluidFS cluster before you can reattempt to add the NAS appliance or add a different NAS appliance.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Hardware** view, expand **Appliances** and select the appliance ID.
4. Click **Delete**.
   The **Delete** dialog box opens.
5. Click **OK**.

Detaching, Attaching, and Replacing a NAS Controller

Use these procedures to replace a failed NAS controller.

Detach a NAS Controller

Detach a NAS controller only if the NAS controller needs to be replaced with a new NAS controller. After you detach a NAS controller, it resets to its factory defaults and powers off, if possible. Otherwise, you must reinstall the FluidFS software to reset the NAS controller to its factory defaults.

About this task

Only one NAS controller can be detached from a NAS appliance at a time. Detaching a NAS controller disconnects client connections while clients are being transferred to other NAS controllers. Clients will then automatically reconnect to the FluidFS cluster. While a NAS controller is detached from the FluidFS cluster, SMB shares and NFS exports remain available (although performance might decrease because data is no longer cached); however, most FluidFS cluster configuration changes are not allowed.

CAUTION: Detach a NAS controller only under the direction of technical support.

Steps

1. In the **Storage** view, select a FluidFS cluster.

2. Click the **Hardware** tab.
3. In the **Hardware** view, expand **Appliances** to select an appliance ID and a NAS controller ID.
4. Click **Detach**.
   The **Detach** dialog box opens.
5. Click **OK**.
   The **Detach** dialog box displays the progress of the detach process. If you close the dialog box, the process will continue to run in the background.

   The NAS controller is detached when the state of the NAS controller changes to `Detached`. (Click the **Hardware** tab→ **Appliances**→ **Controller** to display the state of the controller.)

Attach a NAS Controller

Attach a new NAS controller when replacing an existing NAS controller. After it is attached, the new NAS controller inherits the FluidFS cluster configuration settings of the existing NAS controller.

Prerequisites

Verify that the NAS controller being attached is in standby mode and powered on. A NAS controller is on and in standby mode if the power LED is flashing green at around two flashes per second.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **Hardware** tab.
3. In the **Hardware** view, expand **Appliances** to select an appliance ID and a NAS controller ID.
4. Click **Attach**.
   The **Attach** dialog box opens.
5. Click **OK**.
   The **Attach** dialog box displays the progress of the attach process . If you close the dialog box, the process will continue to run in the background.

   The NAS controller is attached when the state of the NAS controller changes to `Formatted`. (Click the **System** tab→ **Appliances**→ **Controller** to display the state of the controller.)
6. (Fibre Channel only) After the attach operation completes, record the new WWNs and manually update fabric zoning on the Fibre Channel switch.

Replace a NAS Controller

In the event of a failure where a NAS controller cannot be brought back online (for example, a malfunctioning NAS controller), you must remove the existing NAS controller from the FluidFS cluster and replace it with a different NAS controller.

Prerequisites

Before replacing the NAS controller ensure that the existing NAS controller is verified as failed by technical support.

About this task

While a NAS controller is detached from the FluidFS cluster, SMB shares and NFS exports remain available (although performance might decrease because data is no longer cached); however, most FluidFS cluster configuration changes are not allowed. Therefore, it is important to replace a failed NAS controller as soon as possible.

NOTE: Only replace a NAS controller under the direction of technical support.

Steps

1. Detach the existing NAS controller.
2. Ensure that all cables are labeled.
3. Disconnect all cables from the back of the existing NAS controller.
4. Remove the existing NAS controller from the NAS appliance chassis.
   a. Press the controller release button to disengage the controller handle.

b. Push the controller handle down until the controller disengages from the appliance.
c. Use the controller handle to pull the controller out of the appliance.

5. Insert the new NAS controller in the NAS appliance chassis.
   a. Ensure that the controller cover is closed.
   b. Align the controller with the appropriate slot in the appliance.
   c. Push the controller into the appliance until the controller seats into place.
   d. Push the handle toward the front of the appliance until it locks.
6. Reconnect all cables to the same ports on the new NAS controller. The NAS controller automatically powers on if at least one power supply is connected to a power source.
7. Attach the new NAS controller.

Managing Service Packs

The FluidFS cluster uses a service pack methodology to upgrade the FluidFS software. Service packs are cumulative, meaning that each service pack includes all fixes and enhancements provided in earlier service packs.

View the Update History

View a list of service pack updates that have been installed on the FluidFS cluster.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **Cluster Maintenance**.
4. In the right pane, click the **Software Versions** tab. The update history for the FluidFS cluster is displayed.

Receive Email Notifications for Available Updates

Storage Manager can send an email to notify you when a FluidFS service pack update is available. Storage Manager sends only one alert email for every 24 hour period.

Prerequisites

Storage Manager must be configured to send diagnostic data using SupportAssist.

Steps

1. Configure the SMTP settings for the Data Collector.
   a. In the top pane of the Storage Manager Client, click **Edit Data Collector Settings**. The **Edit Data Collector Settings** dialog box appears.
   b. Click the **SMTP Server** tab.
   c. In the **From Email Address** field, enter the email address to display as the sender of emails from the Data Collector.
   d. In the **Host or IP Address** field, enter the host name or IP address of the SMTP server.
   e. If the port number of the SMTP server is not 25, enter the correct port number in the **Port** field.
   f. If the SMTP server requires authentication, select the **Authentication** check box, then enter the username and password in the **SMTP User Name** and **SMTP User Password** fields.
   g. Click **OK**.
2. Configure an email address for your Storage Manager user account.
   a. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **General** tab of the **Edit User Settings** dialog box appears.
   b. Enter the email address of the current user in the **Email Address** field.
   c. Select the format for emails to the current user from the **Email Format** drop-down menu.
   d. To send a test message to the email address, click **Test Email** and click **OK**.
   e. Verify that the test message is sent to the specified email address.
   f. Click **OK**.

3. Configure email notifications to receive email notifications for available FluidFS service pack upgrades.
   a. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box appears.
   b. Click the **Manage Events** tab.
   c. Select the checkbox for the event.
   d. Click **OK**.

Install a Service Pack to Update the FluidFS Software

Use the **Upgrade FluidFS Cluster** wizard to update the FluidFS software. Each FluidFS service pack file is downloaded only once and cached locally on the Storage Manager Data Collector at: `C:\Program Files (x86)\Compellent Technologies\Compellent Enterprise Manager\msaservice\etc\appupgrades`. The same service pack file is used to update each FluidFS cluster, but only one FluidFS cluster can be updated at a time.

Prerequisites

- Contact technical support to make service packs available for download to the FluidFS cluster.
- The Storage Manager Data Collector must have enough disk space to store the service pack. If there is not enough space to store the service pack, a message will be displayed shortly after the download starts. You can delete old service packs to free up space if needed.
- Installing a service pack causes the NAS controllers to reboot during the installation process. This might cause interruptions in SMB and NFS client connections. In addition, active NDMP jobs are terminated. Therefore, schedule a maintenance window to perform service pack installations.
- Ensure that all NAS controllers are powered on and their **State** is **Formatted** (the State is displayed at **System** tab→ **Appliances**→ **Controllers**). You cannot upgrade the FluidFS software if a NAS controller is down or detached.
- The Storage Center(s) providing the storage for the FluidFS cluster must be added to Storage Manager.

About this task

NOTE: The service pack installation process is irreversible. The FluidFS cluster cannot revert to a previous version once updated.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a FluidFS cluster.
3. Click the **File System** tab, and click **Maintenance**.
4. In the right pane, click the **Software Versions** tab.
5. In the Software Versions Installed & Available for Upgrade section, click **Look for Software Upgrade**.
6. The **Upgrade FluidFS Cluster** wizard appears and displays a message indicating whether an update is available for the FluidFS cluster. If an update is available, proceed to the next step. If no update is available (for example, the FluidFS cluster is already at the latest version), click **Finish** to exit the wizard.
7. Click **Next** to upload, but not install, the service pack on the FluidFS cluster. The progress of the upload process is displayed. When the upload process is complete, the following message is displayed: `The upgrade package has been delivered to the FluidFS Cluster`.

   NOTE: You can manually cancel the upload process by clicking **Cancel Operation**, and then clicking **Yes** when prompted **Do you want to cancel the upgrade?** This removes the partially uploaded service pack. To restart the upload process, click **Retry Delivery**.

   NOTE: The upload process is a long-running operation. If you close the wizard, the upload process will continue to run in the background. At a later time you can click **Check for Upgrade** again to re-enter the wizard and view the upload progress.

   The following table describes the steps that occur during the upload process.

Step	Description
Check for Update	The Update FluidFS Cluster wizard checks for the latest FluidFS version available.
Download Package	The FluidFS service pack is downloaded to the Data Collector.

Step	Description
Verify Package Integrity	The checksum of the downloaded FluidFS service pack is re-computed to verify the integrity of the service pack.
Upload Package to FluidFS	The FluidFS service pack is uploaded to a NAS controller in the FluidFS cluster.
Register Package	Storage Manager waits for FluidFS to register that the package has arrived and make the service pack available for installation.

8. Click **Finish** when you are ready to install the service pack. The progress of the installation process is displayed.

   NOTE: During the installation process, communication with the FluidFS cluster will be interrupted. This might result in a communication error. However, the installation process will continue to run in the background.

   NOTE: The installation process is a long-running operation. If you close the wizard, the installation process will continue to run in the background. You can view the installation progress using the **File System** tab→**Maintenance** → **Internal**→ **Background Processes** tab.

Managing Firmware Updates

Firmware is automatically updated on NAS controllers during service pack updates and after a failed NAS controller is replaced. After a firmware update is complete, the NAS controller reboots. It is important that you do not remove a NAS controller when a firmware update is in progress. Doing so corrupts the firmware. A firmware update is in progress if both the rear power-on LED and cache active/off-load LED repeatedly blink amber 5 times and then blink green 5 times. If you connect a monitor to a NAS controller VGA port during a firmware update, the following message is displayed: `Executing firmware updates for TopHat system`.

Update Firmware Using FTP

Use this procedure to update controllers to the latest version of FluidFS:

Steps

1. Open Windows File Explorer.
2. In the address bar, type **ftp://Administrator@FLUIDFS-VIP:44421/servicepack** and hit Enter.
   a. Log in as **Administrator**, and enter the Administrator password.
3. Drag and drop the FluidFS ISO into the `servicepack` folder.
4. Wait about two minutes, then open the DSM client and navigate to the **File System tab** > **Cluster Maintenance** > **Software Versions** .
5. Right-click on the version that was just uploaded, and select **Upgrade**.
6. Follow the prompts.

Restoring the NAS Volume Configuration

Restoring the NAS volume configuration provides an effective way to restore the following NAS volume settings without having to manually reconfigure them:

- SMB shares
- NFS exports
- Snapshot schedules
- Quota rules

This is useful in the following circumstances:

- After recovering a system
- After recovering a NAS volume
- When failing over to a replication target NAS volume

NAS Volume Configuration Backups

Whenever a change in the NAS volume's configuration is made, it is automatically saved in a format that allows you to restore it later. The configuration is stored and encrypted in the `.clusterConfig` folder, which is located in the NAS volume's root folder. This folder can be backed up, either individually, or with the NAS volume's user data, and later restored.

The configuration of a NAS volume can be restored on another NAS volume on the same system or on another system.

A NAS volume configuration backup can be made available to be restored using the following methods:

- The storage administrator can manually copy the `.clusterConfig` folder to the NAS volume from its backup or from another NAS volume. When using a backup from another system, the restore operation works only if the saved configuration was taken from a system using the same FluidFS version.
- The storage administrator can copy the `.clusterConfig` folder to the NAS volume from its backup or from another NAS volume using an NDMP restore. When using a backup from another system, the restore operation works only if the saved configuration was taken from a system using the same FluidFS version.
- The `.clusterConfig` folder is automatically copied to target NAS volumes during replication.

Restore the NAS Volume Configuration

When you restore a NAS volume configuration, it overwrites and replaces the existing configuration. Clients that are connected to the FluidFS cluster are disconnected. Clients will then automatically reconnect to the FluidFS cluster.

Steps

1. Ensure the `.clusterConfig` folder has been copied to the root folder of the NAS volume on which the NAS volume configuration will be restored. One way to access the root folder of a NAS volume is to open Windows Explorer and in the address bar type: `\\<client_VIP_or_name>\C$\<NAS_volume>\`.
2. In the **Storage** view, select a FluidFS cluster
3. Click the **File System** tab.
4. In the **File System** tab navigation pane, expand **NAS Volumes** and select a NAS volume.
5. In the right pane, click **Restore Settings**. The **Restore Settings** dialog box appears.
6. Select the settings to restore from backup:
   - To restore SMB shares, select the **SMB Shares** check box.
   - To restore NFS exports, select the **NFS Exports** check box.
   - To restore snapshot schedules, select the **Snapshot Scheduling** check box.
   - To restore quota rules, select the **Quota Rules** check box.
7. Click **OK**.

Restoring Local Users

Restoring the local users configuration provides an effective way to restore all local users without having to manually reconfigure them. This is useful in the following circumstances:

- After recovering a system
- When failing over to a replication target NAS volume

Local Users Configuration Backups

Whenever a change in the local users configuration is made, it is automatically saved in a format that allows you to restore it later. The configuration is stored and encrypted in the `.clusterConfig` folder, which is located in the NAS volume's root folder. This folder can be backed up, either individually, or with the NAS volume's user data, and later restored.

A local users configuration backup can be made available to be restored using the following methods:

- The storage administrator can manually copy the `.clusterConfig` folder to a NAS volume in the system from its backup or from another system. When using a backup from another system, the restore operation works only if the saved configuration was taken from a system using the same FluidFS version.

- The storage administrator can copy the `.clusterConfig` folder to a NAS volume in the system from its backup or from another system using an NDMP restore. When using a backup from another system, the restore operation works only if the saved configuration was taken from a system using the same FluidFS version.
- The `.clusterConfig` folder is automatically copied to target NAS volumes during replication.

Restore Local Users

Local users can be restored by restoring the configuration stored on the most current NAS volume in the FluidFS cluster and restoring it on the same system or on another system.

About this task

When you restore the local users configuration, it overwrites and replaces the existing configuration. Clients that are currently connected to the FluidFS cluster are disconnected. Clients will then automatically reconnect.

Steps

1. Ensure the `.clusterConfig` folder has been copied to the root folder of a NAS volume on the system on which to restore local users. One way to access the root folder of a NAS volume is to open Windows Explorer and in the address bar type: `\\<client_VIP_or_name>\C$\<NAS_volume>\`.
2. In the **Storage** view, select a FluidFS cluster.
3. Click the **File System** tab and select **Client Accessibility**.
4. In the right pane, click the **Local Users and Groups** tab.
5. Click **Restore**. The **Restore Local Users from Replication Source** dialog box appears.
6. From the **Backup Source** drop-down menu, select the backup from which to restore local users.
7. Click **OK**.

Restoring Local Groups

Restoring the local groups configuration provides an effective way to restore all local groups without having to manually reconfigure them. This is useful in the following circumstances:

- After recovering a system
- When failing over to a replication target NAS volume

Local Groups Configuration Backups

Whenever a change in the local groups configuration is made, it is automatically saved in a format that allows you to restore it later. The configuration is stored and encrypted in the `.clusterConfig` folder, which is located in the NAS volume's root folder. This folder can be backed up, either individually, or with the NAS volume's user data, and later restored.

A local groups configuration backup can be made available to be restored using the following methods:

- The storage administrator can manually copy the `.clusterConfig` folder to a NAS volume in the system from its backup or from another system. When using a backup from another system, the restore operation works only if the saved configuration was taken from a system using the same FluidFS version.
- The storage administrator can copy the `.clusterConfig` folder to a NAS volume in the system from its backup or from another system using an NDMP restore. When using a backup from another system, the restore operation works only if the saved configuration was taken from a system using the same FluidFS version.
- The `.clusterConfig` folder is automatically copied to target NAS volumes during replication.

Restore Local Groups

Local groups can be restored by restoring the configuration stored on the most current NAS volume in the FluidFS cluster and restoring it on the same system or on another system.

About this task

When you restore the local groups configuration, it overwrites and replaces the existing configuration. Clients that are currently connected to the FluidFS cluster are disconnected. Clients will then automatically reconnect.

Steps

1. Ensure the `.clusterConfig` folder has been copied to the root folder of a NAS volume on the system on which to restore local groups. One way to access the root folder of a NAS volume is to open Windows Explorer and in the address bar type: `\\client_vip_or_name\C$\nas_volume\`
2. In the **Storage** view, select a FluidFS cluster.
3. Click the **File System** tab.
4. In the **File System** view, select a tenant and then select **Client Accessibility**.
5. Click the **Local Users and Groups** tab.
6. Click **Restore**.
   The **Restore Local Users from Replication Source** dialog box opens.
7. From the **Backup Source** drop-down list, select the backup from which to restore local groups.
8. Click **OK**.

Reinstalling FluidFS from the Internal Storage Device

Each NAS controller contains an internal storage device from which you can reinstall the FluidFS factory image. If you experience general system instability or a failure to boot, you might have to reinstall the image on one or more NAS controllers.

Prerequisites

- If the NAS controller is still an active member in the FluidFS cluster, you must first detach it.
- Connect a monitor to a NAS controller's VGA port and connect a keyboard to one of the NAS controller's USB ports.

CAUTION:

- **Only reinstall the FluidFS software under the direction of technical support.**
- **Reinstalling the FluidFS software on all NAS controllers will revert your system to factory defaults. All data on the FluidFS cluster will be unrecoverable after performing the procedure.**

Steps

1. Press and release the recessed power button at the back of the NAS controller to shut down the NAS controller.

   NOTE: Power off only the NAS controller on which you are reinstalling the FluidFS software. Do not power off the remaining NAS controllers. Powering off a NAS controller disconnects client connections while clients are being transferred to other NAS controllers. Clients will then automatically reconnect to the FluidFS cluster.

2. To turn on the NAS controller, press and release the recessed power button at the back of the NAS controller
3. When you see the **F11 = BIOS Boot Manager** prompt, press **F11**.
4. Select the boot device **USB Flash Disk**.
5. Select **Reinstall Dell FluidFS *<FluidFS_release_to_install>***.
6. Confirm the action by typing `resetmysystem` and pressing **Enter**.
7. Once the reinstallation completes, the NAS controller will reboot into standby mode.
8. After reinstalling FluidFS, attach the NAS controller to a FluidFS cluster.

FS Series VAAI Plugin

The VAAI plugin allows ESXi hosts to offload some specific storage-related tasks to the underlying FluidFS appliances. The plugin supports the following VAAI NAS Primitives:

- **Full File Clone**– Offload the creation of a virtual disk full clone
- **Fast File Clone** (Native Snapshot) – Offload the creation of a virtual disk linked clone
- **Extended Statistics** – Query for space usage on FS series datastores

Installing the plugin enables VAAI NAS primitives for all datastores residing on FS Series v4 or later systems, adding the following functionalities:

1. Virtual machine cloning from vCenter requests FS Series appliances to generate a full copy of the corresponding machine.
2. The creation of virtual machine linked clones is offloaded to FS series appliances.

After the VAAI plugin is installed, you can right-click on a VM and clone it.

The plugin is provided in a zip file that can be downloaded from the FTP server `ftp://<FluidFS_Cluster_public IP>:44421/vaai_plugin`:

- A depot – **FluidFSNASVAAI_For_Esx_v6.0.zip** file

Enable or Disable the FS Series VAAI Plugin

Allows the NAS administrator to enable or disable the VAAI plugin accessibility for security enhancements. VAAI plugin is enabled by default.

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **Cluster Connectivity**.
   a. Choose the **External Servers** tab.
4. In the VAAI area, click **Edit Settings** in the VAAI area.
5. The **Modify VAAI Settings** dialog box appears.
6. To enable VAAI, select the **VAAI Enabled** checkbox.
7. To disable VAAI, clear the **VAAI Enabled** checkbox.
8. Click **OK**.

Installation Instructions

The FS Series VAAI plugin supports ESXi versions 5.5, 6.0, and 6.5.

Prerequisites

NOTE: The FS Series VAAI plugin should be installed on each relevant ESXi host and requires a reboot.

Steps

1. Connect to FS Series via FTP on port 44421 using administrative credentials.
2. Download the VAAI plugin zip file located inside the /vaai_plugin folder.
3. Transfer the file to the /tmp/ folder of the ESXi host.
4. Install the plugin:

```
~ # esxcli software vib install -d /tmp/FluidFSNASVAAI_For_Esx_v7.0.zip
```

5. Reboot the ESXi host.

Plugin Verification

To check if the VAAI plugin is installed in an ESXi host, type the following command in the ESXi console:`# esxcli software vib list | grep Dell_FluidFSNASVAAI`

When running versions earlier than FluidFS v5.0.300109, a positive reply should return `Dell_FluidFSNASVAAI 1.1.0-301 DELL VMwareAccepted 2015-05-17`

When running versions 5.0.300109 or later, a positive reply should return: `Dell_FluidFSNASVAAI 1.1.0-301 DELL VMwareAccepted 2016-07-29`

To verify that an FS Series datastore has VAAI enabled use the command vmkfstools –P in the ESXi host console. The following example illustrates the query and output for a datastore named FSseries_datastore residing on a FS Series v4 or later system:

```
~ # vmkfstools -Ph /vmfs/volumes/FSseries_Datastore/
NFS-1.00 file system spanning 1 partitions
File system label (if any): FSseries_Datastore
Mode: public
Capacity 200 GB, 178.3 GB available, file block size 4 KB, max file size 16777216 TB
UUID: 1cec81cb-6db87d1c-0000-000000000000
Partitions spanned (on "notDCS"):
        nfs:FSseries_Datastore
NAS VAAI Supported: YES
Is Native Snapshot Capable: YES
```

Removal Instructions

To remove the VAAI plugin from an ESXi host:

1. Execute the following command in the ESXi host console:

   ```
   ~ # esxcli software vib remove -n Dell_FluidFSNASVAAI
   ```

2. Reboot the ESXi host.

FluidFS Troubleshooting

This section contains information about troubleshooting problems with the FluidFS cluster. These tasks are performed using the Storage Manager Client.

Viewing the Event Log

A FluidFS cluster generates events when normal operations occur and also when problems occur. Events allow you to monitor the FluidFS cluster, detect and solve problems. Events are logged to the Event Log.

View the Event Log

View events contained in the Event Log.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **Events** tab. The events are displayed.
3. (Optional) Customize the events display as needed. These options are described in the online help.
   - To View events for a different timeframe select one of the time period options.: **Last Day**, **Last 3 Days**, **Last 5 Days**, **Last Week**, **Last Month**, or **Custom**. If you select **Custom**, specify the **Start Time** and **End Time** of the events data to display and then click **Update**.
   - To change the maximum number of events to display, select the maximum number of events (100, 500, or 1000) from the **Max Count** drop-down menu.
   - To filter the events based on severity, select a severity from the **Severity Above** drop-down menu. Options available are **Inform**, **Warning**, **Error**, and **Exception**.

View Details About an Event in the Event Log

View detailed information for an event contained in the Event Log.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **Events** tab.
3. Select an event. The event details are displayed in the bottom pane.

Sort the Event Log

Sort events contained in the Event Log by column heading.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **Events** tab.
3. Click the column headings of the table to sort the events.

Search the Event Log

Search events contained in the Event Log for a specified string.

Steps

1. Click the **Storage** view and select a FluidFS cluster.
2. Click the **Events** tab.

3. In the **Search** field, type the text to search for.
4. Select search parameters as needed:
   - To make the search case-sensitive, select the **Match Case** check box.
   - To prevent the search from wrapping, clear the **Wrap** check box.
     NOTE: By default, when a search reaches the bottom of the list and **Find Next** is clicked, the search wraps around to the first match in the list. When a search reaches the top of the list and **Find Previous** is clicked, the search wraps around to the last match in the list.
   - To match whole phrases within the events, select the **Full Match** check box.
   - To highlight all of the matches of the search, select the **Highlight** check box.
5. Click **Find Next** or **Find Previous** to search for the text you entered.
   - If a match is found, the first event with matching text is selected from the list of events.
   - If a match is not found, an **Error** dialog box displays the text that could not be found.

Running Diagnostics

Running diagnostics helps you detect problems with the FluidFS cluster. The diagnostic options available for the FluidFS cluster are:

- **FluidFS diagnostics**: Used to diagnose software issues.
- **Embedded system diagnostics**: Used to diagnose hardware issues.

Run Diagnostics on a FluidFS Cluster

FluidFS diagnostics can be run while the FluidFS cluster is online and serving data.

About this task

The following FluidFS diagnostic options are available:

- **File System**: Collects information on the core file system activities, resource consumption, and status.
- **General System**: Collects general information about the FluidFS cluster status and settings.
- **FTP** : Collects information for FTP. Submenu for FTP:
  - Authentication
  - File Access
- **HDFS** : Collects Diagnostics on the HDFS activities
- **NDMP** : Collects Diagnostics on the NDMP activities
- **Network** : Collects Network information while tracking Client attempts to connect the cluster. Once the diagnostic is running, ask the client to reattempt the connection.
- **NFS** : Collects Diagnostics on the NFS activities. Submenu for NFS:
  - NFS3, NFS4
  - Interoperability
  - Kerberos
  - Other
  - Slow Access
- **Performance**: Monitors the FluidFS cluster performance while running a basic benchmark and collecting statistics. If possible, run this diagnostic when activity on the FluidFS cluster is minimal.
- **SMB** : Collects Diagnostics on the SMB activities. Submenu for SMB:
  - Antivirus
  - Authentication
  - File Access
  - Interoperability
  - Other
  - Slow Access

To run diagnostics, follow this procedure.

NOTE: For some of the options, there are parameters that might be required, such as Client/IP, User path.

Steps

1. In the **Storage** view, select a FluidFS cluster.
2. Click the **File System** tab.
3. In the **File System** tab navigation pane, select **Cluster Maintenance**.
4. In the right pane, click the **Support** tab.
5. In the Diagnostic Tools area, click **Run Diagnostic**. The **Run Diagnostic** wizard opens.
6. Select the type of diagnostic to run.
7. Select the secondary type (authentication or file access).
8. Click **Next**. The **Run Diagnostics** dialog box opens.
9. Select a **Tenant** from the drop-down list.
10. Enter the **Client IP Address**.
11. Enter or change the **User Path**.
12. Click **Next**.
13. Specify how you want to access the diagnostic files (NFS, SMB, or FTP).
14. Select the files to send to SupportAssist (summary files only, or summary and log files). Click **Run**.
15. After the diagnostics have been run, Storage Manager will send diagnostic data using SupportAssist.

Run Embedded System Diagnostics on a NAS Controller

The embedded system diagnostics (also known as Enhanced Pre-boot System Assessment (ePSA) diagnostics) provide a set of options for particular device groups or devices.

Prerequisites

Connect a monitor to a NAS controller VGA port and connect a keyboard to one of the NAS controller USB ports.

About this task

The embedded system diagnostics allow you to:

- Run tests automatically or in an interactive mode
- Repeat tests
- Display or save test results
- Run thorough tests to introduce additional test options to provide extra information about the failed device(s)
- View status messages that inform you whether tests are completed successfully
- View error messages that inform you of problems encountered during testing

If a major component or device in the system does not operate properly, running the embedded system diagnostics might indicate component failure. To run embedded system diagnostics, a NAS controller must be offline, which means it is not serving data.

The following table summarizes the embedded system diagnostics menu options.

Menu	Description
Configuration	Displays the configuration and status information of all detected devices.
Results	Displays the results of all tests that are executed.
System Health	Provides the current overview of the system performance.
Event Log	Displays a time-stamped log of the results of all tests run on the system. This is displayed if at least one event description is recorded.

Steps

1. Press and release the recessed power button at the back of the NAS controller to shut down the NAS controller.

   NOTE: Power off only the NAS controller on which you are running the embedded system diagnostics. Do not power off the remaining NAS controllers. Powering off a NAS controller disconnects client connections while their clients are being transferred to other NAS controllers. Clients will then automatically reconnect to the FluidFS cluster.

2. Press and release the recessed power button at the back of the NAS controller to turn on the NAS controller.
3. When you see the **F10 = Launch Dell Embedded Diagnostics Module** prompt, press **F10**. The **ePSA Pre-boot System Assessment** window is displayed, listing all devices detected in the system. The diagnostics starts executing the tests on all the detected devices.
4. After you are finished running the embedded system diagnostics, select **Exit** to exit the diagnostics and reboot the NAS controller.

Configuring the BMC Network

You can configure the baseboard management controller (BMC) local area network (LAN) port to provide KVM (keyboard, video, and mouse) service for the FluidFS controller serial console I/O. The BMC KVM service enables the administrator or support engineer to access the FluidFS console I/O to troubleshoot various issues over a computer network.

The FluidFS appliance hardware provides a special physical port known as the Lights-Out Management (LOM) port. This port provides a standard TCP connection to a switch.

As of FluidFS v4, the interconnect network is an IPv6-only network. The BMC network configuration is no longer dependent on the interconnect subnet.

You can configure a different IP address for each controller in the cluster. However, the network and default gateway are shared among all controllers. If you check/uncheck the “Enabled” checkbox, you are enabling/disabling the BMC network on all controllers.

BMC Network Configuration Procedure

Follow this procedure to configure the BMC network.

Steps

1. In the **Storage** view, select the FluidFS cluster that you want to configure.
2. Click the **File System** tab.
3. In the **File System** panel, select **Cluster Connectivity**, and then click the **Management Network** tab.
4. In the **BMC** area, and click **Modify BMC Network Settings**. The **Modify BMC Network Settings** dialog box opens.
5. Enter the controller IP address.

   After you set the controller IP, verify that the netmask and default gateway are correct. Modify them if needed.
6. Click **OK**.

   NOTE: You cannot add or delete a controller IP address, you can only edit the IP address for a controller.

Launching the iBMC Virtual KVM

The iBMC (Integrated Baseboard Management Controller) virtual KVM (keyboard, video, and mouse) allows you to view and manage the NAS controller console remotely over a network.

Prerequisites

- To use the iBMC virtual KVM, you must use a computer with a web browser and JAVA enabled.
- Before connecting to the iBMC virtual KVM, determine the iBMC password. If the FluidFS cluster is configured, the iBMC password is synchronized with the support account password.

Steps

1. Connect a network cable to the LOM (Lights Out Management) Ethernet port on a NAS controller. The LOM Ethernet port is located on the lower right side of the back panel of a NAS controller.
2. Connect a Windows client to the iBMC.
   a. Connect a Windows client to the same network used for the LOM Ethernet port.
   b. Open a web browser. In the address bar of the web browser, type the iBMC IP address of the NAS controller. The iBMC login page appears.
   c. In the **Username** field, type **ADMIN**.

d. In the **Password** field, type the iBMC password.
e. Click **OK**. The iBMC **Properties** page appears.

3. Launch the iBMC virtual KVM.
   a. In the navigation pane, expand **vKVM & vMedia** and click **Launch**.
   b. In the right pane, click **Launch Java KVM Client**. The **Video Viewer** appears and displays the FluidFS cluster console.

Troubleshooting Common Issues

This section contains probable causes of and solutions to common problems encountered when using a FluidFS cluster.

Troubleshoot Active Directory Issues

This section contains probable causes of and solutions to common Active Directory problems.

Group Quota For an Active Directory User Does Not Work

Description	A group quota rule is defined for an Active Directory group; however, when a group member consumes space, the actual usage of the group does not grow and the group limitation is not enforced.
Cause	Quota enforcement is performed based on the UID and GID of the file (UNIX) or the SID and the GSID of the primary group of the user (NTFS), if defined. For Active Directory users, the Primary Group setting is not mandatory, and if not defined, the used space is not accounted to any group. For group quota to be effective with Active Directory users, their primary group must be assigned.
Workaround	To set up the primary group for an Active Directory user: 1. Open the Active Directory management. 2. Right-click on the user and select **Properties**. 3. Select the **Member Of** tab. 4. The group you need must be listed. Click the group and then click **Set Primary Group**. Now quotas takes effect for the user's group.

Active Directory User Authentication Fails

Description	A valid Active Directory user fails to authenticate.
Cause	Probable causes might be: • The user is trying to authenticate using an incorrect password. • The user is locked or disabled in Active Directory. • The Active Directory domain controllers are offline or unreachable. • The FluidFS cluster system time and Active Directory clock are out of sync.
Workaround	1. Check the FluidFS cluster Event Log for errors. 2. Verify that the user is not disabled or locked in Active Directory. 3. Verify that the domain controllers are online and reachable using the network. 4. The FluidFS cluster and Active Directory server must use a common source of time. Configure NTP and verify the system time is in sync with the domain controller time.

Active Directory Configuration Issues

Description	Unable to add Active Directory users and groups to SMB shares.
Cause	Probable causes might be: • Unable to ping the domain using a FQDN.

	• DNS might not be configured. • NTP might not be configured.
Workaround	When configuring the FluidFS cluster to connect to an Active Directory domain: 1. Ensure that you use a FQDN and not the NetBIOS name of the domain or IP address of the domain controller. 2. Ensure that the user has permissions to add systems to the domain. 3. Use the correct password. 4. Configure DNS. 5. The FluidFS cluster and Active Directory server must use a common source of time. Configure NTP and verify the system time is in sync with the domain controller time. 6. If multiple NAS appliances are used, ensure that you set different NetBIOS names. The system defaults to SMB Storage as the name.

Troubleshoot Backup Issues

This section contains probable causes of and solutions to common NDMP problems.

Troubleshooting Snapshots

Description	Snapshot creation and deletion fails.
Cause	Probable causes might be: • There are many client I/O requests waiting to be serviced, including a request to remove a large directory. • There are many snapshot creation/deletion requests being currently processed. • Another snapshot request for the NAS volume is currently being executed. • The total number of snapshots reached the system limit. • The wrong IP address was specified in the backup job.
Workaround	• For a manual request failure, retry taking or deleting the snapshot after a minute or two. • If the request originated from the snapshot scheduler, wait another cycle or two. If the failure persists, try taking or deleting the snapshot manually on the same NAS volume. • If the system is under a heavy workload, wait until the workload decreases and reissue the snapshot request. • Check the snapshot schedule. A very dense snapshot schedule has a negative impact on the overall performance of the system. The accumulated snapshot rate must not exceed 20 snapshots per hour per system. • Check the total number of snapshots in the system. If the number is in the thousands, delete a few snapshots and retry. • Ensure the client VIP is specified in the backup job. • Check if a recent delete of a big volume (TB) was executed. If so, wait for some time and retry the activity.

Troubleshooting an NDMP Internal Error

Description	Backup or restore fails with an internal error.
Cause	NDMP internal errors are indicators of a file system not being accessible or a NAS volume not being available.
Workaround	If the backup application cannot connect to a FluidFS cluster: 1. Verify that NDMP is enabled. 2. Verify that the backup application IP address is configured in NDMP. If the backup appliance can connect to a FluidFS cluster, but cannot log in: 1. Use the default user name “backup_user” configured in Storage Manager for the NDMP client while setting up the NDMP backup/restore in your backup application.

	2. Use the password configured in Storage Manager for the NDMP client while setting up the NDMP backup/restore in your backup application. If the backup application can log into the FluidFS cluster, but no NAS volumes are available for backup, verify that the FluidFS cluster has NAS volumes created on it.

Troubleshoot SMB Issues

This section contains probable causes of and solutions to common SMB problems.

Access to SMB File Denied Due to Unavailable AV Server

Description	When a file on an SMB share is opened by a client application, the FluidFS cluster sends the file to an anti-virus server to be scanned. If no anti-virus server is available, access to the file and to the whole SMB share is disallowed.
Cause	Because the anti-virus servers are not available on the FluidFS cluster, files cannot be opened on an anti-virus enabled SMB share.
Workaround	Ensure that the problem appears only on anti-virus enabled SMB shares, while clients accessing other SMB shares do not experience such problems. Check the status of the anti-virus servers and the network path between the FluidFS cluster and the anti-virus servers.

Access to SMB File/Folder Denied Due to Permissions

Description	SMB access to a file or folder is denied.
Cause	A client without sufficient permissions performs an operation on a file/folder.
Workaround	Check the permissions on the file/folder and set the required permissions.

Access to SMB Shares Unavailable After Microsoft Update

Description	After performing an update to Microsoft Windows 10 version 1903 or Microsoft Windows Server version 1903, Windows clients using SMB 3.1.1 lose access to SMB shares. Accessing an SMB share after the Microsoft Windows update, causes one or more of the following error messages:
	• In FluidFS while accessing the SMB share:
	`Windows cannot access "\\servername" check the spelling.... Error code 0x80004005 Unspecified error`
	• In the Windows event viewer:
	`The server does not support any dialect that the client is trying to negotiate, such as the client has SMB2/SMB3 disabled and the server has SMB1 disabled.`
	• In a UNC path such as \\server\share:
	`0x80070043 "Network name cannot be found`
	• In Network traces:
	`STATUS_INVALID_PARAMETER`

Cause	Two negotiation contexts found in SMB 3.1.1 that FluidFS version 6.0.300135 and lower does not support

Workaround 1	Update to FluidFS MR640 or later.
Workaround 2	Disable SMB v3 and use SMB v2: 1. Start Dell Storage Manager. 2. In the **Storage** view, select a FluidFS cluster. 3. Click the **File System** tab. 4. In the File System view, select **Client Accessibility**. 5. Click the **Protocols** tab. 6. Select **Edit SMB Protocol Settings**. 7. Clear the check box next to **SMBv3 Protocol**. 8. Click **OK** to save settings.

SMB ACL Corruption

Description	SMB ACLs are corrupt.
Cause	• ACLs were accidentally changed by a user or script. • ACLs are corrupted after an anti-virus application accidentally quarantined corresponding files. • ACLs got corrupted after data recovery by a backup application due to compatibility issues. • ACLs got corrupted after migrating data from a different location by using a third-party application, for example, RoboCopy.
Workaround	Check the current ACL setting in the Windows client. Redefine the ACLs for the files by using a Windows client the same way you initially defined it. Verify that you set the ACLs as the owner of the files, directories, and SMB shares. If you cannot redefine your ACLs because you currently do not have permissions, perform the following steps: 1. Restore the files from snapshots or a backup. 2. If you have migrated the data from a different location, for example, using the RoboCopy application, there is a good chance you can restore ACLs by copying only ACLs metadata, instead of re-copying the whole data. 3. If all file system ACLs are corrupted you can restore all data from a NAS replication partner.

SMB Client Clock Skew

Description	SMB client clock skew errors.
Cause	The client clock must be within 5 minutes of the Active Directory clock.
Workaround	Configure the client to clock-synch with the Active Directory server (as an NTP server) to avoid clock skews errors.

SMB Client Disconnect on File Read

Description	The SMB client is disconnected on file read.
Cause	Extreme SMB workload during NAS controller failover.
Workaround	The client needs to reconnect and open the file again.

SMB Client Incorrect Password Login Failure

Description	An SMB client fails to log in.
Cause	The client supplied the wrong password upon connection.
Workaround	1. Interactive clients can retry with the correct password. 2. Applications and servers might need special attention as the user/password, which is usually set in a script or configuration file, has probably expired.

SMB Delete On Close Denial

Description	Files are deleted while they are in use.
Cause	If multiple users are working on the same file and one user deletes the opened file, it is marked for deletion, and is deleted after it is closed. Until then, the file appears in its original location but the system denies any attempt to open it.
Workaround	Notify the client who tried to open the file that the file has been deleted.

SMB File Sharing Conflict

Description	SMB file access is denied due to a sharing conflict.
Cause	When a file is opened using the SMB protocol, the opening application communicates the sharing mode that must be used while this file is open. This sharing mode describes what other clients' activities are allowed on this file, while it is open. This definition is sent by the application and the client cannot control/configure it. Once there is a violation of the sharing definition, the client receives an access denied error and an event is issued.
Workaround	This is an informative event. The administrator may contact the locking client and request to close the application referencing this file. It could be that the application that opened the file did not shut down gracefully. It is recommended to reboot the client if possible.

SMB Locking Inconsistency

Description	The SMB service is interrupted due to SMB interlocking issues.
Cause	There are various SMB client interlocking scenarios.
Workaround	The system recovers itself automatically, an event is issued when recovered.

SMB Maximum Connections Reached

Description	The maximum number of SMB connections per NAS controller has been reached.
Cause	Each NAS appliance is limited to a certain number of connections.
Workaround	• If the system is in an optimal state (all NAS controllers are online) and the number of SMB clients accessing one of the NAS controllers reaches the maximum, consider adding another NAS appliance. • If the system is in optimal state (all NAS controllers are online) but the clients are significantly unbalanced between NAS controllers, rebalance the clients using Storage Manager. • If the system is in a degraded state (one or more NAS controllers are down) and the SMB clients are connected to the remaining NAS controller, wait until the system returns to optimal or decrease the number of SMB clients using the system.

SMB Share Does Not Exist

Description	Client attempts to connect to a nonexistent SMB share.
Cause	• Spelling mistake on client side. • Client is accessing the wrong server.
Workaround	List the available SMB shares and verify that all SMB shares are displayed and nothing has changed unintentionally.

	Verify that you can access the problematic SMB share using a Windows client: 1. Click **Run**. 2. Enter the client access VIP and share name: \ \\<*client_VIP_or_name*>\\<*SMB_share_name*>

SMB Share Name Truncated In Event After Mapping SMB Share

Description	After a client maps a SMB share, the following event is generated and the SMB share name is truncated in the event. In this example, the SMB share name is share1_av. `SMB client connection failure. Un-available share \ \172.22.151.106\share1_a`
Cause	This is a known issue with Windows. Windows attempts to map the SMB share by its name and also by the name truncated by one character.
Workaround	This event can be safely ignored.

SMB Path Share Not Found

Description	Client accessed a share that refers to a nonexistent directory in the NAS volume.
Cause	This error usually occurs in one of the following scenarios: ● The FluidFS cluster is restored from a backup or remote replication. During restore time, the directory structure is not complete and a few directories might not exist. ● When a client with an authorization to access a higher directory in the same path deletes or alters a directory that is being mounted by another client. When multiple clients are accessing the same data set, it is recommended to apply a strict permission level to avoid this scenario.
Workaround	1. If the FluidFS cluster is being restored, communicate the current status to the client and instruct the client to wait for the restore process to complete. 2. In the case of another client deleting or altering a directory, there are three options: ● Restore the problematic path from a backup. ● Manually create the missing directories to enable access. Clients receive errors when trying to access existing data in a deleted path. ● Remove the SMB share and communicate this to the client. 3. List all available SMB shares on the FluidFS cluster and identify the problematic SMB share. It must have an indication that it is not accessible.

SMB Write to Read Only NAS Volume

Description	A client tries to modify a file on a read-only NAS volume.
Cause	A NAS volume is set to read-only when it is the target of a replication. The most frequent reason for this event is either: ● The client meant to access the target system for read purposes, but also tried to modify a file by mistake. ● The client accessed the wrong system due to similarity in name/IP address. ● The client accessed a NAS volume that was made a replication target without the client's knowledge.
Workaround	● Refer the client to the correct NAS volume. ● In order to write to the NAS volume, replication must be terminated first so the NAS volume becomes standalone.

Troubleshoot NFS Issues

This section contains probable causes of and solutions to common NFS problems.

Cannot Mount NFS Export

Description	When attempting to mount an NFS export, the mount command fails due to various reasons such as: ● Permission denied. ● FluidFS cluster is not responding due to port mapper failure - RPC timed out or input/output error. ● FluidFS cluster is not responding due to program not registered. ● Access denied. ● Not a directory.
Cause	● The client connects using NFS/UDP and there is a firewall in the way. ● The client is not in the NFS export list, the FluidFS cluster could not recognize the client system through NIS, or the FluidFS cluster does not accept the identity the client provided. ● The FluidFS cluster is down or has internal file system problems. ● The mount command got through to the port mapper, but the rpc.mountd NFS mount daemon was not registered. ● The client system's IP address, IP range, domain name, or netgroup is not in the NFS export list for the NAS volume it is trying to mount from the FluidFS cluster. ● Either the remote path or the local path is not a directory. ● The client does not have root authority or is not a member of the system group. NFS mounts and unmounts are only allowed for root users and members of the system group.
Workaround	If the issue is due to NFS/UDP and firewall, check whether the client mounts using UDP (this is usually the default) and there is a firewall in the path. If a firewall exists, add an appropriate exception to the firewall. If the issue is due to permissions: ● Verify the path you provided is correct. ● Check that you are trying to mount as root. ● Check that the system's IP address, IP range, domain name, or netgroup is in the NFS exports list. If the FluidFS cluster is not responding due to a port mapper failure: ● Check the FluidFS cluster status. ● Check the network connection by trying to NFS mount from some other system. ● Verify whether other clients experience the same problem. If the FluidFS cluster is not responding due to the program not being registered, check if the port mapper on your client is up. If the issue is due to access denied: ● Get a list of the FluidFS cluster exported file systems using the command: `showmount -e <client_VIP_or_name>` ● Check the system name or netgroup name is not in the user list for the file system. ● Check the file systems related to the NFS export through Storage Manager. If the issue is due to the directory, check the spelling in your command and try to run the mount command on both directories.

NFS Export Does Not Exist

Description	Attempted to mount an export that does not exist.
Cause	This failure is commonly caused by spelling mistakes on the client system or when accessing the wrong server.
Workaround	1. Check the available NFS exports on the FluidFS cluster; verify that all the required exports exist. 2. On the problematic client, verify that the relevant export is available to this client:

	% showmount -e <client_VIP_or_name> Export list for <client_VIP_or_name>: /abc 10.10.10.0 /xyz 10.10.10.0 If the NFS export is available, review the NFS export name spelling in the relevant mount command on the client. It is recommended to copy and paste the NFS export name from the showmount output to the mount command.

NFS File Access Denied

Description	This event is issued when an NFS client does not have enough permissions for the file on a NAS volume.
Cause	File ownership is UID/UNIX and the user is not privileged to access the file, or, file ownership is SID/ACL and after translation to UID/UNIX the permissions do not allow access to the file.
Workaround	• For native access (when a SMB client accesses SID/ACL file or NFS client accesses UID/UNIX file) change the permissions to allow access. • For non-native access, translation rules are involved and it is recommended to contact technical support.

NFS Insecure Access to Secure Export

Description	A client tries to access a secure export from an insecure port.
Cause	The secure NFS export requirement means that the accessing clients must use a well-known port (below 1024), which usually means that they must be root (uid=0) on the client.
Workaround	Identify the relevant NFS export and verify that it is set as secure (requires secure client port). • If the NFS export must remain secure, see the NFS client documentation in order to issue the mount request from a well-known port (below 1024). • If a secure NFS export is not required (for example, the network is not public), ensure that the export is insecure and retry accessing it.

NFS Mount Fails Due to Export Options

Description	This event is issued when an NFS mount fails due to export options.
Cause	The export list filters client access by IP address, network, or netgroup, and screens the accessing client.
Workaround	1. Verify the relevant NFS export details. Write down all existing options so that you are able to revert to them. 2. Remove IP address/client restrictions on the NFS export and retry the mount. If the mount succeeds, verify that the IP address or domain is explicitly specified, or that it is part of the defined network or netgroups. Once the mount succeeds, adjust the original options accordingly. Pay attention to pitfall scenarios, where the network netmask is not intuitive, for example, 192.175.255.254 is part of 192.168.0.0/12 but not of 192.168.0.0/16.

NFS Mount Fails Due to Netgroup Failure

Description	This event is issued when a client fails to mount an NFS export because the required netgroup information cannot be attained.

Cause	This error is usually the outcome of a communication error between the FluidFS cluster and the NIS/LDAP server. It can be a result of a network issue, directory server overload, or a software malfunction.
Workaround	Repeat the below process for each configured NIS/LDAP server, each time leaving just a single NIS/LDAP used, starting with the problematic server. 1. Inspect the NIS/LDAP server logs and see whether the reason for the error is reported in the logs. 2. Network tests: Try pinging the FluidFS cluster from a client located in the same subnet as the NIS/LDAP server. Try pinging the NIS/LDAP server from a client located in the same subnet as the FluidFS cluster. If packet loss is evident on one of the above network tests, resolve the network issues in the environment. 3. Using a Linux client located in the same subnet as the FluidFS cluster and configured to use the same directory server, query the netgroup details from the NIS/LDAP server using the relevant commands. Ensure that the reply is received in a timely manner (up to 3 seconds). You can temporarily work around the problem by removing the netgroup restriction on the NFS export and/or by defining an alternative directory server. Identify the relevant NFS export and the options defined for it, while focusing on the netgroup definition. Document the used netgroup in order to restore it once the issue is solved and remove the netgroup limitation.

NFS Mount Path Does Not Exist

Description	A client tries to mount a mount path that does not exists on a NAS volume.
Cause	This error usually occurs in one of the following scenarios: ● The FluidFS cluster is restored from a backup or remote replication. During restore time, the directory structure is not complete and a few directories might not exist. ● When a client with an authorization to access a higher directory in the same path deletes or alters a directory that is being mounted by another client. When multiple clients are accessing the same data set, it is recommended to apply a strict permission scheme to avoid this scenario.
Workaround	1. If the FluidFS cluster is being restored, communicate the current status to the client and instruct the client to wait for the restore process to complete. 2. In the case of another client deleting or altering a directory, there are three options: ● Restore the problematic path from a backup. ● Manually create the missing directories to enable the mount. Clients receive errors when trying to access existing data in a deleted path. ● Remove the NFS export and communicate this to the client. 3. List all available NFS exports on the FluidFS cluster and identify the problematic NFS export. It must have an indication that it is not accessible.

NFS Owner Restricted Operation

Description	An NFS client is not permitted to perform the requested action to the specific file.
Cause	An NFS client attempted a `chmod` or `chgrp` operation while not being the owner of the file.
Workaround	This is a minor, user-level issue. Frequent events of this type might indicate a malicious attempt to access restricted data.

NFS Write to Read-Only Export

Description	An NFS client tries to perform modifications on a read-only NFS export.
Cause	An NFS export can be defined as a read-only NFS export. A client accessing a read-only NFS export cannot perform write operations or modify included files.
Workaround	This event, by itself, does not require any administrative intervention.

NFS Write To Read-Only NAS Volume

Description	A client tries to modify a file on a read-only NAS volume.
Cause	A NAS volume is set to read-only when it is the target of a replication. The most frequent reason for this event is either: • The client meant to access the target system for read purposes, but also tries to modify a file by mistake. • The client accesses the wrong system due to similarity in name/IP address. • The client is accessing a NAS volume that was made a replication target without the client's knowledge.
Workaround	• Refer the client to the correct NAS volume. • In order to write to the NAS volume, replication must be terminated first so the NAS volume becomes standalone.

NFS Write to Snapshot

Description	An NFS client tries to modify a file located in a snapshot.
Cause	NAS volume snapshots cannot be modified by design.
Workaround	Inform the client that snapshot data cannot be modified. A snapshot is an exact representation of the NAS volume data at the time of its creation.

Troubleshoot NAS File Access and Permissions Issues

This section contains probable causes of and solutions to common NAS file access and permissions problems.

Cannot Change the Ownership of a File or a Folder

Description	Every file on the FluidFS cluster is owned by either a UNIX or NTFS user. Inability to change ownership is treated differently, depending on whether the access is native or non-native.
Cause	The user is not authorized to perform the ownership change.
Workaround	An authorized user must perform this action.

Cannot Modify NAS Files

Description	A user or an application cannot modify a file.
Cause	• The client cannot modify a file due to lack of permissions on the file. • The NAS volume has reached full capacity and the file system denies any write requests, including overwrites. • The NAS volume is a target in a replication and is read-only.
Workaround	1. If the problem appears only on some files, this is a permission issue. Verify that the user account has modify permissions on the file or use a different user account. 2. If the problem is related to a specific NAS volume, verify there is enough free space on the NAS volume or expand it, and verify that the accessed NAS volume is not a target of a replication.

Mixed File Ownership Denied

Description	Both the file owner and group owner must be from the same identity type (UNIX vs. NTFS). An attempt to set different identity types was detected.

Cause	It is impossible to change only the file owner ID to UID if the original file ownership is SID/GSID.
Workaround	To change the file ownership to UNIX style ownership, set UID and GID at same time.

Problematic SMB Access From a UNIX/Linux Client

Description	A UNIX/Linux client is trying to mount a FluidFS cluster SMB share using SMB (using `/etc/fstab` or directly using `smbmount`).
Cause	A UNIX/Linux client is trying to access the file system using the `smbclient` command, for example: `smbclient //<FluidFS_cluster_name>/<SMB_share> -U user%password -c ls`
Workaround	It is recommended that you use the NFS protocol interfaces to access the FluidFS cluster file system from UNIX/Linux clients. To work around this issue: 1. Ensure that the administrator creates NFS exports to the same locations that you use to access using SMB and connect to them using the `mount` command from UNIX/Linux clients. 2. Use NFS-based interfaces to access the FluidFS cluster. For example, from the NAGIOS Linux management system, use the `/check_disk` command instead of the `/check_disk_smb` command.

Strange UID and GID Numbers on Dell NAS System Files

Description	New files created from Ubuntu 7.x clients get the UID and GID of 4294967294 (nfsnone).
Cause	By default, Ubuntu 7.x NFS clients do not specify RPC credentials on their NFS calls. As a result, files created from these clients, by any user, are owned by 4294967294 (nfsnone) UID and GID.
Workaround	To force UNIX credentials on NFS calls, add the **sec=sys** option to the FluidFS cluster mounts in the Ubuntu `fstab` file.

Troubleshoot Networking Problems

This section contains probable causes of and solutions to common networking problems.

Name Server Unresponsive

Description	All NIS, LDAP, or DNS servers are unreachable or not responding.
Workaround	For each server: 1. Ping the server from a client on the FluidFS cluster subnet and verify that it responds. 2. Issue a request to the server from a client on the FluidFS cluster subnet and verify that it responds. 3. Check the server logs to see what is causing the server not to respond to requests.

Troubleshooting DNS Configurations

Description	Clients are unable to connect to the FluidFS cluster using the system name and/or unable to resolve host names.
Cause	Probable causes might be: • Client IP address information is not set correctly. • The FluidFS cluster is not configured to use the correct DNS server. • DNS records are incorrect.
Workaround	1. Verify that the client IP address information is set correctly. 2. Verify that the FluidFS cluster is configured to use the correct DNS server. 3. Contact the DNS server administrator to verify the DNS record creation.

RX and TX Pause Warning Messages

Description	The following warning messages might be displayed when Storage Manager reports connectivity in a Not Optimal state:
	`Rx_pause for eth(x) on node1 is off.`
	`Tx_pause for eth(x) on node 1 is off.`

Cause	Flow control is not enabled on the switch(es) connected to a FluidFS cluster controller.
Workaround	See the switch vendor's documentation to enable flow control on the switch(es).

Troubleshoot Replication Issues

This section contains probable causes of and solutions to common replication problems.

Replication Configuration Error

Description	Replication between the source and target NAS volumes fails because the source and target FluidFS cluster topologies are incompatible.
Cause	The source and target systems are incompatible for replication purposes.
Workaround	Verify that both the source and target have the same number of NAS controllers.

Replication Target FluidFS Cluster is Busy

Description	Replication between the source NAS volume and the target NAS volume fails because the target FluidFS cluster is not available to serve the required replication.
Cause	Replication fails because the target FluidFS cluster is not available to serve the required replication.
Workaround	Verify the replication status on the target FluidFS cluster.

Replication Target File System is Busy

Description	Replication between the source NAS volume and the target NAS volume fails because the target FluidFS cluster file system is temporarily unavailable to serve the required replication.
Cause	Replication fails because the target FluidFS cluster is temporarily unavailable to serve the required replication.
Workaround	The replication continues automatically when the file system releases part of the resources. Verify that the replication continues automatically after a period of time (an hour).

Replication Target is Down

Description	Replication between the source NAS volume and the target NAS volume fails because the target NAS volume is down.
Cause	Replication fails because the file system of the target NAS volume is down.
Workaround	Check whether the file system is down in the target system. If the FluidFS cluster file system is not responding, you must start the file system on the target FluidFS cluster. The replication continues automatically after the file system starts.

Replication Target is Not Optimal

Description	Replication between the source NAS volume and the target NAS volume fails because the target NAS volume is not optimal.
Cause	Replication fails because the file system of the target NAS volume is not optimal.
Workaround	Check the system status of the target system to understand why the file system is not optimal. The replication continues automatically after the file system recovers.

Replication Target Volume is Busy Reclaiming Space

Description	Replication between the source NAS volume and the target NAS volume fails because the target NAS volume is busy freeing up space.
Cause	Replication fails because the target NAS volume is busy freeing up space.
Workaround	The replication continues automatically when the space is available. Verify that the replication automatically continues after a period of time (an hour).

Replication Target Volume is Detached

Description	Replication between the source NAS volume and the target NAS volume fails because the target NAS volume is detached from the source NAS volume.
Cause	Replication fails because the target NAS volume was previously detached from the source NAS volume.
Workaround	Perform the detach action on the source NAS volume. If required, reattach both NAS volumes in a replication relation.

Replication Disconnection

Description	Replication between the source NAS volume and the target NAS volume fails because the connection between the source and target systems is lost.
Cause	Network infrastructure connection issue between the source and the target.
Workaround	Check whether the replication is automatically restored. If the replication is not automatically restored, check the network communication between the source FluidFS cluster and the target FluidFS cluster. Network communication can be checked by using a third-party system in the same subnet that can ping both the source and target FluidFS clusters. Also, verify that the FluidFS replication ports are open on your firewall to allow replication between the source and target FluidFS cluster.

Replication Incompatible Versions

Description	Replication between the source NAS volume and the target NAS volume fails because the FluidFS version of the source FluidFS cluster is higher than the FluidFS version of the target cluster.
Cause	Replication fails because the FluidFS version of the source FluidFS cluster is higher than the FluidFS version of the target FluidFS cluster.
Workaround	Upgrade the FluidFS version of the target FluidFS cluster to match the FluidFS version of the source FluidFS cluster.

Replication Internal Error

Description	Replication between the source and the target NAS volumes fails due to an internal error.

Workaround	Contact technical support to resolve this issue.

Replication Target Does Not Have Enough Space

Description	Replication between the source NAS volume and target NAS volume fails because there is not enough space in the target NAS volume.
Cause	Replication fails because there is not enough space in the target NAS volume.
Workaround	Increase the space of the target NAS volume.

Replication Source FluidFS Cluster is Busy

Description	Replication between the source NAS volume and the target NAS volume fails because the file system of the source NAS volume is busy replicating other NAS volumes.
Cause	Replication fails because the file system of the source NAS volume is busy replicating other NAS volumes.
Workaround	The replication continues automatically when the file system releases part of the resources. Verify that the replication automatically continues after a period of time (an hour).

Replication Source is Down

Description	Replication between the source NAS volume and the target NAS volume fails because the file system of source NAS volume is down.
Cause	The file system of the source NAS volume is down.
Workaround	Check whether the FluidFS cluster is down in the source system. If the FluidFS cluster is down, you must start the file system on the source FluidFS cluster. The replication continues automatically when the file system starts.

Replication Source is Not Optimal

Description	Replication between the source and the target NAS volumes fails because the file system of the source NAS volume is not optimal.
Cause	Replication fails because the file system of the source is not optimal.
Workaround	Check the file system status of the source system to understand why the file system is not optimal.

Replication Source Volume Is Busy Reclaiming Space

Description	Replication between the source NAS volume and the target NAS volume fails because the source NAS volume is busy reclaiming space.
Cause	Replication failed because the source NAS volume is busy reclaiming space.
Workaround	The replication continues automatically when space is available. Verify that the replication automatically continues after a period of time (an hour).

Troubleshoot System Issues

This section contains probable causes of and solutions to common system problems.

NAS System Time Is Wrong

Description	Scheduled tasks are running at the wrong times. The date and time of Event Log messages is wrong.
Cause	• The time on the FluidFS cluster is incorrect. • No NTP server is defined for the FluidFS cluster. • The NTP server servicing the FluidFS cluster is either down or has stopped providing NTP services. • There are network problems communicating with the NTP server.
Workaround	1. If you manually configured the NAS system clock, verify that the time is set correctly in Storage Manager. 2. Identify the FluidFS cluster NTP server from Storage Manager. Record the host name(s) or IP address(es) for further reference. 3. If no NTP server is defined, define one. It is recommended synchronizing the NAS system clock with the NTP server used by the Active Directory domain controller. This avoids time difference issues and possible authentication problems. In many cases the domain controller is also the NTP server. 4. Verify that the NTP server is up and provides the NTP service. 5. Check the network path between the FluidFS cluster and the NTP server, using ping, for example. Verify that the response time is in the millisecond range.

Troubleshooting System Shutdown

Description	During a system shutdown using Storage Manager, the system does not stop and the NAS controllers do not shut down after 20 minutes.
Cause	The system shutdown procedure is comprised of two separate processes: • Stopping the file system • Powering down the NAS controllers The file system might take a long time to clean the cache to storage either due to lot of data, or due to an intermittent connection to the storage. During the powering down stage, the issue could be due to the OS kernel hanging on the NAS controller or failing to sync its state to the local drive.
Workaround	• If the file system has stopped and if one of the NAS controllers is still up, you can physically power down the NAS controller using the power button. • If the file system has not stopped, you must let it continue stopping. The file system reaches a 10 minute timeout, flushes its cache to local storage, and continues the shutdown process.

NAS Volume Security Violation

Description	NAS volume security violation.
Cause	Selecting a security style for a NAS volume dictates the dominant protocol to be used to set permissions on files in the NAS volume: NFS for UNIX security style NAS volumes and SMB for NTFS security style NAS volumes. Consequently, this makes some operations invalid: • Setting UNIX permissions for a file in an NTFS security style NAS volume. • Setting UID/GID ownership for a file in an NTFS security style NAS volume. • Setting an ACL for a file in a UNIX security style NAS volume. • Changing the read-only flag for a file in a UNIX security style NAS volume. • Setting SID/GSID ownership for a file in a UNIX security style NAS volume. The NAS volume security style must reflect the main protocol used to access its files.

Workaround	If a user frequently needs to perform a cross-protocol security related activity, split the data into separate NAS volumes based on the main access protocol.

Attach Operation Fails

Description	The operation to attach the NAS controller to the FluidFS cluster fails.
Workaround	• Connect a keyboard and monitor to the NAS controller that failed the attach operation, and view the error message to determine why the attach operation failed. • Verify that while the NAS controller was detached, the IP assigned to it on the client network was not allocated to another host. While the NAS controller is detached, it loses its identity, including IP addresses. When it is attached, its identity is applied back to the NAS controller, including the IP addresses. • Verify that the default gateway is in the Primary subnet. If the default gateway is not in the Primary subnet, change the default gateway. For attach to succeed, the default gateway must be able to be pinged. • After an attach operation fails, the NAS controller must manually be reset to standby mode.

Controller Taking Long Time to Boot Up After Service Pack Upgrade

Description	The NAS controller takes a long time to boot up after upgrading the service pack of the NAS controller firmware.
Cause	The upgrade process can take up to 60 minutes to complete.
Workaround	• Connect a keyboard and monitor to the NAS controller that is taking a long time to boot up. • If the system is booting, and is at the boot phase, let the upgrades finish. This can take up to 60 minutes to complete. • Do not reboot the NAS controller manually if it is in the boot phase.

13

Remote Storage Centers and Replication QoS

A remote Storage Center is a Storage Center that is configured to communicate with the local Storage Center over the Fibre Channel and/or iSCSI transport protocols. Replication Quality of Service (QoS) definitions control how bandwidth is used to send replication and Live Volume data between local and remote Storage Centers.

Topics:

- Connecting to Remote Storage Centers
- Creating and Managing Replication QoS Definitions

Connecting to Remote Storage Centers

A remote Storage Center is a Storage Center that is configured to communicate with the local Storage Center over the Fibre Channel and/or iSCSI transport protocols.

Storage Centers can be connected to each other using Fibre Channel, iSCSI, or both. Once connected, volumes can be replicated from one Storage Center to the other, or Live Volumes can be created using both Storage Centers.

Connecting Storage Centers Using Fibre Channel

When Storage Centers are connected to the same Fibre Channel fabric and zoning is configured correctly, each Storage Center automatically appears as a remote Storage Center; no additional configuration steps are required.

Steps

1. Connect both Storage Centers to the same Fibre Channel fabric.
2. Configure Fibre Channel zoning to allow the Storage Centers to communicate. When communication is established, each Storage Center automatically appears as a remote Storage Center.

Connecting Storage Centers Using iSCSI

The following tasks describe how to add and remove iSCSI connections to remote Storage Centers.

About this task

NOTE: For user interface reference information, click **Help**.

Configure an iSCSI Connection for Remote Storage Systems

Add an iSCSI connection to a remote Storage Center or PS Group if you want to transfer replication and/or Live Volume data using the iSCSI protocol.

Prerequisites

- The Storage Center or PS Group for which you want to configure iSCSI connections must be added to Storage Manager.
- Remote connections from Storage Center to PS Group require virtual fault domains.
- If the local Storage Center iSCSI ports are configured for virtual port mode and the ports are located behind a router that performs network address translation (NAT), NAT port forwarding must be configured for the iSCSI fault domain.

- If you intend to use Challenge Handshake Authentication Protocol (CHAP) authentication for iSCSI replication traffic, the iSCSI fault domains that are used for replication on each Storage Center have CHAP enabled.

About this task

NOTE: PS Groups do not support Live Volume.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center or PS Group.
3. Open the **Configure iSCSI Connection** wizard.
   - From a Storage Center:
     a. Click the **Storage** tab.
     b. In the **Storage** tab navigation pane, select **Remote Storage Centers**.
     c. In the right pane, click **Configure iSCSI Connection**. The **Configure iSCSI Connection** wizard opens.
   - From a PS Group, select **Actions** > **Replication** > **Configure iSCSI Connection**. The **Configure iSCSI Connection** wizard opens.
4. Select the Storage Center or PS Group for which you want to configure an iSCSI connection, then click **Next**. The wizard advances to the next page.
5. Select iSCSI controller ports and select the network speed.
   a. From the **iSCSI Network Type** drop-down menu, select the option that corresponds to the speed of the connection between the Storage Centers.
   b. In the **Local iSCSI Controller Ports** table, select one or more iSCSI ports on the local Storage Center to use for the iSCSI connection.
   c. In the **Remote iSCSI Controller Ports** table, select one or more iSCSI ports on the remote Storage Center orPS Group to use for the iSCSI connection.
6. If network address translation (NAT) is performed for the connection between the Storage Centers, configure NAT settings.

   NOTE: NAT port forwarding is supported only if both Storage Centers are configured for legacy port mode, or if both Storage Centers are running version 6.5 or later and configured for virtual port mode. PS Groups do not support NAT port forwarding.

   a. The **Configure NAT** dialog box opens.
   b. Configure port forwarding information for each local and remote iSCSI port.
      - In virtual port mode, the **NAT IP Address** and **NAT Public Port** fields display the translated public IP address and port. Click **Change** to modify these fields.
      - In legacy mode, type the translated public IP address and port in the corresponding **NAT IP Address** and **NAT Public Port** fields.
   c. Select the **Prefer IPv6 over IPv4 for remote connection** checkbox if you want to use IPv6 addresses.
   d. When you are finished, click **OK**.
7. (CHAP only) If the local iSCSI fault domain, remote iSCSI fault domain, or both, have CHAP enabled, type a shared secret in the **CHAP Secret** field.
8. (CHAP only) If you have selected fault domains on both Storage Centers that have bidirectional CHAP enabled, select the **Use Bidirectional CHAP** checkbox to enable the Storage Centers to challenge the fault domains on each Storage Center for a shared secret.
9. If replicating to a PS Group, configure the storage pool for the destination volume.
   a. From the **Storage Pool** drop-down menu, select the storage pool that the destination volume will use.
   b. In the **Delegated Space (For Remote PS Group)** field, set the amount of space allowed for the destination volume.

      NOTE: If the replication status changes to **Down** because of insufficient delegated space, increase the delegated space in the **Modify Space Settings** dialog box and wait ten minutes for the replication status to change to **Up**.

10. Click **Finish**.

Related concepts

Configure NAT Port Forwarding for an iSCSI Fault Domain on page 268

Related tasks

Enable Bidirectional CHAP for iSCSI Replication in a Fault Domain on page 271

Remove an iSCSI Connection to a Remote Storage Center

If no replications or Live Volumes are defined for a remote storage system, the iSCSI connection to the remote storage system can be removed.

Prerequisites

The storage system(s) for which you want to configure iSCSI connections must be added to Storage Manager.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the remote Storage Center.
5. In the right pane, click **Configure iSCSI Connection**. The **Configure iSCSI Connection** wizard appears.
6. Clear the check box for each iSCSI port that you want to remove from the connection. If you remove all iSCSI ports, the remote Storage Center is disconnected from the local Storage Center.
7. When you are done, click **Finish**.

Creating and Managing Replication QoS Definitions

Replication Quality of Service (QoS) definitions definitions control how bandwidth is used for replications, Live Volumes, and Live Migrations. Create a QoS definition before you create a replication, Live Volume, or Live Migration.

Create a QoS Definition

Create a QoS definition to control how bandwidth is used to send replication and Live Volume data between local and remote Storage Centers. A QoS definition is also required to create a Live Migration of a volume.

Prerequisites

The Storage Center for which you want to configure a QoS definition must be added to Storage Manager.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **QoS Nodes** tab.
3. In the right pane, click **Create QoS Node**. The **Create Replication QoS** wizard appears.
4. Select the Storage Center for which you want to create a QoS node, then click **Next**. The **Create** page appears.
5. Configure the attributes of the QoS definition.
   a. In the **Name** field, type a name for the QoS definition.
   b. In the **Link Speed** field, specify the speed of the link in megabits per second (Mbps) or gigabits per second (Gbps).
   c. Select the **Bandwidth Limited** check box, then click **Finish**. The wizard closes and the **Edit Replication QoS Schedule** dialog box appears.
6. Configure bandwidth limits for replications and Live Volumes associated with the QoS definition.
   a. Limit bandwidth for a time range by clicking the first cell in the range and dragging to the last cell in the range, then right-click the selection and select the percentage of available bandwidth that can be used.

      NOTE: If you select **Blocked** for a time range, no data is transferred during that period for all replications, Live Volumes, and Live Migrations that are associated with the QoS node. This can cause synchronous replications to become unsynchronized. Live Migrations that use only blocked QoS nodes cannot be completed.

   b. Limit bandwidth for other time ranges as needed.

7. When you are finished, click **OK**.

Rename a QoS Definition

Use the **Edit Settings** dialog box to rename a QoS Definition.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **QoS Nodes** tab, then select the QoS definition.
3. In the right pane, click **Edit Settings**. The **Edit Replication QoS** dialog box appears.
4. In the **Name** field, type a name for the QoS definition.
5. Click **OK**.

Change the Link Speed for a QoS Definition

Use the **Edit Settings** dialog box to change the link speed for a QoS Definition.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **QoS Nodes** tab, then select the QoS definition.
3. In the right pane, click **Edit Settings**. The **Edit Replication QoS** dialog box appears.
4. In the **Link Speed** field, specify the speed of the link in megabits per second (Mbps) or gigabits per second (Gbps).
5. Click **OK**.

Enable or Disable Bandwidth Limiting for a QoS Definition

Use the **Edit Settings** dialog box to enable or disable bandwidth limiting for a QoS Definition.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **QoS Nodes** tab, then select the QoS definition.
3. In the right pane, click **Edit Settings**. The **Edit Replication QoS** dialog box appears.
4. Select or clear the **Bandwidth Limited** check box.
5. Click **OK**.

Modify the Bandwidth Limit Schedule for a QoS Definition

Use the **Edit Schedule** dialog box to modify the bandwidth limit schedule for a QoS definition.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **QoS Nodes** tab, then select the QoS definition.
3. In the right pane, click **Edit Schedule**. The **Edit Replication QoS Schedule** dialog box appears.
4. (Optional) To reset the bandwidth limit schedule to the default, click and drag to select all of the cells, then right-click the table and select **100%**.
5. Configure bandwidth limits for replications and Live Volumes associated with the QoS definition.
   a. Limit bandwidth for a time range by clicking the first cell in the range and dragging to the last cell in the range, then right-click the selection and select the percentage of available bandwidth that can be used.

NOTE: If you select **Blocked** for a time range, no data is transferred during that period for all replications, Live Volumes, and Live Migrations that are associated with the QoS node. This can cause synchronous replications to become unsynchronized. Live Migrations that use only blocked QoS nodes cannot be completed.

b. Limit bandwidth for other time ranges as needed.

6. When you are finished, click **OK**.

Delete a QoS Definition

Delete a QoS definition if it is no longer used by any replications, Live Volumes, or import from external device.

Prerequisites

The QoS definition cannot currently be in use.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **QoS Nodes** tab, then select the QoS definition.
3. In the right pane, click **Delete**. The **Delete Objects** dialog box appears.
4. Click **OK**.

14

Storage Center Replications and Live Volumes

A replication copies volume data from one Storage Center to another Storage Center to safeguard data against local or regional data threats. A Live Volume is a replicating volume that can be mapped and active on a source and destination Storage Center at the same time.

To perform replications, a Remote Instant Replay (Replication) license must be applied to the source and destination Storage Centers.

To create a Live Volume from a replication, a Live Volume license must be applied to the source and destination Storage Centers.

NOTE: The Live Volume feature is not supported on storage systems with front-end SAS connectivity.

Topics:

- Storage Center Replications
- Managing Cross-Platform Replication
- Storage Center Live Volumes

Storage Center Replications

A Storage Center can replicate volumes to a remote Storage Center and simultaneously be the target of Replication from a remote Storage Center. Using Storage Manager, an administrator can set up a replication plan for Storage Centers that supports an overall Disaster Recovery strategy.

In the following example, a server sends an I/O request that modifies the source volume. The changes to the source volume are replicated to the destination Storage Center over Fibre Channel (FC) or iSCSI.

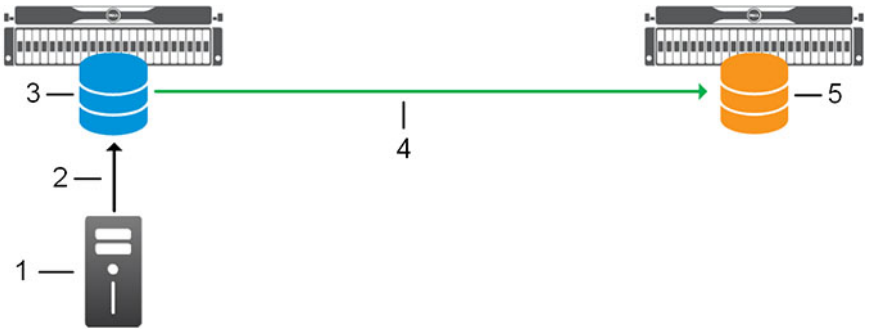


Figure 46. Example Replication Configuration

1. Server
2. Server I/O request to source volume over FC or iSCSI
3. Source volume
4. Replication over FC or iSCSI
5. Destination volume

Replication Types

There are two replication types: asynchronous and synchronous.

Asynchronous replication periodically copies snapshot data to the destination volume after a snapshot is frozen. Synchronous replication writes data to both the source and destination volumes simultaneously to make sure they are synchronized at all times.

Asynchronous Replication

Asynchronous replication copies snapshots from the source volume to the destination volume after they are frozen.

NOTE: By default, data is replicated from the source volume to the lowest storage tier of the destination volume. To change this default, modify the settings for a replication.

For asynchronous replication, you can enable the following options:

- **Replicate Active Snapshot**: Attempts to keep the Active Snapshots (current, unfrozen volume data) of the source and destination volumes synchronized, which could require more bandwidth. Data that is written to the source volume is queued for delivery to the destination volume. If the local Storage Center or site fails before the write is delivered, it is possible that writes will not be delivered to the destination volume. When this feature is disabled, snapshots are copied to the destination after they are frozen.
- **Deduplication**: Reduces the amount of data required to transfer snapshots to the destination Storage Center by copying only the changed portions of the snapshot history. This is accomplished by comparing the changed data in the snapshot being replicated with the previous data block by block, and transmitting only blocks that differ. While deduplication can be resource-intensive, it is useful when replicating volumes over lower bandwidth WAN links.

Synchronous Replication

Synchronous replication makes sure that both the source volume and the destination volume are fully synchronized and there is no data loss in the event of a failure on the source Storage Center.

Synchronization of the source and destination volumes is achieved by making sure that each write is successfully written to both the source volume and the destination volume before responding to the server. Because writes are written to both the source and destination volume, write performance is limited by the speed of the connection to the remote Storage Center.

Synchronous replication copies the volume Active Snapshot (current, unfrozen volume data) and any snapshots to the destination Storage Center. When the source and destination volume are synchronized, new snapshots are created by pausing IO and creating snapshots for both the source volume and the destination volume, and then resuming IO.

Synchronous Replication Modes

The synchronous replication mode controls how the source volume behaves when the destination volume is unavailable.

There are two synchronous replication modes:

- **High Availability Mode**: Accepts IO requests to the source volume when the destination volume is unavailable (or when latency is too high) to avoid interrupting service. However, if writes are accepted to the source volume, the destination volume data becomes stale.
- **High Consistency Mode**: Prevents IO requests to the source volume when the destination volume is unavailable to make sure that the volumes remain identical. However, the source volume cannot be modified during this time, which can interrupt operations.

When the destination volume comes back online, both modes resume transferring snapshots and Active Snapshot data from the source volume.

Deduplication for Synchronous Replication

Deduplication reduces the amount of data required to transfer snapshots to the destination Storage Center by copying only the changed portions of the snapshot history. This is accomplished by comparing the changed data in the snapshot being replicated with the previous data block by block, and transmitting only blocks that differ. While deduplication can be resource-intensive, it is useful when replicating volumes over lower bandwidth WAN links.

NOTE: When you enable replication deduplication, the Storage Center creates a secondary 'Delta' volume. This secondary volume adds to the overall volume memory usage and therefore will reduce the amount of configurable volume space that can be deployed. The additional volume memory usage affects the overall System Scalability Guidelines that are documented in the Storage Center Release Notes.

Replication Requirements

To replicate a volume from one Storage Center to another Storage Center, the requirements listed in the following table must be met.

Requirement	Description
Storage Center license	The source and destination Storage Centers must be licensed for Remote Instant Replay (Snapshot).
Storage Manager configuration	The source and destination storage system must be added to Storage Manager Data Collector. **NOTE:** Replications cannot be created or managed when Unisphere is connected directly to a Storage Center.
Storage Center communication	The storage systems must be connected using Fibre Channel or iSCSI, and each storage system must be defined on the other storage system.
QoS Definition	A quality of service (QoS) definition must be set up for the replication on the source Storage Center.

Related concepts

Connecting to Remote Storage Centers on page 495

Related tasks

Add a Storage Center on page 93
Creating and Managing Replication QoS Definitions on page 497

Replication Behavior When a Destination Volume Fails

When the destination volume becomes unavailable, each replication type behaves slightly differently. The replication types also recover differently when the destination volume comes back online.

Scenario	Asynchronous Replication	Synchronous Replication
Destination volume is unavailable	Allows IO requests to the source volume	• **High Consistency mode**: Fails IO requests to the source volume • **High Availability mode**: Allows IO requests to the source volume
Destination volume comes back online	Resumes transferring snapshots from the source volume and re-copies Active Snapshot data (if enabled)	• **High Consistency mode**: Resumes accepting IO requests to the source volume • **High Availability mode**: Resumes transferring snapshots from the source volume and copies the Active Snapshot data that was missed while the destination volume was unavailable

Replicating a Single Volume to Multiple Destinations

Multiple replications can be configured for a single source volume. Two topologies are supported:

- **Mixed mode**: A source volume is replicated in parallel to multiple Storage Centers.

  Example: Two replications are created in parallel:

- Replication 1: Storage Center A → Storage Center B
- Replication 2: Storage Center A → Storage Center C

- **Cascade mode**: A source volume is replicated in series to multiple Storage Centers.

  Example: Two replications are created in series:

  - Replication 1: Storage Center A → Storage Center B
  - Replication 2: Storage Center B → Storage Center C

Topology Limitations for Volumes Associated with Multiple Replications

The following limitations apply to volumes that are associated with multiple replications.

- Only one synchronous replication can be configured per source volume. Subsequent replications must be asynchronous.
- For cascade mode (replications configured in series), only the first replication can be a synchronous replication. Subsequent replications in the series must be asynchronous.

Disaster Recovery Limitations for Volumes Associated with Multiple Replications

The following disaster recovery limitations apply to volumes that are associated with multiple replications.

- Activating disaster recovery for a volume removes other cascade mode replications associated with the volume.
- Restoring a replication removes all other associated mixed mode replications.

Replications that are removed by disaster recovery must be manually recreated. To use the original destination volumes for the secondary replications, remove the remote Storage Center mappings, then select the **Use an Existing Volume** check box when recreating the replications.

Replication on SCv2000 Series Storage Systems

SCv2000 series storage systems have limited replication functionality. The following replication limitations apply to SCv2000 series storage systems:

- Live Volume is not supported
- High Availability is not supported
- High Consistency is not supported

NOTE: All replications require a Data Collector. When directly connected to a Storage Center, replication options are not available.

Replication Icons

The icons displayed for replications on the **Storage** tab of the **Storage** view indicate whether the volume is the source or destination of the replication.

Icon	Description
	The volume is the source for a replication to a remote Storage Center or the source volume in a copy, mirror, or migrate relationship.
	The volume is the destination for a replication from a remote Storage Center.

Simulating Replications

Simulated replications allow you to estimate requirements for replication and determine an optimal balance between volumes, snapshot schedules, bandwidth schedules, and your recovery plan.

About this task

NOTE: For user interface reference information, click **Help**.

Simulate a Replication

Run a synchronous replication simulation to verify bandwidth requirements and optimal data movement.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center that hosts the volume for which you want to simulate replication.
3. In the **Summary** tab, click **Actions**, then select **Replication→ Simulate Replicate Volumes**.
   - If one or more QoS definitions exist, the **Create Simulation Replication** wizard appears.
   - If a QoS definition has not been created, the **Create Replication QoS** wizard appears. Use this wizard to create a QoS definition before you configure replication.
4. In the **Simulate Volume(s) to Replicate** table, select the volume(s) for which you want to simulate replication, then click **Next**. The wizard advances to the next page.
5. (Optional) In the **Replication Attributes** area, modify default settings that determine how replication behaves.
6. Click **Next**. The wizard advances to the next page.
7. (Optional) To modify replication attributes for an individual simulated replication, select it, then click **Edit Settings**.
8. Click **Finish**. Use the **Replications** tab on the **Replications & Live Volumes** view to monitor the simulated replication(s).

Related concepts

Replication Types on page 501

Convert a Simulated Replication to a Real Replication

If you are satisfied with the outcome of a simulated replication, you can convert it to a real replication.

Prerequisites

The replication requirements must be met.

Steps

1. Click the **Replications & Live Volumes** view.
2. In the **Replications** tab, select the simulated replication, then click **Convert to Replication**. The **Convert to Replication** wizard appears.
3. Select the remote Storage Center to which you want to replicate the volume, then click **Next**.
   - The wizard advances to the next page.
   - If Fibre Channel or iSCSI connectivity is not configured between the local and remote Storage Centers, a dialog box appears. Click **Yes** to configure iSCSI connectivity between the Storage Centers.
4. (Optional) Modify replication default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volume(s).
5. Click **Next**. The wizard advances to the next page.
6. Review the replications.
   a. (Optional) If you want to modify a replication before it is created, select it, then click **Edit Settings**.
   b. Click **Finish**. The replication(s) is created and begins to replicate to the secondary Storage Center.

Related concepts

Replication Requirements on page 502
Replication Types on page 501

Replicating Volumes

Create a replication to copy a volume from one Storage Center to another Storage Center to safeguard data against local or regional data threats.

Create a Single Replication

Create a single replication to copy one volume from a Storage Center to another Storage Center.

Prerequisites

The Replication Requirements on page 502 must be met.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center that hosts the volume you want to replicate.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation tree, select the volume you want to replicate.
5. In the right pane, click **Replicate Volume**.
   - If one or more QoS definitions exist, the **Create Replication** wizard appears.
   - If a QoS definition has not been created, the **Create Replication QoS** wizard appears. Use this wizard to create a QoS definition before you configure replication.

   NOTE: If the volume is a replication destination, Replication QoS settings are enforced. If the volume is a Live Volume secondary, the Replication QoS settings are not enforced.
6. Select a remote storage system to which you want to replicate the volume, then click **Next**.
   - The wizard advances to the next page.
   - If iSCSI connectivity is not configured between the local and remote storage system, a dialog box appears. Click **Yes** to configure iSCSI connectivity between the storage systems.
7. (Optional) Modify replication default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volume.
8. Click **Finish**. The volume begins to replicate to the remote storage system.

Related concepts

Replication Requirements on page 502
Replication Types on page 501

Create Multiple Replications

Create multiple replications to copy several volumes from a Storage Center to another Storage Center.

Prerequisites

The replication requirements must be met.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, click **Replicate Volumes**.
   - If one or more QoS definitions exist, the **Create Replication** wizard appears.
   - If a Quality of Service (QoS) definition has not been created, the **Create Replication QoS** wizard appears. Use this wizard to create a QoS definition before you configure replication.

NOTE: If the volume is a replication destination, Replication QoS settings are enforced. If the volume is a Live Volume secondary, the Replication QoS settings are not enforced.

3. Select the Storage Center that hosts the volumes you want to replicate, then click **Next**. The wizard advances to the next page.
4. Select the remote Storage Center to which you want to replicate the volumes, then click **Next**.
   - The wizard advances to the next page.
   - If Fibre Channel or iSCSI connectivity is not configured between the local and remote Storage Centers, a dialog box appears. Click **Yes** to configure iSCSI connectivity between the Storage Centers.
5. Select the check box for each volume that you want to replicate, then click **Next**. The wizard advances to the next page.
6. (Optional) Modify replication default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volume.
7. Click **Next**. The wizard advances to the next page.
8. Review the replications.
   a. (Optional) If you want to modify a replication before it is created, select it, then click **Edit Settings**.
   b. Click **Finish**. The volumes begin to replicate to the remote Storage Center.

Related concepts

Replication Requirements on page 502
Replication Types on page 501

Migrating Volumes to Another Storage Center

Migrating a volume to another Storage Center moves the data on that volume to a volume on another Storage Center.

Using the following steps to migrate a volume to another Storage Center does not require a Remote Instant Replay (Replication) license or a Live Volume license.

SCv2000 series storage systems running Storage Center 7.2 or earlier and all other storage systems running Storage Center 7.0 or earlier can move a volume to another Storage Center using the following steps:

1. Create a snapshot from the volume you intend to migrate.
2. Create a view volume from the snapshot.
3. Replicate the view volume to the destination Storage Center.
4. Unmap servers from the volume you intend to migrate.
5. Replicate the volume to the destination Storage Center.

NOTE: An SCv2000 series storage system running Storage Center 7.3 or later and all other storage systems running Storage Center 7.1 or later can move a volume to another Storage Center using the Live Migration feature. For more information on creating a Live Migration, see Create a Live Migration for a Single Volume.

Migrate a Volume to Another Storage Center

Migrate a volume to another Storage Center to move data in a volume from one Storage Center to another.

Prerequisites

The Replication Requirements must be met.

Steps

1. Create a snapshot for the volume you want to migrate.
   For more information on creating a snapshot, see Manually Create a Snapshot for a Volume.
2. Create a view volume from the snapshot.
   For more information on creating a view volume from a snapshot, see Create a Local Recovery Volume from a Snapshot.
3. Use Replicate One Time Copy to migrate the view volume to the destination Storage Center.

a. From the navigation pane, select the view volume.
b. Click **Replicate One Time Copy of Volume**.
The **Create Replication** wizard appears.
c. Select a destination Storage Center.
d. Click **Next**.
e. Modify the replication options as needed.
For more information on creating a replication, see Create a Single Replication.
f. Click **Finish**.

4. Shut down the servers mapped to the source volume.
5. Unmap servers mapped to the source volume.
6. Use Replicate One Time Copy to migrate the view volume to the destination Storage Center.
   a. From the navigation pane, select the source volume.
   b. Click **Replicate One Time Copy of Volume**.
   The **Create Replication** wizard appears.
   c. Select the destination Storage Center.
   d. Click **Next**.
   e. Modify the replication options as needed.
   For more information on creating a replication, see Create a Single Replication.
   f. Select the **Use an Existing Volume** check box.
   A confirmation dialog box appears.
   g. Click **Yes**
   The **Select Volume** dialog box appears.
   h. Select the volume created in step 3.
   i. Click **OK**.
   j. Click **Finish**.

Modifying Replications

Modify a replication if you want to enable or disable replication options, convert it to a Live Volume, or delete it.

Change the Type for a Replication

A replication can be changed from synchronous to asynchronous or asynchronous to synchronous with no service interruption.

Prerequisites

The source and destination Storage Centers must be running version 6.5 or later.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication, then click **Edit Settings**. The **Edit Replication Settings** dialog box appears.
3. In the **Type** area, select **Asynchronous** or **Synchronous**.
4. Click **OK**.

Related concepts

Replication Types on page 501

Change the Synchronization Mode for a Synchronous Replication

The synchronization mode for a synchronous replication can be changed with no service interruption. The replication temporarily becomes unsynchronized when the synchronization mode is changed.

Prerequisites

The source and destination Storage Centers must be running version 6.5 or later.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication, then click **Edit Settings**. The **Edit Replication Settings** dialog box appears.
3. In the **Sync Mode** area, select **High Availability** or **High Consistency**.
4. Click **OK**.

Related concepts

Synchronous Replication on page 501
Synchronous Replication Modes on page 501

Include Active Snapshot Data for an Asynchronous Replication

The Active Snapshot represents the current, unfrozen volume data.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication, then click **Edit Settings**. The **Edit Replication Settings** dialog box appears.
3. Select or clear the **Replicate Active Snapshot** check box then, click **OK**.

Enable or Disable Deduplication for a Replication

Deduplication reduces the amount of data transferred and enhances the storage efficiency of the remote Storage Center by copying only the changed portions of the snapshot history on the source volume, rather than all data captured in each snapshot.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication, then click **Edit Settings**. The **Edit Replication Settings** dialog box appears.
3. Select or clear the **Deduplication** check box, then click **OK**.

Select a Different QoS Definition for a Replication

Select a different QoS definition for a replication to change how the replication uses bandwidth.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication, then click **Edit Settings**. The **Edit Replication Settings** dialog box appears.
3. From the **QoS Node** drop-down menu, select a QoS definition.
4. Click **OK**.

Configure a Replication to Write Data to the Lowest Tier at the Destination

The **Replicate Storage To Lowest Tier** option forces all data written to the destination volume to the lowest storage tier configured for the volume. By default, this option is enabled for asynchronous replications.

Prerequisites

The replication must be asynchronous. The **Replicate Storage To Lowest Tier** option is not available for synchronous replications.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication, then click **Edit Settings**. The **Edit Replication Settings** dialog box appears.
3. Select the **Replicate Storage To Lowest Tier** check box.
4. Click **OK**.

Allow Replicate Storage to Lowest Tier Selection During Initial Replication Configuration

By default, the **Replicate Storage To Lowest Tier** option is only available when modifying an existing replication. To allow this option to be configured when replications are being created, modify the Data Collector settings.

Steps

1. In the top pane of the Storage Manager Client, click **Edit Data Collector Settings**. The **Edit Data Collector Settings** dialog box appears.
2. Click the **Replication Settings** tab.
3. Select the **Allow Select to Lowest Tier on Replication Create** check box.
4. Click **OK**.

Pause a Replication

Pausing a replication temporarily prevents volume data from being copied to the remote Storage Center. Pausing a synchronous replication can cause it to become unsynchronized.

Steps

1. Click the **Replications & Live Volumes** view.
2. In the **Replications** tab, select the replication, then click **Pause**. The **Pausing Replication** dialog box appears.
3. Click **OK**.

Resume a Paused Live Volume

Resume a Live Volume to allow volume data to be copied to the secondary Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the paused replication, then click **Resume**. The **Resuming Replication** dialog box opens.
3. Click **OK**.

Convert a Replication to a Live Volume

If servers at both the local and remote site need to write to a volume that is currently being replicated, you can convert a replication to a Live Volume.

Prerequisites

- The Live Volume requirements must be met.
- If the replication is synchronous, the source and destination Storage Centers must be running version 6.5 or later.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication, then click **Convert to Live Volume**. The **Convert to Live Volume** dialog box appears.
3. Modify the Live Volume attributes as necessary. These attributes are described in the online help.
4. When you are finished, click **OK**.

Related concepts

Live Volume Requirements on page 518

Set Threshold Alert Definitions for a Replication

Configure one or more Threshold Alert Definitions for a replication if you want to be notified when a replication reaches specific thresholds, such as the amount of replication data waiting to be transferred or the percentage of replication data that has been transferred.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication, then click **Set Threshold Alert Definitions**. The **Set Threshold Alert Definitions** dialog box appears.
3. Select the alert definition for which you want to configure a threshold alert, then click **Create Threshold Definition**. The **Create Threshold Definition** dialog box appears.
4. Configure the threshold definition attributes as needed. These attributes are described in the online help. Click **Available Alert Definition** to set the definition and make it available. Click **OK**.
5. Click **OK** to close the **Set Threshold Alert Definitions** dialog box.

Monitoring Replications

Monitor a replication to determine how much progress has been made.

About this task

NOTE: For user interface reference information, click **Help**.

Filter Replications by Source Storage Center

To reduce the number of replications that are displayed on the **Replications & Live Volumes** view, you can filter the replications by source Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. In the **Source Storage Centers** pane, hide replications that originate from one or more Storage Centers by clearing the corresponding check boxes.

3. (Optional) When you are finished, you can revert to the default view by clicking **Select All** in the **Source Storage Centers** pane.

Filter Replications by Destination Storage Center

To reduce the number of replications that are displayed on the **Replications & Live Volumes** view, you can filter the replications by destination Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. In the **DR Storage Centers** pane, hide replications that are destined to one or more Storage Centers by clearing the corresponding check boxes.
3. (Optional) When you are finished, you can revert to the default view by clicking **Select All** in the **DR Storage Centers** pane.

View the Managing Live Volume for a Managed Replication

A managed replication replicates a Live Volume primary volume to a third Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. In the **Replications** tab, select the managed replication, then click **Managing Live Volume**. The **Live Volumes** tab appears and selects the Live Volume that manages the managed replication.

Related concepts

Managed Replications for Live Volumes on page 524

View the Snapshots for a Replication

When a replication is selected, the **Snapshots** subtab displays the snapshots for the source volume and the destination volume.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication.
3. In the bottom pane, click the **Snapshots** tab.

View the Progress Report for a Replication

When a replication is selected, the **Progress Reports** subtab displays charts for the amount of data waiting to be copied and the percent complete.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the replication.
3. In the bottom pane, click the **Progress Reports** tab.

View IO/sec and MB/sec Charts for a Replication

When a replication is selected, the **IO Reports** subtab displays the Replication IO/Sec and Replication MB/Sec charts.

About this task

The charts contain performance data for the replication of a volume from the primary Storage Center to the secondary Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select a replication.
3. In the bottom pane, click the **IO Reports** tab.

Managing Cross-Platform Replication

The following section describes managing replications between PS Series groups and Storage Centers.

NOTE: A Storage Center to PS Group replication displays a **% Complete** value that is based on a calculation for Storage Center to Storage Center replications.

NOTE: A PS Group to Storage Center replication displays a **% Complete** value that is based on a calculation for PS Group to PS Group replications.

Cross-Platform Replication Requirements

Storage Centers and PS Groups must meet the following minimum requirements to allow replication between Storage Center and PS Group.

Table 22. Cross-Platform Replication Requirements

Component	Requirement
Storage Center firmware	7.0
PS Group firmware	9.0

NOTE: SCv2000 series storage controllers do not support replication between Storage Center and PS Group storage systems.

PS Group Management Limitation

A Storage Manager administrator cannot add the same PS Group that has already been added to the Storage Manager Data Collector by another Storage Manager administrator.

To map the previously added PS Group to an Storage Manager account, the Storage Manager administrator must use the **PS Groups** subtab under the **Users & System** tab in the **Data Collector** view of Unisphere Central.

Managing Replications Between PS Series Groups and Storage Centers

This section includes information for managing replications between PS Series groups and Storage Centers.

Create a Replication From a PS Group to a Storage Center

Create a replication from a PS Group to a Storage Center to setup a replication relationship. After setting up the replication, replicate a volume from a PS Group to a Storage Center using a replication schedule or Replicate Now.

Prerequisites

The Storage Center and PS Group must meet the minimum requirements for cross-platform replication.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
5. Click **Replicate Volume**.
6. Select a remote storage system from the table.
7. Click **Next**.
   If a remote iSCSI connection is not configured, the **Configure iSCSI Connection** wizard opens. For instructions on setting up a remote iSCSI connection, see Configure an iSCSI Connection for Remote Storage Systems.
8. Configure the replication settings as needed.

   NOTE: For information on the replication settings, click **Help**.

9. Click **Finish**.

Related concepts

Cross-Platform Replication Requirements on page 512

Replicate to a Storage Center on Demand

Use Replicate Now to copy volume data from the source PS Group to the destination Storage Center. Replicating from a PS Group to a Storage Center copies a snapshot from the PS Group as a restore point. Before the data on the PS Group can be used, the restore point must be activated.

Prerequisites

A replication must be created between the Storage Center and PS Group.

Steps

1. Click the **Replications and Live Volumes** tab.
2. Select the replication from the replications table.
3. Click **Replicate Now**.
   The **Replicate Now** dialog box opens.
4. Click **OK**

Edit a Cross-Platform Replication

Edit a cross-platform replication to change the settings of the replication. Setting vary based on which platform hosts the source volume.

Steps

1. Click the **Replications & Live Volumes** view.
2. In the **Replications** tab, select a replication.
3. Click **Edit Settings.**
   The **Edit Replication Settings** dialog box appears.
4. Modify the settings.

   NOTE: For more information on the options on the dialog box, click **Help**.

5. Click **OK**.

Modify Replication Time to Live

When using PS Series v10.0 or later, you can modify the amount of time a replica remains in the PS Series Group. The edit option to change TTL is for the PS snapshots of SC-PS replication only.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Group that has been replicated from the Storage Center to a PS Series Group.
3. Click the **Replications & Live Volumes** tab.
4. From the center of the **Replications** tab (default) navigation pane, select the **Snapshots** subtab.
5. Click **Edit Settings**.
6. Type the amount of time for the replica to remain in the PS Series Group.
7. Click **OK**.

Delete a PS Group Replication

Delete a PS Group replication when it is no longer needed.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Group.
3. Click the **Replications & Live Volumes** tab.
4. From the Replications & Live Volumes tab navigation pane, select a PS Group to Storage Center replication.
5. Right-click on the PS Group to Storage Center replication and select **Delete**.
   The **Delete** dialog box opens.
6. Select **Delete Destination Volume**.
7. Click **OK**.

Create a Replication from a Storage Center to a PS Group

Replicating volumes from a Storage Center to a PS Group is similar to replicating volumes from a Storage Center to another Storage Center.

Prerequisites

You must configure an iSCSI connection between the PS Group and the Storage Center.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center that hosts the volume you want to replicate.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation tree, select the volume you want to replicate.
5. In the right pane, click **Replicate Volume**.
   - If one or more QoS definitions exist, the **Create Replication** wizard appears.
   - If a QoS definition has not been created, the **Create Replication QoS** wizard appears. Use this wizard to create a QoS definition before you configure replication.

   NOTE: If the volume is a replication destination, Replication QoS settings are enforced. If the volume is a Live Volume secondary, the Replication QoS settings are not enforced.
6. Select a remote storage system to which you want to replicate the volume, then click **Next**.
   - The wizard advances to the next page.
   - If iSCSI connectivity is not configured between the local and remote storage system, a dialog box appears. Click **Yes** to configure iSCSI connectivity between the storage systems.
7. (Optional) Modify replication default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volume.
8. Click **Finish**. The volume begins to replicate to the remote storage system.

Managing Replication Schedules

Replication schedules set when replications from a PS Series group run on a daily, hourly, or one-time basis. They also determine the number of snapshots the destination storage system retains for the replication.

Create an Hourly Replication Schedule

An hourly replication schedule determines how often a PS Series group replicates data to the destination volume at a set time or interval each day.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. Click **Create Schedule**.
   The **Create Schedule** dialog box opens.
6. Click the **Enable Schedule** checkbox.
7. In the **Name** field, type a name for the schedule.
8. From the **Frequency** drop-down menu, select **Hourly Schedule**.
9. Select the **Replication Schedule** radio button.
10. From the **Start Date** drop-down menu, select the start date of the schedule.
11. To enable an end date for the schedule, select the checkbox next to **End Date** then select a date from the **End Date** drop-down menu.
12. Specify when to start the replication.
    - To start the replication at a set time each day, select **At specific time**, then select a time of day.
    - To repeat the replication over a set amount of time, select **Repeat Interval**, then select how often to start the replication and the start and end times.
13. From the **Replica Settings** field, type the maximum number of replications the schedule can initiate.

Create a Daily Replication Schedule

A daily replication schedule determines how often a PS Series group replicates data to the destination volume at a set time or interval on specified days.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. Click **Create Schedule**.
   The **Create Schedule** dialog box opens.
6. Click the **Enable Schedule** checkbox.
7. In the **Name** field, type a name for the schedule.
8. From the **Frequency** drop-down menu, select **Daily Schedule**.
9. Select the **Replication Schedule** radio button.
10. From the **Start Date** drop-down menu, select the start date of the schedule.
11. To enable an end date for the schedule, select the checkbox next to **End Date** then select a date from the **End Date** drop-down menu.
12. In the **Run every** field, specify the how often to run the replication.
13. Specify the when to start the replication.
    - To start the replication at a set time each day, select **At specific time**, then select a time of day.
    - To repeat the replication over a set amount of time, select **Repeat Interval**, then select how often to start replication and the start and end times.
14. From the **Replica Settings** field, type the maximum number of replications the schedule can initiate.

Schedule a Replication to Run Once

Create a schedule for one replication to replicate the volume at a future date and time.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Series group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. Click **Create Schedule**.
   The **Create Schedule** dialog box opens.
6. Click the **Enable Schedule** checkbox.
7. In the **Name** field, type a name for the schedule.
8. From the **Frequency** drop-down menu, select **Run Once**.
9. From the **Date** field, select the start date of the replication.
10. In the **Time** field, specify the start time of the replication.
11. From the **Replica Settings** field, type the maximum number of replications the schedule can initiate.

Edit a Replication Schedule

After creating a replication schedule, edit it to change how often the schedule initiates replications.

Steps

1. Click the **Storage** view.

2. In the **Storage** pane, select a PS Group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. From the **Schedules** tab, select the replication schedule to edit.
6. Click **Edit**.
   The **Edit Schedule** dialog box appears.
7. Modify the schedule settings as needed.

   NOTE: For more information on the schedule settings, click **Help**.

8. Click **OK**.

Enable or Disable a Replication Schedule

After creating a replication schedule, enable or disable the schedule to allow the schedule to initiate replications or prevent the schedule from initiating replications.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. From the **Schedules** tab, select the replication schedule to enable or disable.
6. Click **Edit**.
   The **Edit Schedule** dialog box appears.
   - To enable the replication schedule, select the **Enable Schedule** checkbox.
   - To disable the replication schedule, clear the **Enable Schedule** checkbox.
7. Click **OK**.

Delete a Replication Schedule

Delete a replication schedule to prevent it from initiating replications after the schedule is no longer needed.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a PS Group.
3. Click the **Storage** tab.
4. From the Storage tab navigation pane, select a volume.
   The volume must be the source of a replication relationship.
5. From the **Schedules** tab, select the replication schedule to delete.
6. Click **Delete**.
   A confirmation dialog box appears.
7. Click **OK**.

Storage Center Live Volumes

A Live Volume is a replicating volume that can be mapped and active on a source and destination Storage Center at the same time. While both Storage Centers can accept writes, when a server writes to the destination volume, the writes are redirected to the source volume before being replicated back to the destination.

Unlike replicated volumes, Live Volume primary and secondary volumes share the same volume identity, which means that servers recognize the primary and secondary volumes as the same volume.

NOTE: The Live Volume feature is not supported on storage systems with front-end SAS connectivity.

Behavior of Volume QoS Settings in Live Volume Operations

Any Volume or Replication QoS settings that have been defined are enforced only on the primary side of a Live Volume. If the secondary Storage Center becomes primary Storage Center as the result of a swap or DR Activate, the Volume QoS attributes and Replication QoS settings from that Storage Center are enforced. This behavior differs from how Volume QoS settings are enforced for a replication.

Live Volume Requirements

To create Live Volumes, the requirements listed in the following table must be met.

Requirement	Description
Storage Center version	The primary and secondary Storage Centers must be running the same version of Storage Center software.
Storage Center license	The primary and secondary Storage Centers must be licensed for Live Volume.
Storage Manager configuration	The primary and secondary Storage Centers must be added to Storage Manager. **NOTE:** A Live Volume must use the same LUN number on both the primary and secondary Storage Centers.
Storage Center communication	The primary and secondary Storage Centers must be connected using Fibre Channel or iSCSI, and each Storage Center must be defined on the other Storage Center. • On the primary Storage Center, the secondary Storage Center must be defined as a remote Storage Center. • On the secondary Storage Center, the primary Storage Center must be defined as a remote Storage Center.
QoS definitions	Quality of Service (QoS) definitions must be defined on the primary and secondary Storage Centers.
Server	• MPIO must be enabled on the server to prevent I/O interruption.

Live Volume Types

Live Volumes can be created using asynchronous replication or synchronous replication.

Storage Center version 7.3 and later provides support for ALUA optimization of Live Volumes.

Live Volume ALUA allows the Storage Center to report path priority to servers for Live Volumes. The servers can make use of this path priority to prefer sending I/O to the better performing paths. In practice, I/O is directed towards the paths of the Primary Live Volume.

In Storage Manager, the Summary tab of a Live Volume reports whether a Live Volume is ALUA optimized. If Live Volumes exist that are not ALUA optimized, Storage Manager displays an alert and provides a link to a guided process to update Live Volumes to ALUA optimized.

Related concepts

Asynchronous Replication on page 501

Synchronous Replication on page 501

Live Volume Icon

The Live Volume icon indicates Live Volumes on the **Storage** tab of the **Storage** view to differentiate it from regular volumes and replicated volumes.

NOTE: To determine whether a Live Volume is primary or secondary from the **Storage** tab, select the Live Volume, then review the **Live Volume Attributes** section under the **Summary** subtab.

Live Volume Roles

There are two roles for Live Volumes: primary and secondary. These roles determine the direction of the replication, and they can be swapped automatically or manually. Write performance is reduced for the secondary volume because the primary volume must also acknowledge these writes.

Live Volume Role	Description
Primary	• Hosts the primary volume, which is like the source volume for a conventional replication • Replicates the primary volume to the secondary volume • Processes all I/O from both the primary and secondary site
Secondary	• Hosts the secondary volume • Accepts I/O for the Live Volume and routes it to the primary volume on the primary Storage Center

Live Volume Roles Example

In the following examples, a server sends an IO request that modifies the primary volume. The changes to the primary volume are replicated to the secondary Storage Center over Fibre Channel or iSCSI. When a server connected to the secondary Storage Center sends an IO request to the secondary volume, the secondary Storage Center forwards the IO request to the primary volume on the primary Storage Center.

Live Volume Before Swap Role

In the following diagram, the primary Storage Center is on the left and the secondary Storage Center is on the right.

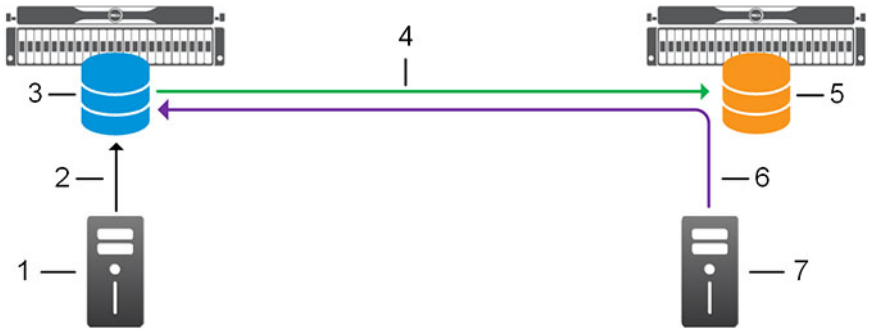


Figure 47. Example Live Volume Configuration

1. Server
2. Server IO request to primary volume over Fibre Channel or iSCSI
3. Primary volume
4. Live Volume replication over Fibre Channel or iSCSI
5. Secondary volume
6. Server IO request to secondary volume (forwarded to primary Storage Center by secondary Storage Center)
7. Server

Live Volume After Swap Role

In the following diagram, a role swap has occurred so the secondary Storage Center is on the left and the primary Storage Center is on the right.

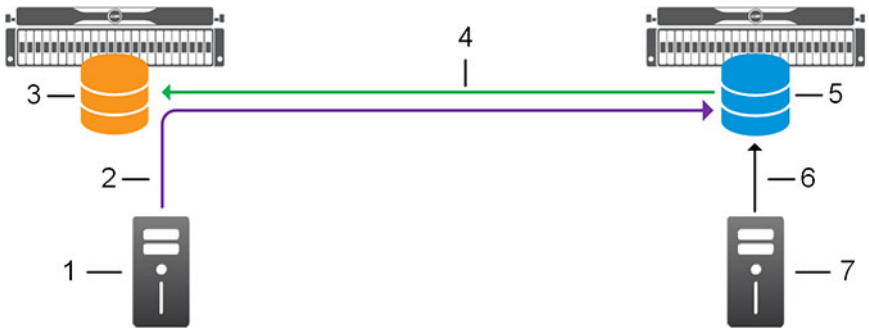


Figure 48. Example Live Volume Configuration After Swap Role

1. Server
2. Server IO request to secondary volume (forwarded to primary Storage Center by secondary Storage Center)
3. Secondary volume
4. Live Volume replication over Fibre Channel or iSCSI
5. Primary volume
6. Server IO request to primary volume over Fibre Channel or iSCSI
7. Server

Automatic Swap Role for Live Volumes

Live Volumes can be configured to swap primary and secondary volumes automatically when certain conditions are met to avoid situations in which the secondary volume receives more IO than the primary volume.

Attributes that Control Swap Role Behavior

When automatic swap role is enabled, the following limits determine when a role swap occurs.

Swap Role Limit	Description
Min Amount Before Swap	Specifies the minimum amount of storage space that must be written to the Live Volume on the secondary Storage Center before the roles can be swapped
Min Time As Primary Before Swap (Minutes)	Specifies the number of minutes that must pass before the roles can be swapped.
Min Secondary Percent Before Swap (%)	Specifies the minimum percentage of IO that must take place on the secondary volume before the roles can be swapped.

Triggering an Automatic Swap Role

For an automatic swap role to occur, the following events must take place.

Steps

1. The **Automatically Swap Roles** feature must be enabled for the Live Volume.
2. The timeout specified in the **Min Time As Primary Before Swap (Minutes)** field must expire.
3. Over a five minute period, one of the following limits must be exceeded for least 70% of the samples conducted during that time.
   - **Min Amount Before Swap**

- **Min Secondary Percent Before Swap (%)**

Automatic Failover for Live Volumes

With Automatic Failover applied, the secondary Live Volume will automatically be promoted to primary in the event of a failure. After the primary Live Volume comes back online, Automatic Restore optionally restores the Live Volume relationship.

Live Volume Automatic Failover Requirements

The following requirement must be met to enable Automatic Failover on a Live Volume.

Component	Requirement
Live Volume attributes	• Synchronous • High-Availability • Protected
Server host operating system	• Any of the following operating systems: • VMware ESX 6.5 • Windows Server 2012 R2 with Microsoft Hyper-V • Windows Server 2016 with Microsoft Hyper-V • Windows Server 2019 with Microsoft Hyper-V
Data Collector Ports	Enable inbound traffic on port 3033

Tiebreaker

The tiebreaker is a service running on the Data Collector that prevents the primary and secondary Live Volumes from simultaneously becoming active. If the secondary Storage Center cannot communicate with the primary Storage Center, it consults the tiebreaker to determine if the primary Storage Center is down. If the primary Storage Center is down, the secondary Live Volume activates.

Automatically Failing Over

Enabling Automatic Failover on a Live Volume allows the secondary Live Volume to automatically activate in the event of a failure. The following steps occur during an automatic failover.

Callout	Object	Callout	Object
1	Primary Storage Center	4	Primary Live Volume
2	Tiebreaker	5	Secondary Live Volume
3	Secondary Storage Center	6	Servers

1. The primary Storage Center fails.

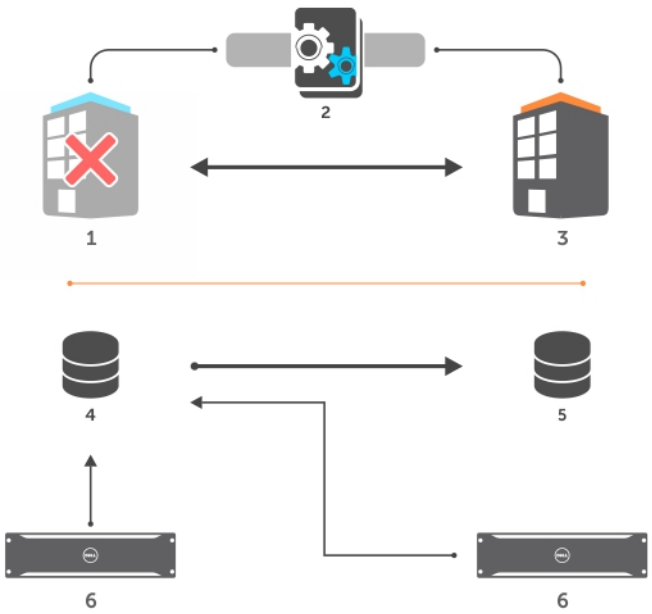


Figure 49. Step One

2. The secondary Storage Center cannot communicate with the primary Storage Center.
3. The secondary Storage Center communicates with the tiebreaker and receives permission to activate the secondary Live Volume.
4. The secondary Storage Center activates the secondary Live Volume.

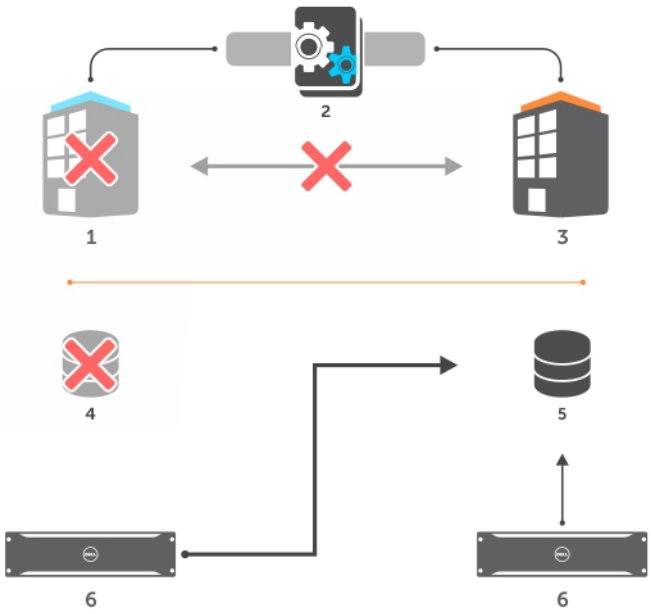


Figure 50. Step Four

NOTE: When the primary Storage Center recovers, Storage Center prevents the Live Volume from coming online.

Automatic Restore of a Live Volume

Enabling Automatic Restore repairs the Live Volume relationship between the primary and secondary Live Volumes after recovering from a failure. After an automatic restore, the original secondary Live Volume remains as the primary Live Volume. The following steps occur during an automatic repair of a Live Volume.

NOTE: The Live Volume will automatically restore only if the failover was automatically activated.

1. The primary Storage Center recovers from the failure.

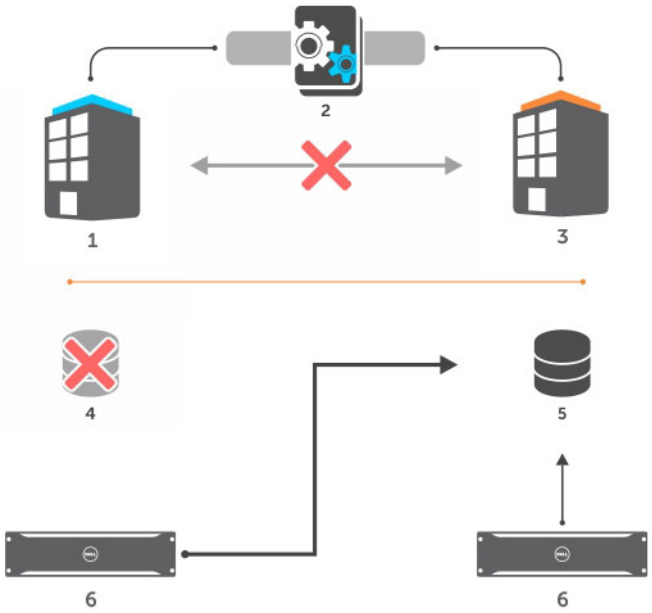


Figure 51. Step One

2. The primary Storage Center recognizes that the secondary Live Volume is active as the primary Live Volume.
3. The Live Volume on the secondary Storage Center becomes the primary Live Volume.
4. The Live Volume on the primary Storage Center becomes the secondary Live Volume.

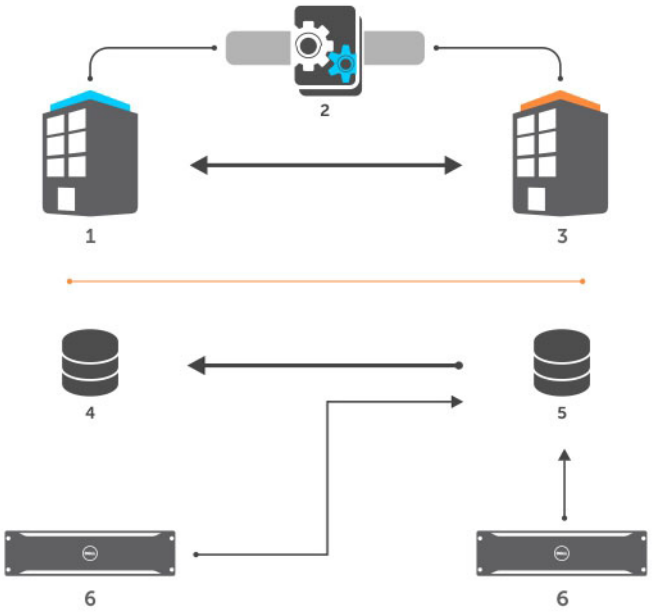


Figure 52. Step Four

Managed Replications for Live Volumes

A managed replication allows you to replicate a primary Live Volume to a third Storage Center, protecting against data loss in the event that the site where the primary and secondary Storage Centers are located goes down. When a Live Volume swap role occurs, the managed replication follows the primary volume to the other Storage Center.

Supported Live Volume with Managed Replication Topologies

Three specific combinations of Live Volume type and managed replication type are supported. The following table lists the supported combinations.

Live Volume Type	Managed Replication Type
Asynchronous	Synchronous
Asynchronous	Asynchronous
Synchronous	Asynchronous

Live Volume with Managed Replication Example Configuration

The following examples show how a managed replication behaves before and after a Live Volume swap role.

- **Live Volume behavior**: When a server near the primary Storage Center sends an IO request that modifies the primary volume, the changes to the primary Live Volume are replicated to the secondary Storage Center over Fibre Channel or iSCSI. When a server near the secondary Storage Center sends an IO request to the secondary Live Volume, the secondary Storage Center forwards the IO request to the primary volume on the primary Storage Center. These changes to the primary volume are ultimately replicated to the secondary volume.
- **Managed replication behavior**: The changes to the primary Live Volume are replicated to the third Storage Center over Fibre Channel or iSCSI. When a Live Volume swap role occurs, the managed replication follows the primary volume to the other Storage Center.

Managed Replication Before Live Volume Swap Role

In the following diagram, the primary Storage Center is on the left and the secondary Storage Center is located on the right.

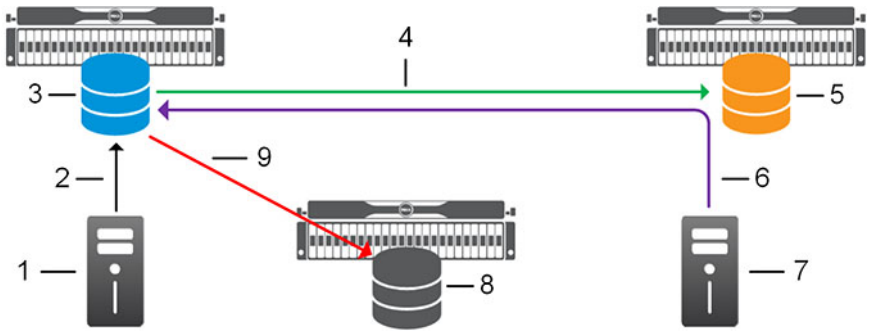


Figure 53. Live Volume with Managed Replication Example Configuration

1. Server
2. Server IO request to primary volume over Fibre Channel or iSCSI
3. Primary volume (Live Volume and managed replication)
4. Live Volume replication over Fibre Channel or iSCSI
5. Secondary volume (Live Volume)
6. Server IO request to secondary volume (forwarded to primary Storage Center by secondary Storage Center)
7. Server
8. Destination volume (managed replication)
9. Managed replication over Fibre Channel or iSCSI

Managed Replication After Live Volume Swap Role

In the following diagram, a swap role has occurred so the secondary Storage Center is on the left and the primary Storage Center is located on the right. The managed replication has moved to follow the primary volume.

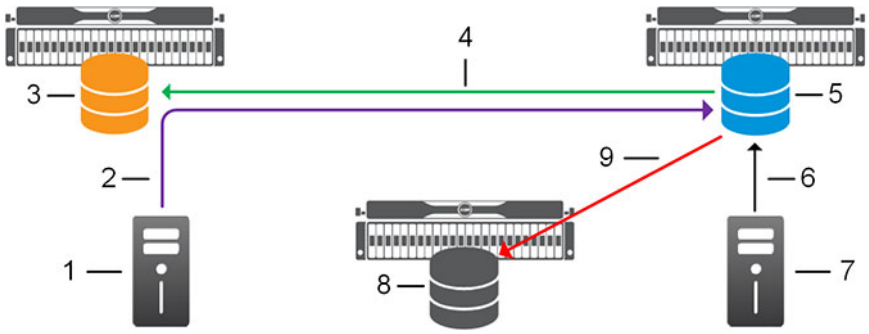


Figure 54. Live Volume with Managed Replication Example Configuration After Swap Role

1. Server
2. Server IO request to secondary volume (forwarded to primary Storage Center by secondary Storage Center)
3. Secondary volume (Live Volume)
4. Live Volume replication over Fibre Channel or iSCSI
5. Primary volume (Live Volume and managed replication)
6. Server IO request to primary volume over Fibre Channel or iSCSI
7. Server
8. Destination volume (managed replication)
9. Managed replication over Fibre Channel or iSCSI

Managed Replication Requirements

Each Storage Center that participates in the Live Volume and managed replication configuration must meet specific requirements.

- The primary and secondary Storage Centers (Live Volume) must be running version 6.5 or later and meet the Live Volume requirements.
- The destination Storage Center (managed replication) must be running version 6.5 or later and meet the replication requirements.

Related concepts

Replication Requirements on page 502
Live Volume Requirements on page 518

Creating Live Volumes

Create a Live Volume to replicate a volume to another Storage Center while allowing servers to send IO for the volume to both Storage Centers. This additional flexibility can be used to perform planned outages without interrupting volume availability.

About this task

NOTE: For user interface reference information, click **Help**.

Convert a Single Volume to a Live Volume

To convert a single volume to a Live Volume, create the Live Volume from the **Storage** view.

Prerequisites

The Live Volume requirements must be met. See Live Volume Requirements.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center that hosts the volume you want to replicate.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation tree, select the volume.
5. In the right pane, click **Convert to Live Volume**.
   - If one or more QoS definitions exist, the **Convert to Live Volume** wizard appears.
   - If a Quality of Service (QoS) definition has not been created, the **Create Replication QoS** wizard appears. Use this wizard to create a QoS definition before you configure a Live Volume.

   NOTE: Live Volume QoS settings are only enforced on the primary Storage Center and are not enforced on the secondary Storage Center until it becomes the primary Storage Center.
6. Select the secondary Storage Center for the Live Volume, then click **Next**.
   - The wizard advances to the next page.
   - If Fibre Channel or iSCSI connectivity is not configured between the local and remote Storage Centers, a dialog box appears. Click **Yes** to configure iSCSI connectivity between the Storage Centers.
7. (Optional) Modify Live Volume default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volume and map the destination volume to a server.
   - In the **Live Volume Attributes** area, select a QoS node for the secondary Storage Center, configure the automatic swap role policy, enable automatic failover and automatic restore, or enable reporting of non-optimized paths.
   - In the **Managed Replications** area, configure a managed replication that replicates the Live Volume primary volume to a third Storage Center.
8. Click **Finish**.
   The volume is converted to a Live Volume and begins to replicate to the secondary Storage Center.

Related concepts

Live Volume Requirements on page 518
Live Volume Types on page 518
Managed Replications for Live Volumes on page 524

Convert Multiple Volumes to Live Volumes

To convert multiple volumes to Live Volumes, create the Live Volumes from the **Replications & Live Volumes** view.

Prerequisites

The Live Volume requirements must be met. See Live Volume Requirements on page 518.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, click **Create Live Volumes**. The **Create Live Volumes** wizard opens.
3. Select the Storage Center that hosts the volumes you want to convert, then click **Next**. The wizard advances to the next page.
4. Select the secondary Storage Center for the Live Volumes, then click **Next**
   - The wizard advances to the next page.

- If Fibre Channel or iSCSI connectivity is not configured between the local and remote Storage Centers, a dialog box opens. Click **Yes** to configure iSCSI connectivity between the Storage Centers.

5. Select the check box for each volume that you want to convert, then click **Next**. The wizard advances to the next page.
6. (Optional) Modify Live Volume default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volumes.
   - In the **Live Volume Attributes** area, select a QoS node for the secondary Storage Center, configure the automatic swap role policy, enable automatic failover and automatic restore, or enable reporting of non-optimized paths.

     NOTE: Live Volume QoS settings are only enforced on the primary Storage Center and are not enforced on the secondary Storage Center until it becomes the primary Storage Center.
7. Click **Next**. The wizard advances to the next page.
8. Review the Live Volumes you have configured.
   a. (Optional) If you want to add a managed replication or modify a Live Volume before it is created, select it, then click **Edit Settings**.
   b. Click **Finish**. The Live Volumes are created and they begin to replicate to the secondary Storage Center.

Related concepts

Live Volume Requirements on page 518
Live Volume Types on page 518
Managed Replications for Live Volumes on page 524

Modifying Live Volumes

Modify a Live Volume if you want to change replication attributes, Live Volume attributes, convert it to a replication, or delete it.

Swap the Primary Storage Center for a Live Volume

If the secondary Storage Center is receiving more IO for a Live Volume than the primary Storage Center, swap roles to improve performance. If an outage is planned at the site where the primary Storage Center is located, swap roles before the outage to make sure there is no interruption to volume availability. After swapping roles, save restore points to make sure that the restore point for the Live Volume stays current.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Swap Primary Storage Center of Live Volume**. The **Swap Primary Storage Center of Live Volume** dialog box appears.
3. Click **OK**.

Next steps

Save restore points to make sure that the restore point for the Live Volume stays current. See Save Replication Restore Points for One or More Storage Centers.

Change the Replication Type for a Live Volume

The replication type used by a Live Volume can be changed with no service interruption.

Prerequisites

- The source and destination Storage Centers must be running version 6.5 or later.
- If the Live Volume manages a synchronous replication, the replication type for the Live Volume must be asynchronous.

Steps

1. Click the **Replications & Live Volumes** view.

2. On the **Live Volumes** tab, select the Live Volume, then click **Edit Settings**. The **Edit Live Volume** dialog box appears.
3. In the **Type** area, select **Asynchronous** or **Synchronous**.
4. Click **OK**.

Related concepts

Live Volume Types on page 518

Change the Synchronization Mode for a Synchronous Live Volume

The synchronization mode for a synchronous Live Volume can be changed with no service interruption.

Prerequisites

The source and destination Storage Centers must be running version 6.5 or later.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Edit Settings**. The **Edit Live Volume** dialog box appears.
3. In the **Sync Mode** area, select **High Availability** or **High Consistency**.
4. Click **OK**.

Related concepts

Synchronous Replication on page 501
Synchronous Replication Modes on page 501

Add a Managed Replication to a Live Volume

Add a managed replication to a Live Volume to replicate the primary volume to a third Storage Center.

Prerequisites

The primary, secondary, and managed replication destination Storage Centers must meet the managed replication requirements.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Add Managed Replication**. The **Managed Replication Settings** wizard appears.
3. Select a destination Storage Center for the managed replication, then click **Next**.
   - The wizard advances to the next page.
   - If Fibre Channel or iSCSI connectivity is not configured between the local and remote Storage Centers, a dialog box appears. Click **Yes** to configure iSCSI connectivity between the Storage Centers.
4. (Optional) Modify managed replication default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
     - The **Transport Type** and **QoS Node** options are configured independently for the primary Storage Center and the secondary Storage Center.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volume.
5. Click Finish.
   The managed replication is created and begins replicating to the destination Storage Center.

Related concepts

Managed Replications for Live Volumes on page 524
Supported Live Volume with Managed Replication Topologies on page 524
Live Volume with Managed Replication Example Configuration on page 524

Managed Replication Requirements on page 525

Include Active Snapshot Data for an Asynchronous Live Volume

The Active Snapshot represents the current, unfrozen volume data.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Edit Settings**. The **Edit Live Volume** dialog box appears.
3. Select or clear the **Replicate Active Snapshot** check box then, click **OK**.

Enable or Disable Deduplication for a Live Volume

Deduplication reduces the amount of data transferred and enhances the storage efficiency of the remote Storage Center by copying only the changed portions of the snapshot history on the source volume, rather than all data captured in each snapshot.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Edit Settings**. The **Edit Live Volume** dialog box appears.
3. Select or clear the **Deduplication** check box, then click **OK**.

Select Different QoS Definitions for a Live Volume

Select a different QoS definitions for a Live Volume to change how the Live Volume uses bandwidth.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Edit Settings**. The **Edit Live Volume** dialog box appears.
3. From the **Primary QoS Node** drop-down menu, select a QoS definition that will be used for the Live Volume by the primary Storage Center.
4. From the **Secondary QoS Node** drop-down menu, select a QoS definition that will be used for the Live Volume by the secondary Storage Center.
5. Click **OK**.

Configure a Live Volume to Write Data to the Lowest Tier at the Destination

The **Replicate Storage To Lowest Tier** option forces all data written to the destination volume to the lowest storage tier configured for the volume. By default, this option is enabled for asynchronous Live Volumes.

Prerequisites

- The Live Volume must be asynchronous. The **Replicate Storage To Lowest Tier** option is not available for synchronous Live Volumes.
- The option **Allow Select to Lowest Tier on Live Volume Create** must be set in the Data Collector replication settings.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Edit Settings**. The **Edit Live Volume** dialog box opens.
3. Select the **Replicate Storage To Lowest Tier** check box.
4. Click **OK**.

Allow Replicate Storage to Lowest Tier Selection

To replicate data to the lowest storage tier, the option must be set in the Data Collector.

Steps

1. In the top pane of the Storage Manager Client, click **Edit Data Collector Settings**. The **Edit Data Collector Settings** dialog box appears.
2. Click the **Replication Settings** tab.
3. Select the **Allow Select to Lowest Tier on Live Volume Create** check box.
4. Click **OK**.

Allow a Live Volume to Automatically Swap Roles

Live Volumes can be configured to swap primary and secondary volumes automatically when certain conditions are met to avoid situations in which the secondary volume receives more IO than the primary volume.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Edit Settings**. The **Edit Live Volume** dialog box appears.
3. Select the **Automatically Swap Roles** check box.
4. (Optional) Modify the default swap behavior by editing the **Min Amount Before Swap**, **Min Secondary Percent Before Swap (%)**, and **Min Time As Primary Before Swap (Minutes)** fields. These fields are described in the online help.
5. Click **OK**.

Related concepts

Automatic Swap Role for Live Volumes on page 520

Revert a Live Volume to a Replication

If the remote Storage Center does not need to accept I/O for the Live Volume, you can convert the Live Volume to a conventional replication.

About this task

If the Live Volume manages a replication, the managed replication is converted into a non-managed replication when the Live Volume is reverted.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Revert to Replication**.
   The **Revert to Replication** dialog box opens.
3. Click **OK**.

Pause a Live Volume

Pausing a Live Volume temporarily prevents volume data from being copied from the primary volume to the secondary volume.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Pause**. The **Pausing Live Volume** dialog box opens.
3. Click **OK**.

Resume a Paused Live Volume

Resume a Live Volume to allow volume data to be copied to the secondary Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Replications** tab, select the paused replication, then click **Resume**. The **Resuming Replication** dialog box opens.
3. Click **OK**.

Set Threshold Alert Definitions for a Live Volume

Configure one or more Threshold Alert Definitions for a Live Volume if you want to be notified when specific thresholds are reached, such as the amount of replication data waiting to be transferred or the percentage of replication data that has been transferred.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Set Threshold Alert Definitions**. The **Set Threshold Alert Definitions** dialog box appears.
3. Select the alert definition for which you want to configure a threshold alert, then click **Create Threshold Definition**. The **Create Threshold Definition** dialog box appears.
4. Configure the threshold definition attributes as needed, then click **OK**. These attributes are described in the online help.
5. Click **OK** to close the **Set Threshold Alert Definitions** dialog box.

Delete a Live Volume

Use the **Live Volumes** tab to delete a Live Volume.

Prerequisites

Delete all associated replications, Live Volumes, or Live Migrations before deleting a Live Volume

About this task

If the Live Volume manages a replication, the managed replication is converted into a standalone replication when the Live Volume is deleted.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Delete**. The **Delete Objects** dialog box appears.
3. Select deletion options:
   - **Convert to Replication**: Select this check box to convert the Live Volume to a replication.
     NOTE: When you delete a Live Volume, the QoS settings are retained on the primary Storage Center volume and the QoS settings on the secondary Storage Center volume are modified to the system defaults.
   - **Recycle Secondary Volume:** Enable this check box if you want to move the secondary volume to the Recycle Bin on the secondary Storage Center.
   - **Delete Secondary Volume:** Select this check box if you do not want to retain the deleted secondary volume in the Recycle Bin (not recommended).
     WARNING: If you delete the secondary volume, you cannot recover the volume — it is permanently deleted from the Storage Center.
   - **Delete Restore Point:** Select this check box to delete the restore point for the Live Volume.
4. When you are finished, click **OK**.

Force Delete a Live Volume

Force Delete is an option for Live Volumes in a fractured state or if Storage Manager can view only one side of the Live Volume because the other side is down. A Live Volume is fractured if both secondary and primary Live Volumes are designated as primary or if Storage Manager can communicate with only the primary Live Volume.

Prerequisites

Both Live Volumes are inactive or Storage Manager is managing only one of the Storage Centers.

About this task

The following scenarios allow force delete.

Live Volume to Delete	Failed Over	Active Live Volume	Visible to Storage Manager
Primary	No	Primary	Primary only
Primary	Yes	Secondary	Primary and secondary
Secondary	No	Primary	Secondary only
Secondary	Yes	Secondary	Secondary only

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Live Volumes** tab then select a Live Volume.
3. Click **Force Delete**.
   The **Force Delete** dialog box appears.
4. Select the Storage Center that will retain the volume device ID.

   NOTE: Only managed Storage Centers can be selected.

   NOTE: If a Storage Center is selected to retain the volume device ID, the QoS setting is also retainedl. The Storage Centers not selected to retain the volume device ID will have the QoS setting modified to the system defaults.

5. Click **Next**.
   A confirmation page appears.
6. Click **Next**.
   A warning page appears if Storage Manager is managing only one of the Storage Centers.
7. Click **Finish**.
   The **Results Summary** page appears.
8. Click **OK**.

Manually Bring Primary Live Volume Online

After a failure, the primary Live Volume may be offline preventing the Live Volume relationship to be restored. In this case, manually bring the primary Live Volume online to activate the Live Volume and restore the Live Volume relationship with the secondary Live Volume. If both Live Volumes are down after a failover, Bring Primary Online selects the Live Volume to activate.

Prerequisites

- If visible to the Data Collector, the primary Live Volume must be down.
- If visible to the Data Collector, the secondary Live Volume must be down.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Live Volumes** tab then select a Live Volume.
3. Click **Bring Primary Online**.
   The **Bring Primary Online** dialog box appears.

4. Select a Live Volume.
5. Click **Next**.
6. Select the Storage Center where the Live Volume will be activated.
7. Click **Next**.

   NOTE: A warning page appears if Storage Manager is managing only one of the Storage Centers.

8. Click **Finish**.

Modifying Live Volumes with Automatic Failover

The following tasks apply to Live Volumes with Automatic Failover.

Update to the Local Tiebreaker

Updating to the local tiebreaker configures the Data Collector that Storage Manager is connected to as the tiebreaker. Storage Manager provides the option to update to the local tiebreaker when the current Data Collector is not configured as the tiebreaker. If another Data Collector is configured as the tiebreaker, such as a Remote Data Collector, do not configure the current Data Collector as the tiebreaker.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Live Volumes** tab then select a Live Volume.
3. Click **Update to Local Tiebreaker**.
   The **Update to Local Tiebreaker** dialog box opens.
4. Select a Live Volume.
5. Click **OK**.

Enable Automatic Failover on a Live Volume

Enabling Automatic Failover allows the Live Volume to automatically failover to the secondary Live Volume after a failure. Automatic Restore recreates the Live Volume relationship between the two Live Volumes. The active (previously secondary) Live Volume will remain the in the primary role and the original primary Live Volume will become the secondary Live Volume.

Prerequisites

- The Live Volume must be configured as synchronous and high-availability.
- Both primary and secondary Storage Centers must be managed by Storage Manager.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Live Volumes** tab.
3. Select a Live Volume then click **Edit Settings**. The **Edit Live Volume** dialog box opens.
4. Select the **Failover Automatically** check box.
5. To enable automatic restore, select the **Restore Automatically** check box.
6. Click **OK**.

Live Volume ALUA

Asymmetric Logical Unit Access (ALUA) is a set of SCSI concepts and commands that define path prioritization for SCSI devices. It allows paths to be described as fast, slow, or down and allows transitions between these states using a common standard. Live Volume ALUA reports Active/Optimized and Active/Non-optimized ALUA states on the primary and secondary volumes/storage systems, respectively.

Storage Center supports Live Volume ALUA beginning in version 7.3.

Live Volume ALUA Optimization Considerations

Live Volume ALUA is used to control the priority of paths for the Primary and Secondary Live Volume components. By default, volume mapping is Active/Optimized on the primary volume path and Active/Non-optimized on the secondary volume path. This section provides information about the design features of Live Volume ALUA.

- **ALUA is Automatically enabled**: Live Volume ALUA is automatically applied when creating Live Volumes in any of the following circumstances. Both the primary and secondary Storage Centers must support ALUA optimization.
  - Creating a new Live Volume
  - Converting a replicated volume to a Live Volume
  - Converting an existing volume to a Live Volume
  - Creating a Live Volume from a restore point (The restore point does not retain the new optimized ALUA information.)

  When a Live Volume is created, the **Report Non-optimized Paths** feature is enabled by default.
- **ALUA is not automatically enabled** Live Volume ALUA is not automatically enabled under the following circumstances:
  - Swapping Roles. However if ALUA is enabled on one or more of the systems, that status is reported and persists.
  - Existing Live Volumes after system upgrades. Use the ALUA optimization wizard to enable Live Volume ALUA.
- **ALUA Optimization Wizard**: If one or more Live Volumes are not ALUA optimized, a message is displayed in a banner at the top of the **Live Volume** tab in the **Replications & Live Volumes** view. Clicking the **Update to ALUA Optimized** link in the banner opens the ALUA optimization wizard. The wizard provides a guided process to enable ALUA optimization on existing Live Volumes.

  NOTE: The system must undergo a service outage (such as server rescans or reboots) to fully enable Live Volume ALUA support. This requirement is due to the path information memory of Multipath Input Output (MPIO) drivers on various servers. Because it is a disruptive operation, enabling Live Volume ALUA on existing Live Volumes should be performed during a maintenance window.
- **Non-optimized path reporting** Non-optimized path reporting is enabled or disabled using one of these methods:
  - In the **ALUA Optimization Wizard**: Disable or enable non-optimized path reporting by selecting or clearing the **Report Non-optimized Paths** check box (see Enable Live Volume ALUA Optimization).
  - In the **Edit Live Volume Settings** dialog box: Enable or disable non-optimized path reporting by clearing or selecting the **Report Non-optimized Paths** check box (see Enable or Disable Non-Optimized Path Reporting).
- **Microsoft Windows Environments**: Using non-optimized paths is not recommended in Microsoft Windows environments and reporting non-optimized path reporting should be disabled. When all paths are reported as non-optimized, MPIO drivers do not function in a round-robin as expected. Data transfer is reduced to a single path causing a delayed failover.

  NOTE: Certain Windows Server 2016 versions can support non-optimized path reporting properly. For more information and best practice guidelines for configuring MPIO on Microsoft Server 2016, see the Dell EMC SC Series Storage and Microsoft Multipath I/O white paper on the Dell support site.

Enable Live Volume ALUA Optimization

Use the ALUA optimization wizard to enable ALUA optimization on existing Live Volumes that are eligible to be upgraded.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Live Volumes** tab.
   The **Live Volumes** view is displayed.
3. In the right pane, a Live Volume ALUA banner message is indicates that Live Volumes are available that are eligible for ALUA optimization. On the right side of the banner, click **Update to ALUA Optimized**.
   The **Update to ALUA Optimized** wizard opens. The first dialog box displays a list of Live Volumes that are not ALUA optimized but are capable of becoming ALUA optimized.

   NOTE: The Live Volume ALUA banner message is displayed if Storage Manager detects one or more Live Volumes that have not been ALUA optimized and both Storage Centers support ALUA optimization.
4. Select the Live Volumes that you want to optimize and click **Next**.
   A dialog box displays a warning message and an option to reset the secondary server mappings.
   - If you select the **Reset Secondary Server Mappings** check box, the server mappings of the Secondary Live Volumes are reset and will cause an immediate outage. A manual rescan must be performed.
   - By default, the **Reset Secondary Server Mappings** check box is cleared. This will not cause an outage. The secondary side servers must be restarted later during a maintenance operation.

NOTE: Because enabling Live Volume ALUA is a disruptive process, is should be performed during a maintenance operation.

5. Click **Next**.
   A dialog box displays a warning message and an option to enable or disable reporting non-optimized paths.
   - By default, the **Report Non-optimized Paths** check box is selected. This will cause Live Volumes to report non-optimized ALUA paths from the secondary system.
   - If you clear the **Reset Secondary Server Mappings** check box, Live Volumes will not report non-optimized ALUA paths from the secondary system.

   NOTE: When all paths are reported as non-optimized, Microsoft Multipath Input Output (MPIO) drivers does not perform round-robin path usage as expected. As a result, data transfer is reduced to a single path and causes a long delay for failover. Therefore, using non-optimized paths is not recommended in Microsoft Windows environments and non-optimized path reporting should be disabled.

   NOTE: Certain Windows Server 2016 versions can support non-optimized path reporting properly. For more information and best practice guidelines for configuring MPIO on Microsoft Server 2016, refer to Dell EMC SC Series Storage and Microsoft Multipath I/O white paper located on the Dell support site.
6. Click **Finish**.
   The results of the ALUA optimization process are displayed.
7. Click **OK**.

Enable or Disable Non-Optimized Path Reporting

When Live Volume ALUA is enabled, non-optimized paths are reported by default. However, this setting can be enabled or disabled to optimize path I/O.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Live Volumes** tab.
   The **Live Volumes** view is displayed.
3. In the Live Volume attribute pane, click **Edit Settings**.
   The **Edit Live Volume Settings** dialog box opens.
4. In the **Live Volume Attributes** area, select or clear the non-optimized path setting.
   - Select the **Report Non-optimized Paths** checkbox to enable Live Volumes to report non-optimized ALUA paths from the secondary system.
   - Clear the **Report Non-optimized Paths** checkbox to disable Live Volumes from reporting non-optimized ALUA paths from the secondary system.
5. Click **OK**.

Monitoring Live Volumes

Monitor a Live Volume to determine how much progress has been made.

Filter Live Volumes By Primary Storage Center

To reduce the number of Live Volumes that are displayed on the **Replications & Live Volumes** view, filter the Live Volumes by primary Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Live Volumes** tab.
3. In the **Source Storage Centers** pane, hide Live Volumes that originate from one or more Storage Centers by clearing the corresponding check boxes.
4. (Optional) When you are finished, you can revert to the default view by clicking **Select All** in the **Source Storage Centers** pane.

Filter Live Volumes By Secondary Storage Center

To reduce the number of Live Volumes that are displayed on the **Replications & Live Volumes** view, filter the Live Volumes by secondary Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Live Volumes** tab.
3. In the **DR Storage Centers** pane, hide Live Volumes that are destined to one or more Storage Centers by clearing the corresponding check boxes.
4. (Optional) When you are finished, you can revert to the default view by clicking **Select All** in the **DR Storage Centers** pane.

View the Replication Managed by a Live Volume

A managed replication replicates a Live Volume primary volume to a third Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume, then click **Managed Replication**. The **Replications** tab opens and selects the managed replication.

Related concepts

Managed Replications for Live Volumes on page 524

View the Snapshots for a Live Volume

When a Live Volume is selected, the **Snapshots** subtab displays the snapshots for the primary volume and the secondary volume.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume.
3. In the bottom pane, click the **Snapshots** tab.

View the Progress Report for a Live Volume

When a Live Volume is selected, the **Progress Reports** subtab displays charts for the amount of data waiting to be copied and the percent complete.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select the Live Volume.
3. In the bottom pane, click the **Progress Reports** tab.

View IO/sec and MB/sec Charts for a Live Volume

When a Live Volume is selected, the **IO Reports** subtab displays the Replication IO/Sec and Replication MB/Sec charts.

About this task

The charts contain performance data for the replication of a Live Volume from the primary Storage Center to the secondary Storage Center.

Steps

1. Click the **Replications & Live Volumes** view.
2. On the **Live Volumes** tab, select a Live Volume.
3. In the bottom pane, click the **IO Reports** tab.

15

Storage Center DR Preparation and Activation

Activate disaster recovery to restore access to your data in the event of an unplanned disruption.

Topics:

- How Disaster Recovery Works
- Disaster Recovery Administration Options
- Preparing for Disaster Recovery
- Activating Disaster Recovery
- Activating Disaster Recovery for PS Series Group Replications
- Restarting Failed Replications
- Restoring Replications and Live Volumes
- Deleting Restore Points

How Disaster Recovery Works

Disaster recovery (DR) is the process activating a replicated destination volume when the source site fails. When the source site comes back online, the source volume can be restored based on the volume at the DR site.

The following diagrams illustrate each step in the DR process. Although this example shows a replication, DR can also be used for a Live Volume.

Step 1: A Volume is Replicated to a DR Site

A volume is protected from disaster by replicating it to a Storage Center located at a DR site.

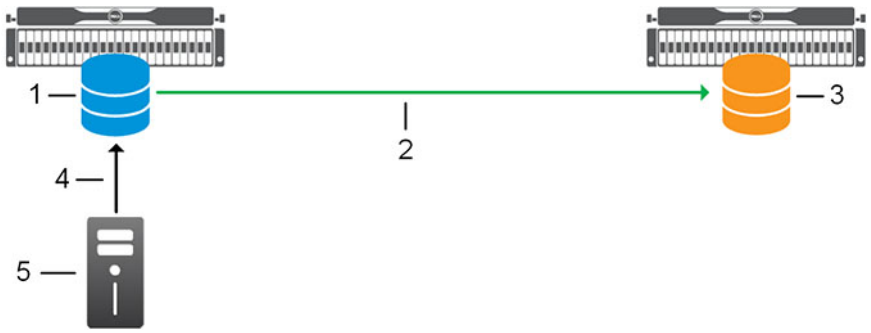


Figure 55. Volume Replicating to a DR Site

1. Source volume
2. Replication over Fibre Channel or iSCSI
3. Destination volume
4. Server mapping to source volume
5. Server mapped to the source volume

Step 2: The Source Site Goes Down

When the source site goes down, the data on the source volume can no longer be accessed directly. However, the data has been replicated to the destination volume.

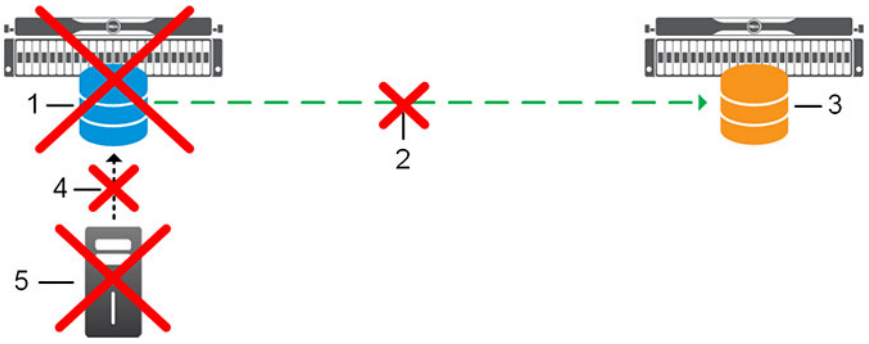


Figure 56. Replication When the Source Site Goes Down

1. Source volume (down)
2. Replication over Fibre Channel or iSCSI (down)
3. Destination volume
4. Server mapping to source volume (down)
5. Server mapped to the source volume (down)

Step 3: An Administrator Activates Disaster Recovery

An administrator activates DR to make the data in the destination volume accessible. When DR is activated, Storage Manager brings the destination volume on line and maps it to a server at the DR site. The server sends IO to the activated DR volume for the duration of the source site outage.

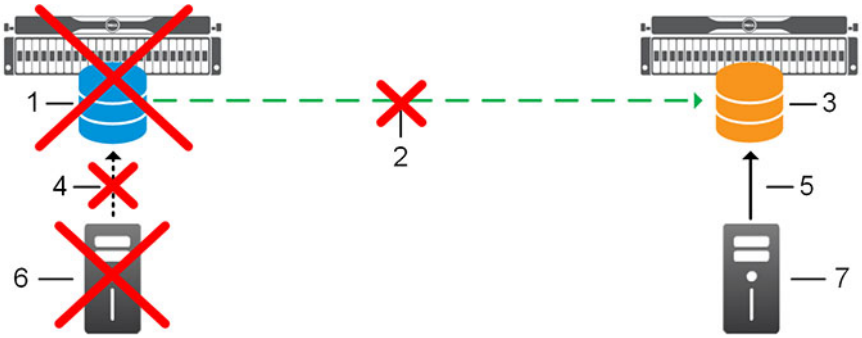


Figure 57. Replication When DR is Activated

1. Source volume (down)
2. Replication over Fibre Channel or iSCSI (down)
3. Destination volume (activated)
4. Server mapping to source volume (down)
5. Server mapping to activated DR volume
6. Server at source site
7. Server at DR site

Step 4: Connectivity is Restored to the Source Site

When the outage at the source site is corrected, Storage Manager Data Collector regains connectivity to the source Storage Center. The replication cannot be restarted at this time because the destination volume contains newer data than the original source volume.

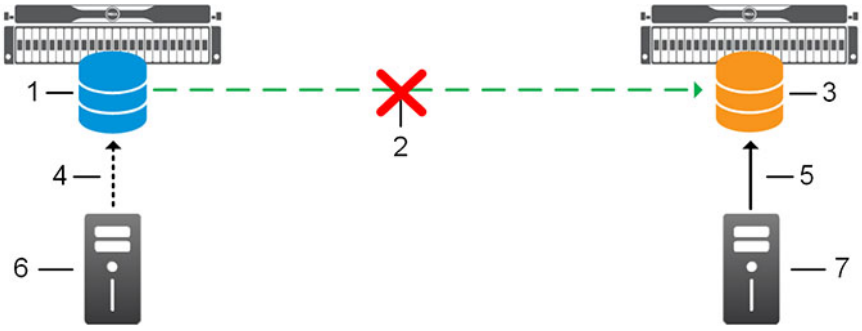


Figure 58. Replication After the Source Site Comes Back Online

1. Source volume
2. Replication over Fibre Channel or iSCSI (down)
3. Destination volume (activated)
4. Server mapping to source volume (may be up or down)
5. Server mapping to activated DR volume
6. Server at source site (may be up or down)
7. Server at DR site

Step 5: An Administrator Restores the Source Volume

After verifying that the source site is back up and fully functional, an administrator begins the process of restoring the original source volume based on the activated DR volume. Administrator intervention is required during the restore process to make sure that IO is halted to the destination volume at the appropriate time.

Step 5A: The Destination Volume Replicates Back to the Source Site

When the restore operation is initiated, the activated destination begins replicating to the original source volume. The most recent common snapshot for the original source and activated DR volume is located, and subsequent snapshots are replicated to the original source volume. If all common snapshots expired after the destination volume was activated for DR, a new volume is created and the original is placed in the recycle bin so that it can be retrieved if necessary. During this time, the activated DR volume continues to accept IO.

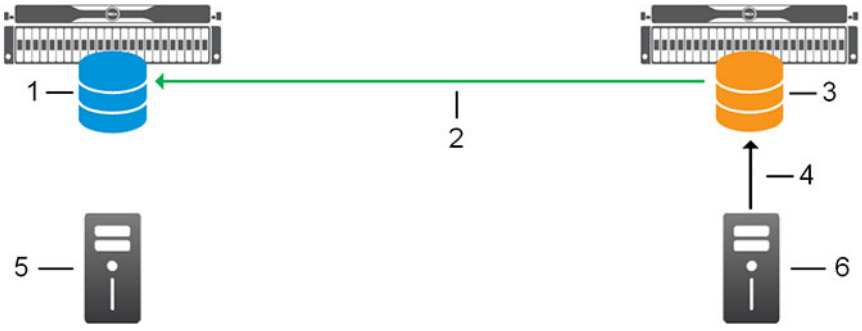


Figure 59. Activated DR Volume Replicating Back to the Source Site

1. Source volume being recovered
2. Replication over Fibre Channel or iSCSI
3. Destination volume (activated)
4. Server mapping to activated DR volume
5. Server at source site (not mapped)
6. Server at DR site

Step 5B: The Activated DR Volume is Deactivated

After the replication from the activated DR volume to the original source volume is synchronized, Storage Manager prompts the administrator to halt IO to the secondary volume.

NOTE: IO must be halted before the destination volume is deactivated because the deactivation process unmaps the volume from the server.

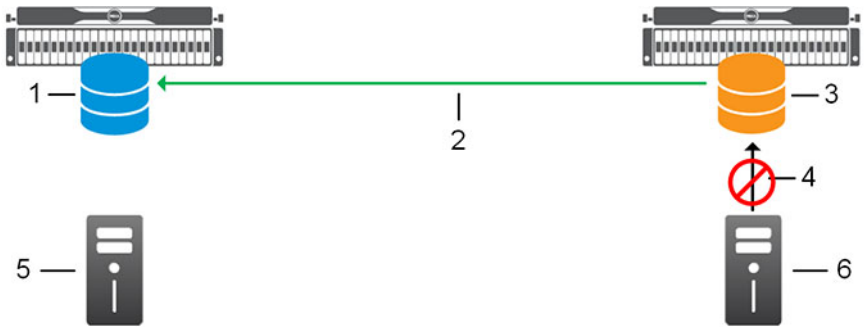


Figure 60. DR-Activated Volume is Deactivated

1. Source volume being recovered
2. Replication over Fibre Channel or iSCSI
3. Destination volume (activated)
4. Server mapping to activated DR volume (IO halted)
5. Server at source site (not mapped)
6. Server at DR site

Step 5C: The Source Volume is Activated

Storage Manager prompts the administrator to deactivate and unmap the destination volume. The source volume resumes replicating to the destination volume, and the source volume is activated and mapped to the server at the source site.

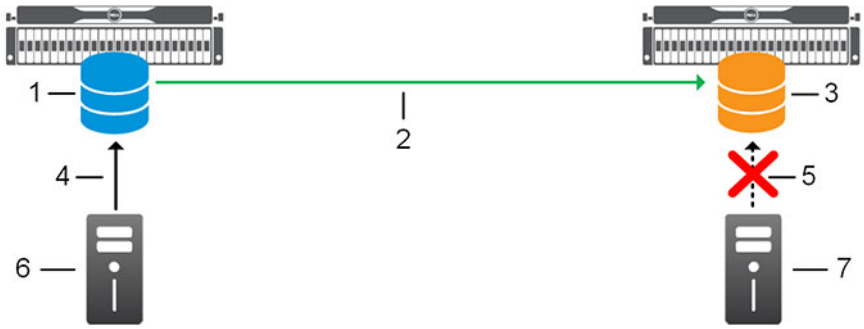


Figure 61. Recovered Source Volume is Activated

1. Recovered and activated source volume
2. Replication over Fibre Channel or iSCSI
3. Destination volume (deactivated)
4. Server at source site mapped to recovered and activated source volume
5. Server mapping removed from destination volume
6. Server at source site
7. Server at DR site

Disaster Recovery Administration Options

Use Storage Manager to prepare for DR, activate DR, and restore failed volumes. To make sure that a site outage does not prevent you from accessing Storage Manager to perform DR operations, you can optionally install a remote Data Collector at a DR site.

A remote Data Collector provides access to Storage Manager DR options when the primary Data Collector is unavailable. In the event that the primary Data Collector is unavailable, use a locally installed Client to connect to the remote Data Collector.

Related concepts

Remote Data Collector on page 555

Preparing for Disaster Recovery

Prepare for DR by saving restore points, predefining DR settings, and testing those settings.

Perform these tasks to implement a DR plan:

- Saving and Validating Restore Points on page 542
- Predefining Disaster Recovery Settings for Replications on page 543
- Test Activating Disaster Recovery on page 544

Saving and Validating Restore Points

A restore point includes information about a replication or Live Volume, including the source and destination volumes, source and destination Storage Centers, and the QoS definitions used. If a Storage Center goes down, this information becomes the basis for restoring the replication or Live Volume.

- A restore point for a Live Volume that manages a replication does not contain information about the managed replication.
  - If DR is activated for the Live Volume using the **Preserve Live Volume** option, the managed replication continues to operate and follows the DR-activated volume.
  - If DR is activated for the Live Volume without using the **Preserve Live Volume** option, the managed replication is removed and must be re-created manually.
- A restore point for a replication that is managed by a Live Volume does not contain information about the Live Volume. If DR is activated for the managed replication, the Live Volume must be re-created manually.

Save Replication Restore Points for One or More Storage Centers

Save replication restore points after creating replications or Live Volumes. Storage Manager automatically saves restore points for replications and Live Volumes.

Steps

1. Click the **Replications & Live Volumes** view.
2. In the **Actions** pane, click **Save Restore Points**. The **Save Restore Points** dialog box opens.
3. Select the check boxes for Storage Centers for which you want to save restore points, then click **OK**.

Set a Schedule for Automatically Saving and Validating Restore Points

Set a schedule for automatically saving and validating restore points to make sure that good restore points are always available to perform Disaster Recovery.

Steps

1. In the top pane of the Storage Manager Client, click **Edit Data Collector Settings**. The **Edit Data Collector Settings** dialog box opens.
2. Click the **Schedules** tab.
3. Select the **Automatically save and validate restore points** check box.

4. From the **Frequency** drop-down menu, select how often you want restore points to be automatically saved and validated.
5. (Conditional) If you selected **Daily** in the previous step, select the time of day to save and validate restore points from the **Time** drop-down menu.
6. Click **OK**.

Validate Replication Restore Points

Validate replication restore points before testing or activating DR to make sure they can be used for DR.

Steps

1. Click the **Replications & Live Volumes** view.
2. In the **Actions** pane, click **Validate Restore Points**. Storage Manager reviews all saved replications and makes sure that they are still running and displays the results on the **Restore Points** tab. The **Status** column displays the results of the validation operation. Possible status values are:
   - **Up:** The replication is up and running normally.
   - **Degraded:** There is something wrong with the replication. See to the **State** column information about why replication is no longer running. This replication is eligible for DR.
   - **Down:** The replication is not running. See to the **State** column information about why replication is no longer running. This could be because the destination system is no longer available or that the source and Destination volume are no longer up and running. This replication is not eligible for DR.
3. If one or more restore points are degraded or down, take corrective action.
   - If a restore point is degraded, you can perform either of the following actions:
     - Activate a DR site
     - Restore or restart the replication to the source or destination Storage Center
   - If a restore point is degraded or down because you purposefully deleted or aborted the corresponding replication, you can delete the restore point. To do so, right-click the restore point, then select **Delete**.

Related references

Activating Disaster Recovery on page 546

Related tasks

Restarting Failed Replications on page 551
Restoring Replications and Live Volumes on page 552

Predefining Disaster Recovery Settings for Replications

Predefining DR for a replication restore point is an optional step that configures DR activation settings for a replication restore point ahead of time, so that the DR site is ready if the destination volume needs to be activated. If you do not intend to access data from a destination site, you do not need to predefine DR settings. DR settings cannot be predefined for Live Volume restore points.

Predefine Disaster Recovery for Multiple Restore Points

If a pair of Storage Centers host multiple replications, DR settings can be predefined for all of the corresponding restore points simultaneously.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab, then click **Predefine Disaster Recovery**. The **Predefine Disaster Recovery** wizard appears.
3. Select the source/destination Storage Center pair for which you want to predefine DR, then click **Next**. The wizard advances to the next page.
4. (Optional) Configure DR settings for each restore point.

a. Select the restore point that you want to modify, then click **Edit Settings**. The **Predefine Disaster Recovery** dialog box appears.
b. Modify the recovery volume settings as needed, then click **OK**. These attributes are described in the online help.

5. When you are done, click **Finish**.

Predefine Disaster Recovery Settings for a Single Restore Point

If you need to make sure a recovery site has access to a replicated volume when DR is activated, predefine DR settings for the corresponding restore point.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab.
3. Right-click the restore point, then select **Predefine Disaster Recovery**. The **Predefine Disaster Recovery** dialog box appears.
4. In the **Name** field, type the name for the recovery volume.
5. Select the server to which the recovery volume will be mapped.
   a. Next to the **Server** label, click **Change**. The **Select Server** dialog box appears.
   b. Select the server, then click **OK**.
6. Modify the remaining recovery volume settings as needed. These attributes are described in the online help.
7. Click **OK**.

Test Activating Disaster Recovery

Testing DR activation for a replication restore point creates a test-activated view volume and maps it to the appropriate server without interrupting service for the original volume. This allows you to make sure that your DR plan is viable.

- Periodically test-activate DR for restore points to ensure their the restore point is viable.
- DR activation settings specified for test activation are retained for future DR activation and test activation.
- Live Volume restore points cannot be tested.

Test DR Activation for Multiple Restore Points

If a pair of Storage Centers host multiple replications, all of the corresponding restore points can be tested simultaneously.

Prerequisites

- The restore points must be associated with replications. Live Volume restore points cannot be tested.
- The destination volume for each replication must be present on the remote Storage Center. If the destination volume for a replication restore point is missing, it cannot be tested.
- A server must be present at the DR site to perform test activation.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab, then click **Test Activate Disaster Recovery**. The **Test Activate Disaster Recovery** wizard appears.
3. Select the source/destination Storage Center pair for which you want to test-activate DR, then click **Next**. The wizard advances to the next page.
4. In the **Available Restore Points** pane, select the restore points that you want to test, then click **Next**. The wizard advances to the next page.
5. Configure DR test-activation settings for each restore point.
   a. Select the restore point that you want to modify, then click **Edit Settings**. The **Test Activate Disaster Recovery** dialog box appears.

      If the restore point corresponds to a synchronous replication, the dialog box displays additional information about the state of the replication:

- The **Sync Data Status** field displays the synchronization status for the replication at the time the restore point was validated.
- A recommendation about whether the destination volume is currently synchronized with the source volume is displayed below the **Sync Data Status** field in green or yellow text.

NOTE: For high consistency mode synchronous replications that are current, the **Use Active Snapshot** check box is automatically selected.

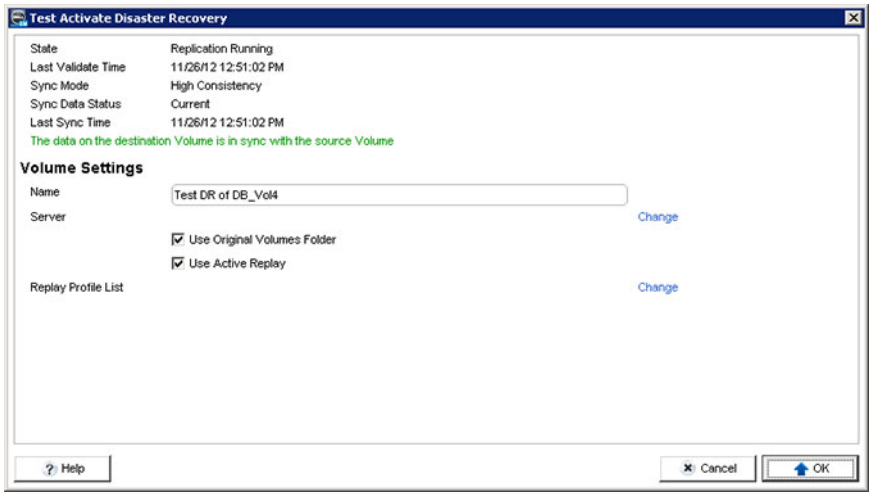


Figure 62. Test Activate Disaster Recovery Dialog Box

b. Select the server to which the test-activated volume will be mapped by clicking **Change** next to the **Server** label.
c. Modify the remaining settings for the test-activated volume as needed, then click **OK**. These attributes are described in the online help.

6. When you are done, click **Finish**.
   - Storage Manager creates test-activated view volumes and maps them to the configured server(s).
   - Use the **Recovery Progress** tab to monitor DR test-activation

Test DR Activation for a Single Restore Point

To test DR activation for a replication, use the corresponding restore point.

Prerequisites

- The restore point must be associated with a replication. Live Volume restore points cannot be tested.
- The destination volume must be present on the remote Storage Center. If the destination volume for a replication restore point is missing, it cannot be tested.
- A server must be present at the DR site to perform test-activation.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab.
3. Right-click the restore point, then select **Test Activate Disaster Recovery**. The **Test Activate Disaster Recovery** dialog box appears.

   If the restore point corresponds to a synchronous replication, the dialog box displays additional information about the state of the replication:

   - The **Sync Data Status** field displays the synchronization status for the replication at the time the restore point was validated.
   - A recommendation about whether the destination volume is currently synchronized with the source volume is displayed below the **Sync Data Status** field in green or yellow text.

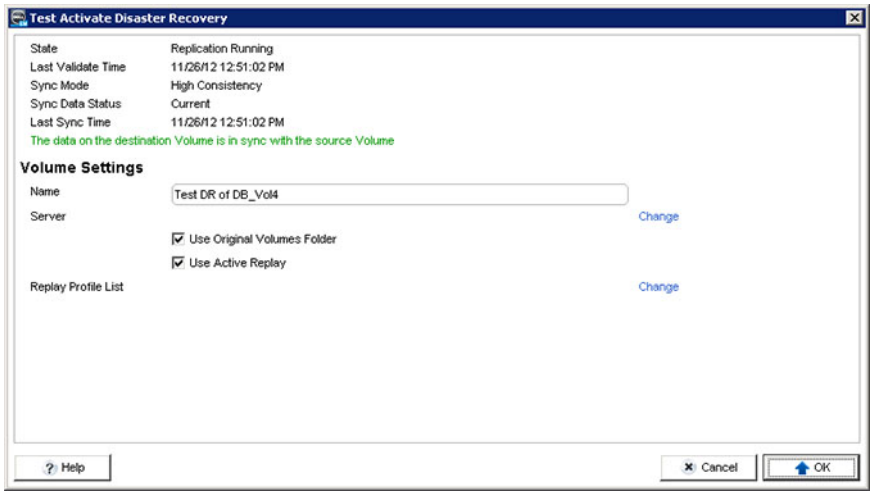


Figure 63. Test Activate Disaster Recovery Dialog Box

4. In the **Name** field, type the name for the activated view volume.
5. Select the server to which the activated view volume will be mapped.
   a. Next to the **Server** label, click **Change**. The **Select Server** dialog box appears.
   b. Select the server, then click **OK**.
6. Modify the remaining activation settings as needed. These attributes are described in the online help.

   NOTE: For high consistency mode synchronous replications that are current, the **Use Active Snapshot** check box is automatically selected.

7. When you are finished, click **OK**.
   - Storage Manager activates the test recovery volume.
   - Use the **Recovery Progress** tab to monitor DR test-activation

Delete Test-Activated Disaster Recovery Volumes

After you are finished testing DR, delete the volumes that were created as part of the testing.

Steps

1. Click the **Replications & Live Volumes** view.
2. In the **Actions** pane, click **Delete Test DR Volumes**. The **Delete Test DR Volumes** dialog box appears.
3. Select the check boxes for the test DR volumes you want to delete, then click **OK**.

Activating Disaster Recovery

Activate DR when a volume or site becomes unavailable. When DR is activated, a view volume of the original destination volume (replication) or secondary volume (Live Volume) is brought on line and mapped to a server at the DR site. Before DR can be activated for a volume, at least one snapshot must have been Replicated to the DR site.

Types of Disaster Recovery Activation for Live Volumes

Storage Center supports two types of Disaster Recovery for Live Volumes:

- **Preserve Live Volume**: Directs IO requests to the secondary volume by promoting it to primary. The Live Volume is not deleted and may be repaired when an administrator restores the volume after the source Storage Center comes back online. Volume identity is preserved so that administrator intervention is not required on the servers mapped to the volume. If a replication is managed by the Live Volume, the managed replication is preserved and follows the DR-activated volume.
- **Recreate Live Volume**: If **Preserve Live Volume** is not selected or not available, Storage Manager deletes the Live Volume, creates a view volume, and maps it to a server. During the recovery process, the Live Volume is recreated. If a replication is managed by the Live Volume, the managed replication is removed during the recovery process.

Disaster Recovery Activation Limitations

Activating DR for a replication removes any replications that use the activated volume (original destination/secondary volume) as the source volume.

Related concepts

Replicating a Single Volume to Multiple Destinations on page 502

Planned vs Unplanned Disaster Recovery Activation

During disaster recovery activation, you may choose whether you want to allow planned DR activation. The following table displays some of the differences between planned and unplanned DR activation.

Planned DR Activation	Unplanned DR Activation
The servers on the production site are shut down.	The servers on the production site are not shut down.
The Storage Centers on the production site do not have to be shut down.	The Storage Centers on the production site are shut down.
The source volume is no longer mapped to the server.	The source volume is still mapped to the production servers.
You can copy any remaining data prior to activation, eliminating data loss.	Data may be lost, depending on the recovery point objective (RPO).
The production site will not come back online while service has switched to the DR site.	The production Storage Centers and the servers may come back online, creating the danger of a split brain.

Disaster Recovery Activation Procedures

If an entire site becomes unavailable, DR can be activated for all affected volumes in a single operation. If a single volume becomes unavailable, activate DR for the corresponding restore point.

Activate Disaster Recovery for Multiple Restore Points

If a pair of Storage Centers host multiple replications and/or Live Volumes, disaster recovery can be activated for all of the corresponding restore points simultaneously.

Prerequisites

Save and validate restore points.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab, then click **Activate Disaster Recovery**. The **Activate Disaster Recovery** wizard appears.
3. Select the source/destination Storage Center pair for which you want to activate DR, then click **Next**. The wizard advances to the next page.
4. Choose whether you want to allow planned DR activation.
   a. (Optional, replication only) To allow DR to be activated while the replication is functioning normally, select the **Allow Planned Activate Disaster Recoveries** check box.
   b. Click **Next**. The wizard advances to the next page.
5. In the **Available Restore Points** pane, select the restore points that you want to activate, then click **Next**. The wizard advances to the next page.
6. Configure DR settings for each restore point.
   a. Select the restore point that you want to modify, then click **Edit Settings**. The **Activate Disaster Recovery** dialog box appears.

If the restore point corresponds to a synchronous replication, the dialog box displays additional information about the state of the replication:

- The **Sync Data Status** field displays the synchronization status for the replication at the time the restore point was validated.
- A recommendation about whether the destination volume is currently synchronized with the source volume is displayed below the **Sync Data Status** field in green or yellow text.

NOTE: For high consistency mode synchronous replications that are current, the **Use Active Snapshot** check box is automatically selected.

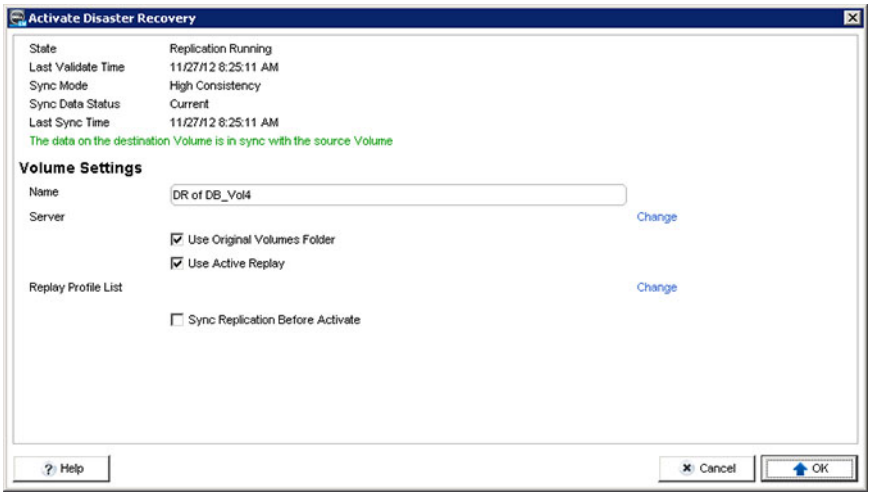


Figure 64. Activate Disaster Recovery Dialog Box

b. (Live Volume, Storage Center 6.5 and later only) Select the **Preserve Live Volume** check box to direct IO requests to the secondary volume without deleting the Live Volume. If the Live Volume manages a replication, **Preserve Live Volume** must be selected to preserve the managed replication later in the restore process.
   - If **Preserve Live Volume** is selected, Storage Center directs IO requests to the secondary volume by promoting it to primary. The Live Volume is not deleted and may be repaired when the original primary Storage Center comes back online. Volume identity is preserved so that administrator intervention is not required on the servers mapped to the volume. If a replication is managed by the Live Volume, it moves to follow the newly promoted primary volume. Fewer volume settings are available because the existing Live Volume settings are used.
   - If **Preserve Live Volume** is not selected, Storage Manager deletes the Live Volume, creates a view volume, and maps it to a server. During the restore process, the Live Volume is recreated. If a replication is managed by the Live Volume, the managed replication is removed later during the restore process.

c. Select a server to map the recovery volume to by clicking **Change** next to the **Server** label.
   - A server is required for each restore point.
   - Click **Advanced Mapping** to configure LUN settings, restrict mapping paths, or present the volume as read-only.
   - This option is not available if the **Preserve Live Volume** check box is selected.

d. Choose which snapshot will be used for the activated volume.
   - If **Preserve Live Volume** is not available or not selected, use the current state of the volume by selecting **Use Active Snapshot**, or select a frozen snapshot by clicking **Change** next to **Snapshot**. By default, the last frozen snapshot is used.
   - If **Preserve Live Volume** is selected, the last frozen snapshot is used unless **Use Active Snapshot** is selected.

e. (Optional) If **Preserve Live Volume** is not available or not selected, click **Change** next to **Snapshot Profile List** to specify which snapshot profiles will be associated with the activated volume.

f. Click **OK**.

7. Click **Finish**.
   - Storage Manager activates the recovery volumes.
   - Use the **Recovery Progress** tab to monitor DR activation

Related concepts

Saving and Validating Restore Points on page 542

Activate Disaster Recovery for a Single Restore Point

To activate DR for a replication or Live Volume, use the corresponding restore point.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab.
3. Right-click the restore point, then select **Activate Disaster Recovery**. The **Activate Disaster Recovery** dialog box appears.

   If the restore point corresponds to a synchronous replication, the dialog box displays additional information about the state of the replication:

   - The **Sync Data Status** field displays the synchronization status for the replication at the time the restore point was validated.
   - A recommendation about whether the destination volume is currently synchronized with the source volume is displayed below the **Sync Data Status** field in green or yellow text.

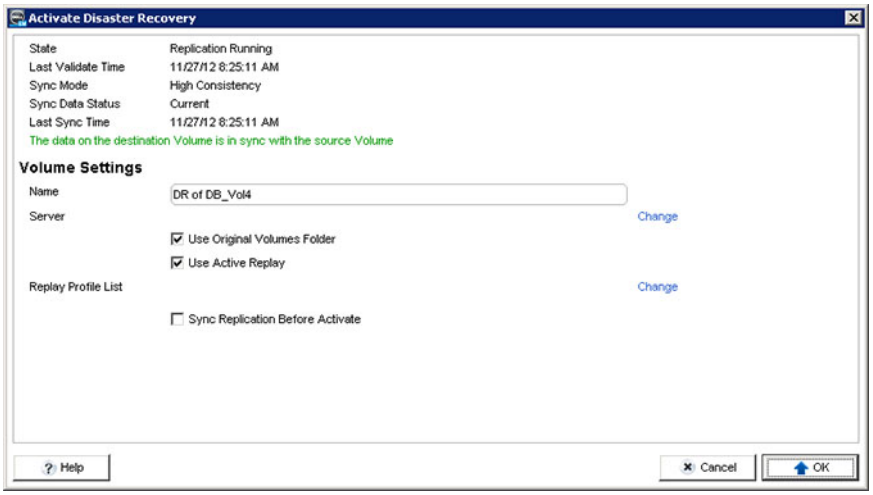


Figure 65. Activate Disaster Recovery Dialog Box

4. (Live Volume, Storage Center 6.5 and later only) Select the **Preserve Live Volume** check box to direct IO requests to the secondary volume without deleting the Live Volume. If the Live Volume manages a replication, **Preserve Live Volume** must be selected to preserve the managed replication later in the restore process.
   - If **Preserve Live Volume** is selected, Storage Center directs IO requests to the secondary volume by promoting it to primary. The Live Volume is not deleted and may be repaired when the original primary Storage Center comes back online. Volume identity is preserved so that administrator intervention is not required on the servers mapped to the volume. If a replication is managed by the Live Volume, it moves to follow the newly promoted primary volume. Fewer volume settings are available because the existing Live Volume settings are used.
   - If **Preserve Live Volume** is not selected, Storage Manager deletes the Live Volume, creates a view volume, and maps it to a server. During the restore process, the Live Volume is recreated. If a replication is managed by the Live Volume, the managed replication is removed later during the restore process.
5. In the **Name** field, type the name for the recovery volume.
6. Select a server to map the recovery volume to by clicking **Change** next to the **Server** label.
   - A server is required for each restore point unless the **Preserve Live Volume** check box is selected.
   - Click **Advanced Mapping** to configure LUN settings, restrict mapping paths, or present the volume as read-only.
7. Choose which snapshot will be used for the activated volume.
   - If **Preserve Live Volume** is not available or not selected, use the current state of the volume by selecting **Use Active Snapshot**, or select a frozen snapshot by clicking **Change** next to **Snapshot**. By default, the last frozen snapshot is used.
   - If **Preserve Live Volume** is selected, the last frozen snapshot is used unless **Use Active Snapshot** is selected.

     NOTE: For high consistency mode synchronous replications that are current, the **Use Active Snapshot** check box is automatically selected.

8. (Optional) If **Preserve Live Volume** is not available or not selected, click **Change** next to **Snapshot Profile List** to specify which snapshot profiles will be associated with the activated volume.
9. Click **OK**.
   - Storage Manager activates the recovery volume.
   - Use the **Recovery Progress** tab to monitor DR activation

Related concepts

Saving and Validating Restore Points on page 542

Access Data on an Original Primary Volume After DR Activation

If DR is activated for a Live Volume using the **Preserve Live Volume** option, the original primary Storage Center prevents the original primary volume from being active until the Live Volume is restored. If you need to access data on the original primary volume before the Live Volume is restored, use the **Bring Primary Copy Online** option to create a view volume of the original primary volume and map it to the same server.

Prerequisites

DR must have been activated for the Live Volume with the **Preserve Live Volume** option selected.

About this task

- The view volume that is created is not part of the Live Volume. Use this option only to access primary volume data while disaster recovery is activated.
- Volume identity is not preserved when the view volume is created, so the server may not recognize it as the original primary volume.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Live Volumes** tab.
3. Select the Live Volume, then click **Bring Primary Copy Online**. The **Bring Primary Copy Online** dialog box appears.
4. Click **OK**.

Activating Disaster Recovery for PS Series Group Replications

After replicating a volume to a PS Group from a Storage Center the destination volume must be activated on the destination PS Group. After it is activated, it can be mapped to a server.

Prerequisites

- The source volume must have at least one snapshot
- Both storage systems must be managed by the Data Collector

About this task

NOTE: Activating the destination volume is not required for PS Group to Storage Center replications. For replications from a PS Group to a Storage Center, follow the instructions in *Activating Disaster Recovery for Storage Center Replications*.

Steps

1. Click the **Replications and Live Volumes** tab.
2. Click the **Restore Points** tab.
3. Select a restore point for the replication from the table.
4. Click **Activate Disaster Recovery**.
   The Activate Disaster Recovery dialog box opens.

5. Select the replication from the table.
6. Click **Next**.
7. Modify the Volume settings for the destination volume as needed.
8. Click **OK**.
   - Storage Manager activates the recovery volume.
   - Use the **Recovery Progress** tab to monitor DR activation

Restarting Failed Replications

If a source volume is current and functional, and the destination system is available but a Replication failed or was deleted, you can restart the Replication. To see if a Replication can be restarted, validate Restore Points.

Restart Replication for Multiple Restore Points

If multiple replications and/or Live Volumes hosted by a Storage Center pair failed or were deleted, you can restart them simultaneously.

About this task

NOTE: Restarting replications removes replications that are configured in series (cascade mode) or that replicate the same volume to multiple destinations (mixed mode).

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab, then click **Restore/Restart DR Volumes**. The **Restore/Restart DR Volumes** wizard appears.
3. Select the source/destination Storage Center pair for which you want to restart replications, then click **Next**. The wizard advances to the next page.
4. Read the **Restart Warning** and **Recovery Warning** text, modify any settings that are displayed as necessary, then click **Next**. The wizard advances to the next page.
5. In the **Available Restore Points** pane, select the restore points for which you want to restart replication, then click **Next**. The wizard advances to the next page.
6. (Optional) Configure replication settings for each restore point.
   a. Select the restore point that you want to modify, then click **Edit Settings**. The **Restore/Restart DR Volumes** dialog box appears.
   b. Modify the replication settings as needed, then click **OK**. These settings are described in the online help.
7. When you are done, click **Finish**.
   - Storage Manager restarts the replications.
   - Use the **Recovery Progress** tab to monitor the recovery.

Restart a Replication for a Single Restore Point

If a replication or Live Volume failed or was deleted, you can use the corresponding restore point to restart replication.

About this task

NOTE: Restarting replications removes replications that are configured in series (cascade mode) or that replicate the same volume to multiple destinations (mixed mode).

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab.

3. Right-click the restore point that corresponds to the replication, then select **Restore/Restart DR Volumes**. The **Restore/Restart DR Volumes** dialog box appears.
4. Enable or disable the replication options as needed, then click **OK**. These options are described in the online help.

Restoring Replications and Live Volumes

A replication source volume or Live Volume primary volume can be restored from a replication destination volume or Live Volume secondary volume. Restoring a volume is necessary when it has been deleted or DR has been activated and data has been written to the activated volume.

Volume Restore Options

The options to restore a volume differ depending on whether DR was activated.

- **Recover from a destination volume that was not activated**: If a source volume no longer exists, Storage Manager restores the data from the destination volume by replicating it back to a newly created source volume. Once the replication is complete, Storage Manager maps the new source volume to a selected server and restarts the replication back from the source system to the destination system.
- **Recover from a destination volume that was activated**: Storage Manager recovers data from the destination volume, including all new writes to the volume after it has been activated, to the original source volume. If the original source volume is no longer there it will be re-created. Once the restore is complete, Storage Manager maps the source volume to the selected server and restarts the replication from the source volume to the destination volume.

NOTE: To restore a volume to an alternate site, consult with technical support (see https://www.dell.com/support).

Volume Restore Limitations

The following limitations apply to the volume restore process.

- Restoring a volume removes replications that use it as a source volume.
- Restoring an original primary Live Volume volume using a managed replication removes the associated Live Volume.

Related concepts

Replicating a Single Volume to Multiple Destinations on page 502
Managed Replications for Live Volumes on page 524

Restoring a Live Volume and a Managed Replication

After a failover of a Live Volume with a Managed Replication, Storage Manager creates a new managed replication for the secondary Live Volume. When the original primary Live Volume system is brought back online and the Live Volume is not restored, there will be two managed replications for the Live Volume. Restoring the Live Volume will delete the managed replications on the original primary Live Volume and keep the Managed Replication on the secondary Live Volume. Swapping the roles of the Live Volume will recreate the managed replication on the original primary Live Volume and delete the Managed Replication on the secondary Live Volume.

Volume Restore Procedures

If DR was activated for multiple replications and/or Live Volumes hosted by a Storage Center pair, the affected volumes can be restored in a single operation. If DR was activated for a single volume, use the corresponding restore point to restore it.

Restore Failed Volumes for Multiple Restore Points

If multiple volumes hosted by a Storage Center pair failed, you can restore them simultaneously.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab, then click **Restore/Restart DR Volumes**. The **Restore/Restart DR Volumes** wizard appears.
3. Select the source/destination Storage Center pair for which you want to restore failed volumes, then click **Next**. The wizard advances to the next page.
4. Read the **Restart Warning** and **Recovery Warning** text, modify any settings that are displayed as necessary, then click **Next**. The wizard advances to the next page.
5. In the **Available Restore Points** pane, select the restore points for which you want to restore volumes, then click **Next**. The wizard advances to the next page.
6. (Optional) Configure replication settings for each restore point.
   a. Select the restore point that you want to modify, then click **Edit Settings**. The **Restore/Restart DR Volumes** dialog box appears.
   b. (Storage Center 6.5 and later, Live Volume only) Choose a recovery method.
      - If the **Recover Live Volume** check box is available, select it to repair the Live Volume by reestablishing connectivity between the original source volume and activated volume. This option must be selected to preserve volume identity. If the Live Volume manages a replication, this option must be selected to preserve the managed replication. When selected, the **New Source Volume Settings** and **Replication Settings** are not available because the existing Live Volume settings are used.
      - If the **Recover Live Volume** check box is not available or not selected, the Live Volume is recreated using the **New Source Volume Settings** and **Replication Settings** you specify. Volume identity is lost, and if the Live Volume manages a replication, the managed replication is removed.
   c. (Replication only) If a source volume is being restored:
      - Select the **Mirror Back Only** check box to skip recreating the replication in the original direction and use the DR site as the source.
      - Select the **Automatically Deactivate Destination** check box to automatically remove server mappings from the activated volume without requiring administrator intervention. This option is available only if DR has been activated for the restore point. If this option is selected, IO to the activated volume should be halted before performing the restore.
   d. Modify the **New Source Volume Settings** as needed. These settings are described in the online help.
   e. Modify the **Replication Settings** as needed. These settings are described in the online help.
   f. When you are finished, click **OK**.
7. When you are done, click **Finish**.
   - Storage Manager restores the replications and/or Live Volumes.
   - Use the **Recovery Progress** tab to monitor the replications and/or Live Volumes.
8. On the **Recovery Progress** tab, when the restore point message displays **Mirror is synced waiting for destination to be deactivated**, halt IO to the destination volumes.
9. Deactivate each destination volume.
   a. Select a restore point and click **Deactivate Destination**. The destination volume is deactivated, the recovered volume is activated and mapped to the configured server, and the replication direction is reversed so that the recovered volume becomes the source.
   b. Repeat the previous step for each destination volume that must be deactivated.

Restore a Failed Volume for a Single Restore Point

If a single volume failed, you can use the corresponding restore point to restore the volume.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab.
3. Right-click the restore point that corresponds to the failed volume, then select **Restore/Restart DR Volumes**. The **Restore/Restart DR Volumes** dialog box appears.
4. (Storage Center 6.5 and later, Live Volume only) Choose a recovery method.
   - If the **Recover Live Volume** check box is available, select it to repair the Live Volume by reestablishing connectivity between the original source volume and activated volume. This option must be selected to preserve volume identity. If the Live Volume manages a replication, this option must be selected to preserve the managed replication. When selected, the **New Source Volume Settings** and **Replication Settings** are not available because the existing Live Volume settings are used
   - If the **Recover Live Volume** check box is not available or not selected, the Live Volume is recreated using the **New Source Volume Settings** and **Replication Settings** you specify. Volume identity is lost, and if the Live Volume manages a replication, the managed replication is removed.
5. (Replication only) If a source volume is being restored:
   - Select the **Mirror Back Only** check box to skip recreating the replication in the original direction and use the DR site as the source.
   - Select the **Automatically Deactivate Destination** check box to automatically remove server mappings from the activated volume without requiring administrator intervention. This option is available only if DR has been activated for the restore point. If this option is selected, IO to the activated volume should be halted before performing the restore.
6. Modify the **New Source Volume Settings** as needed. These settings are described in the online help.
7. Modify the **Replication Settings** as needed. These settings are described in the online help.
8. Click **OK**.
   - Storage Manager restores the replication or Live Volume.
   - Use the **Recovery Progress** tab to monitor the replication or Live Volume.
9. On the **Recovery Progress** tab, when the restore point message displays **Mirror is synced waiting for destination to be deactivated**, halt IO to the destination volume.
10. Deactivate the destination volume by selecting the restore point and clicking **Deactivate Destination**. The destination volume is deactivated, the recovered volume is activated and mapped to the configured server, and the replication direction is reversed so that the recovered volume becomes the source.

Deleting Restore Points

If a replication or Live Volume has been removed or is no longer functioning and you want to remove it permanently, delete the associated restore point.

Prerequisites

The Status for the restore point must be Degraded or Down.

Steps

1. Click the **Replications & Live Volumes** view.
2. Click the **Restore Points** tab.
3. Right-click the restore point, then select **Delete**. A confirmation dialog box appears.
4. Click **OK** to confirm that you want to delete the restore point.

16

Remote Data Collector

A remote Data Collector provides access to Storage Manager disaster recovery options when the primary Data Collector is unavailable.

Topics:

- Remote Data Collector Management
- Remote Data Collector Requirements
- Virtual Appliance Requirements
- Installing and Configuring a Remote Data Collector
- Disconnecting and Reconnecting a Remote Data Collector
- Using a Remote Data Collector to Activate Disaster Recovery
- Enabling Email Notifications for the Remote Data Collector

Remote Data Collector Management

The Storage Manager Client can connect to the primary Data Collector or the remote Data Collector. In the event that the primary Data Collector is unavailable and you need to access Storage Manager disaster recovery options, use the Storage Manager Client to connect to the remote Data Collector.

When a remote Data Collector is installed and connected to the primary Data Collector, additional administrative options are available:

- **Primary Data Collector** – A Storage Manager Client connected to the primary Data Collector displays the remote Data Collector status on the **Remote Data Collector** tab in the **Replications & Live Volumes** view.
- **Remote Data Collector** – A Storage Manager Client connected to the remote Data Collector displays only the **Replications & Live Volumes** view. Configuration actions are limited to disaster recovery preparation and activation, which can be performed on the **Restore Points** tab. The **Primary Data Collector** tab displays status information about the primary Data Collector.

Remote Data Collector Requirements

To use a remote Data Collector, configuration and software requirements must be met.

Configuration Requirements

The following table lists the configuration requirements that must be met to use a remote Data Collector.

Requirement	Description
Primary Data Collector	Before installing and configuring a remote Data Collector, the primary Data Collector must be installed, configured, and started (running). The remote Data Collector connects to the primary Data Collector.
Storage Manager version	The primary Data Collector and remote Data Collector must running the same version of Storage Manager.
Storage Manager username and password	To connect the remote Data Collector to the primary Data Collector, you must provide an existing Storage Manager username and password. **NOTE:** The remote Data Collector does not support Active Directory users.

Requirement	Description
DNS configuration	All managed Storage Centers must be defined in DNS at the local and remote sites. The primary Data Collector host and remote Data Collector host must be defined in DNS to allow the Data Collectors to communicate.

Software Requirements

The software requirements that apply to the primary Data Collector also apply to the remote Data Collector. However, a remote Data Collector uses the file system to store data so there is no database requirement.

Virtual Appliance Requirements

The following table lists the Storage Manager Virtual Appliance requirements:

Table 23. Storage Manager Virtual Appliance Requirements

Component	Requirement
VMware ESXi host version	6.5, 6.7, or 7.0
VMware vCenter Server version	6.5, 6.7, or 7.0
Datastore size	55 GB
CPU	64-bit (x64) microprocessor with two or more cores **NOTE:** The Data Collector requires a microprocessor with four cores for environments that have 100,000 or more Active Directory members or groups.
Memory	Varies based on size of the storage environment: • 4 GB – One to ten Storage Centers, or up to 3000 total volumes • 8 GB – More than ten Storage Centers, or up to 6000 total volumes • 16 GB – More than ten Storage Centers, or up to 12,000 total volumes • 32 GB – More than ten Storage Centers, or more than 12,000 total volumes
Software	• VMware vCenter Server • VMware vSphere High Availability

Installing and Configuring a Remote Data Collector

To install and configure a remote Data Collector at a disaster recovery site, install the Data Collector on a server, and then configure it to connect to the primary Data Collector.

NOTE: To change a remote Data Collector, remove the current remote Data Collector before configuring a new remote Data Collector.

NOTE: For user interface reference information, click **Help**.

Install a Remote Data Collector

Install the Data Collector on a server located at a disaster recovery site.

Prerequisites

- Your site must meet the remote Data Collector configuration requirements.
- The server must meet the Data Collector software and hardware requirements.

Steps

1. Download the Storage Manager Data Collector software.

   The Storage Manager Data Collector is available for download from the Drivers & Downloads tab of the storage system support page located at Dell.com/support.
2. Unzip the software, and double-click the Storage Manager Data Collector Setup file.
   The Storage Manager Data Collector - InstallShield Wizard appears.
3. Select a language from the drop-down menu, and click **OK**.
4. Click **Next**.
   The **License Agreement** page appears.
5. Read the license agreement and click **Yes** to accept it.
6. (Optional) Change the destination folder of Data Collector installation:
   a. Click **Browse**.
   b. Navigate to the folder in which to install the Data Collector.
   c. Click **OK**.
7. Click **Next**.

   The **Data Collector** page is displayed.
8. Select the **Configure as Remote Data Collector** radio button.
   a. Type the host name or IP address of the Primary Data Collector in the **Server** field.
   b. Type the web server service port number of the Primary Data Collector in the **Web Server Service Port** field.
   c. Type the user name of the administrator user on the Primary Data Collector in the **User Name** field.
   d. Type the password of the administrator user on the Primary Data Collector in the **Password** field.
9. Click **Next**.
   The Remote Data Collector connects to the Primary Data Collector, and the **Ports** page is displayed.
10. To specify a different port number for the Web server service, type the port number in the **Enable Web Server Service Port** field.
11. To enable Server Agent services, select the **Enable Server Agent Services Port** checkbox.

    To specify a different port number for the Server Agent services, type the port number in the **Enable Server Agent Services Port** field.
12. Click **Next**.
    The **Summary** page is displayed.
13. Click **Install**.

Installing and Configuring the Storage Manager Virtual Appliance as a Remote Data Collector

Install the Virtual Appliance and configure it as a Remote Data Collector.

Deploy the Virtual Appliance

Deploy the Storage Manager Virtual Appliance on a VMware vCenter server.

Prerequisites

- The VMware ESXi host and VMware vCenter Server must meet the Storage Manager Virtual Appliance requirements in the *Storage Manager 2020 R1 Release Notes*.
- The local computer used to deploy the Virtual Appliance must have the VMware Client Integration plug-in installed.

About this task

The Storage Manager Virtual Appliance is available for download from the Drivers & Downloads tab of the storage system support page located at https://www.dell.com/support.

Steps

1. Download the Storage Manager Virtual Appliance zip file.

The name of the zip file is `DellEMCStorageManagerVA-x.x.x.x.zip`, where *x.x.x.x* is the version number.

2. Extract the Storage Manager Virtual Appliance OVA file from the `DellEMCStorageManagerVA-x.x.x.x.zip` file. The filename of the OVA file is `Storage Manager VA x.x.x.x.ova` , where *x.x.x.x* is the version number.
3. Log on to the VMware vCenter server with the vSphere Web Client.
4. In the right pane, click **Host and Clusters**.
5. Right-click on ESXi and select **Deploy OVF Template**.
   The **Deploy OVF Template** wizard opens.
6. Select the **Local File** radio button.
7. Click **Choose Files** and select the Storage Manager Virtual Appliance .ova template file.
8. Click **Next**.
   The **Select a name and folder** page is displayed.
9. Type a name for the virtual machine in the **Virtual machine name** field and select a location for the Storage Manager Virtual Appliance.
10. Click **Next**.
    The **Select a compute resource** page is displayed.
11. Select a the destination compute resource on which to deploy the Storage Manager Virtual Appliance.
12. Click **Next**.
    The **Review details** page is displayed.
13. Confirm the details for the Storage Manager Virtual Appliance and click **Next**.
    The **License agreements** page is displayed.
14. Select the **I accept all license agreements** checkbox.
15. Click **Next**.
    The **Configuration** page is displayed.
16. Select the size of the Storage Manager Virtual Appliance deployment configuration.

    The configuration options are:
    - **Small** – Use this configuration for deployments of one to ten Storage Centers or up to 3000 total volumes. This deployment requires 2 vCPUs and 8 GB of memory for the vApp.
    - **Medium** – Use this configuration for deployments of more than ten Storage Centers or up to 6000 total volumes. This deployment requires 4 vCPUs and 16 GB of memory for the vApp.
    - **Large** – Use this configuration for deployments of more than ten Storage Centers or up to 12,000 total volumes. This deployment requires 6 vCPUs and 32 GB of memory for the vApp.
    - **Extra Large** – Use this configuration for deployments of more than ten Storage Centers or more 12,000 total volumes. This deployment requires 8 vCPUs and 64 GB of memory for the vApp.
17. Click **Next**.
    The **Select storage** page is displayed.
18. Select **Thin Provision** from the **Select virtual disk format** drop-down menu.
19. Select the datastore in which to store the Storage Manager Virtual Appliance data.
20. Click **Next**.
    The **Select networks** page is displayed.
21. Select a network for the Storage Manager Virtual Appliance from the **Destination Network** drop-down menu.
22. Click **Next**.

    The **Customize template** page is displayed.
    a. Type the hostname for the Storage Manager Virtual Appliance in the **Hostname** field.
    b. If **DHCP** is selected from the **IP Address Type** drop-down menu, skip to the next step.
    c. If **Static** is selected from the **IP Address Type** drop-down menu, type the **IP Address**, **Netmask**, **Default Gateway**, and **DNS** servers for the Virtual Appliance, and click Next.
23. Click **Next**.
    The **Ready to complete** page is displayed.
24. Click **Finish**.
25. (Optional) To change the maximum amount of memory available to the Data Collector on theStorage Manager Virtual Appliance:
    a. Right-click on the Virtual Appliance in the vSphere Web Client and select **Edit Settings**.
       The **Edit Settings** dialog box opens.
    b. Type the maximum amount of memory to allocate for the Virtual Appliance in the **Memory** field.
    c. Click **OK.**

26. Power on the Storage Manager Virtual Appliance after it is deployed.

Results

After a Storage Manager Virtual Appliance is deployed using a static IP address, a different IP address might be displayed in the web console. If this issue occurs, reset the Virtual Appliance to force the correct IP address to be displayed in the web console.

Configure the Virtual Appliance as a Remote Data Collector

Configure the Virtual Appliance as a Remote Data Collector to use it for disaster recovery when the Primary Data Collector is inaccessible.

Prerequisites

The Virtual Appliance must be deployed.

Steps

1. In a web browser, navigate to https://*virtual_appliance_IP_address*/ui/.

   NOTE: Depending on your web browser settings, you may need to acknowledge security alerts to continue.

2. Log in to Storage Manager using the following temporary user:
   - User name: config
   - Password: dell

   The **Getting Started** page of the **Data Collector Initial Setup** wizard is displayed.
3. Click **Next**.
4. Select the **Configure as Remote Data Collector** radio button.
5. Specify the following information about the Primary Data Collector:
   a. Type the hostname or IP address of the Primary Data Collector in the **Server** field.
   b. In the **Web Server Port** field, type the port number of the Primary Data Collector web service.
      The default port is 3033.
   c. Type the user name of the administrator user on the Primary Data Collector in the **User Name** field.
   d. Type the password of the administrator user on the Primary Data Collector in the **Password** field.
   e. Select a time zone for the Primary Data Collector from the **Timezone** drop-down menu.
6. Click **Next**.
   The **Ports** page appears.
7. To change the port number of a service or enable/disable a service:
   a. Select the service to modify and click **Edit**.
      The **Edit Port** dialog box open.
   b. To change the port number of the service, type a different port number in the **Port** field.
   c. To enable or disable the service, select or clear the **Enabled** check box.
   d. Click **OK**.
8. Click **Next**.
   The **Summary** page appears.
9. Verify the information on the **Summary** page.
10. Click **Finish**.
    A confirmation dialog box is displayed.
11. Click **Yes**.
    After the Remote Data Collector setup is complete, the Data Collector restarts, and the login page for Unisphere Central is displayed.

Disconnecting and Reconnecting a Remote Data Collector

Perform these tasks to disconnect or reconnect a remote Data Collector.

NOTE: For user interface reference information, click **Help**.

Temporarily Disconnect a Remote Data Collector

Stop the Data Collector service on the remote Data Collector to temporarily disconnect it from the primary Data Collector.

Steps

1. On the remote Data Collector server:
   a. Open the Data Collector.
   b. On the **General Information** tab, click **Stop** to stop the Data Collector service.
2. Use the Storage Manager Client to connect to the primary Data Collector and log on.
3. Click the **Replications & Live Volumes** view, then click the **Remote Data Collector** tab.

   The **Connection Status** of the remote Data Collector shows **Down** the next time the primary Data Collector attempts to synchronize with the remote Data Collector.

Reconnect a Remote Data Collector to a Storage Center

If the remote Data Collector loses connectivity to a Storage Center, make sure that the remote Data Collector is using the correct host name or IP address for the Storage Center.

Steps

1. Use the Storage Manager Client to connect to the remote Data Collector.
2. On the **Primary Data Collector** tab, locate the down Storage Center, then click **Reconnect to Storage Center**. The **Reconnect to Storage Center** dialog box appears.
3. In the **Remote Data Collector Host or IP Address** field, type the host name or IP address of the Storage Center.
4. Click **OK**.

Remove a Remote Data Collector

Perform the following steps to remove a Remote Data Collector:

About this task

Restart or stop the Remote Data Collector, then remove it from the primary Data Collector.

If you intend to permanently remove the Remote Data Collector, remove the Remote Data Collector from the server.

Steps

1. Connect to the Remote Data Collector.
   a. Open a web browser.
   b. Type the address of the Remote Data Collector in the web browser using the following format:
   https://*remote_data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click **Restart Data Collector**.
5. While the Remote Data Collector is restarting, connect to the Primary Data Collector.
6. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
      https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
      The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
7. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
8. Click **Data Collector**.
   The **Data Collector** view is displayed.
9. Click **Remove Remote Data Collector**. A confirmation dialog box appears.
10. Click **Yes**.

Using a Remote Data Collector to Activate Disaster Recovery

If the primary Data Collector is unavailable, you can perform Storage Manager DR tasks using the remote Data Collector.

NOTE: When activating disaster recovery with a remote Data Collector, create a local Storage Manager user on the remote Data Collector.

Log in to the Remote Data Collector

Use the Storage Manager Client to connect to the remote Data Collector.

About this task

NOTE: Remote Data Collectors do not support Active Directory users.

Steps

1. Start the **Storage Manager Client** application. The Storage Manager Client appears.
2. If the Storage Manager Client welcome screen displays, click **Log in to a Storage Center or Data Collector**.

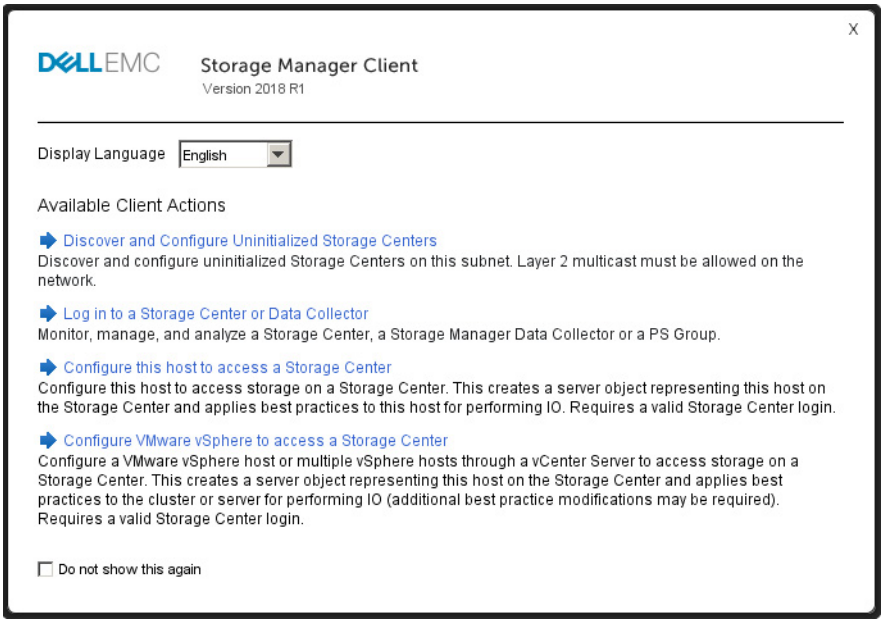


Figure 66. Storage Manager Client Welcome Screen

The login screen appears.

3. Complete the following fields:
   - **User Name** – Type the name of an Storage Manager user.
   - **Password** – Type the password for the user.
   - **Host/IP** – Type the host name or IP address of the server that is hosting the remote Data Collector.
   - **Web Server Port** – If you changed the Web Server Port during installation, type the updated port number.
4. Click **Log In**.

   The Client connects to the remote Data Collector and displays the **Primary Data Collector** tab.

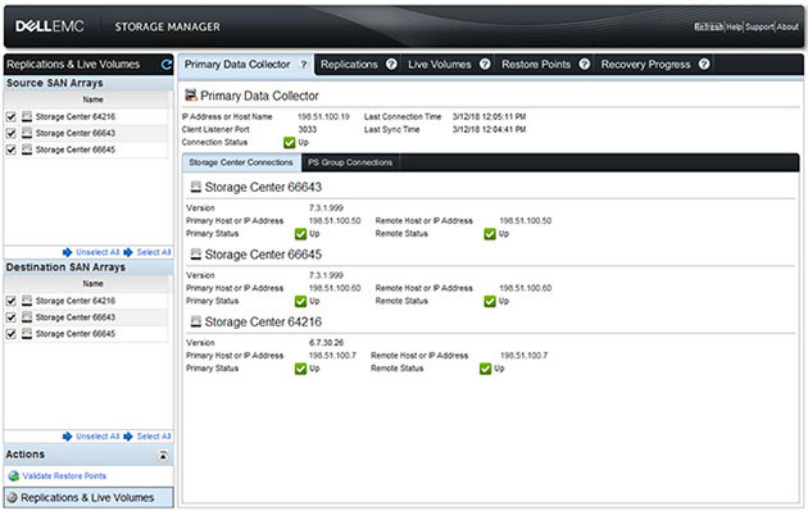


Figure 67. Primary Data Collector Tab

Create a User

Create a user account to allow a person access to Storage Manager.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.
5. Click **+(New User)**.
   The **Create User** dialog box opens.
6. Enter information for the new user.
   a. Type the user name of the user in the **User Name** field.
   b. (Optional) Type the email address of the user in the **Email Address** field.
   c. Select the role to assign to the user from the **Role** drop-down menu.
   d. Select a language from the **Preferred Language** drop-down menu.
   e. Enter a password for the user in the **Password** and **Confirm Password** fields.
   f. To force the user to change the password after the first login, select the **Requires Password Change** checkbox.
7. Click **OK**.

Related concepts

Storage Manager User Privileges on page 651

Use a Remote Data Collector to Prepare for Disaster Recovery

You can use a remote Data Collector to validate restore points and test activate disaster recovery.

Prerequisites

To validate restore points, the primary Data Collector must be down.

Steps

1. Use the Storage Manager Client to connect to the remote Data Collector.
2. Click the **Restore Points** tab.
3. Click one of the following buttons to prepare for disaster recovery:
   - **Validate Restore Points**
   - **Test Activate Disaster Recovery**

Related concepts

Saving and Validating Restore Points on page 542
Test Activating Disaster Recovery on page 544

Use a Remote Data Collector to Test Activate Disaster Recovery

Testing disaster recovery functions the same way for primary and remote Data Collectors.

Steps

1. Use the Storage Manager Client to connect to the remote Data Collector.
2. Click the **Restore Points** tab.
3. Click **Test Activate Disaster Recovery**.

Related concepts

Test Activating Disaster Recovery on page 544

Use a Remote Data Collector to Activate Disaster Recovery

Activating disaster recovery functions the same way for primary and remote Data Collectors.

Steps

1. Use the Storage Manager Client to connect to the remote Data Collector.
2. Click the **Restore Points** tab.
3. Click **Activate Disaster Recovery**.

Related concepts

Activating Disaster Recovery on page 546

Enabling Email Notifications for the Remote Data Collector

You can configure the primary Data Collector to send you an email notification if communication with the remote Data Collector is lost.

Steps

1. Start the Storage Manager Client and log on to the primary Data Collector.
2. In the top pane, click **Edit User Settings**. The **Edit User Settings** dialog box appears.
3. On the **General** tab, make sure your email address is entered in the **Email Address** field.
4. Click the **Manage Events** tab.
5. In the table, select the **Remote Data Collector Down** check box.
6. Click **OK**.

17

Storage Replication Adapter for VMware SRM

VMware vCenter Site Recovery Manager (SRM) supports storage vendors using Storage Replication Adapters. The Dell Storage Replication Adapter (SRA) allows sites to use the VMware vCenter SRM on Storage Centers managed by the Storage Manager software.

Topics:

- Where to Find Dell SRA Deployment Instructions
- Dell SRA for Windows Limitations
- Dell SRA Requirements for VMware SRM
- VMware SRM and Storage Manager Prerequisites
- Dell SRA with Stretched Storage and vMotion
- Storage Manager SRA Configurations

Where to Find Dell SRA Deployment Instructions

This chapter provides overview information about using SRM on Storage Centers through Storage Manager and the Dell Storage Replication Adapter (SRA). For complete information on installing and configuring VMware vCenter Site Recovery Manager, including downloading and installing Storage Replication Adapters, refer to the SRM documentation provided by VMware.

Before installing the Dell SRA, check the SRA readme file for the most current information regarding the installation and configuration process.

Dell SRA for Windows Limitations

The Dell SRA for Windows has the following limitations:

An HBA rescan timeout might occur when a recovery operation is triggered for multiple recovery plans simultaneously. The workaround for the issue is to either retry the SRM workflow after the background HBA rescan operation completes, or increase the default timeout for the storageProvider.hostRescanTimeoutSec setting.

The following features are not supported by the Dell SRA for Windows:

- Storage Center consistent Snapshot Profiles

  NOTE: Consistent Snapshot Profiles can be used to create consistent snapshots, but the Dell SRA does not guarantee that SRM activates asynchronously replicated snapshots that are consistent with each other.
- VMware Consistency Groups

Dell SRA Requirements for VMware SRM

The following table lists the requirements for using the Dell SRA with VMware SRM.

Component	Version Requirements
Dell SRA for Windows	Version 18.1.1.173
Dell SRA for Photon-based SRM	Version 20.1.1.13
VMware vCenter Site Recovery Manager (SRM) for Windows	Version 8.1, 8.1.1, 8.2, 8.3

Component	Version Requirements
VMware vCenter for Photon-based SRM	Version 8.2 and 8.3
Microsoft .NET Framework	Version 4.5 installed on the SRM server

VMware SRM and Storage Manager Prerequisites

To use the Dell SRA with VMware vCenter Site Recovery Manager, the following configuration requirements must be met.

Requirement	Description
Data Collector Deployment	A Storage Manager Data Collector must be visible to all Storage Centers within the SRM configuration. Three options are available: • Install and configure the Storage Manager Data Collector on the recovery SRM site only. • Install and configure Storage Manager Primary Data Collector on the protected site; install and configure Storage Manager Remote Data Collector on the recovery site. • Install and configure Storage Manager Primary Data Collector on the recovery site; install and configure Storage Manager Remote Data Collector on the protected site.
Storage Center Configuration	• VMware vSphere server objects must be created on both the source and destination Storage Centers. • Replication QoS Nodes must be defined on the source and destination Storage Centers.
Storage Manager Users	Three users are required: • **To install SRM** – A Storage Manager user that can access all Storage Centers at the protected and recovery sites. • **To manage the protected site with SRM** – A Storage Manager user that can access only the Storage Centers at the protected site. • **To manage the recovery site with SRM** – A Storage Manager user that can access only the Storage Centers at the recovery site.
Communication between Storage Manager and SRM	The firewall (if any) between SRM and Storage Manager must allow SOAP over HTTP on TCP port 3033.
Replications	• Using Storage Manager, create replications or Live Volumes from the protected site to the recovery site. • Source and destination volumes must not be replicating anywhere else. • Restore points for replications must be validated and saved.
Restore Points	Restore points are not available to VMware vCenter SRM until they have been saved. Using Storage Manager, save restore points for the replications. If you are using Data Collectors on both the recovery and protected sites, you must save restore points on both sites.

Dell SRA with Stretched Storage and vMotion

SupportedDell SRAs include support for Stretched Storage with VMware Sitre Recovery Manager (SRM). Stretched Storage allows SRM to manage Storage Center Live Volume replications. vMotion, when used with stretched storage, allows virtual machines to migrate to another host without downtime.

To enable vMotion on Storage Center Live Volumes managed with SRM perform the following tasks:

- Enable vMotion on ESXi hosts
- Configure vCenter servers in enhanced linked mode

Storage Manager SRA Configurations

This section presents two supported configurations for using VMware Site Recovery Manager with Storage Manager: using a primary Data Collector only, or using a primary Data Collector and a remote Data Collector.

NOTE: For information on setting up Stretched Storage for Live Volumes, see VMware documentation for configuring Stretched Storage.

Primary Data Collector Only Configuration

In the following figure, the Protected and the Recovery sites are connected by a single Storage Manager Primary Data Collector.

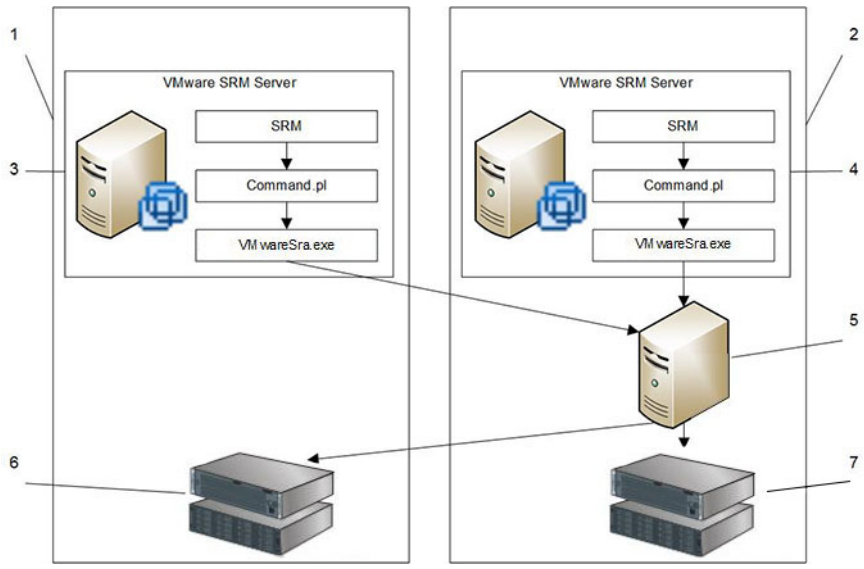


Figure 68. SRA Configuration with a Single Data Collector

1. Protected site
2. Recovery site
3. VMware SRM server at protected site
4. VMware SRM server at recovery site
5. Primary Data Collector at recovery site
6. Storage Center at protected site
7. Storage Center at recovery site

In a configuration with only one Storage Manager Data Collector, locate the Data Collector at the Recovery Site.

Remote Data Collector Configuration

In the following configuration, the Protected Site is connected to a Storage Manager Primary Data Collector; the Recovery Site is connected to a Storage Manager Remote Data Collector.

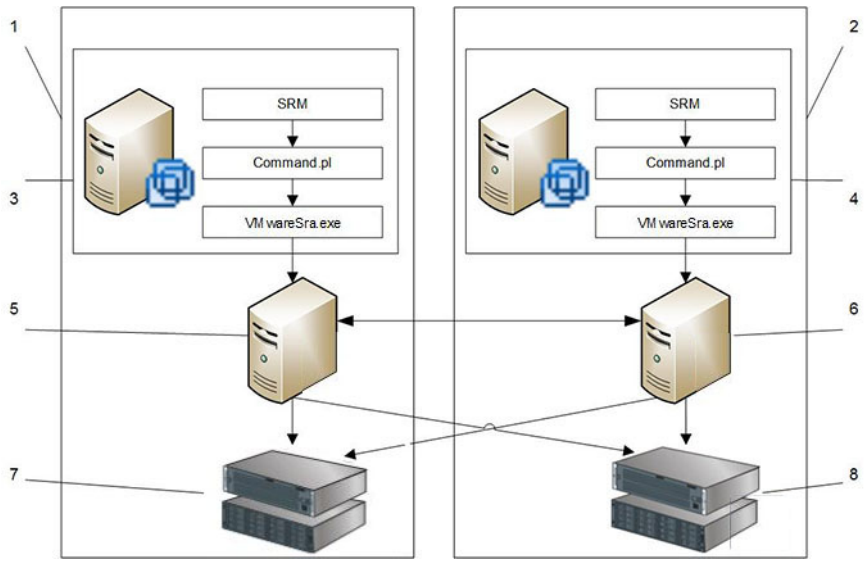


Figure 69. SRA Configuration with a Primary and Remote Data Collector

1. Protected site
2. Recovery site
3. VMware SRM server at protected site
4. VMware SRM server at recovery site
5. Primary Data Collector at protected site
6. Remote Data Collector at recovery site
7. Storage Center at protected site
8. Storage Center at recovery site

In a configuration with a Storage Manager Remote Data Collector, locate the Remote Data Collector on the Recovery Site. This configuration allows DR activation from the remote site when the Protected Site goes down. By design, the Storage Manager Remote Data Collector is connected to the same Storage Centers as the Storage Manager Primary Data Collector.

18

Threshold Alerts

Threshold alerts are automatically generated when user-defined threshold definitions for storage object usage are crossed. Threshold queries allow you to query historical data based on threshold criteria.

Topics:

- Configuring Threshold Definitions
- Viewing and Deleting Threshold Alerts
- Configuring Volume Advisor Movement Recommendations
- Export Threshold Alerts
- Configuring Email Notifications for Threshold Alerts
- Performing Threshold Queries

Configuring Threshold Definitions

Threshold definitions monitor the usage metrics of storage objects and generate alerts if the user-defined thresholds are crossed.

The types of usage metrics that can be monitored are I/O usage, storage, and replication. Storage Manager collects the usage metric data from managed Storage Centers. By default, Storage Manager collects I/O usage and replication metric data every 15 minutes and storage usage metric data daily at 12 AM. Storage objects on the Storage Centers are assigned to threshold definitions and each threshold definition contains one or more threshold values. When the value of a monitored metric reaches a threshold value, an alert occurs. If an SMTP server is configured on the Data Collector, Storage Manager sends an email with the threshold alert. It sends only one email alert every 24 hours.

NOTE: Storage Manager sends only one email per alert occurrence. If after 24 hours the metric is still at or above the threshold alert value, an alert email is not sent. The metric must fall below the threshold value and then exceed the threshold again to generate an alert email.

Perform the tasks in the following sections to set up and view threshold definitions:

- Setting Up Threshold Definitions on page 569
- Assigning Storage Objects to Threshold Definitions on page 572
- Assigning Threshold Definitions to Storage Objects on page 573

Setting Up Threshold Definitions

You can create, view, edit, and delete threshold definitions.

Create a Threshold Definition

Create a threshold definition to monitor IO usage, storage, or replications.

Prerequisites

To receive email notifications for threshold alerts, the following settings must be configured:

- SMTP server settings for the Data Collector
- Email address for your user account
- Notification settings for your user account

About this task

Storage Manager generates threshold alerts after Storage Usage checks usage metrics and notices a threshold definition has been exceeded. Storage Usage runs daily at 12 AM by default.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Click **Create Threshold Definition**. The **Create Threshold Definition** dialog box opens.
4. Enter a name for the threshold definition in the **Name** field.
5. Select the type of threshold definition to create from the **Type** drop-down menu.
   - **IO Usage**: Read and write IO performance.
   - **Storage**: Use and growth of storage.
   - **Replication**: Status of replications.
6. Select the type of storage object to assign to the threshold definition from the **Alert Object Type** drop-down menu.
7. Select the type of usage metric to monitor from the **Alert Definition** drop-down menu.
8. (Optional) To assign the threshold definition to all of the storage objects that are of the type specified in the **Alert Object Type**, select the **All Objects** check box.
   The **All Objects** setting cannot be modified after the threshold definition is created.
9. Specify the alert notification settings for the Error, Warning, and Inform thresholds:
   - **Error Settings**: Enter the threshold value that the usage metric must exceed to trigger an Error threshold alert. To email Error threshold alerts to the Storage Manager administrators, select the **Email** check box. Then enter the number of concurrent events that must occur to trigger an alert email.
   - **Warning Setting**: Enter the threshold value that the usage metric must exceed to trigger a Warning threshold alert. To email Warning threshold alerts to the Storage Manager administrators, select the **Email** check box. Then enter the number of concurrent events that must occur to trigger an alert email.
   - **Inform Settings**: Enter the threshold value that the usage metric must exceed to trigger an Inform threshold alert. To email Inform threshold alerts to the Storage Manager administrators, select the **Email** check box. Then enter the number of concurrent events that must occur to trigger an alert email.

     NOTE: Storage Manager sends only one threshold alert email for every 24-hour period. The number of threshold alert emails per 24-hour period cannot be configured. In addition, if the metric remains at or above the threshold alert value, a second alert email is not sent. The metric must fall below the threshold value and then exceed the threshold again to generate an alert email.
10. (Optional) To configure the threshold definition to generate Volume Advisor recommendations to move one or more volumes to a different Storage Center, select the **Recommend Storage Center** check box.
    - Recommendations are generated when the error threshold is exceeded.
    - The **Recommend Storage Center** checkbox is available only for threshold definitions that support Volume Advisor.
11. To specify the time that Storage Manager monitors the threshold definition:
    a. Select the **Time Constraint** check box.
    b. Specify the start of the time period in the **Start Time** field.
    c. Specify the end of the time period in the **End Time** field.
12. To specify which days of the week that Storage Manager monitors the threshold definition:
    a. Select the **Day Constraint** check box.
    b. Select the check boxes of the days of the week to monitor the threshold definition.
    c. Clear the check boxes of the days of the week to not monitor the threshold definition.
13. Select the storage objects to assign to the threshold definition in the **Add Objects** dialog box. Additional objects can be added to a threshold definition after it is created.
14. Click **Finish**.

Related concepts

Assigning Storage Objects to Threshold Definitions on page 572
Configuring Email Notifications for Threshold Alerts on page 583
Configuring Volume Advisor Movement Recommendations on page 576

View an Existing Threshold Definition

Select a threshold definition on the **Definitions** tab to view assigned objects, current threshold alerts, and historical threshold alerts.

Steps

1. Click **Threshold Alerts** in the view pane to display the **Threshold Alerts** window.
2. Click the **Definitions** tab.
3. Select the threshold definition to view.
   The threshold definition is displayed in the bottom pane of the **Definitions** tab.

   The following tabs are also displayed in the bottom pane of the **Definitions** tab:

   - **Assigned Objects** – Displays the storage objects assigned to the selected threshold definition.
   - **Current Threshold Alerts** – Displays the threshold alerts that are active for the selected threshold definition.
   - **Historical Threshold Alerts** – Displays recent threshold alerts that are no longer active for the selected threshold definition.

Edit an Existing Threshold Definition

Edit a threshold definition to change the name, notification settings, or schedule settings.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Select the threshold definition to edit and click **Edit Settings** in the bottom pane.
   The **Edit Threshold Definition** dialog box opens.
4. To change the name of the threshold definition, enter a new name in the **Name** field.
5. To change the threshold value and email notification settings for the Error threshold alert, enter new values in the **Error Settings** fields.
6. To change the threshold value and email notification settings for the Warning threshold alert, enter new values in the **Warning Settings** fields.
7. To change the threshold value and email notification settings for the Info threshold alert, enter new values in the **Inform Settings** fields.
8. To change the period of time that Storage Manager monitors the threshold definition
   - Select or clear the **Time Constraint** check box to enable or disable the time constraint.
   - If the **Time Constraint** check box is selected, specify the start of the time period in the **Start Time** field and specify the end of the time period in the **End Time** field.
9. To change the days of the week that Storage Manager monitors the threshold definition:
   - Select or clear the **Day Constraint** check box to enable or disable the days of the week constraint.
   - If the **Day Constraint** check box is selected, select the check boxes of the days of the week to monitor the threshold definition and clear the check boxes of the days of the week to not monitor the threshold definition.
10. Click **OK**.

Delete a Threshold Definition

If you no longer need a threshold definition, you can delete it.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Select the threshold definition to remove and click **Delete** in the bottom pane.
   The **Delete Threshold Alert Definitions** dialog box opens.
4. Click **OK**.

Delete Multiple Threshold Definitions

If you no longer need multiple threshold definitions, you can delete them.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Use Shift+click or Control+click to select the threshold definitions to remove.
4. Click **Delete** in the bottom pane.
   The **Delete Threshold Alert Definitions** dialog box opens.
5. Click **OK**.

Assigning Storage Objects to Threshold Definitions

You can add or remove the storage objects that are monitored by threshold definitions.

Assign Storage Objects to a Threshold Definition

Add storage objects to a threshold definition to monitor the storage objects.

About this task

Storage objects cannot be added to a threshold definition that has the **All Objects** checkbox selected.

Steps

1. Click **Threshold Alerts** in the view pane to display the **Threshold Alerts** window.
2. Click the **Definitions** tab.
3. Select the threshold definition to which to assign storage objects.
4. Click **Add Objects** in the bottom pane.
   The **Add Objects** dialog box opens.
5. Select the storage objects to assign to the threshold definition.
6. Click **Finish**.

Unassign Storage Objects from a Threshold Definition

Remove storage objects from a threshold definition to stop monitoring the storage objects.

About this task

Storage objects cannot be removed from a threshold definition that has the **All Objects** check box selected.

Steps

1. Click **Threshold Alerts** in the view pane to display the **Threshold Alerts** window.
2. Click the **Definitions** tab.
3. Select the threshold definition from which you want to remove storage objects.
4. Click **Remove Objects**.
   The **Remove Objects** dialog box opens.
5. Select check boxes of the storage objects to remove from the threshold definition.
6. Click **OK**.

Assigning Threshold Definitions to Storage Objects

You can assign threshold definitions to storage objects that are accessible from **Storage** view.

View the Threshold Definitions Assigned to a Storage Object or Storage Center

View the threshold definitions assigned to a storage object or Storage Center in the Threshold Alerts tab.

Steps

1. Click the **Storage** view.
2. Select a Storage Center in the **Storage** pane.
3. Click the **Storage** tab.
4. To display the threshold definitions assigned to a storage object, select one of the following:
   - **Volumes** – Select the volume for which to display the assigned threshold definitions, and click the **Threshold Alerts** tab in the right pane.
   - **Servers** – Select the server for which to display the assigned threshold definitions, and click the **Threshold Alerts** tab in the right pane.
   - **Remote Storage Centers** – Select the remote Storage Center for which to display the assigned threshold definitions, and click the **Threshold Alerts** tab in the right pane.
   - **Disks** – Select the disk for which to display the assigned threshold definitions, and click the **Threshold Alerts** tab in the right pane.
   - **Storage Profiles** – Select the storage profile for which to display the assigned threshold definitions, and click the **Threshold Alerts** tab in the right pane.
5. To display the threshold definitions assigned to the Storage Center, select the Storage Center node and click the **Threshold Alerts** tab in the right pane.

Assign a Threshold Definition to a Storage Object

Select a storage object and then click the **Set Threshold Alert Definitions** to assign a threshold definition.

Steps

1. Click the **Storage** view.
2. Select a Storage Center in the **Storage** pane.
3. Click the **Summary**, **Storage**, **IO Usage**, or **Charting** tab.
4. To display the threshold definitions assigned to the Storage Center, skip to the next step.

   To display the threshold definitions assigned to a storage object, select one of the following:

   - **Volumes**: Select the volume for which to display the assigned threshold definitions.
   - **Servers**: Select the server for which to display the assigned threshold definitions.
   - **Remote Storage Centers**: Select the remote Storage Center for which to display the assigned threshold definitions.
   - **Disks**: Select the disk for which to display the assigned threshold definitions.
   - **Storage Profiles**: Select the storage profile for which to display the assigned threshold definitions.
5. In the right pane, click **Set Threshold Alert Definitions**. The **Set Threshold Alert Definitions** dialog box appears.
6. In the top pane, select storage object usage metric to which to assign a threshold definition.
7. In the bottom pane, select the threshold definition to assign to the usage metric.
8. Click **OK**.

Related tasks

Setting Up Threshold Definitions on page 569

Assign a Threshold Definition to a Controller or a Storage Center

Select a controller or a Storage Center, then click the **Set Threshold Alert Definitions** to assign a threshold definition.

Steps

1. Click the **Storage** view.
2. Select a Storage Center in the **Storage** pane.
3. Click the **Hardware** tab.
4. To display the threshold definitions assigned to the Storage Center, skip to the next step.

   To display the threshold definitions assigned to a storage object, select one of the following nodes in the **Hardware** tab navigation pane:

   - **Storage Center name**: Select the Storage Center for which to display the assigned threshold definitions.
   - **Controller name**: Select the controller for which to display the assigned threshold definitions.
5. In the right pane, click **Set Threshold Alert Definitions**. The **Set Threshold Alert Definitions** dialog box appears.
6. Select alert definition to which to assign a threshold definition.

   The threshold definitions that appear in the **Available Alert Definitions** pane depend on the type of alert definition selected.

   If a threshold definition for the selected alert definition does not exist, create a threshold definition by clicking **Create Threshold Definition**.
7. Select the threshold definition to assign to the alert definition .
8. Click **OK**.

Related tasks

Setting Up Threshold Definitions on page 569

Viewing Threshold Alerts for Threshold Definitions

Use the **Definitions** tab to view the current threshold alerts and historical threshold alerts for a threshold definition.

View the Current Threshold Alerts for a Threshold Definition

When a threshold definition is selected on the **Definitions** tab, the **Current Threshold Alerts** subtab displays the active alerts for the definition.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Select the threshold definition to view. The threshold definition appears in the bottom pane of the **Definitions** tab.
4. Click the **Current Threshold Alerts** tab, in the bottom pane, to display active threshold alerts for the selected threshold definition.

View the Historical Threshold Alerts for a Threshold Definition

When a threshold definition is selected on the **Definitions** tab, the **Historical Threshold Alerts** subtab displays the past alerts for the definition.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Select the threshold definition to display. The threshold definition appears in the bottom pane of the **Definitions** tab.

4. Click the **Historical Threshold Alerts** tab, in the bottom pane, to display past threshold alerts for the selected threshold definition.

Viewing and Deleting Threshold Alerts

The current and historical threshold alerts for the managed Storage Centers are displayed on the **Alerts** tab.

The alerts are updated when the Storage Report report-gathering tasks are run. By default, IO Usage and Replication report gathering is performed every 15 minutes and Storage report gathering is performed daily at midnight.

Related tasks

Configure the Storage Center Data Gathering Schedule on page 318

View Current and Historical Threshold Alerts

The **Alerts** tab displays the threshold alerts that are currently active and the historical threshold alerts that are no longer active.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Alerts** tab.
   - The **Active Alerts** tab displays all of the threshold alerts that are currently active for the selected Storage Centers.
   - The **Historical Alerts** tab displays threshold alerts that are no longer active for the selected Storage Centers.
   - The **Current Threshold Alerts** pane displays all of the threshold alerts that are currently active for the selected Storage Centers.
   - The **Historical Threshold Alerts** pane displays threshold alerts that are no longer active for the selected Storage Centers.

Filter Threshold Alerts by Storage Center

By default, alerts are displayed for all managed Storage Centers.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Alerts** tab.
3. Use the **Filters** pane to filter threshold alerts by Storage Center.
   - To hide threshold alerts for a single Storage Center, clear the checkbox for the Storage Center.
   - To display threshold alerts for a Storage Center that is deselected, select the checkbox for the Storage Center.
   - To hide threshold alerts for all of the Storage Centers, clear the **Storage Centers** checkbox.
   - To display threshold alerts for all of the Storage Centers, select the **Storage Centers** check box.
4. Use the **Storage Centers** pane to filter threshold alerts by Storage Center.
   - To hide threshold alerts for a single Storage Center, clear the checkbox for the Storage Center.
   - To display threshold alerts for a Storage Center that is deselected, select the checkbox for the Storage Center.
   - To hide threshold alerts for all of the Storage Centers, click **Unselect All**.
   - To display threshold alerts for all of the Storage Centers, click **Select All**.

Filter Threshold Alerts by Threshold Definition Properties

You can filter the threshold alerts based on the properties of the threshold definitions that triggered the alerts.

Steps

1. Click the **Threshold Alerts** view.

2. Click the **Alerts** tab.
3. Use the **Filter** pane to filter threshold alerts by threshold definition properties.
   - To filter the displayed threshold alerts by type (IO Usage, Storage, or Replication) select the **Filter Type** check box, and then select the type from the drop-down menu.
   - If the **Filter Type** check box is selected, the **Filter Alert Object Type** check box can be selected to filter threshold alerts by the type of storage object selected from the drop-down menu.
   - If the **Filter Alert Object Type** check box is selected, the **Filter Definition Type** check box can be selected to filter threshold alerts by the usage metric selected from the drop-down menu.

View the Threshold Definition that Generated an Alert

If you want to view the threshold definition that generated an alert in detail, you can go to the definition directly from the alert.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Alerts** tab.
3. Right-click on a current or historical threshold alert and select **Go to Definition**.
   The **Threshold Definition** window appears and the threshold definition that triggered the alert is highlighted.

Delete Historical Threshold Alerts

If a historical alert is no longer needed, you can delete it.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Alerts** tab.
3. Select the historical alerts to delete from the **Historical Alerts** subtab.
4. Select the historical alerts to delete from the **Historical Threshold Alerts** pane.
5. Right-click on the selected alerts and select **Delete**.
   The **Delete Alerts** dialog box opens.
6. Click **OK**.

Configuring Volume Advisor Movement Recommendations

Volume Advisor can recommend moving a volume to a different Storage Center to improve performance and/or alleviate high storage usage for a Storage Center. Volume Advisor is configured using threshold definitions, which generate recommendations along with threshold alerts when error thresholds are exceeded. Volume movement recommendations are calculated based on the current capacity and past performance of the available Storage Centers.

Threshold Definitions That Support Volume Advisor

Four types of threshold definitions can trigger an alert and a recommendation to move one or more volumes.

Supported Threshold Definitions			Threshold Alert Recommendation
Type	**Alert Object Type**	**Alert Definition**	
IO Usage	Storage Center	FE IO/Sec	When front-end IO for a Storage Center exceeds the configured error threshold, the alert recommends moving volumes to a specific Storage Center.

Supported Threshold Definitions			Threshold Alert Recommendation
Type	**Alert Object Type**	**Alert Definition**	
IO Usage	Volume	Latency	When latency for a volume exceeds the configured error threshold, the alert recommends moving the volume to a specific Storage Center, and gives you the option to act on the recommendation by creating a Live Volume.
IO Usage	Controller	CPU Usage	When CPU usage for a Storage Center controller exceeds the configured alert threshold, the alert recommends moving volumes to a specific Storage Center.
Storage	Storage Center	Percent Used	When the used space percentage for a Storage Center exceeds the configured alert threshold, the alert recommends moving the volume to a specific Storage Center.

General Volume Advisor Requirements

Storage Centers must meet the following requirements to be considered for volume movement recommendations.

Requirement	Description
Management	The Storage Center must be added to Storage Manager. **NOTE:** Storage Centers that are not mapped to your user account are not presented as recommendations, but might be presented as recommendations to other users.
Licensing	(Storage Center 7.0 and below) The Storage Center must be licensed for Live Volume.
Storage Center version	The Storage Center must be running the same version (*x.y*) as the original Storage Center.
Tier 1 disk type	The Storage Center must have the same Tier 1 disk type as the original Storage Center, such as a 7.2K, 10K, 15K, or Solid State Disk (SSD).

Additional Requirements for the Volume Latency Threshold Definition

The original volume and candidate Storage Centers must meet the following additional requirements to be considered for volume movement recommendations triggered by the volume latency threshold definition.

Requirement	Description
Original volume configuration	• The volume cannot be part of a replication, Live Volume, or Live Migrate. • The volume cannot be associated with a consistent Snapshot Profile.
Candidate Storage Center configuration	• The Storage Center must have a server object that matches the server to which the original volume is mapped. • The Storage Center must be less than 80% full when including the size of the volume to be moved. • The combined original volume IO/sec and Storage Center front end IO/sec must be below a predefined threshold.

Types of Volume Movement Recommendations

There are two types of recommendations: those that are triggered by volume latency threshold definitions, and those that are not. Both recommend moving one or more volumes to a different Storage Center, but volume latency recommendations provide more detail and include an option to automatically act on the recommendation.

Both types of recommendations can be viewed from the current threshold alerts that contain them. On the Alerts tab of the Threshold Alerts view, current threshold alerts that contain recommendations display Yes in the Recommend column.

To view the recommendation contained by a current threshold alert, right-click the alert and select **Recommend Storage Center** to open the **Recommend Storage Center** dialog box.

Recommendations Based on Volume Latency

If the recommendation was triggered by a threshold definition that monitors volume latency, the **Recommend Storage Center** dialog box displays a recommendation to move a specific volume to a specific Storage Center.

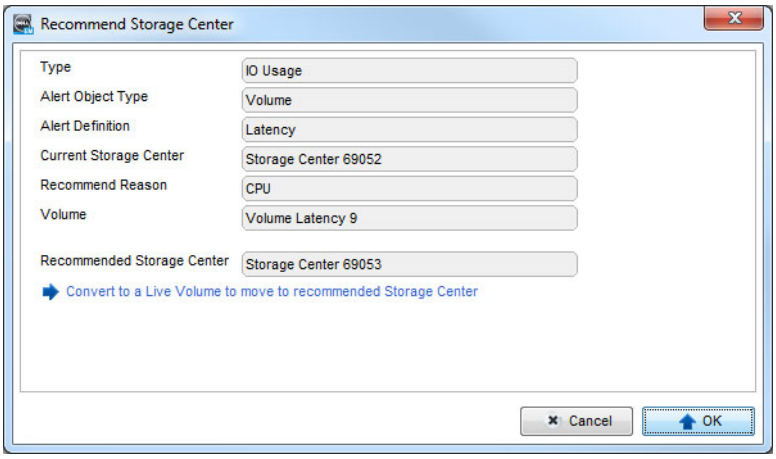


Figure 70. Recommended Storage Center Dialog Box

If Storage Manager identified a possible reason for the increased volume latency, the reason is displayed in the **Recommend Reason** field. Once the **Recommend Reason** is calculated, it is not updated for a 24-hour period. If you view the recommendation after 24 hours have elapsed, the reason is recalculated. If Storage Manager is unable to determine a reason, no reason is provided.

The following reasons can be displayed:

- **CPU**- Indicates that CPU usage for the controller that hosts the volume is high.
- **IO Count**: Indicates that IO for the Storage Center that hosts the volume is high.
- **Disk Latency**: The disks that provide storage for the volume are experiencing high latency.
- **Tier 1 Space**: Tier 1 storage space is full or nearly full for the Storage Center that hosts the volume.

The **Convert to a Live Volume to move to recommended Storage Center** or **Live Migrate the volume to the recommended Storage Center** link opens a dialog box that allows you to move the volume automatically to the recommended Storage Center by converting it to a Live Volume or creating a Live Migration.

Recommendations Based on Other Thresholds

If the recommendation was triggered by a threshold definition that monitors Storage Center front-end IO, Storage Center controller CPU usage, or the percentage of storage used for a Storage Center, the **Recommend Storage Center** dialog box displays a recommended Storage Center without suggesting specific volumes to move or populating the **Recommended Reason** field.

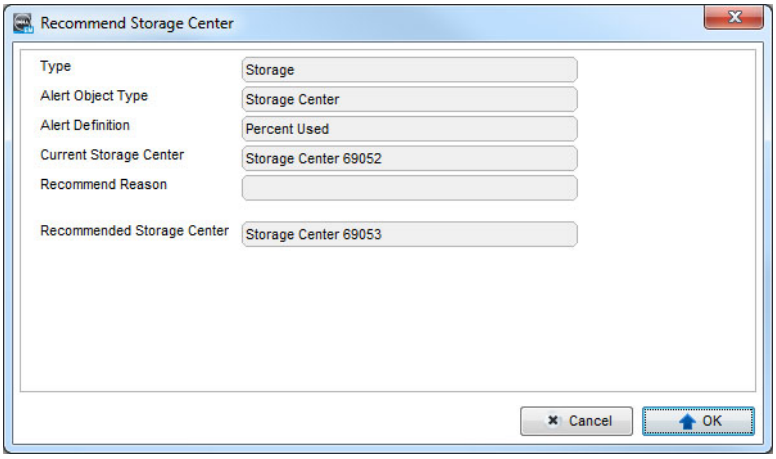


Figure 71. Recommended Storage Center Dialog Box

Creating Threshold Definitions to Recommend Volume Movement

Create a threshold definition to recommend volume movement based on the rate of Storage Center front-end IO, volume latency, Storage Center controller CPU usage, or percentage of storage used for a Storage Center.

Create a Threshold Definition to Monitor Front-End IO for a Storage Center

When Storage Center front-end IO exceeds the value set for the error threshold, Storage Manager triggers a threshold alert with a volume movement recommendation.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Click **Create Threshold Definition**. The **Create Threshold Definition** dialog box appears.
4. In the **Name** field, type a name for the threshold definition.
5. Configure the threshold definition to monitor Storage Center front-end IO.
   a. From the **Type** drop-down menu, select **IO Usage**.
   b. From the **Alert Object Type** drop-down menu, select **Storage Center**.
   c. From the **Alert Definition** drop-down menu, select **FE IO/Sec**.
6. (Optional) Select the **All Objects** check box to apply the threshold definition to all Storage Centers
7. Configure the IO/sec value that must be exceeded to trigger an error threshold alert with a volume movement recommendation.
   a. In the **Error Setting** field, type the rate of IO/sec that must be exceeded.
   b. Next to the **Error Setting** field, in the **Iterations before email** field, type the number of times the threshold must be exceeded to trigger the alert.
8. Select the **Recommend Storage Center** check box.
9. Configure the other options as needed. These options are described in the online help.
10. When you are finished, click **OK**.
    - If you selected the **All Objects** check box, the threshold definition is created and the **Create Threshold Definition** dialog box closes.
    - If you did not select the **All Objects** check box, the **Add Objects** dialog box appears.
11. Select the check box for each Storage Center that you want to monitor with the threshold definition, then click **Finish**. The **Create Threshold Definition** dialog box closes.

Create a Threshold Definition to Monitor Latency for a Volume

When latency for a volume exceeds the value set for the error threshold, Storage Manager triggers a threshold alert with a volume movement recommendation.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Click **Create Threshold Definition**. The **Create Threshold Definition** dialog box appears.
4. In the **Name** field, type a name for the threshold definition.
5. Configure the threshold definition to monitor volume latency.
   a. From the **Type** drop-down menu, select **IO Usage**.
   b. From the **Alert Object Type** drop-down menu, select **Volume**.
   c. From the **Alert Definition** drop-down menu, select **Latency**.
6. (Optional) Select the **All Objects** check box to apply the threshold definition to all volumes.
7. Configure the volume latency value that must be exceeded to trigger a threshold alert with a volume movement recommendation.
   a. In the **Error Setting** field, type the volume latency that must be exceeded.

b. Next to the **Error Setting** field, in the **Iterations before email** field, type the number of times the threshold must be exceeded to trigger the alert.

8. Select the **Recommend Storage Center** check box.
9. Configure the other options as needed. These options are described in the online help.
10. When you are finished, click **OK**.
    - If you selected the **All Objects** check box, the threshold definition is created and the **Create Threshold Definition** dialog box closes.
    - If you did not select the **All Objects** check box, the **Add Objects** dialog box appears.
11. Choose the volumes that you want to monitor.
    a. In the table, select the Storage Center that hosts the volumes.
    b. Below the table, choose a method to select volumes:
        - To apply the threshold definition to all volumes on a Storage Center, select **All Volumes on Storage Center**, then click **Finish**. The threshold definition is added and the **Create Threshold Definition** dialog box closes.
        - To apply the threshold definition to all volumes in a volume folder, select **All Volumes in Folder/Container**, then click **Next**. The wizard advances to the next page and displays a table of volume folders.
        - To apply the threshold definition to individual volumes on a Storage Center, select **Select Volumes**, then click **Next**. The wizard advances to the next page and displays a table of volumes.
    c. Select the check box for each volume or volume folder that you want to monitor with the threshold definition, then click **Finish**. The threshold definition is added and the **Create Threshold Definition** dialog box closes.

Create a Threshold Definition to Monitor CPU Usage for a Controller

When the CPU usage percentage for a Storage Center controller exceeds the value set for the error threshold, Storage Manager triggers a threshold alert with a volume movement recommendation.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Click **Create Threshold Definition**. The **Create Threshold Definition** dialog box appears.
4. In the **Name** field, type a name for the threshold definition.
5. Configure the threshold definition to monitor Storage Center controller CPU usage.
    a. From the **Type** drop-down menu, select **IO Usage**.
    b. From the **Alert Object Type** drop-down menu, select **Controller**.
    c. From the **Alert Definition** drop-down menu, select **CPU Usage**.
6. (Optional) Select the **All Objects** check box to apply the threshold definition to all Storage Center controllers.
7. Configure the Storage Center controller CPU usage percentage that must be exceeded to trigger an error threshold alert with a volume movement recommendation.
    a. In the **Error Setting** field, type the CPU usage percentage that must be exceeded.
    b. Next to the **Error Setting** field, in the **Iterations before email** field, type the number of times the threshold must be exceeded to trigger the alert.
8. Select the **Recommend Storage Center** check box.
9. Configure the other options as needed. These options are described in the online help.
10. When you are finished, click **OK**.
    - If you selected the **All Objects** check box, the threshold definition is created and the **Create Threshold Definition** dialog box closes.
    - If you did not select the **All Objects** check box, the **Add Objects** dialog box appears.
11. Choose the Storage Center controllers that you want to monitor.
    a. In the table, select the Storage Center to which the controllers belong.
    b. Below the table, choose a method to select controllers:
        - To apply the threshold definition to all controllers in a Storage Center, select **All Controllers on Storage Center**, then click **Finish**. The threshold definition is added and the **Create Threshold Definition** dialog box closes.
        - To apply the threshold definition to individual controllers in a Storage Center, select **Select Controllers**, then click **Next**. The wizard advances to the next page and displays a table of volumes.

c. Select the check box for each Storage Center controller that you want to monitor with the threshold definition, then click **Finish**. The threshold definition is added and the **Create Threshold Definition** dialog box closes.

Create a Threshold Definition to Monitor the Percentage of Used Storage for a Storage Center

When the Storage Center storage usage percentage exceeds the value set for the error threshold, Storage Manager triggers a threshold alert with a volume movement recommendation.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Definitions** tab.
3. Click **Create Threshold Definition**. The **Create Threshold Definition** dialog box appears.
4. In the **Name** field, type a name for the threshold definition.
5. Configure the threshold definition to monitor Storage Center storage usage.
   a. From the **Type** drop-down menu, select **Storage**.
   b. From the **Alert Object Type** drop-down menu, select **Storage Center**.
   c. From the **Alert Definition** drop-down menu, select **Percent Used**.
6. (Optional) Select the **All Objects** check box to apply the threshold definition to all Storage Centers.
7. Configure the storage usage percentage that must be exceeded to trigger a threshold alert with a volume movement recommendation.
   a. In the **Error Setting** field, type the storage usage percentage that must be exceeded.
   b. Next to the **Error Setting** field, in the **Iterations before email** field, type the number of times the threshold must be exceeded to trigger the alert.
8. Select the **Recommend Storage Center** check box.
9. Configure the other options as needed. These options are described in the online help.
10. When you are finished, click **OK**.
    - If you selected the **All Objects** check box, the threshold definition is created and the **Create Threshold Definition** dialog box closes.
    - If you did not select the **All Objects** check box, the **Add Objects** dialog box appears.
11. Select the check box for each Storage Center that you want to monitor with the threshold definition, then click **Finish**. The **Create Threshold Definition** dialog box closes.

Moving a Volume Based on a Recommendation

If the volume movement recommendation was triggered by a threshold definition that monitors volume latency, automatically move the volume by creating a Live Volume or Live Migration. If the recommendation was triggered by a threshold definition that monitors Storage Center front-end IO, Storage Center controller CPU usage, or the percentage of storage used for a Storage Center, move the volume(s) manually.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Alerts** tab.
3. In the **Current Threshold Alerts** pane, locate the threshold alert that contains the volume movement recommendation. Alerts that contain recommendations display **Yes** in the **Recommend** column.
4. Right-click the threshold alert, then select **Recommend Storage Center**. The **Recommend Storage Center** dialog box opens.
   - If the recommendation was triggered by a threshold definition that monitors volume latency, the dialog box displays a Storage Center recommendation and allows you to move the volume by creating a Live Volume or Live Migration. If Storage Manager identified a possible reason for the increased volume latency, the reason is displayed in the **Recommend Reason** field
   - If the recommendation was triggered by a threshold definition that monitors Storage Center front-end IO, Storage Center controller CPU usage, or the percentage of storage used for a Storage Center, the dialog box displays a recommended Storage Center without suggesting specific volumes to move.

To act on the recommendation, record the Storage Center names displayed in the **Current Storage Center** and **Recommended Storage Center** fields.

Automatically Create a Live Volume and Move the Volume Based on a Recommendation

Use the **Recommend Storage Center** dialog box to automatically move a volume based on a recommendation.

About this task

NOTE: The option to create a Live Volume appears only for Storage Centers running version 7.0 or earlier.

Steps

1. In the **Recommend Storage Center** dialog box, click **Convert to a Live Volume to move to recommended Storage Center**. The **Convert to Live Volume** dialog box opens.
2. Map the destination volume to the server that is currently mapped to the volume.
   a. Next to **Server**, click **Change**. The **Select Server** dialog box opens.
   b. Select the server that is currently mapped to the original volume, then click **OK**.
3. Modify the other Live Volume options as necessary. These options are described in the online help.
4. When you are done, click **Finish**. The Live Volume is created and you return to the **Alerts** tab on the **Threshold Alerts** view.
5. After the Live Volume is synchronized, swap roles to make the recommended Storage Center the primary for the Live Volume.
   a. Click the **Replications & Live Volumes** view, then click the **Live Volumes** tab.
   b. Wait until the Live Volume is synchronized, then select the Live Volume and click **Swap Primary Storage Center of Live Volume**. A confirmation dialog box opens.
   c. Click **OK** to confirm the swap.
6. If you decide that you want to make the recommended Storage Center the permanent host for the volume, delete the Live Volume and select the **Recycle Secondary Volume** check box to recycle the secondary volume (original volume).
   a. Select the Live Volume and click **Delete**. The Delete Objects dialog box opens.
   b. Clear the **Convert to Replication** check box.
   c. Select the **Recycle Secondary Volume** check box.
   d. Click **OK**.

Automatically Live Migrate a Volume Based on a Recommendation

Use the **Recommend Storage Center** dialog box to automatically create a live migration based on a recommendation.

About this task

NOTE: The option to create a Live Migration appears only for Storage Centers running version 7.1 or later.

Steps

1. In the **Recommend Storage Center** dialog box, click **Live Migrate the volume to the recommended Storage Center**. The **Create Live Migration** dialog box opens.
2. (Optional) Modify Live Migration default settings.
   - In the **Replication Attributes** area, configure options that determine how replication behaves.
   - In the **Destination Volume Attributes** area, configure storage options for the destination volume and map the destination volume to a server.
   - In the **Live Migration Attributes** area, enable or disable automatic role swap. When automatic role swap is enabled, Live Migrate swaps the roles immediately after the volume is synced. When it is disabled, you may swap the roles manually any time after the volume is synced.
3. Click **Create**.
   Live Migration begins to migrate the volume to the destination Storage Center.

Manually Move a Volume Based on a Recommendation

If a threshold alert recommends moving volumes to a different Storage Center but does not recommend moving a specific volume, decide which volumes to move and manually create Live Volumes to move them.

About this task

NOTE: This method is the only way to move a volume for Storage Centers running version 7.0 or earlier. For other Storage Centers running version 7.1 or later, create a Live Migration to move the volume. For more information on creating a Live Migration, see Create a Live Migration for a Single Volume.

Steps

1. Examine the volumes hosted by the current Storage Center and decide which volume(s) to move to the recommended Storage Center.
2. Convert each volume that you want to move to a Live Volume.
   - Use the recommended Storage Center as the destination.
   - Map the destination volume to the server that is currently mapped to the volume.
3. After the Live Volume is synchronized, swap roles to make the recommended Storage Center the primary for the Live Volume.
   a. Click the **Replications & Live Volumes** view, then click the **Live Volumes** tab.
   b. Find the Live Volume Wait until the Live Volume is synchronized, then select the Live Volume and click **Swap Primary Storage Center of Live Volume**. A confirmation dialog box appears.
   c. Click **OK** to confirm the swap.
4. If you decide that you want to make the recommended Storage Center the permanent host for the volume, delete the Live Volume and recycle the secondary volume (original volume).
   a. Select the Live Volume and click **Delete**. The **Delete Objects** dialog box appears.
   b. Clear the **Convert to Replication** check box.
   c. Select the **Recycle Secondary Volume** check box.
   d. Click **OK**.

Export Threshold Alerts

Threshold alert data can be exported to CSV, Text, Excel, HTML, XML, or PDF file formats.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Alerts** tab.
3. Click **Save Threshold Alerts** in the **Threshold Alerts** pane. The **Save Threshold Alerts** dialog box appears.
4. To export active threshold alerts, select the **Current Threshold Alerts** checkbox.
5. To export historical threshold alerts, select the **Historical Threshold Alerts** checkbox.
6. Select the radio button for the type of file to export.
7. Click **Browse** to specify the name of the file and the location to which to export the file, then click **Save**.
8. Click **OK**.

Configuring Email Notifications for Threshold Alerts

Storage Manager can be configured to send email notification when a threshold alert is exceeded.

To receive email notifications for threshold alerts:

1. Configure the SMTP server settings on the Data Collector.
2. Add an email address to your user account.
3. Configure your user account settings to send an email notification when a threshold alert is exceeded.

NOTE: Storage Manager can send only one threshold alert email for every 24 hour period. The number of threshold alert emails per 24 hour period cannot be configured.

The combination of a 24 hour time period for threshold alert emails and a default Storage Usage collection interval of four hours might result in a day when a threshold alert email is not sent. The following table shows how a threshold alert email might not be sent on a Sunday, if the threshold alert emails started on a Monday at 12:00 AM:

Table 24. Example threshold alert email times

Weekday	Time of threshold alert email	Threshold alert email period + Storage Usage collection interval
Monday	12:00 AM (00:00) on Monday	24 hour period + 4 hr collection interval
Tuesday	04:00 AM (04:00) on Tuesday	24 hour period + 4 hr collection interval
Wednesday	08:00 AM (08:00) on Wednesday	24 hour period + 4 hr collection interval
Thursday	12:00 PM (12:00) on Thursday	24 hour period + 4 hr collection interval
Friday	04:00 PM (16:00) on Friday	24 hour period + 4 hr collection interval
Saturday	08:00 PM (20:00) on Saturday	24 hour period + 4 hr collection interval
Sunday / Monday	12:00 AM (00:00) on Monday	24 hour period + 4 hr collection interval

Configure SMTP Server Settings

The SMTP server settings must be configured to allow Storage Manager to send notification emails.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Environment** tab and, then click the **SMTP Server** subtab.
5. Click **Edit**.
   The **SMTP Server Configuration** dialog box opens.
6. Configure the SMTP server settings by performing the following steps:
   a. In the **From Email Address** field, type the email address to display as the sender of emails from the Data Collector.
   b. In the **Host or IP Address** field, type the host name or IP address of the SMTP server.
   c. If the port number of the SMTP server is not 25, type the correct port number in the **Port** field.
   d. If the SMTP server requires authentication, select the **Authentication** checkbox, then type the user name and password in the **SMTP User Name** and **SMTP User Password** fields.
7. Click **OK**.

Configure an Email Address for Your User Account

To receive email notifications, you must specify an email address for your user account.

Prerequisites

The SMTP server settings must be configured for the Data Collector. If these settings are not configured, the Data Collector is not able to send emails.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box opens.
2. Type an email address for the user account in the **Email Address** field.
3. Select the format for emails from the **Email Format** drop-down menu.
4. To send a test message to the email address, click **Test Email** and click **OK**.
   Verify that the test message is sent to the specified email address,
5. Click **OK**.

Related tasks

Configure SMTP Server Settings on page 584

Configure Email Notification Settings for Your User Account

Make sure that Storage Manager is configured to send email notifications to your account for the events that you want to monitor.

Prerequisites

- The SMTP server settings must be configured for the Data Collector. If these settings are not configured, the Data Collector is not able to send emails.
- An email address must be configured for your user account.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box opens.
2. Click the **Manage Events** tab.
3. Select the checkbox for each event you want to be notified about.
4. Click **OK**.

Related tasks

Configure SMTP Server Settings on page 584
Configure an Email Address for Your User Account on page 585

Performing Threshold Queries

Threshold queries allow you to query historical data based on threshold criteria.

For example, if a Storage Center experiences a spike of I/O usage, you can create a threshold query to discover the threshold criteria that can detect I/O usage spikes. When you find the correct threshold criteria, you can use create a threshold definition to monitor I/O usage on the Storage Center in the future.

View Saved Queries

Saved threshold queries are displayed in the **Saved Queries** pane.

About this task

Public queries are accessible to all of the Storage Manager users.Personal queries are accessible only to the Storage Manager user that created the query.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Queries** tab.
   The public and personal queries are displayed in in the **Saved Queries** pane.
3. In the **Saved Queries** pane, double-click the query to view.
   Information about the query is displayed in the **Query Filter** area.

Create a Threshold Query

Create a threshold query to test threshold definition settings against historical data. New queries can be run immediately or saved for future use.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Queries** tab.
3. Perform the following steps in the **Save Query Filter Values** pane:
   a. Click **New**. If the **New** button is grayed out, skip to step b.
   b. Type a name for the query in the **Name** field.
   c. To make the query available to other Storage Manager users, select the **Public** checkbox.
4. Perform the following steps in the **Query Filter** pane:
   a. Select whether the query is for all Storage Centers or a specific Storage Center.
      - To select all of the Storage Centers for the query, select the **All Storage Centers** check box.
      - To select a specific Storage Center for the query, clear the **All Storage Centers** check box and select a Storage Center from the drop-down menu.
   b. Select the type of query to create from the first **Definition** drop-down menu.
   c. Select the type of storage object to query from the second **Definition** drop-down menu.
   d. Select the type of usage metric to query from the third **Definition** drop-down menu.
   e. Select the period of time to query the data from the **Start Time** drop-down menu.
   f. Type the threshold value that the usage metric must exceed in the **Threshold Value** field.
   g. To specify the number of times that the usage metric must exceed the threshold value, type a value in the **Occurrences** field.

      To only return results that occurred in consecutively, select the **Consecutive Occurrences** check box.
5. Run or save the threshold query.
   - To save the query for future use, click **Save As**. The threshold query appears in the **Saved Queries** tab.
   - To run the query, click **Run**. The results of the query appear in the **Query Results** pane at the bottom of the **Queries** tab.

Run a Saved Threshold Query

You can select and run a saved threshold query.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Queries** tab.
   The public and personal queries are displayed in the **Saved Queries** pane.

3. In the **Saved Queries** pane, double-click the query to run.
4. Click **Run**.
   The results of the query are displayed in the **Query Results** pane.

Export the Results of a Threshold Query

The results of a threshold results can be exported to CSV, text, Excel, HTML, XML, or PDF file formats.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Queries** tab.
   The public and personal queries are displayed in the **Saved Queries** pane.
3. Select a query from **Saved Queries** pane.
4. Click **Run**.
   The results of the query are displayed in the **Query Results** pane.
5. Click **Export**.
   The **Export Query Results** dialog box opens.
6. Click **Save Results**.
   The **Save Results** dialog box opens.
7. Select the radio button for the type of file to export.
8. Click **Browse** to specify the file name and location to save the file.
9. Click **OK**.

Related tasks

Create a Threshold Definition on page 569

Edit a Saved Threshold Query

Modify a saved threshold query if you want to change the filter settings.

Steps

1. Click the **Threshold Alerts** view.
2. Click the **Queries** tab.
   The public and personal queries are displayed in the **Saved Queries** pane.
3. In the **Saved Queries** pane, double-click the query to edit.
4. Modify the settings in the **Query Filter** area as needed.

   To undo changes to a query and display the saved values of the query, click **Revert**.
5. Save the query.
   - If the name of the query was changed, click **Save** to change the name of the query to the new name or click **Save As** to save a copy of the query with the new name.
   - If only the query filter values were changed, click **Save** to save the changes to the query.

Related tasks

Create a Threshold Query on page 586

19

Storage Center Reports

The Reports view allows users to view realtime reports generated by Storage Center and historical reports Storage Manager.

Topics:

- Chargeback Reports
- Storage Center Automated Reports
- Displaying Reports
- Working with Reports
- Configuring Automated Report Generation
- Testing Automated Reports Settings
- Configure Storage Manager to Email Reports

Chargeback Reports

The information displayed in a Chargeback report includes a sum of charges to each department and the cost/storage savings realized by using a Storage Center as compared to a legacy SAN. The Chargeback reports are in PDF format and present the same data that can be viewed on the **Chargeback** view.

The following tabs are available for Chargeback reports:

- **Chargeback**: Displays the sum of all charges to each department for the selected Chargeback run.
- **Chargeback Savings**: Displays the estimated cost and storage space savings realized by using a Storage Center as compared to a legacy SAN.

Related concepts

Storage Center Chargeback on page 596

Storage Center Automated Reports

The information displayed in the **Automated Reports** tab depends on the type of report and the automated report settings.

Table 25. Types of Reports

Report Name	Description
Daily	Generated at the end of each day and displays the following information: • **Alerts** - Displays Storage Center alerts. • **Volume Storage** - Displays volume storage statistics. • **Replications** - Displays information about replications. • **Live Volumes** - Displays information about Live Volumes.
Weekly	Generated at the end of each week and displays the following information: • **Storage Center Summary** - Displays information about storage space and the number of storage objects on the Storage Center. • **Alerts** - Displays Storage Center alerts. • **Volume Storage**: Displays volume storage statistics. • **Disk Class** - Displays information about storage space on each disk class. • **Replications** - Displays information about replications. • **Disk Power On Time** - Displays information about how long each disk has been powered on. • **Live Volumes** - Displays information about Live Volumes.

Table 25. Types of Reports (continued)

Report Name	Description
Monthly	Generated at the end of each month and displays the following information: • **Storage Center Summary** - Displays information about storage space and the number of storage objects on the Storage Center. • **Volume Storage** - Displays volume storage statistics. • **Disk Class** - Displays information about storage space on each disk class. • **Replications** - Displays information about replications. • **Disk Power On Time** - Displays information about how long each disk has been powered on. • **Live Volumes** - Displays information about Live Volumes.

Displaying Reports

The **Reports** view can display Storage Center Automated reports and Chargeback reports.

View a Storage Center Automated Report

The content of Storage Center reports are configured in the Data Collector automated reports settings.

Steps

1. Click the **Reports** view.
   The **Automated Reports** tab is displayed.
2. To display reports for an individual Storage Center, click the plus sign (+) next to the Storage Center in the **Reports** pane.
   The name of each report that is displayed consists of two parts:
   - The first part of the name displays Daily, Weekly, or Monthly, which indicates how often the report is generated.
   - The second part of the name displays the date and time that the report was generated.

   For example, the name of a daily report for June 1st, 2013 would be: `Daily - 06/1/2013 23:56:02`
3. Select the report to view in the **Reports** pane or double-click on the report to view in the **Automated Reports** tab.

   The report tabs that are displayed depend on whether the report is a Daily, Weekly, or Monthly report.

Related concepts

Configuring Automated Report Generation on page 591
Storage Center Automated Reports on page 588

View a Chargeback Report

You can view a Chargeback report PDF on the **Reports** view. The Chargeback view also displays **Chargeback** data.

Prerequisites

- Chargeback must be enabled.
- The Chargeback and Chargeback Savings reports must be enabled in the Data Collector automated reports settings.

Steps

1. Click the **Reports** view. The **Automated Reports** tab appears and it displays all of the Storage Center and Chargeback reports that can be viewed.
2. To display only Chargeback reports, click the plus sign (+) next to the **Chargeback** folder. The name of each report consists of the text Chargeback followed by the date and time that the report was generated.

   For example, the name of a daily report for June 12th, 2013 would be: `Chargeback - 06/12/2013 23:15:00`

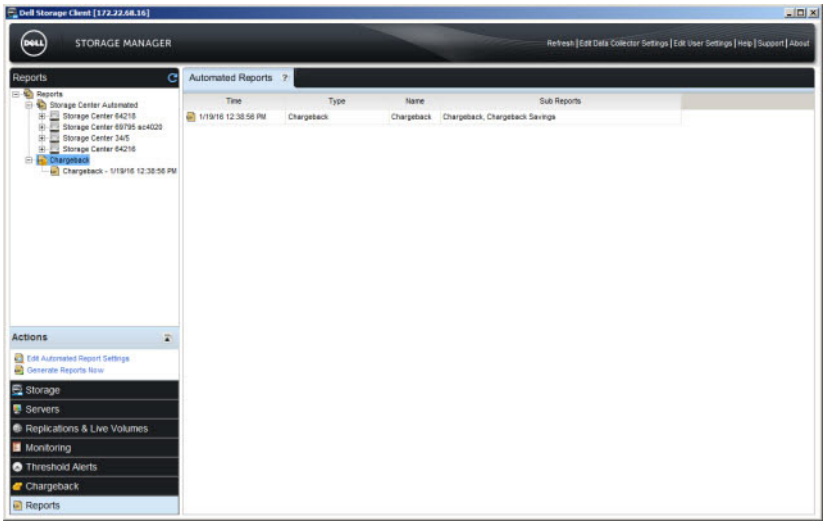


Figure 72. Chargeback Reports

3. Select the report to view in the **Reports** pane or double-click on the report to view in the **Automated Reports** tab.

Related concepts

Chargeback Reports on page 588
Configuring Automated Report Generation on page 591
Viewing Chargeback Runs on page 605

Working with Reports

You can update the list of reports and use the report options navigate, print, save, and delete reports.

Update the List of Reports

Update the list of reports to display new reports that were automatically or manually generated.

Steps

1. Click the **Reports** view.
2. Click **Refresh** on the **Reports** pane.

Navigate Through the Pages of a Report

Use the next and previous buttons to move forward and backward in the report. If you want to jump to a specific page, you can type the page number.

Steps

1. Click the **Reports** view.
2. Select the report to view from the **Reports** pane.
3. Perform the following actions to navigate through the pages of the report:
   - To display a specific page of the report, type the page number in the **Page Number** field and press **Enter**.
   - To display the next page of the report, click **Next**.
   - To display the previous page of the report, click **Previous**.

Print a Report

Perform the following steps to save a report:

Steps

1. Click the **Reports** view.
2. Select the report to print from the **Reports** pane.
3. Click **(Print)**.
   The **Print** dialog box opens.
4. Select the printer to use from the **Name** drop-down menu.

   NOTE: For best results, print reports using the Landscape orientation.

5. Click **OK**.

Save a Report

Perform the following steps to save a report:

Steps

1. Click the **Reports** view.
2. Select the report to save from the **Reports** pane.
3. Click **(Save)**.
   The **Select File** dialog box opens.
4. Select a location to save the PDF file and enter a name for the file in the **File name** field.
5. Click **OK**.

Delete a Report

Perform the following steps to delete a report:

Steps

1. Click the **Reports** view.
2. Select the report to delete from the **Reports** pane.

   To select multiple reports, hold the Shift or Control key while you select the reports.
3. Right-click on the selected report and select **Delete**.
   The **Delete Automated Reports** dialog box opens.
4. Click **OK**.

Configuring Automated Report Generation

The settings for automated reports can be set up globally for all Storage Centers or customized for individual Storage Centers.

- The global automated report settings are defined on the **Automated Reports** tab in the **Edit Data Collector Settings** dialog box.
- The automated report settings for individual Storage Centers are defined on the **Automated Reports** tab in the **Edit Settings** dialog box of the selected Storage Center.

In addition to viewing automated reports in the **Report** view, Storage Manager can be configured to email automated reports to users or save automated reports to a public directory.

NOTE: Automated reports cannot be saved to a public directory when using a Virtual Appliance.

Set Up Automated Reports for All Storage Centers

Configure automated report settings on the Data Collector if you want to use the same report settings for all managed Storage Centers. Configure the global settings first, and then customize report settings for individual Storage Centers as needed.

Steps

1. In the top pane of Storage Manager, click **Edit Data Collector Settings**
   The **Edit Data Collector Settings** page is displayed.
2. Click the **Automated Reports** tab.
3. Select the checkboxes in the **Automated Report Settings** area to specify which reports to generate and how often to generate them.
4. Select the checkboxes in the **Automated Table Report Settings** area to specify which reports to generate and how often to generate them.

   NOTE: Automated table reports can be saved in a public directory or attached to automated emails, but they do not appear in the **Reports** view.

5. Select the checkboxes in the **Automated FluidFS Report Settings** area to specify which reports to generate and how often to generate them.
6. Set the **Automated Report Options**
   a. To export the reports to a public directory, select the **Store report in public directory** checkbox and enter the full path to the directory in the **Directory** field.

      NOTE: The directory must be located on the same server as the Data Collector.

      NOTE: Automated reports cannot be saved to a public directory when using a Virtual Appliance.

   b. To email the reports selected in the **Automated Reports Settings** area, select the **Attach Automated Reports to email** checkbox.
   c. To email the reports selected in the **Automated Table Reports Settings** area, select the **Attach Table Reports to email** checkbox.
   d. Select the file format for **Table Reports** from the **File Type for Table Reports** drop-down menu.
7. Click **OK**.

Related tasks

Configure Chargeback or Modify Chargeback Settings on page 596
Configure Storage Manager to Email Reports on page 594

Set Up Automated Reports for an Individual Storage Center

By default, Storage Centers are configured to use the global automated report settings that are specified for the Data Collector. If you want to use different report settings for a Storage Center, you can configure the automated report settings in the Storage Center properties.

Steps

1. If the Storage Manager Client is connected to a Data Collector, select a Storage Center from the **Storage** view.
2. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
3. Click the **Automated Reports** tab.
4. Deselect the **Use global automated reporting settings for this Storage Center** checkbox.
5. Select the checkboxes in the **Automated Report Settings** area to specify which reports to generate and how often to generate them.
6. Select the checkboxes in the **Automated Table Report Settings** area to specify which reports to generate and how often to generate them.

NOTE: Automated table reports can be saved in a public directory or attached to automated emails but they do not appear in the Reports view.

7. Set the **Automated Report Options**
   a. To export the reports to a public directory, select the **Store report in public directory** checkbox and enter the full path to the directory in the **Directory** field.

      NOTE: The directory must be located on the same server as the Data Collector.

      NOTE: Automated reports cannot be saved to a public directory when using a Virtual Appliance.

   b. To configure the Data Collector to email the reports when they are generated:
      - Select the **Attach Automated Reports to email** checkbox to email the reports specified in the **Automated Reports Settings** area.
      - Select the **Attach Table Reports to email** checkbox to email the reports specified in the **Automated Table Reports Settings** area.

        NOTE: Storage Manager sends emails to the email address specified in the User Properties.

   c. Select the file format for exported and emailed **Table Reports** from the **File Type for Table Reports** drop-down box.
8. Click **OK**.

Testing Automated Reports Settings

You can manually generate reports to test the configured automated report settings without waiting for the reports to be generated automatically. By default, Storage Manager generates reports into a folder named for the day when the report was generated.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **Automated Reports** subtab.
5. Review the current report settings:
   - If the settings are acceptable, click **Generate**.
   - To change the report settings, click **Edit**, adjust the settings, and click **Generate**.

   The **Generate Reports Now** dialog box opens.
6. Select the checkboxes of the reports to generate.
7. Click **OK**. The reports are generated and the **Generate Reports** dialog box closes.

   NOTE: Generating a report overwrites previously generated reports in the folder for that day. To prevent these reports from being overwritten, specify a different directory in the **Automated Report Options** area of the **Automated Reports** dialog box.
8. Click **OK**.

Configure Storage Manager to Email Reports

Storage Manager can be configured to send automated reports by email.

About this task

To send automated reports by email:

Steps

1. Configure the SMTP server settings for the Data Collector.
2. Add an email address to your user account.
3. Configure email notification settings for your user account.

Configure SMTP Server Settings

The SMTP server settings must be configured to allow Storage Manager to send notification emails.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Environment** tab and, then click the **SMTP Server** subtab.
5. Click **Edit**.
   The **SMTP Server Configuration** dialog box opens.
6. Configure the SMTP server settings by performing the following steps:
   a. In the **From Email Address** field, type the email address to display as the sender of emails from the Data Collector.
   b. In the **Host or IP Address** field, type the host name or IP address of the SMTP server.
   c. If the port number of the SMTP server is not 25, type the correct port number in the **Port** field.
   d. If the SMTP server requires authentication, select the **Authentication** checkbox, then type the user name and password in the **SMTP User Name** and **SMTP User Password** fields.
7. Click **OK**.

Configure an Email Address for Your User Account

To receive email notifications, you must specify an email address for your user account.

Prerequisites

The SMTP server settings must be configured for the Data Collector. If these settings are not configured, the Data Collector is not able to send emails.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box opens.

2. Type an email address for the user account in the **Email Address** field.
3. Select the format for emails from the **Email Format** drop-down menu.
4. To send a test message to the email address, click **Test Email** and click **OK**.
   Verify that the test message is sent to the specified email address,
5. Click **OK**.

Related tasks

Configure SMTP Server Settings on page 584

Configure Email Notification Settings for Your User Account

Make sure that Storage Manager is configured to send email notifications to your account for the events that you want to monitor.

Prerequisites

- The SMTP server settings must be configured for the Data Collector. If these settings are not configured, the Data Collector is not able to send emails.
- An email address must be configured for your user account.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box opens.
2. Click the **Manage Events** tab.
3. Select the checkbox for each event you want to be notified about.
4. Click **OK**.

Related tasks

Configure SMTP Server Settings on page 584
Configure an Email Address for Your User Account on page 585

20

Storage Center Chargeback

Chargeback monitors storage consumption and calculates data storage operating costs per department. Chargeback can be configured to charge for storage based on the amount of allocated space or the amount of configured space. When cost is based on allocated space, Chargeback can be configured to charge based on storage usage (the amount of space used), or storage consumption (the difference in the amount space used since the last automated Chargeback run).

Topics:

- Configure Chargeback or Modify Chargeback Settings
- Configuring Chargeback Departments
- Perform a Manual Chargeback Run
- Viewing Chargeback Runs
- Working with Charts
- Exporting Chargeback Data

Configure Chargeback or Modify Chargeback Settings

The Chargeback settings specify how to charge for storage consumption, how to assign base storage costs, and how to generate reports. During the initial setup of Chargeback settings, the **Default Department** drop-down menu is empty because the departments do not exist yet.

Steps

1. Click the **Chargeback** view.
2. Click **Edit Chargeback Settings** in the **Actions** pane. The **Edit Chargeback Settings** wizard appears.

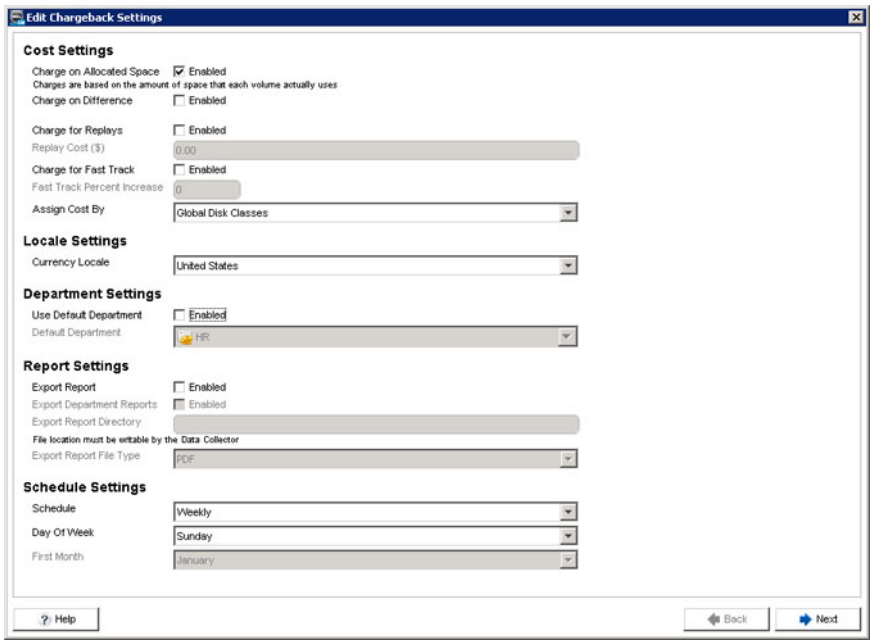


Figure 73. Edit Chargeback Settings Wizard

3. Select whether to charge on the allocated space of a volume or the configured space of a volume:
   - To charge based on the amount of space that a volume actually uses, select the **Charge on Allocated Space** check box.
   - To charge based on the amount of space that each volume is configured to use, clear the **Charge on Allocated Space** check box.

4. If the **Charge on Allocated Space** check box was selected in the previous step, select the **Charge on Difference** check box if you want to configure Chargeback to charge based on the difference between the amount of space a volume currently uses and the amount of space that a volume used during the last automated Chargeback run.
5. To add additional charges that are based on the number of snapshots that have been created for a volume, select the **Charge for Snapshots** check box and enter the cost per snapshot in the **Snapshot Cost** field.
6. To charge a higher rate for volume data that uses Fast Track disk space, select the **Charge Extra for Fast Track** check box and enter the percentage to increase the cost for volumes that use Fast Track disk space in the **Fast Track Percent Increase** field.
7. Select how to assign a base cost to storage from the **Assign Cost By** drop-down.
   - **Global Disk Classes**: Costs are assigned to each available disk class.
   - **Individual Storage Center Disk Tier**: Costs are assigned per storage tier level for each Storage Center.
8. Select a location from the **Currency Locale** drop-down menu to specify the type currency to display in Chargeback.

   For example, if the selected location is United States, the currency unit is dollars ($).

   NOTE: If selecting a location causes characters to be displayed incorrectly, download the appropriate Windows language pack.

9. To specify a department that unassigned volumes will be assigned to when Chargeback is run, select the **Use Default Department** check box and enter select the department from the **Default Department** drop-down menu.
10. To automatically create a report when Chargeback is run:
    a. Select the **Export Report** check box.
    b. To automatically create individual department reports when Chargeback is run, select the **Export Department Reports** check box.
    c. Enter the complete path of a directory to save the reports to in the **Export Report Directory** field. The directory must be a public directory that exists on the same server as the Storage Manager Data Collection Manager.
    d. Select the file format of the Chargeback reports from the **Export Report File Type** drop-down menu.
11. Select how often to perform an automated Chargeback run from the **Schedule** drop-down menu.
    - **Daily**: An automated Chargeback run is performed once a day.
    - **Weekly**: An automated Chargeback run is performed once a week on the day selected from the **Day of Week** drop-down menu.
    - **Monthly**: An automated Chargeback run is performed once a month.
    - **Quarterly**: An automated Chargeback run is performed once a quarter starting with the month selected the **First Month** drop-down menu and every third month thereafter.
12. Click **Next**.
    - If you selected Global Disk Classes in step 7, see Assign Storage Costs for Global Disk Classes on page 597.
    - If you selected Individual Storage Center Disk Tier in step 7, see Assign Storage Costs for Storage Center Disk Tiers on page 598.

Assign Storage Costs for Global Disk Classes

If the **Edit Chargeback Settings** wizard displays this page, assign a cost to each disk class.

Steps

1. For each available disk class, select the unit of storage on which to base the storage cost from the **per** drop-down menu.
2. For each available disk class, enter an amount to charge per unit of storage in the **Cost** field.

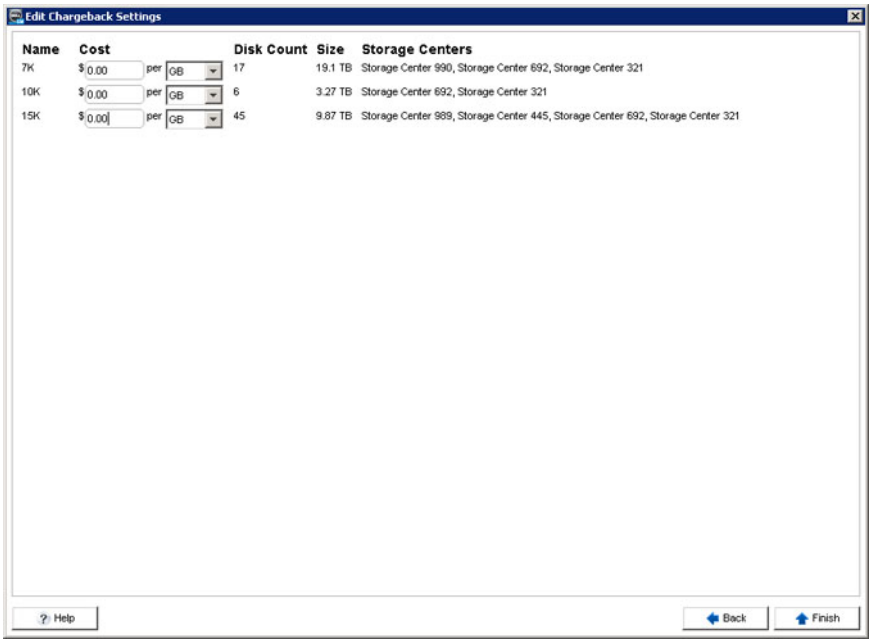


Figure 74. Storage Costs Per Disk Class

3. Click **Finish** to save the Chargeback settings.

Assign Storage Costs for Storage Center Disk Tiers

If the **Edit Chargeback Settings** wizard displays this page, assign storage cost for each Storage Center disk tier.

Steps

1. For each storage tier, select the unit of storage on which to base the storage cost from the **per** drop-down menu.
2. For each storage tier, enter an amount to charge per unit of storage in the **Cost** field.

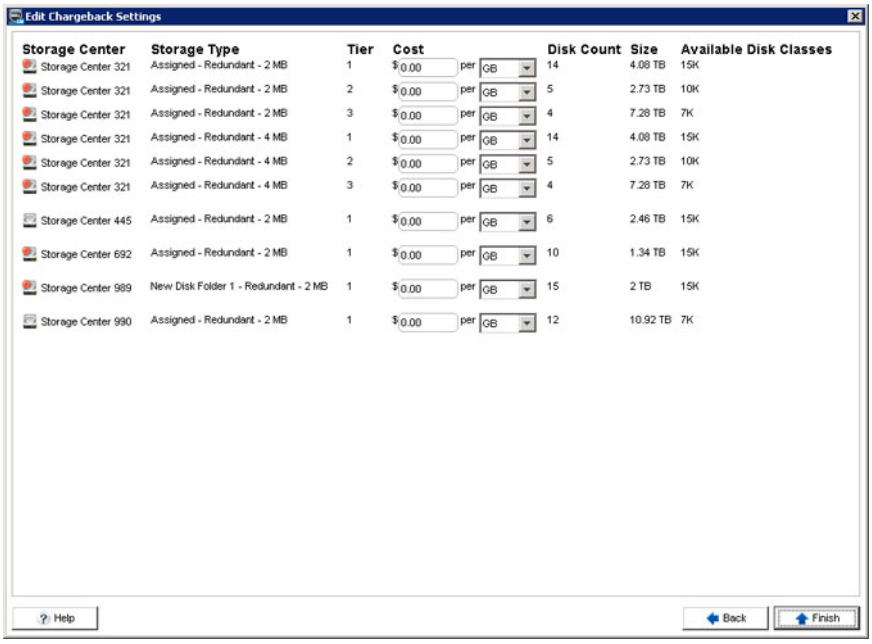


Figure 75. Storage Costs Per Storage Center Disk Tiers

3. Click **Finish** to save the Chargeback settings.

Configuring Chargeback Departments

Chargeback uses departments to assign base billing prices to departments and department line items to account for individual IT-related expenses. Volumes and volumes folder are assigned to departments for the purpose of charging departments for storage consumption.

Setting Up Departments

You can add, modify, and delete Chargeback departments as needed.

Add a Department

Add a chargeback department for each organization that you want to bill for storage usage.

Steps

1. Click the **Chargeback** view.
2. Click the **Departments** tab.
3. In the **Chargeback** pane, select **Departments**.
4. Click **Add Department**. The **Add Department** dialog box appears.

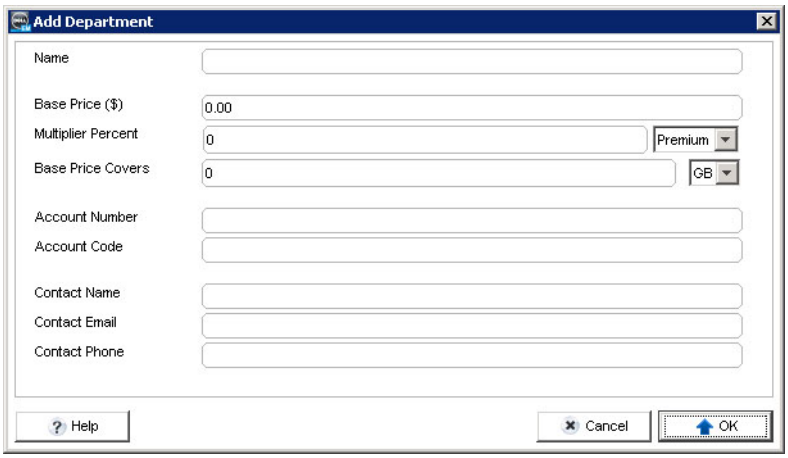


Figure 76. Add Department Dialog Box

5. Enter the name of the department in the **Name** field.
6. Enter the base price for storage in the **Base Price** field.
7. Enter percentage to apply to the global cost of storage in the **Multiplier Percent** field.
   - To apply a discount to the cost of storage, enter the percentage by which to decrease the global cost and select **Discount** from the drop-down menu.
   - To apply a premium to the cost of storage, enter the percentage by which to increase the global cost and select **Premium** from the drop-down menu.
8. Enter the account number of the department in the **Account Number** field.
9. Enter the purchasing code of the department in the **Account Code** field.
10. Enter the name of the department contact in the **Contact Name** field.
11. Enter the email address of the department contact in the **Contact Email** field.
12. Enter the phone number of the department contact in the **Contact Phone** field.
13. Click **OK** to add the department.

Edit a Department

You can modify the base storage price charged to a department, change the department attributes, and change the department contact information.

Steps

1. Click the **Chargeback** view.
2. Click the **Departments** tab.
3. Select the department that you want to edit from the list of departments on the **Chargeback** pane.
4. Click **Edit Settings** or right-click on the department and select **Edit Settings**. The **Edit Settings** dialog box appears.
5. Modify the department options as needed. These options are described in the online help.
6. Click **OK** to save changes to the department.

Delete a Department

Delete a department if it is no longer used.

Steps

1. Click the **Chargeback** view.
2. Click the **Departments** tab.
3. Select the department to delete from the list of departments on the **Chargeback** pane.
4. Click **Delete** or right-click on the department and select **Delete**. The Delete Objects dialog box appears.
5. Click **OK** to delete the selected department.

Managing Department Line Items

You can add, edit, or remove line-item expenses.

Add a Department Line Item

A line item is a fixed cost that is not tied to storage usage.

Steps

1. Click the **Chargeback** view.
2. Click the **Departments** tab.
3. Select the department to which you want to add the line item from the list of departments on the **Chargeback** pane.

   Information about the selected department appears on the **Department** tab.
4. Click **Add Line Item**. The **Add Line Item** dialog box appears.

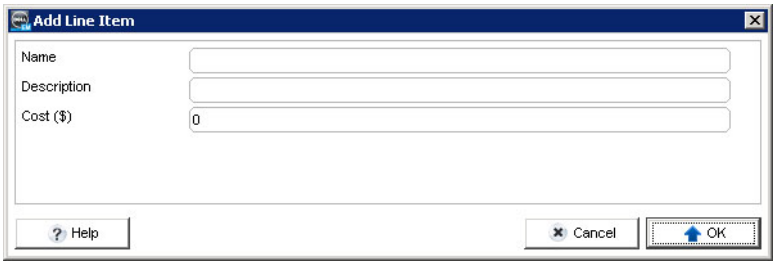


Figure 77. Add Line Item Dialog Box

5. Enter a name for the line item in the **Name** field.
6. Enter a short description for the line item in **Description** field.
7. Enter the cost for the line item in the **Cost** field.

8. Click **OK** to add the line item to the department.

Edit a Department Line Item

You can modify the name, description, and cost for a line item.

Steps

1. Click the **Chargeback** view.
2. Click the **Departments** tab.
3. Select the department that contains the line item that you want to edit from the list of departments on the **Chargeback** pane.
4. Select the line item you want to edit from the **Department Line Items** pane.
5. Click **Edit Settings** or right-click on the line item and select **Edit Settings**. The **Edit Line Item** dialog box appears.

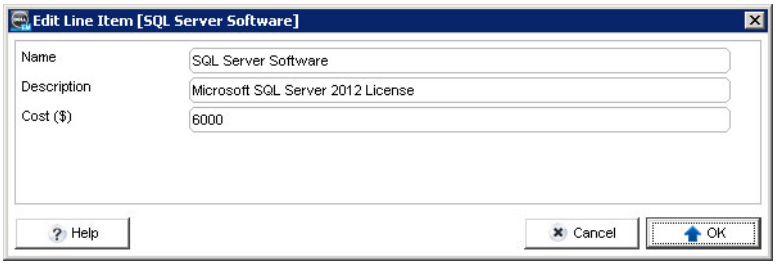


Figure 78. Edit Line Item Dialog Box

6. To change the name of the line item, edit the value in the **Name** field.
7. To change the small description of the line item, edit the value in the **Description** field.
8. To change the cost for the line item, edit the value in the **Cost** field.
9. Click **OK** to save changes to the line item.

Delete a Department Line Item

Delete a line item if you no longer want to charge the department for it.

Steps

1. Click the **Chargeback** view.
2. Click the **Departments** tab.
3. Select the department that contains the line item that you want to delete from the list of departments on the **Chargeback** pane.
4. Select the line item you want to delete from the **Department Line Items** pane.
5. Click **Delete** or right-click on the line item and select **Delete**. The **Delete Objects** dialog box appears.
6. Click **OK** to delete the selected line item.

Assigning Volumes to Chargeback Departments

To charge a department for the storage used by a volume or volume folder, assign the volume or volume folder to a Chargeback department. You can accomplish this from the **Storage** view or the **Chargeback** view.

About this task

Assign Volumes to a Department in the Chargeback View

Use the **Chargeback** view to assign multiple volumes to a department simultaneously.

Steps

1. Click the **Chargeback** view.
2. Click the **Departments** tab.
3. Select the department to which you want to assign the volume from the list of departments on the **Chargeback** pane.

   Information about the selected department appears on the **Department** tab.
4. Click **Add Volumes**. The **Add Volumes** dialog box appears.

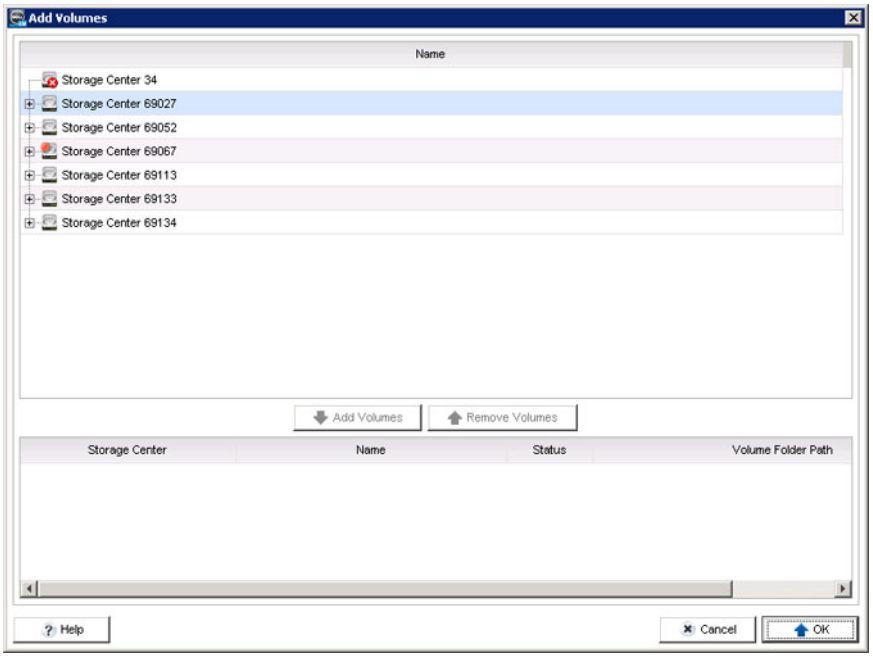


Figure 79. Add Volume Dialog Box

5. Select the volumes to assign to the department.
6. Click **Add Volumes** to add the selected volumes to the list of volumes to assign to the department.
7. Click **OK** to assign the volumes to the department.

Assign Volume Folders to a Department in the Chargeback View

Use the **Chargeback** view to assign multiple volume folders to a department simultaneously.

Steps

1. Click the **Chargeback** view.
2. Click the **Departments** tab.
3. Select the department to which you want to assign the volume folder from the list of departments on the **Chargeback** pane.

   Information about the selected department appears on the **Department** tab.
4. Click **Add Volume Folders**. The **Add Volume Folders** dialog box appears.

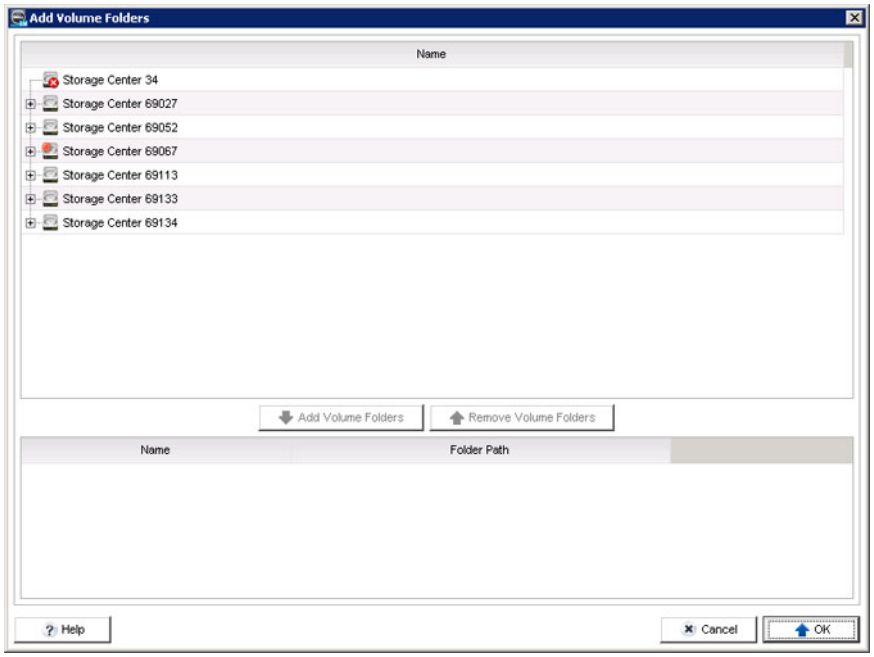


Figure 80. Add Volume Folders Dialog Box

5. Select the volume folders to assign to the department.
6. Click **Add Volume Folders** to add the selected volume folders to the list of volume folders to assign to the department.
7. Click **OK** to assign the volume folders to the department.

Remove Volumes/Volume Folders from a Department in the Chargeback View

Use the **Chargeback** view to remove multiple volumes from a department simultaneously.

Steps

1. Click the **Chargeback** view.
2. Click the **Departments** tab.
3. Select the department that contains the volumes or volume folders that you want to unassign.

   Information about the selected department appears on the **Department** tab.
4. Click the **Storage Center Objects** tab to display the volumes or volume folders assigned to the department.
5. Select the volumes or volume folders to unassign from the department.
6. Click **Delete** on the Storage Center Objects tab. The **Delete** dialog box appears.
7. Click **OK** to unassign the selected volumes or volume folders from the department.

Assign a Volume/Volume Folder to a Department in the Storage View

Use the **Storage** view to assign volumes and volume folders to a department one at a time.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the volume or volume folder.
5. In the right pane, click **Edit Settings**. A dialog box appears.
6. Next to **Chargeback Department**, click **Change**. The **Add Chargeback Department** dialog box appears.

7. Select the appropriate Chargeback department, then click **OK**.
8. Click **OK** to close the dialog box.

Remove a Volume/Volume Folder from a Department in the Storage View

Use the **Storage** view to remove volumes and volume folders from a department one at a time.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center.
3. Click the **Storage** tab.
4. In the **Storage** tab navigation pane, select the volume or volume folder.
5. In the right pane, click **Edit Settings**. A dialog box appears.
6. Next to **Chargeback Department**, click **Change**. The **Add Chargeback Department** dialog box appears.
7. Click **OK** without selecting a Chargeback department. The **Add Chargeback Department** dialog box closes and clears the **Chargeback Department** field.
8. Click **OK** to close the dialog box.

Perform a Manual Chargeback Run

Chargeback is scheduled to run automatically but it can also be run manually. When a Chargeback run is performed manually, a Manual Run entry is added to the **Runs** folder on the **Chargeback Runs** navigation pane.

Steps

1. Click the **Chargeback** view.
2. Click **Run Now** in the **Actions** pane. The **Run Now** dialog box appears.

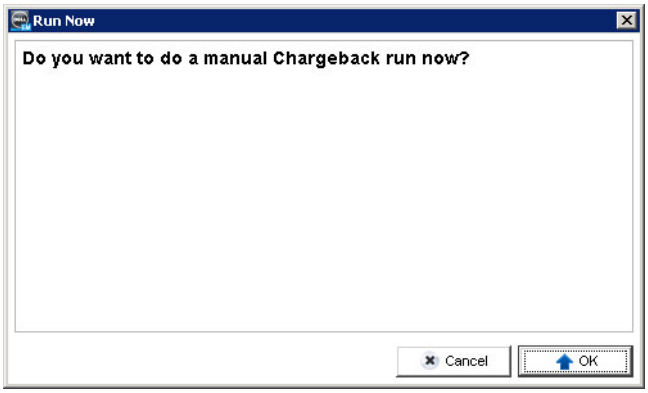


Figure 81. Run Now Dialog Box

3. Click **OK**.

   Storage Manager performs the Chargeback run and creates a Manual Run entry in the **Runs** folder on the Chargeback pane.

Viewing Chargeback Runs

Use the **Chargeback Runs** tab in the **Chargeback** view to view scheduled and manual Chargeback runs. Each Chargeback run is displayed in the **Chargeback** pane. The Chargeback runs names indicate the type of Chargeback run (Manual Run, Day Ending, Week Ending, Month Ending, or Quarter *1–4* Ending) and the date of the run.

View a Chart of Department Costs for a Chargeback Run

The **Chart** subtab displays a bar chart that shows the sum of all charges to each department for the Chargeback run.

Steps

1. Click the **Chargeback** view.
2. Click the **Chargeback Runs** tab.
3. Select the Chargeback run to display from the **Runs** folder on the **Chargeback** pane.
4. Click the **Chart** subtab.
5. (Optional) Filter the departments that are displayed in the bar chart.
   a. Click **Filter Objects**. The Filter Objects dialog box appears.
   b. Select the check box(es) of the department(s) to display and clear the check box(es) of the department(s) to hide.
      - To select all of the department check boxes, click **Select All**.
      - To clear all of the department check boxes, click **Unselect All**.
   c. Click **OK**. The bar chart hides the departments that had their check boxes cleared in the **Filter Objects** dialog box.

View the Results of the Chargeback Run in Table Format

The **Table** subtab displays a summary of the charges and storage usage for each department. When a department is selected, the bottom pane of the tab displays costs and size in numerical and graphical formats.

Steps

1. Click the **Chargeback** view.
2. Click the **Chargeback Runs** tab.
3. Select the Chargeback run to display from the **Runs** folder on the **Chargeback** pane.
4. Click the **Table** subtab.

Related tasks

Export Chargeback Run Data on page 607

View Cost and Storage Savings Realized by Dynamic Capacity for a Chargeback Run

The **Dynamic Capacity Savings** subtab displays an estimated amount of cost and storage space savings realized by using a Storage Center with Dynamic Capacity as compared to a legacy SAN configuration. These savings are achieved because Storage Center allocates space as needed, whereas a legacy SAN allocates space when a volume is created.

Steps

1. Click the **Chargeback** view.
2. Click the **Chargeback Runs** tab.
3. Select the Chargeback run to display from the **Runs** folder on the **Chargeback** pane.
4. Click the **Dynamic Capacity Savings** subtab.

View Cost and Storage Savings Realized by Using Data Instant Snapshots for a Chargeback Run

The **Data Instant Snapshot Savings** subtab shows the estimated cost and storage space savings realized by using a Storage Center with Data Instant Snapshots as compared to legacy SAN point-in-time-copies. These savings are achieved because Data Instant Snapshots allocates space for a snapshot only when data is written and saves only the delta between snapshots; a legacy SAN allocates space for every point-in-time-copy.

Steps

1. Click the **Chargeback** view.
2. Click the **Chargeback Runs** tab.
3. Select the Chargeback run to display from the **Runs** folder on the **Chargeback** pane.
4. Click the **Data Instant Snapshot Savings** subtab.

View Cost Savings Realized by Using Data Progression for a Chargeback Run

The **Data Progression Savings** tab shows the estimated cost savings realized by using a Storage Center with Data Progression as compared to a legacy SAN.

Steps

1. Click the **Chargeback** view.
2. Click the **Chargeback Runs** tab.
3. Select the Chargeback run to display from the **Runs** folder on the **Chargeback** pane.
4. Click the **Data Progression Savings** subtab.

Working with Charts

You can zoom in and out on charts, save them as images, or print them.

Zoom in on an Area of the Chart

Zoom in on an area to see more details.

Steps

1. Use the mouse to select an area of the chart in which to zoom.
   a. Click and hold the right or left mouse button on the chart.
   b. Drag the mouse to the right to select an area of the chart.
2. Release the mouse button to zoom into the selected area of the chart.

Return to the Normal Zoom Level of the Chart

After you have zoomed in, you can return to the default zoom level.

Steps

1. Click and hold the right or left mouse button on the chart.
2. Drag the mouse to the left to return to the normal zoom level of the chart.

Save the Chart as a PNG Image

Save the chart as an image if you want to use it elsewhere, such as in a document or an email.

Steps

1. Right-click the chart and select **Save As**. The **Save** dialog box appears.
2. Select a location to save the image and enter a name for the image in the **File name** field.
3. Click **Save** to save the chart.

Print the Chart

Print the chart if you want a paper copy.

Steps

1. Right-click the chart and select **Print**. The **Page Setup** dialog box appears.
2. Select the paper size to print to from the **Size** drop-down menu.
3. Select the **Landscape** radio button to allow the entire chart to print.
4. Click **OK**. The Print dialog box appears.
5. Select the printer to use from the **Name** drop-down menu.
6. Click **OK** to print the chart.

Exporting Chargeback Data

You can export all data for a Chargeback run or export Chargeback run data for a single department.

Export Chargeback Run Data

Chargeback run data can be exported to CSV, Text, Excel, HTML, XML, or PDF.

Steps

1. Click the **Chargeback** view.
2. Make sure the **Chargeback Runs** tab is selected.
3. In the **Chargeback** pane, select the Chargeback run for which you want to export data.
4. In the **Chargeback** pane, click **Save Chargeback Data**. The **Save Chargeback Data** dialog box appears.
5. Select the type of file to output: CSV, Text, Excel, HTML, XML, or PDF.
6. Click **Browse** to specify the name of the file and the location to which to export the file, then click **Save**.
7. Click **OK**.

Export Chargeback Run Data for a Single Department

Chargeback run data for a department can be exported to CSV, Text, Excel, HTML, XML, or PDF.

Steps

1. Click the **Chargeback** view.
2. Make sure the **Chargeback Runs** tab is selected.
3. In the **Chargeback** pane, select the Chargeback run for which you want to export data.
4. Click the **Table** subtab.
5. Select the department for which you want to export data, then click **Save Department Run Data**. The **Save Department Run Data** dialog box appears.

6. Select the type of file to output: CSV, Text, Excel, HTML, XML, or PDF.
7. Click **Browse** to specify the name of the file and the location to which to export the file, then click **Save**.
8. Click **OK**.

21

Storage Center Monitoring

Storage Manager provides a centralized location to view Storage Center and PS Series group alerts, events, indications, and logs collected by the Storage Center. System events logged by the Storage Center can also be viewed.

Topics:

- Storage Alerts
- Events
- Storage Logs
- Audit Logs
- Export Monitoring Data
- Configure Data Collection Schedules

Storage Alerts

Alerts represent current issues present on the storage system, which clear themselves automatically if the situation that caused them is corrected. Indications warn you about a condition on the storage system that might require direct user intervention to correct.

Status Levels for Alerts and Indications

Status levels indicate the severity of storage system alerts and indications.

Table 26. Alert and Indication Status Levels

Status	Description
Complete	Indicates that an operation on the Storage Center has completed.
Critical	• Indicates an item on the Storage Center is in a critical state and may be nearing failure. • Indicates a serious problem on the PS Series group that can cause damage to the array or data loss
Degraded	Indicates an item on the Storage Center is currently operating in a degraded mode. Items in this condition may operate in degraded mode indefinitely, but are not functioning to their full capability.
Down	Indicates an item on the Storage Center is down and not currently operational.
Emergency	Indicates an item on the Storage Center requires immediate attention in order to remain operational.
Inform/Okay	Provide information regarding some operation that is occurring or has occurred on the Storage Center.
Unavailable	Indicates that an item on the Storage Center that is expected to be present cannot currently be found for use.
Warning	Indicates a condition on the PS Series group that decreases performance or can become critical if it is not corrected.

Viewing Storage System Alerts

Use the **Alerts** tab in the **Storage** view or the **Storage Alerts** tab in the **Monitoring** view to display and search storage system alerts.

Alerts represent current issues present on the storage system, which clear themselves automatically if the situation that caused them is corrected.

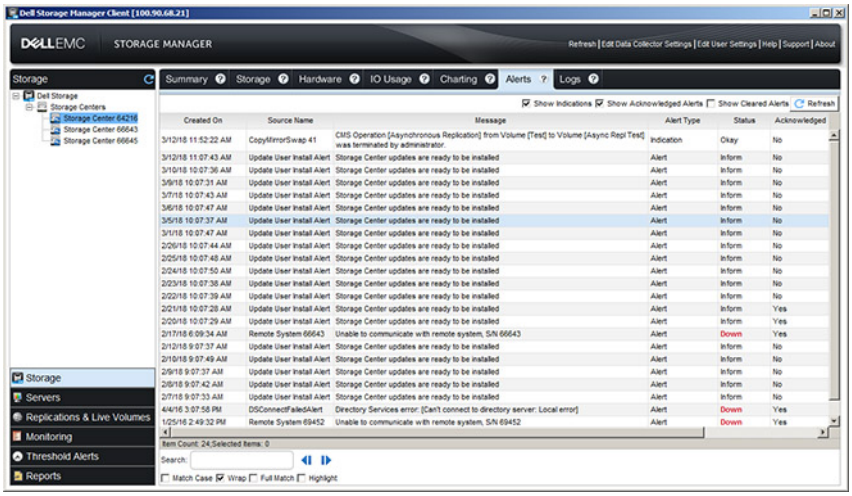


Figure 82. Alerts Tab

Display Storage Alerts on the Monitoring View

Alerts for managed storage systems can be displayed on the Storage Alerts tab.

Steps

1. Click the **Monitoring** view.
2. Click the **Storage Alerts** tab.
3. Select the check boxes of the storage systems to display and clear the check boxes of the storage systems to hide.
   The **Storage Alerts** tab displays alerts for the selected storage systems.
4. To display indications, select the **Show Indications** check box.
5. To display acknowledged alerts, select the **Show Acknowledged Alerts** check box.
6. To display cleared alerts, select the **Show Cleared Alerts** check box.
7. To refresh the alert data for the selected storage systems, click **Refresh** on the Storage Alerts tab.

Filter Alerts by Storage System

By default, storage alerts are displayed for all managed storage systems.

Steps

1. Click the **Monitoring** view.
2. Click the **Storage Alerts** tab.
3. Use the **Storage Centers** pane to filter alerts by Storage Center.
   - To hide alerts for a single Storage Center, clear the check box for the Storage Center.
   - To display alerts for a Storage Center that is deselected, select the check box for the Storage Center.
   - To hide alerts for all of the Storage Centers, click **Unselect All**.
   - To display alerts for all of the Storage Centers, click **Select All**.
4. Use the **PS Groups** pane to filter alerts by PS Series group.
   - To hide alerts for a single PS Series group, clear the check box for the group.
   - To display alerts for a PS Series group that is deselected, select the check box for the group.

- To hide alerts for all of the PS Series groups, click **Unselect All**.
- To display alerts for all of the PS Series groups, click **Select All**.

Select the Date Range of Storage Alerts to Display

You can view storage alerts for the last day, last 3 days, last 5 days, last week, or specify a custom time period.

Steps

1. Click the **Monitoring** view
2. Click the **Storage Alerts** tab.
3. Select the date range of the storage alerts to display by clicking one of the following:
   - **Last Day**: Displays the past 24 hours of storage alerts.
   - **Last 3 Days**: Displays the past 72 hours of storage alerts.
   - **Last 5 Days**: Displays the past 120 hours of storage alerts.
   - **Last Week**: Displays the past 168 hours of storage alerts.
   - **Last Month**: Displays the past month of storage alerts.
   - **Custom**: Displays options that allow you to specify the start time and the end time of the storage alerts to display.
4. If you clicked **Custom**, perform the following tasks to specify the start time and end time of the storage alerts to display.

   To specify the start time:

   a. Select **Other** from the **Start Time** drop-down menu.
   b. Select the start date of the time period to display from the date drop-down menu calendar.
   c. Specify the start time of the time period in the time field.

      To set the start time to the beginning of the day, select the **Start of Day** check box.

   d. Click **Update** to display the storage alerts using the specified start time.

   To specify the end time:

   a. Clear the **Use Current** check box.
   b. Select the stop date of the time period to display from the date drop-down menu calendar.
   c. Specify the stop time of the time period in the time field.

      To set the stop time to the end of the day, select the **End of Day** check box.

   d. Click **Update** to display the storage alerts using the specified end time.

Search for Storage Alerts

Use the **Search** field to find text in the list of storage alerts.

Steps

1. Click the **Monitoring** view
2. Click the **Storage Alerts** tab.
3. Enter the text to search for in the **Search** field.
4. To make the search case sensitive, select the **Match Case** check box.
5. To prevent the search from wrapping, clear the **Wrap** check box.
6. To match whole phrases within the alerts, select the **Full Match** check box.
7. To highlight all of the matches of the search, select the **Highlight** check box.
8. Click **Find Next** or **Find Previous** to search for the text.

   If a match is found, the first alert with matching text is selected from the list of storage alerts.

   If a match is not found, an **Error** dialog box appears and it displays the text that could not be found.

   NOTE: By default, when a search reaches the bottom of the list and **Find Next** is clicked, the search wraps around to the first match in the list. When a search reaches the top of the list and **Find Previous** is clicked, the search wraps around to the last match in the list.

Acknowledge Storage Center Alerts

Alerts can be acknowledged to indicate to the Storage Center that you have read the alert message and are aware of the problem.

Steps

1. Click the **Monitoring** view
2. Click the **Storage Alerts** tab.
3. Select the Storage Center alerts to acknowledge, then click **Acknowledge**. The **Acknowledge Alert** dialog box opens.

   NOTE: The option to acknowledge an alert will not appear if an alert has already been acknowledged.

4. Click **OK** to acknowledge the Storage Center alerts displayed in the **Acknowledge Alert** dialog box.

Send Storage Center Alerts and Indications to the Data Collector Immediately

By default, the Data Collector retrieves alerts and indications from a Storage Center at a regular interval. If you want alerts and indications to be displayed in Storage Manager immediately when they are triggered, configure a Storage Center to send them to the Data Collector.

Steps

1. Click the **Storage** view.
2. In the **Storage** view, select the Storage Center that you want to configure to send alerts and indications to the Data Collector.
3. In the **Summary** tab, click **Edit Settings**. The **Edit Storage Center Settings** dialog box opens.
4. Click the **Alerts and Logs** tab.
5. Select the **Send Alerts to Data Collector** checkbox.
6. Click **OK**.

Events

Events are messages that have been generated by events in Storage Manager.

You can view events on the **Events** tab or configure Storage Manager to email you when events occur.

Storage Manager Event Types

Storage Manager events are categorized by functionality and area.

The following table lists the types of Storage Manager events.

Event Name	Description
Automated Report Generation Errors	An error occurred when generating or storing an automated report.
Automated Reports Generated	New automated reports are generated.
Data Collector Error	An error occurred on the Data Collector.
Data Collector Exception	An exception occurred on the Data Collector.
Data Collector Resource Warning	One or more Data Collector resource alert conditions were reached.
Database Errors	Errors interacting with the database.

Event Name	Description
Directory Services Communication	The Data Collector cannot communicate with the Directory Services.
Exception Sending Email	Unable to send email to configured user.
Failed to Startup	The Data Collector service failed to startup.
Port Conflicts	Required ports are not available.
Remote Data Collector Down	Data Collector no longer communicating with the Remote side.
Replication Validation Errors	Automated replication validation errors found an error.
SMI-S Server Error	Error installing, starting, or running the SMI-S server
Space Recovery Report	Report of an automated space recovery run.
Storage Center Connect Timeout	Storage Center connect timeout threshold has been exceeded.
Storage Center Down	A Storage Center is no longer able to communicate with the Data Collector.
Storage Center Ping Timeout	Storage Center ping timeout threshold has been exceeded.
Storage Center Read Timeout	Storage Center read timeout threshold has been exceeded.
SupportAssist Errors	Sending information to the SupportAssist Server has had errors
Threshold Alerts	At least one threshold alert has exceeded its limit.

Example of a Storage Manager Data Collector alert

An alert is generated when the disk partition on which the Storage Manager Data Collector is located starts to run out of space.

- If the amount of disk space remaining is less than 25%, an event with a severity of `Warning` and the message `Disk partition containing Dell Storage Manager is running low on space` is displayed.
- If the amount of disk space remaining is less than 10%, an event with a severity of `Error` and the message `Disk partition containing Dell Storage Manager is running low on space` is displayed
- If the amount of disk space remaining is less than 3%, an event with a severity of `Exception` and the message `Disk partition containing Dell Storage Manager is full` is displayed.

Viewing Data Collector Events

Use the **Events** tab in the **Monitoring** view to display events collected by the Data Collector.

About this task

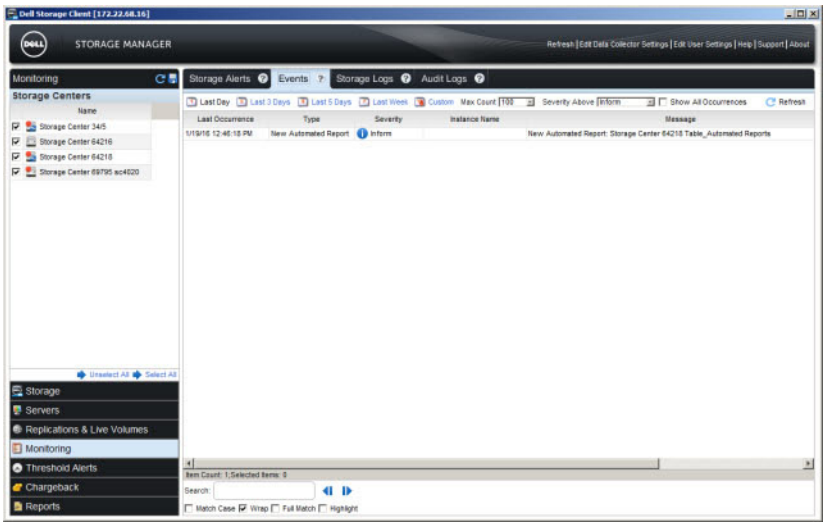


Figure 83. Storage Manager Events Tab

Display Storage Manager Events

View Storage Manager events on the **Events** tab.

Steps

1. Click the **Monitoring** view
2. Click the **Events** tab.
3. Select the check boxes of the storage systems to display and clear the check boxes of the storage systems to hide.

   The tab displays the events logged by the Storage Manager for the selected storage systems.
4. To specify the maximum number of events to display, select a value from the **Max Counts** drop-down list.
5. To specify the lowest severity of events to display, select a severity from the **Severity Above** drop-down list.
6. To display all occurrences of the events, select the **Show All Occurrences** check box.
7. To refresh the Storage Manager events log for the selected storage systems, click **Refresh** on the **Events** tab.

Filter Events by Storage System

By default, events are displayed for all managed storage systems.

Steps

1. Click the **Monitoring** view
2. Click the **Events** tab.
3. Use the **Storage Centers** pane to filter events by Storage Center.
   - To hide events for a single Storage Center, clear the check box for the Storage Center.
   - To display events for a Storage Center, select the check box for the Storage Center.
   - To hide events for all of the Storage Centers, click **Unselect All**.
   - To display events for all of the Storage Centers, click **Select All**.
4. Use the **PS Groups** pane to filter alerts by PS Series group.
   - To hide events for a single PS Series group, clear the check box for the group.

- To display events for a PS Series group that is deselected, select the check box for the group.
- To hide events for all of the PS Series groups, click **Unselect All**.
- To display events for all of the PS Series groups, click **Select All**.

Select the Date Range of Storage Manager Events to Display

You can view Storage Manager events for the last day, last 3 days, last 5 days, last week, last month, or specify a customtime period.

Steps

1. Click the **Monitoring** view
2. Click the **Events** tab.
3. Expand the Dell Storage Manager menu, and then click **Events**.
4. Select the date range of the Storage Manager events to display by clicking one of the following options:
   - **Last Day** – Displays the past 24 hours of event log data.
   - **Last 3 Days** – Displays the past 72 hours of event log data.
   - **Last 5 Days** – Displays the past 120 hours of event log data.
   - **Last Week** – Displays the past 168 hours of event log data.
   - **Last Month** – Displays the past month of event log data.
   - **Custom** – Displays options that allow you to specify the start time and the end time of the event log data to display.
5. If you clicked **Custom**, perform the following tasks to specify the start time and end time of the event log data to display.

   To specify the start time:

   a. Select **Other** from the **Start Time** drop-down menu.
   b. Select the start date of the time period to display from the date drop-down menu calendar.
   c. Specify the start time of the time period in the time field.

      To set the start time to the beginning of the day, select the **Start of Day** check box.

   d. Click **Update** to display the event log data using the specified start time.

   To specify the end time:

   a. Clear the **Use Current** check box.
   b. Select the stop date of the time period to display from the date drop-down menu calendar.
   c. Specify the stop time of the time period in the time field.

      To set the stop time to the end of the day, select the **End of Day** check box.

   d. Click **Update** to display the event log data using the specified end time.

Search for Storage Manager Events

Use the **Search** field to find text in the list of Storage Manager events.

Steps

1. Click the **Monitoring** view
2. Click the **Events** tab.
3. Enter the text to search for in the **Search** field.
4. To make the search case sensitive, select the **Match Case** check box.
5. To prevent the search from wrapping, clear the **Wrap** check box.
6. To only match whole words or phrases within the events, select the **Full Match** check box.
7. To highlight all of the matches of the search, select the **Highlight** check box.
8. Click **Find Next** or **Find Previous** to search for the text.

   If a match is found, the first event with matching text is selected from the list of Storage Manager events.

   If a match is not found, an **Error** dialog box appears and it displays the text that could not be found.

NOTE: By default, when a search reaches the bottom of the list and **Find Next** is clicked, the search wraps around to the first match in the list. When a search reaches the top of the list and **Find Previous** is clicked, the search wraps around to the last match in the list.

Configuring Email Alerts for Storage Manager Events

Storage Manager can be configured to send automated reports when monitored events occur.

About this task

To configure Storage Manager to send automated reports by email:

Steps

1. Configure the SMTP server settings on the Data Collector.
2. Add an email address to your user account.
3. Configure email notification settings for your user account.

Configure SMTP Server Settings

The SMTP server settings must be configured to allow Storage Manager to send notification emails.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Environment** tab and, then click the **SMTP Server** subtab.
5. Click **Edit**.
   The **SMTP Server Configuration** dialog box opens.
6. Configure the SMTP server settings by performing the following steps:
   a. In the **From Email Address** field, type the email address to display as the sender of emails from the Data Collector.
   b. In the **Host or IP Address** field, type the host name or IP address of the SMTP server.
   c. If the port number of the SMTP server is not 25, type the correct port number in the **Port** field.
   d. If the SMTP server requires authentication, select the **Authentication** checkbox, then type the user name and password in the **SMTP User Name** and **SMTP User Password** fields.
7. Click **OK**.

Configure an Email Address for Your User Account

To receive email notifications, you must specify an email address for your user account.

Prerequisites

The SMTP server settings must be configured for the Data Collector. If these settings are not configured, the Data Collector is not able to send emails.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box opens.
2. Type an email address for the user account in the **Email Address** field.
3. Select the format for emails from the **Email Format** drop-down menu.
4. To send a test message to the email address, click **Test Email** and click **OK**.
   Verify that the test message is sent to the specified email address,
5. Click **OK**.

Related tasks

Configure SMTP Server Settings on page 584

Configure Email Notification Settings for Your User Account

Make sure that Storage Manager is configured to send email notifications to your account for the events that you want to monitor.

Prerequisites

- The SMTP server settings must be configured for the Data Collector. If these settings are not configured, the Data Collector is not able to send emails.
- An email address must be configured for your user account.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box opens.
2. Click the **Manage Events** tab.
3. Select the checkbox for each event you want to be notified about.
4. Click **OK**.

Related tasks

Configure SMTP Server Settings on page 584
Configure an Email Address for Your User Account on page 585

Storage Logs

Storage logs are records of event activity on the managed storage systems. Use the **Storage Logs** tab to display and search for events in storage system logs.

Viewing Storage Logs

To display and search for events in the Storage Center logs, use the **Logs** tab in the **Storage** view or use the **Storage Logs** tab in the **Monitoring** view. To display and search for events in the PS Series group logs, use the **Events Logs** node in the **Monitoring** tab of the **Storage** view or use the **Storage Logs** tab in the **Monitoring** view.

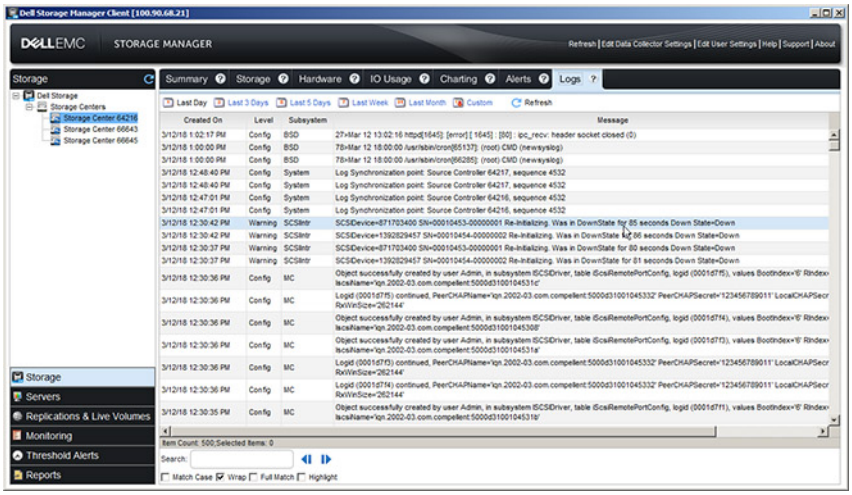


Figure 84. Storage Logs Tab

Display Events in the Storage Logs

Storage logs represent event activity on the selected storage systems.

Steps

1. Click the **Monitoring** view.
2. Click the **Storage Logs** tab.
3. Select the check boxes of the storage systems to display and clear the check boxes of the storage systems to hide.

   The **Storage Logs** tab displays event log data for the selected storage systems.
4. To refresh the log data for the selected storage systems, click **Refresh** on the **Storage Logs** tab.

Filter Storage Logs by Storage System

By default, storage logs are displayed for all managed storage systems.

Steps

1. Click the **Monitoring** view
2. Click the **Storage Logs** tab.
3. Use the **Storage Centers** pane to filter logs by Storage Center.
   - To hide logs for a single Storage Center, clear the check box for the Storage Center.
   - To display logs for a Storage Center that is deselected, select the check box for the Storage Center.
   - To hide logs for all of the Storage Centers, click **Unselect All**.
   - To display logs for all of the Storage Centers, click **Select All**.
4. Use the **PS Groups** pane to filter alerts by PS Series group.

- To hide events for a single PS Series group, clear the check box for the group.
- To display events for a PS Series group that is deselected, select the check box for the group.
- To hide events for all of the PS Series groups, click **Unselect All**.
- To display events for all of the PS Series groups, click **Select All**.

Select the Date Range of Log Events to Display

You can view log events for a specific time period.

Steps

1. Click the **Monitoring** view
2. Click the **Storage Logs** tab.
3. Select the date range of the event log data to display by clicking one of the following options:
   - **Last Day** – Displays the past 24 hours of event log data.
   - **Last 3 Days** – Displays the past 72 hours of event log data.
   - **Last 5 Days** – Displays the past 120 hours of event log data.
   - **Last Week** – Displays the past 168 hours of event log data.
   - **Last Month** – Displays the past month of event log data.
   - **Custom** – Displays options that allow you to specify the start time and the end time of the event log data to display.
4. If you clicked **Custom**, perform the following steps to specify the start time and end time of the event log data to display.

   To specify the start time:

   a. Select **Other** from the **Start Time** drop-down menu.
   b. Select the start date of the time period to display from the date drop-down menu calendar.
   c. Specify the start time of the time period in the time field.

      To set the start time to the beginning of the day, select the **Start of Day** checkbox.
   d. Click **Update** to display the event log data using the specified start time.

   To specify the end time:

   a. Clear the **Use Current** checkbox.
   b. Select the stop date of the time period to display from the date drop-down menu calendar.
   c. Specify the stop time of the time period in the time field.

      To set the stop time to the end of the day, select the **End of Day** checkbox.
   d. Click **Update** to display the event log data using the specified end time.
5. Click **(Column Filters)**.
   The **Filters** dialog box opens.
6. Click **Apply**.
7. Click **X** to close the **Filters** dialog box.

Search for Events in the Storage Logs

Use the **Search** field to search the list of log events.

Steps

1. Click the **Monitoring** view
2. Click the **Storage Logs** tab.
3. Enter the text to search for in the **Search** field.
4. To make the search case sensitive, select the **Match Case** check box.
5. To prevent the search from wrapping, clear the **Wrap** check box.
6. To only match whole words or phrases within the logs, select the **Full Match** check box.
7. To highlight all of the matches of the search, select the **Highlight** check box.
8. Click **Find Next** or **Find Previous** to search for the text.

   If a match is found, the first log entry with matching text is selected from the list of storage logs.

If a match is not found, an **Error** dialog box appears and it displays the text that could not be found.

NOTE: By default, when a search reaches the bottom of the list and **Find Next** is clicked, the search wraps around to the first match in the list. When a search reaches the top of the list and **Find Previous** is clicked, the search wraps around to the last match in the list.

Send Storage Center Logs to a Syslog Server

Modify the Storage Center settings to send logs directly to a syslog server.

Steps

1. In the Storage Center Summary view, click the **Storage** view.
2. In the **Storage** pane, select the Storage Center on which you want to configure the logging settings.
3. Click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
4. Click the **Alerts and Logs** tab.
5. Select **Send Logs Directly to Syslog Server**.
6. In the **Host or IP Address** field, type the host name or IP address of the syslog server.
7. Click **OK**.

Stop Sending Logs To a Syslog Server

Modify Storage Center settings to stop sending logs to a syslog server.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select a Storage Center.
3. Click **Edit Settings**. The **Edit Storage Center Settings** dialog box opens.
4. Click the **Alerts and Logs** tab.
5. Select **Do Not Send Logs**.
6. Click **OK**.

Apply Log Settings to Multiple Storage Centers

Log settings that are assigned to a single Storage Center can be applied to other Storage Centers.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with Administrator privileges.

Steps

1. Click the **Storage** view.
2. In the **Storage** pane, select the Storage Center that has the log settings you want to apply to other Storage Centers.
3. In the **Summary** tab, click **Edit Settings**. The **Edit Settings** dialog box appears.
4. Click the **Alerts and Logs** tab.
5. Select the **Apply these settings to other Storage Centers** check box.
6. Click **Apply**. The Select Storage Center dialog box appears.
7. Select the check box for each Storage Center to which you want to apply the settings.
8. When you are finished, click **OK**.

Audit Logs

Audit logs are records of logged activity that are related to the user accounts on the PS Series group.

Use the **Audit Logs** tab to display information specific to PS Series group user accounts.

Viewing Audit Logs

To display and search for PS Series group events in the audit logs, use the **Audit Logs** node in the **Storage** view or use the **Audit Logs** tab in the **Monitoring** view.

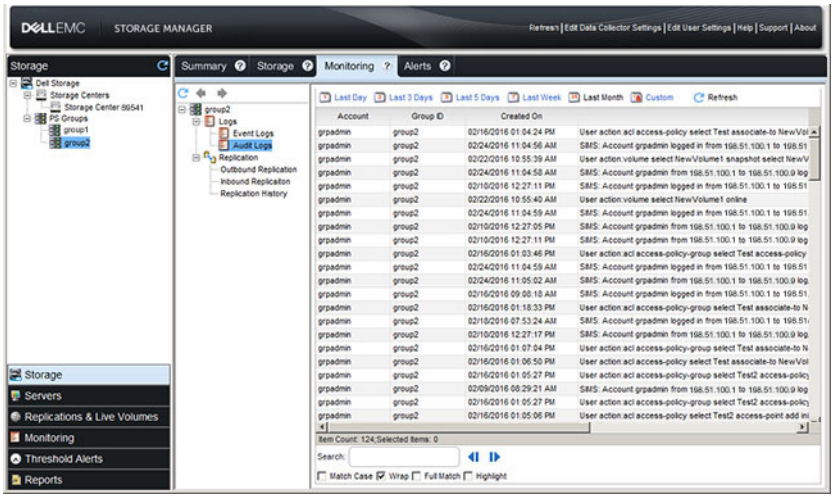


Figure 85. Audit Logs Node

Display Audit Logs

Audit logs represent user account activity on the selected PS Series groups.

Steps

1. Click the **Monitoring** view.
2. Click the **Audit Logs** tab.
3. Select the check boxes of the PS Series groups to display and clear the check boxes of the PS Series groups to hide.

   The **Audit Logs** tab displays user account activity for the PS Series groups.
4. To refresh the log data for the selected PS Series groups, click **Refresh** on the **Audit Logs** tab.

Filter Audit Logs by PS Series Group

By default, audit logs are displayed for all managed PS Series groups.

Steps

1. Click the **Monitoring** view
2. Click the **Audit Logs** tab.
3. Use the **PS Groups** pane to filter alerts by PS Series group.
   - To hide events for a single PS Series group, clear the check box for the group.
   - To display events for a PS Series group that is deselected, select the check box for the group.
   - To hide events for all of the PS Series groups, click **Unselect All**.
   - To display events for all of the PS Series groups, click **Select All**.

Select the Date Range of Audit Logs to Display

You can view audit logs for the last day, last 3 days, last 5 days, last week, or specify a custom time period.

Steps

1. Click the **Monitoring** view
2. Click the **Audit Logs** tab.
3. Select the date range of the audit log data to display by clicking one of the following:
   - **Last Day**: Displays the past 24 hours of audit log data.
   - **Last 3 Days**: Displays the past 72 hours of audit log data.
   - **Last 5 Days**: Displays the past 120 hours of audit log data.
   - **Last Week**: Displays the past 168 hours of audit log data.
   - **Custom**: Displays options that allow you to specify the start time and the end time of the audit log data to display.
4. If you clicked **Custom**, perform the following tasks to specify the start time and end time of the audit log data to display.

   To specify the start time:

   a. Select **Other** from the **Start Time** drop-down menu.
   b. Select the start date of the time period to display from the date drop-down menu calendar.
   c. Specify the start time of the time period in the time field.

      To set the start time to the beginning of the day, select the **Start of Day** check box.

   d. Click **Update** to display the audit log data using the specified start time.

   To specify the end time:

   a. Clear the **Use Current** check box.
   b. Select the stop date of the time period to display from the date drop-down menu calendar.
   c. Specify the stop time of the time period in the time field.

      To set the stop time to the end of the day, select the **End of Day** check box.

   d. Click **Update** to display the audit log data using the specified end time.

Search the Audit Logs

Use the **Search** field to search the audit logs.

Steps

1. Click the **Monitoring** view
2. Click the **Audit Logs** tab.
3. Enter the text to search for in the **Search** field.
4. To make the search case sensitive, select the **Match Case** check box.
5. To prevent the search from wrapping, clear the **Wrap** check box.
6. To only match whole words or phrases within the audit logs, select the **Full Match** check box.
7. To highlight all of the matches of the search, select the **Highlight** check box.
8. Click **Find Next** or **Find Previous** to search for the text.

   If a match is found, the first log entry with matching text is selected from the list of audit logs.

   If a match is not found, an **Error** dialog box appears and it displays the text that could not be found.

   NOTE: By default, when a search reaches the bottom of the list and **Find Next** is clicked, the search wraps around to the first match in the list. When a search reaches the top of the list and **Find Previous** is clicked, the search wraps around to the last match in the list.

Export Monitoring Data

Export Storage Center alerts, indications, logs, and Storage Manager events to a file using the **Save Monitoring Data** dialog box.

Steps

1. Click the **Monitoring** view
2. Click **Save Monitoring Data** in the **Monitoring** pane. The **Save Monitoring Data** dialog box appears.

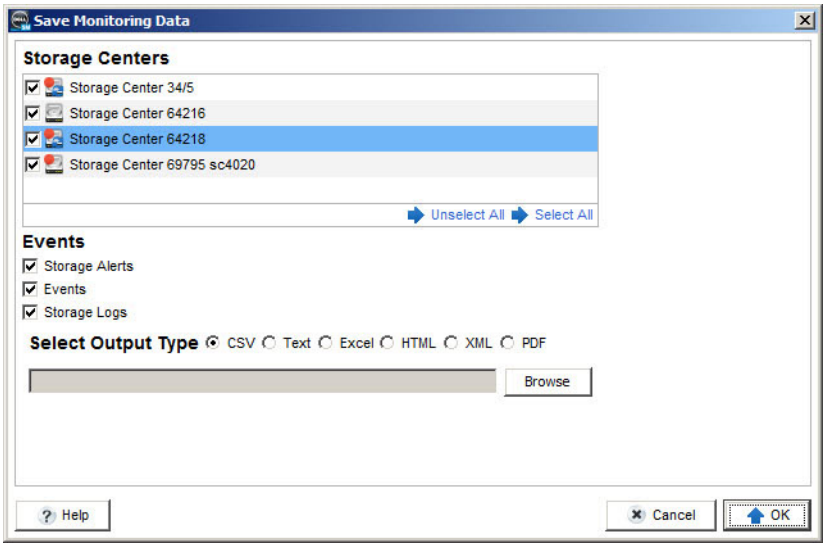


Figure 86. Save Monitoring Data Dialog Box

3. Select the Storage Centers from which to export the monitoring data.
   - To select all of the listed Storage Centers, click **Select All**.
   - To deselect all of the listed Storage Centers, click **Unselect All**.
4. Select the type(s) of monitoring data to export:
   - **Storage Center Alerts**: Error messages that have been generated by the selected Storage Centers.
   - **Storage Center Indications**: Conditions on the selected Storage Centers that may require direct user intervention to correct.
   - **Storage Manager Events**: Messages that have been generated by an event on the Storage Manager software.
   - **Storage Center Logs**: Records of activity on the selected Storage Centers.
5. Select a file type for the output: **CSV** (.csv), **Text** (.txt), **Excel** (.xls), **HTML** (.htm), **XML** (.xml), or **PDF** (.pdf).

   If the output is an Excel file, the numerical value displayed within the parentheses of the Alerts, Indications, and Logs worksheets is the serial number of the Storage Center.
6. Click **Browse** to specify the name of the file and the location to which to export the file, then click **Save**.
7. Click **OK**.

Configure Data Collection Schedules

Configure the interval at which the Data Collector collects monitoring data from Storage Centers.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.

d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **Data Collection** subtab.
5. Click **Edit**.
The **Data Collection** dialog box opens.
6. Configure the data collection schedules by performing the following steps:
a. To change how often I/O usage data is collected, select a period of time from the **IO Usage** drop-down menu.
b. To change how often replication usage data is collected, select a period of time from the **Replication Usage** drop-down menu.
c. To change how often storage usage data is collected, select a period of time from the **Storage Usage** drop-down menu.

   If **Daily** is selected from the Storage Usage drop-down menu, the time of the day that storage usage data is collected can be selected from the **Storage Usage Time** drop-down menu.

d. To change the number of days after which a log is expired, set the number of days in the **Alert Lifetime** field.
e. To change the number of days after which reporting data is expired, set the number of days in the **Reporting Data Lifetime** field.
7. Click **OK**.

22

Data Collector Management

The Storage Manager Data Collector is a service that collects reporting data and alerts from managed Storage Centers.

When you access the Data Collector using a web browser, the Data Collector management program Unisphere Central for SC Series opens. Unisphere Central manages most functions of the Data Collector service.

Topics:

- Access the Data Collector View
- Configuring Data Collector Settings
- Managing Available Storage Centers
- Managing Available PS Series Groups
- Managing Available FluidFS Clusters
- Managing the Storage Manager Virtual Appliance
- Migrate a Microsoft SQL Server Database
- Uninstalling the Data Collector

Access the Data Collector View

Perform the following steps to access the Data Collector view in Unisphere Central.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.

Configuring Data Collector Settings

Use Unisphere Central to configure and update Data Collector properties and settings.

Configuring General Settings

The Data Collector **General** settings include a configuration summary, security, settings, port identification and database selection.

Restart the Data Collector

Use Unisphere Central to stop and restart the Data Collector.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **General** tab, and then select the **Summary** subtab.
5. Click **OK**.
   The **Data Collector Restart** dialog box opens.
6. Click **Yes**.
   The Data Collector service stops and restarts.

Enable the Chargeback Feature

To enable the Chargeback feature, add a Chargeback license file or product key to the Data Collector.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **General** tab, and then click the **Summary** subtab.

5. In the **License Information** section, click **Submit License**.
   The **License information** dialog box opens.
6. To enable the Chargeback feature using a license file:
   a. Select the **License File (*.lic)** radio button.
   b. Click **Browse** and navigate to the location of the license file.
   c. Select the license file and click **Open**
   d. Click **OK**.
7. To enable the Chargeback feature using a product key:
   a. Select the **Product Key** radio button.
   b. Type the product key in the **Product Key** field.
   c. Click **OK**.

Change Storage Center Timeout Settings

Use the **Edit Advanced Settings** to set Storage Center timeout values.

About this task

NOTE: The Data Collector must be restarted to apply timeout setting changes.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **General** tab, and then click the **Summary** subtab.
5. Expand the **Advanced** area located below the **License Information** section.
6. Click **Edit**.
   The **Edit Advanced Settings** dialog box opens.
7. Set the timeout and delay settings as needed:
   - **Storage Center Connection Timeout** – Maximum time that the Storage Center waits for a response for queries sent to the Data Collector.
   - **Storage Center Connection Delay** – Maximum time that the Storage Center waits to successfully connect to the Data Collector.
   - **Storage Center Ping Timeout** – Maximum time that the Storage Center waits for a response to a ping command to the Data Collector.
   - **Storage Center Read Timeout** – Maximum time that the Storage Center waits while attempting read data from the Data Collector.
8. Click **OK**.
   The **Data Collector Restart** dialog box opens.
9. Click **Yes**.
   The Data Collector service stops and restarts.

Set the Maximum Memory for a Data Collector on a Windows Server

Use the **Edit Advanced Settings** dialog box to set the maximum amount of memory to allocate to a Data Collector on a Windows server.

About this task

NOTE: The Data Collector must be restarted to save changes to the maximum memory setting.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **General** tab, and then click the **Summary** subtab.
5. Expand the **Advanced** area located below the **License Information** section.
6. Click **Edit**.
   The **Edit Advanced Settings** dialog box opens.
7. Type the maximum amount of memory to allocate to the Data Collector in the **Maximum Server Memory Usage** box.
8. Click **OK**.
   The **Data Collector Restart** dialog box opens.
9. Click **Yes**.
   The Data Collector service stops and restarts.

Set the Maximum Memory for a Data Collector on a Virtual Appliance

Use the **Edit Settings** dialog box the vSphere Web Client to set the maximum amount of memory to allocate to a Data Collector on a Virtual Appliance.

Steps

1. In the vSphere Web Client, right-click on the Storage Manager Virtual Appliance and select **Power** > **Shut Down Guest OS** to shut down the Virtual Appliance.
2. Right-click on the Virtual Appliance and select **Edit Settings**.
   The **Edit Settings** dialog box opens.
3. Type the maximum amount of memory to allocate for the Virtual Appliance in the **Memory** field.
4. Right-click on the Storage Manager Virtual Appliance and select **Power** > **Power On** to start the Virtual Appliance

Select a Network Adapter

The Data Collector attempts to automatically select the network adapter to use by default. If the host server has multiple network adapters, automatic detection can fail and the network adapter must be selected manually.

Prerequisites

The network adapter must have connectivity to the devices managed by Storage Manager Client.

NOTE: The Data Collector must be restarted to save network adapter changes.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **General** tab, and then click the **Summary** subtab.
5. Expand the **Advanced** area located below the **License Information** section.
6. Click **Edit**.
   The **Edit Advanced Settings** dialog box opens.
7. To select a network adapter, clear the **Automatically Select Network Adapter** checkbox and select a network adapter from the drop-down menu.
   To allow the Data Collector to select a network adapter, select the **Automatically Select Network Adapter** checkbox.
8. Click **OK**.
   The **Data Collector Restart** dialog box opens.
9. Click **Yes**.
   The Data Collector service stops and restarts.

Configure a Custom SSL Certificate

Configure a custom SSL certificate to avoid certificate errors when connecting to the Data Collector. An SSL certificate is also required to communicate with a directory service using LDAP with the StartTLS extension or the LDAPS protocol.

Prerequisites

- The Subject CN value in the custom SSL certificate must contain the IP address or fully qualified domain name (FQDN) of the Data Collector server.
- The custom SSL certificate must be signed by a Certificate Authority (CA) that is trusted by the hosts in your network.
  NOTE: If the certificate is signed by an intermediate CA instead of a root CA, then the entire certificate chain must be imported in PEM format. The certificate chain must also include the root CA apart from all the intermediate CAs.
- The certificate public key file must be in DER or PEM format.
- The certificate private key file must be in PKCS #12 format.
- You must know the alias and password for the private key.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **General** tab, and then click the **Security** subtab.
5. To generate SSL certificates:
   a. Click **Generate Certificate**.
      The **Generate Certificate** dialog box is displayed.
   b. Select the type of certificate to generate from the **Certificate type** drop-down menu.
      The options are:
      - **All certificates** - Generates Data Collector and VASA Provider certificates.
      - **DSM Server** - Generates Data Collector certificates.
      - **VASA Server** - Generates VASA Provider certificates.
   c. Select the new IP address or FQDN of the Data Collector from the **Certificate Subject** drop-down menu.
   d. If you are generating a VASA Provider certificate, type the username and password of a Data Collector user with Administrator privileges in the **DSM User Name** and **Password** fields.
   e. Click OK.
6. To upload registered SSL certificates, click **Edit**.
   The **Register Certificate** dialog box opens.
7. To upload a public key file.
   a. Click **Choose File** located to the right of the **Public Key** text.
   b. Browse to the location of the public key file, and then select it.
   c. Click **Open**.
      The **Public Key** field is populated with the path to the public key file.
8. To upload the private key file.
   a. Click **Browse** located to the right of the **Private Key** text.
   b. Browse to the location of the private key file, and then select it.
   c. Click **Open**.
      The **Private Key** field is populated with the path to the public key file.
9. Type the name of the entry in the PKCS #12 private key file to use as the private key in the In the **Alias** field.
10. Type the password for the private key file in the **Password** field.
11. Click **OK**.
    The **Data Collector Restart** dialog box opens.
12. Click **Yes**.
    The Data Collector service stops and restarts.

Configure a Login Banner Message

Set a login banner to display a message to users when they connect to a Data Collector.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
      https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
      The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.

The **Data Collector** view is displayed.

4. Click the **General** tab, and then click the **Security** subtab.
5. In the Login Message section, click **Edit**.
   The **Login Message** dialog box opens.
6. Type a message to display on the login screen in the **Login Banner Message** field.
7. Click **OK**.

Configure Data Collector Ports

Use the Ports tab to modify Data Collector ports to avoid port conflicts.

About this task

NOTE: The Data Collector must be restarted to apply port changes.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **General** tab, and then select the **Ports** subtab.
5. Click **Edit**.
   The **Edit Port** dialog box opens.
6. Select the name of the service to edit.
   - Web Server Service (cannot be disabled)
   - Server Agent Service
   - SMI-S Service (Windows installations only)
   - VASA Service
7. Select or clear the **Enabled** checkbox to enable or disable a port.
8. If the port is enabled, type a port number in the **Port** field.
9. Click **OK**.
   The **Data Collector Restart** dialog box opens.
10. Click **Yes**.
    The Data Collector service stops and restarts.

Change Data Collector Data Source

Change the data source if you want to use a different database to store Storage Manager data.

About this task

The Change Data Source option re-configures an existing primary Data Collector to use a new database.

CAUTION: To prevent data corruption, make sure that another Data Collector is not using the new database.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **General** tab, and then click the **Database** subtab.
5. Click **Change Data Source**.
   The **Change Data Source** dialog box opens.
6. Select the type of database from the **Database Type** drop-down menu.
7. Type the host name or IP address of the database server in the **Hostname or IP Address** field.
8. Type the port number of the database server in the **Port** field.
9. Type the user name and password of a user account that has database administrator rights in the **User Name** and **Password** fields.
10. If **Auto-Create Database Password** is selected, the default password for the compmsauser database user is `R3p0r!cty4sgs`.

    To specify a password for the compmsauser database user, select **Specify Database Password** and type the password in the **DSM DB User Password** and **Confirm Password** fieldd.
11. To migrate historical data from the current database to the new database, clear the **Do not migrate any data from previous data source** checkbox.
    - To migrate I/O usage data, select the **Migrate IO Usage Data** checkbox, then select either **Day** or **Week** from the drop-down menu and specify the number of days or weeks of I/O usage data to move in the **Migrate Last** field.
    - To migrate storage data, select the **Migrate Storage Usage Data** checkbox, then select either **Day** or **Week** from the drop-down menu and specify the number of days or weeks of storage data to move in the **Migrate Last** field.
    - To migrate replication data, select the **Migrate Replication Usage Data** checkbox, then select either **Day** or **Week** from the drop-down menu and specify the number of days or weeks of replication data to move in the **Migrate Last** field.
12. Click **OK**.

Change the Database Connection

Use this procedure to change database server information such as the hostname, IP Address, port, username, and password.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.

3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **General** tab, and then click the **Database** subtab.
5. Click **Change Connection**.
   The **Change Data Connection** dialog box opens.
6. Type the host name or IP address of the database server in the **Database Server** field.
7. Type port number of the database server in the **Database Port** field.
8. Type the user name and password of a user account that has database administrator rights in the **User Name** and **Password** fields.
9. Click **OK**.
   The **Data Collector Restart** dialog box opens.
10. Click **Yes**.
    The Data Collector service stops and restarts.

Configuring Environment Settings

The Data Collector **Environment** settings include remote data collector information, server settings and directory service settings.

View Remote Data Collector Settings

If a Remote Data Collector has been configured, use Storage Manager to view the settings and status.

Prerequisites

Remote Data Collector has been configured for the system.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Environment** tab, and then click the **Remote Data Collector** subtab.
   The settings and status of the Remote Data Collector are displayed.

Access the Remote Data Collector

If a Remote Data Collector has been configured, use Storage Manager to access the Remote Data Collector.

Prerequisites

Remote Data Collector has been configured for the system.

Steps

1. Connect to the Data Collector.

a. Open a web browser.
b. Type the address of the Data Collector in the web browser using the following format:
https://*data_collector_host_name_or_IP_address*:3033/
c. Press Enter.
The Unisphere Central login page is displayed.
d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Environment** tab, and then click the **Remote Data Collector** subtab.
The settings and status of the Remote Data Collector are displayed.
5. Click the url in the **RDC URL** field.
The Unisphere Central login page for the Remote Data Collector is displayed.

Configure SMTP Server Settings

The SMTP server settings must be configured to allow Storage Manager to send notification emails.

Steps

1. Connect to the Data Collector.
a. Open a web browser.
b. Type the address of the Data Collector in the web browser using the following format:
https://*data_collector_host_name_or_IP_address*:3033/
c. Press Enter.
The Unisphere Central login page is displayed.
d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Environment** tab and, then click the **SMTP Server** subtab.
5. Click **Edit**.
The **SMTP Server Configuration** dialog box opens.
6. Configure the SMTP server settings by performing the following steps:
a. In the **From Email Address** field, type the email address to display as the sender of emails from the Data Collector.
b. In the **Host or IP Address** field, type the host name or IP address of the SMTP server.
c. If the port number of the SMTP server is not 25, type the correct port number in the **Port** field.
d. If the SMTP server requires authentication, select the **Authentication** checkbox, then type the user name and password in the **SMTP User Name** and **SMTP User Password** fields.
7. Click **OK**.

Configure Server Usage Data Update Frequency

Configure the Server Agent to update usage data every 30 minutes.

Steps

1. Connect to the Data Collector.
a. Open a web browser.

b. Type the address of the Data Collector in the web browser using the following format:
https://*data_collector_host_name_or_IP_address*:3033/
c. Press Enter.
The Unisphere Central login page is displayed.
d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Environment** tab, and then click the **Server Agent** subtab.
5. Click **Edit**.
The **Server Agent** dialog box opens.
6. Select the **Periodically Update Usage Data** checkbox.
When selected, server usage data is updated every 30 minutes.
7. Type the number of days of usage data to include in the **Usage Data Range** field
8. Click **OK**.

Configuring Monitoring Settings

The **Monitoring** settings include SupportAssist access and configuration, automated report generation, data collection settings, and support data configuration.

Configure a Proxy Server for a Data Collector

Configure the proxy server settings to allow the Data Collector to use a proxy server when sending diagnostic data using SupportAssist.

Steps

1. Connect to the Data Collector.
a. Open a web browser.
b. Type the address of the Data Collector in the web browser using the following format:
https://*data_collector_host_name_or_IP_address*:3033/
c. Press Enter.
The Unisphere Central login page is displayed.
d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **SupportAssist** subtab.
5. Expand the **Proxy Server** area.
6. Click **Edit** in the **Proxy Server** area.
The **Network Proxy Configuration** dialog box opens.
7. Select the **Enabled** checkbox to enable the proxy server.

NOTE: The proxy server must be enabled to configure the settings.

8. Type the host name or IP address of the proxy server in the **Host or IP Address** field.
9. Type the port number of the proxy server in the **Port** field.

10. If the proxy server requires a user name and password, type a user name and password in the **User Name** and **Password** fields.
11. Click **OK**.
    The **Change Values** dialog box opens, which states that the Data Collector service must be stopped and restarted.
12. Click **Yes**.
    The Data Collector service stops and restarts.

Storage Center Automated Reports

The information that Storage Center displays in an automated report depends on the configured Automated Report settings.

Report Frequency – Automated reports are generated at the end of each day, week, or month, depending on the options selected in Automated Reports from the Storage Center Settings area. You can also generate automated reports manually, at any time.

The following table lists the available Storage Center reports related to volumes, servers, and disks:

Report Type	Description
Automated Reports	Generates a report for the following: • **Storage Center Summary**: Displays information about storage space and the number of storage objects on the Storage Center. • **Disk Class**: Displays information about storage space on each disk class. • **Disk Power On Time**: Displays information about how long each disk has been powered on. • **Alerts**: Displays Storage Center alerts. • **Volume Storage**: Displays volume storage statistics. • **Replications**: Displays information about replications. • **Live Volumes**: Displays information about Live Volumes.

Automated Table Reports	Generates a report for the following:
	• **I/O Reports**: Displays I/O information about the following:
	  ○ Most Active Volumes
	  ○ Most Active Disks
	  ○ Most Active Servers
	• **Storage Reports**: Displays detailed information about the following:
	  ○ Volume Reports: Volume, Volume Folder, Volume Growth, and Volume Profile
	  ○ Server Reports: Server and Server Folder
	  ○ Disk Reports: Disk, Disk Folder, Disk Class, and Disk Tier
	  ○ Storage Type Reports: Pressure Report

Set Up Automated Reports for All Storage Centers

Configure automated report settings on the Data Collector if you want to use the same report settings for all managed Storage Centers. Configure the global settings first, and then customize report settings for individual Storage Centers as needed.

Steps

1. In the top pane of Storage Manager, click **Edit Data Collector Settings**
   The **Edit Data Collector Settings** page is displayed.
2. Click the **Automated Reports** tab.
3. Select the checkboxes in the **Automated Report Settings** area to specify which reports to generate and how often to generate them.
4. Select the checkboxes in the **Automated Table Report Settings** area to specify which reports to generate and how often to generate them.

   NOTE: Automated table reports can be saved in a public directory or attached to automated emails, but they do not appear in the **Reports** view.

5. Select the checkboxes in the **Automated FluidFS Report Settings** area to specify which reports to generate and how often to generate them.

6. Set the **Automated Report Options**
   a. To export the reports to a public directory, select the **Store report in public directory** checkbox and enter the full path to the directory in the **Directory** field.

      NOTE: The directory must be located on the same server as the Data Collector.

      NOTE: Automated reports cannot be saved to a public directory when using a Virtual Appliance.

   b. To email the reports selected in the **Automated Reports Settings** area, select the **Attach Automated Reports to email** checkbox.
   c. To email the reports selected in the **Automated Table Reports Settings** area, select the **Attach Table Reports to email** checkbox.
   d. Select the file format for **Table Reports** from the **File Type for Table Reports** drop-down menu.
7. Click **OK**.

Related tasks

Configure Chargeback or Modify Chargeback Settings on page 596
Configure Storage Manager to Email Reports on page 594

Testing Automated Reports Settings

You can manually generate reports to test the configured automated report settings without waiting for the reports to be generated automatically. By default, Storage Manager generates reports into a folder named for the day when the report was generated.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **Automated Reports** subtab.
5. Review the current report settings:
   - If the settings are acceptable, click **Generate**.
   - To change the report settings, click **Edit**, adjust the settings, and click **Generate**.

   The **Generate Reports Now** dialog box opens.
6. Select the checkboxes of the reports to generate.
7. Click **OK**. The reports are generated and the **Generate Reports** dialog box closes.

   NOTE: Generating a report overwrites previously generated reports in the folder for that day. To prevent these reports from being overwritten, specify a different directory in the **Automated Report Options** area of the **Automated Reports** dialog box.
8. Click **OK**.

Configure Data Collection Schedules

Configure the interval at which the Data Collector collects monitoring data from Storage Centers.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **Data Collection** subtab.
5. Click **Edit**.
   The **Data Collection** dialog box opens.
6. Configure the data collection schedules by performing the following steps:
   a. To change how often I/O usage data is collected, select a period of time from the **IO Usage** drop-down menu.
   b. To change how often replication usage data is collected, select a period of time from the **Replication Usage** drop-down menu.
   c. To change how often storage usage data is collected, select a period of time from the **Storage Usage** drop-down menu.

      If **Daily** is selected from the Storage Usage drop-down menu, the time of the day that storage usage data is collected can be selected from the **Storage Usage Time** drop-down menu.

   d. To change the number of days after which a log is expired, set the number of days in the **Alert Lifetime** field.
   e. To change the number of days after which reporting data is expired, set the number of days in the **Reporting Data Lifetime** field.
7. Click **OK**.

Enable Debug Logs

Enable debug logs to gather additional information for troubleshooting purposes. Do not set debug log options unless instructed to do so by technical support.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **Support** subtab.

5. Click **Edit**.
   The **Edit Support** dialog box opens.
6. Select the checkboxes of the debug logs to enable.
7. Click **OK**.

Configure Log File Limits

Configure the size limits for the log files.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **Support** subtab.
5. Click **Edit**.
   The **Edit Support** dialog box opens.
6. To modify the maximum file size of the Data Collector debug logs, change value in the **Maximum Log File Size** field.
7. To modify the maximum number of log files for each Data Collector debug log type, change the value in the **Maximum Log Files Per Logger** field.
8. To modify the number of days after which a log file is expired, change the period of time in the **Log File Lifetime** field.
9. Click **OK**.

Clear Debug Logs

Clear the debug log files to delete all Storage Manager debug log files.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **Support** subtab.
5. Click **Clear All Debug Logfiles**.
   A confirmation dialog box opens.

6. Click **Yes**.

Export Configuration and Log Data for Troubleshooting

Export configuration and log data as a compressed file if it is requested by technical support.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **Support** subtab.
5. Click **Gather Support Data**.
   The **Gather Support Data** dialog box opens.
6. Choose the time period of the data to send by selecting the start time and end time.
7. To send the configuration and log data to technical support for evaluation, select **Send to SupportAssist**.
8. To save configuration and log data to the Data Collector, select **Download to file system**.
9. Click **OK**.
   - If you selected **Send to SupportAssist**, the data is gathered and sent to a SupportAssist server.
   - If you selected **Download to file system**, the support data is saved as a compressed file to the following location on the Data Collector server: `C:\Program Files\Dell EMC\Storage Manager\msaservice\node\package\node_modules\dsm-ui-plugin\DsmSupportDump`.

Configuring Virtual Appliance Settings

Use the **Virtual Appliance** tab to configure network, proxy server, and time settings for a Virtual Appliance.

Configure Network Settings for a Virtual Appliance

Use the **Network Configuration** dialog box to configure network settings and enable or disable SSH on the Virtual Appliance.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.

3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Virtual Appliance** tab, and then click the **Network** subtab.
5. Click **Edit**.
   The **Network Configuration** dialog box opens.
6. In the **Hostname** field, type the host name of the Virtual Appliance.
7. In the **Domain** field, type the domain name of the Virtual Appliance.
8. To enable the Secure Shell (SSH), select the **Enable SSH** checkbox.
9. Select the network configuration type from the **Configuration** drop-down menu.
   - **DHCP** - Dynamic IP address
   - **Static** - Static IP address
10. If the network configuration is set to Static:
    a. Type the IP address of one or more Domain Name System (DNS) servers in the **DNS** field.

       NOTE: Separate multiple IP addresses using commas.

    b. To configure IPv4 network settings, select the **IPv4** radio button, and type the IP Address, netmask, and gateway in the associated fields.

       To configure IPv6 network settings, select the **IPv6** radio button, and type the IP Address, gateway, and prefix length in the associated fields.
11. Click **OK**.

Configure Time Settings for a Virtual Appliance

Configure the time settings to set the time zone and specify how to synchronize the time on the Virtual Appliance. It is recommended to set the time zone to the local time zone in which the Virtual Appliance is located.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
      https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
      The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Virtual Appliance** tab, and then click the **Time** subtab.
5. Click **Edit**. The **Time Configuration** dialog box opens.
6. Select a time zone for the Virtual Appliance from the **Timezone** drop-down menu.
7. To sync the time on the Virtual Appliance with Network Time Protocol (NTP) servers, select **Sync with NTP Servers (recommended)** and type the name of one or more NTP servers in the **NTP Servers** field.
8. To sync the time on the Virtual Appliance with the ESX host select **Sync with ESX Host**.
9. Click **OK**.

Managing Available Storage Centers

Use the Data Collector **Users & System** tab to manage available Storage Centers that have been mapped to one or more Data Collector user accounts.

Delete an Available Storage Center

Remove a Storage Center when you no longer want to manage it from the Data Collector. If a Storage Center is removed from all Data Collector user accounts, historical data for the Storage Center is also removed.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, and then select the **Storage Centers** subtab.
5. Select the Storage Center to delete.
6. Click **Delete Storage Center**.
   A warning message is displayed.
7. Click **Yes**.

Clear All Data for a Storage Center

Clear data for a Storage Center to remove historical data from Storage Manager.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, and then select the **Storage Centers** subtab.
5. Select the Storage Center for which you want to clear all data.
6. Click **Clear Storage Center Data**.
   A warning message is displayed.

7. Click **Yes**.

Remove a Storage Center from a Data Collector User Account

To prevent the user from viewing and managing a Storage Center, remove the Storage Center from the Data Collector user account .

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, and then select the **Storage Centers** subtab.
5. Select the Storage Center from which you want to delete a User/Storage Center map.
6. In the **User/Storage Center Maps** pane, select the user to unmap from the Storage Center.
7. Click **(Delete)**.
   A warning message is displayed.
8. Click **Yes**.

Managing Available PS Series Groups

Use the **PS Groups** subtab to manage available PS Series groups that have been mapped to a Data Collector user account.

Delete an Available PS Series Group

Remove a PS Series group when you no longer want to manage it from Storage Manager.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **PS Groups** subtab.

5. Select the PS Series group to delete.
6. Click **Delete PS Group**.
7. Click **Yes**.

Remove a PS Series Group from a Data Collector User

To prevent a user from managing a PS Series group, remove the PS Series group from the Data Collector user account.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **PS Groups** subtab.
5. In the **User/PS Groups Maps** pane, select the user to unmap from the PS Series group.
6. Click **(Delete User/PS Group Map)**.
7. Click **Yes**.

Managing Available FluidFS Clusters

Use the **FluidFS Clusters** subtab to manage available FluidFS clusters.

Delete an Available FluidFS Cluster

Remove a FluidFS cluster when you no longer want to manage it from Storage Manager.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **FluidFS Clusters** subtab.
5. Select the FluidFS cluster to delete.

6. Click **(Delete System)**.
   A confirmation dialog box is displayed.
7. Click **Yes**.

Remove a FluidFS Cluster from a Data Collector User Account

To prevent a user from viewing and managing the FluidFS cluster, remove the FluidFS cluster from the Data Collector user account.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **FluidFS Clusters** subtab.
5. Select the FluidFS cluster for which you want to delete a User/FluidFS cluster map.
6. In the **User/FluidFS Cluster Maps** pane, select the user you want to unmap from the FluidFS cluster.
7. Click **(Delete User/FluidFS Cluster Map)**.
   A confirmation dialog box is displayed.
8. Click **Yes**.

Managing the Storage Manager Virtual Appliance

The Storage Manager Virtual Appliance console includes configuration options that allow you to configure network settings, view diagnostic data, and update the Storage Manager Virtual Appliance.

Log in to the Storage Manager Virtual Appliance CLI

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. At the login prompt, type **em** and press Enter.
3. At the **EM Username** prompt, type the user name of the Data Collector local admin user and press Enter.
4. At the **EM Password** prompt, type the password of the Data Collector local admin user and press Enter.
   The Storage Manager Virtual Appliance CLI is displayed.

Configure Virtual Appliance Settings

Use the Configuration menu in the Storage Manager Virtual Appliance CLI to change network and partition settings for the Storage Manager Virtual Appliance.

Configure an NTP Server

A network time protocol (NTP) server provides the time and date to the Storage Manager Virtual Appliance.

Prerequisites

The NTP server must be accessible from the Storage Manager Virtual Appliance.

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. Log in to the Storage Manager Virtual Appliance CLI.
3. Press 2 and Enter to enter the **Configuration** menu.
4. Press 1 and Enter to enter the **NTP** menu.
5. Press 1 and Enter to launch the **NTP** setup.
6. Type the IP address or host name of an NTP server.
7. Press Enter.

Configure IPv4 Settings

Use the Storage Manager Virtual Appliance console to modify the IPv4 network settings.

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. Log in to the Storage Manager Virtual Appliance CLI.
3. Press 2 and Enter to display the **Configuration** menu.
4. Press 2 and Enter to start the **Network IPv4** setup.
5. Press 1 or 2 to enable or disable DHCP, then press Enter.
6. To modify the IP address, type an IP address, and then press Enter.
7. To modify the netmask, type a new netmask, and then press Enter.
8. To modify the gateway address, type a new gateway address, and then press Enter.
9. To assign a new hostname, type a hostname, and then press Enter.
10. To modify the domain name used by the Storage Manager Virtual Appliance, type a new domain name, and then press Enter.
11. To add a new DNS server, type the IP address of one or more DNS servers. If there are multiple IP addresses, separate them with a comma, and then press Enter.
12. Press 1 to confirm the changes and press Enter.
13. Press Enter to complete the configuration.

Configure IPv6 Settings

Use the Storage Manager Virtual Appliance console to modify the IPv6 network settings.

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. Log in to the Storage Manager Virtual Appliance CLI.
3. Press 2 and Enter to display the **Configuration** menu.
4. Press 2 then Enter to start the **Network IPv6** setup.
5. Press 1 or 2 to enable or disable DHCP, then press Enter.

6. To assign a new hostname, type a hostname, then press Enter.
7. To modify the domain name used by the Storage Manager Virtual Appliance, type a new domain name, and then press Enter.
8. To add a new DNS server, type the IP address of one or more DNS servers. If there are multiple IP addresses, separate them with a comma, and then press Enter.
9. Press 1 to confirm the changes and press Enter.
10. Press Enter to complete the configuration.

Enable SSH for the Virtual Appliance

Use the Storage Manager Virtual Appliance console to enable SSH communication with the Storage Manager Virtual Appliance.

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. Log in to the Storage Manager Virtual Appliance CLI.
3. Press 2 and Enter to display the **Configuration** menu.
4. Press 4 and Enter to display the SSH configuration.
5. Enable or disable SSH.
   - To enable SSH, press 1 and Enter.
   - To disable SSH, press 2 and Enter.
6. Press Enter.

Enable or Disable the Support Account for the Virtual Appliance

Use the Storage Manager Virtual Appliance console to enable or disable the support account for the Storage Manager Virtual Appliance.

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. Log in to the Storage Manager Virtual Appliance CLI.
3. Press 2 and Enter to display the **Configuration** menu.
4. Press 5 and Enter to display the **Support Account Enable/Disable** setup.
5. Enable or disable the support account.
   - To enable the support account, press 1 and Enter.
   - To disable the support account, press 2 and Enter.
6. Press Enter.

Modify the Size of a Virtual Appliance Partition

There are three partitions for the Storage Manager Virtual Appliance: Data Collector, database, and root partitions.

About this task

The Data Collector partition contains data used for running the Storage Manager Virtual Appliance. The database partition contains database data stored for the Data Collector. The Storage Manager Virtual Appliance allows you to expand the Data Collector and database partitions. In the VMware vSphere Client the Data Collector partition is labeled Hard disk 2 and the database partition is labeled Hard disk 3.

Steps

1. Using the VMware vSphere Client, connect to the vCenter server hosting the Storage Manager Virtual Appliance.
2. Rignt-click on the Storage Manager Virtual Appliance then select **Edit Settings**.
   The **Virtual Hardware** dialog box opens.
3. Select the hard disk for the partition you wish to expand.
   - For the Data Collector partition, select **Hard disk 2**.

- For the database partition, select **Hard disk 3**.

4. Modify the size of the disk to one of the suggested sizes.
   - For the Data Collector partition, change the disk size to 15 GB, 20 GB, or 40 GB.
   - For the database partition, change the disk size to 20 GB, 40 GB, or 80 GB.
5. Click **OK**.
   The server expands the disk size.
6. Launch the console for the Storage Manager Virtual Appliance.
7. Log in to the Storage Manager Virtual Appliance.
8. Press 2 and Enter to display the **Configuration** menu.
9. Press 6 and Enter to resize a partition.
10. Select which partition to resize.
    - Press 1 and Enter to select the Data Collector partition.
    - Press 2 and Enter to select the database partition.

    The Storage Manager Virtual Appliance expands the partition to the available size of the disk.

View a Summary of the Configuration Settings

Use the Storage Manager Virtual Appliance console to view a summary of the Storage Manager Virtual Appliance configuration settings.

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. Log in to the Storage Manager Virtual Appliance CLI.
3. Press 2 and Enter to display the **Configuration** menu.
4. Press 7 and Enter.
   The Storage Manager Virtual Appliance CLI displays a summary of the configuration settings.
5. Press Enter to return to the **Configuration** menu.

View Diagnostic Information for the Virtual Appliance

Using the Diagnostic menu in the Storage Manager Virtual Appliance console you can view information used to diagnose network connectivity issues with the Storage Manager Virtual Appliance.

Ping an IP Address

Use the Storage Manager Virtual Appliance CLI to ping an IP address from the Storage Manager Virtual Appliance.

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. Log in to the Storage Manager Virtual Appliance CLI.
3. Press 3 and Enter to display the **Diagnostics** menu.
4. Press 1 to ping an IPv4 address or press 2 to ping an IPv6 address, and then press Enter.
5. Type the host name or IP address to ping.
6. Press Enter.
   The Storage Manager Virtual Appliance CLI displays the results of the ping command.
7. Press Enter to return the **Diagnostics** menu.

View Routing Information

Use the Storage Manager Virtual Appliance CLI to view routing information for the Storage Manager Virtual Appliance.

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. Log in to the Storage Manager Virtual Appliance CLI.
3. Press 3 and Enter to display the **Diagnostics** menu.
4. Press 3 and Enter.
   The Storage Manager Virtual Appliance CLI displays a table of routing information.
5. Press Enter to return to the **Diagnostics** menu.

View the Hosts Table

Use the Storage Manager Virtual Appliance CLI to view the hosts table for the Storage Manager Virtual Appliance.

About this task

The hosts table shows network information for the Storage Manager Virtual Appliance.

Steps

1. Using the VMware vSphere Client, launch the console for the Storage Manager Virtual Appliance.
2. Log in to the Storage Manager Virtual Appliance CLI.
3. Press 3 and Enter to display the **Diagnostics** menu.
4. Press 4 and Enter.
   The Storage Manager Virtual Appliance CLI displays the hosts table.
5. Press Enter to return to the **Diagnostics** menu.

Migrate a Microsoft SQL Server Database

If the database server is Microsoft SQL Server 2012, 2014, or 2016, the Data Collector database can be migrated to a new Microsoft SQL Server.

Steps

1. Back up the database on the original Microsoft SQL Server.
2. Set up a new Microsoft SQL Server and configure it to use mixed mode authentication (SQL Server and Windows Authentication mode).
3. Perform a restore of the database on the new Microsoft SQL Server.
4. After the database is restored, create the required database user.
   a. Create a database user named **compmsauser**, but do not assign the user to a schema .
   b. Set the password of the **compmsauser** database user to the password it was assigned in the previous database.
      - If you did not previously change the password, the default password is `R3p0r!cty4sgs`.
      - If you do not remember the password or you want to use a different password, you must enter the new password when you run the **Change Data Source** wizard in Step 6.
5. Run the following query on the `compmsadb` database:

   ```
   sp_change_users_login 'update_one', 'compmsauser', 'compmsauser'
   ```

6. After the query finishes, use the Data Collector to change the data source to the new database.

   NOTE: If you changed the password, select the **Use Custom Password** checkbox and type the password in the **Custom Password** field.

Uninstalling the Data Collector

On the server that hosts the Data Collector, use the Windows **Programs and Features** control panel item to uninstall the **Storage Manager Data Collector** application.

Deleting Old Data Collector Databases

Delete the old Data Collector database if you have migrated the database to a different database server or if you have removed the Data Collector from your environment.

Clean up a MySQL Database

Remove Storage Manager data from the MySQL database and reinstall the Data Collector.

Steps

1. Enter the following SQL commands as an Admin user:

```
Drop Database compmsadb;
DELETE FROM mysql.user WHERE User = 'compmsauser';
DELETE FROM mysql.db WHERE user = 'compmsauser';
FLUSH PRIVILEGES;
```

2. Reinstall the Storage Manager Data Collector.

Clean up a Microsoft SQL Database

Remove Storage Manager data from the database and reinstall the Data Collector.

Steps

1. Enter the following SQL commands as an Admin user:

```
Drop Database compmsadb;
```

```
EXEC SP_DropLogin 'compmsauser';
```

2. Reinstall the Storage Manager Data Collector.

23

Storage Manager User Management

Use the Data Collector to add new users and manage existing users. To change preferences for your user account, use the Storage Manager Client.

Topics:

- Storage Manager User Privileges
- Authenticating Users with an External Directory Service
- Managing Local Users Through the Data Collector
- Managing Local User Password Requirements
- Managing User Settings with the Storage Manager Client

Storage Manager User Privileges

The Data Collector controls user access to Storage Manager functions and associated Storage Centers based on the privileges assigned to users: Reporter, Volume Manager, or Administrator. The following tables define Storage Manager user level privileges with the following categories.

NOTE: Storage Manager user privileges and Storage Center user privileges share the same names but they are not the same. Storage Center user privileges control access to Storage Centers, and Storage Manager users control access to Storage Manager functionality.

Reporter Privileges

The Reporter privilege level is the most limited type of user in Storage Manager.

A Reporter user can view most features of Storage Manager. However, a Reporter user is not able to manage, create, or edit any feature. In addition, a Reporter user cannot view FluidFS clusters, SupportAssist properties, Data Collector properties, or Storage Profiles.

NOTE: A Storage Manager Reporter user can map Storage Centers to other Reporter users if they have Storage Manager Reporter credentials.

Volume Manager Privileges

The Volume Manager privilege level is similar to the Administrator level, but has more restrictions.

A Volume Manager user is able to view, manage, and add/create most objects in Storage Manager. However, a Volume Manager user does not have access to Data Collector properties.

Administrator Privileges

The Administrator privilege level is the most powerful user profile in Storage Manager.

An Administrator user has full access to all of the Storage Manager features.

NOTE: A user account that is created with Administrator access cannot be downgraded to Reporter / Volume Manager rights.

Related concepts

Storage Center User Privileges and User Groups on page 92

Authenticating Users with an External Directory Service

The Data Collector can be configured to authenticate Storage Manager users with an Active Directory or OpenLDAP directory service. If Kerberos authentication is also configured, users can log in with the Client automatically using their Windows session credentials.

Storage Manager access can be granted to directory service users and groups that belong to the domain to which the Data Collector is joined. For Active Directory, access can also be granted to users and groups that belong to domains in the same forest, as well as domains that belong to forests for which one-way or two-way trusts are configured.

Configuring an External Directory Service

Before users can be authenticated with an external directory service, the Data Collector must be configured to use the directory service.

Configure the Data Collector to Use a Directory Service

Configure the Data Collector to use an Active Directory or OpenLDAP directory service.

Prerequisites

- An Active Directory or OpenLDAP directory service must be deployed in your network environment.
- The directory service must meet specific configuration requirements.
  - **Active Directory**: The directory service must be configured to use Kerberos authentication.
  - **OpenLDAP**: The directory service must be configured to use LDAP with the StartTLS extension or LDAPS (LDAP over SSL).
- If the directory service is OpenLDAP, the SSL certificate public key file (DER or PEM encoding) for the directory server must be exported and transferred to the server that hosts the Data Collector.
- The Data Collector must have network connectivity to the directory service.
- DNS SRV records must be correctly configured in your environment to allow the Data Collector to determine how to interact with the directory service. If SRV records are not defined or are improperly configured, you must configure the directory service settings manually.
- The Data Collector requires a user that has permission to query the directory service. For Active Directory, this user must also have a User Principal Name attribute (*username@example.com*) on his or her entry in the directory.
- To use Kerberos authentication, you must provide the user name and password for a directory service user who has Administrator privileges or use an existing service account.
- If a directory service is configured and you want to reconfigure the Data Collector to use a directory service in a different domain, the directory services configuration must be disabled and applied before you continue.
- To authenticate Active Directory users that belong to domains in a different forest, a one-way or two-way trust must be configured between the local forest and remote forest.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.

The **Data Collector** view is displayed.

4. Click the **Environment** tab and then select the **Directory Service** subtab.
5. Click **Edit**.
   The **Service Settings** dialog box opens.
6. Configure LDAP settings.
   a. Select the **Enabled** checkbox.
   b. In the **Domain** field, type the name of the domain to search.

      NOTE: If the server that hosts the Data Collector belongs to a domain, the **Domain** field is automatically populated.

   c. In the **Authentication Bind DN** field, type the Distinguished Name or User Principal Name of the user that the Data Collector uses to connect to and search the LDAP server. The user name Administrator is not allowed.
      - *Example Distinguished Name:* CN=Firstname Lastname,CN=users,DC=corp,DC=Company,DC=COM
      - *Example User Principal Name*: username@example.com

   d. In the **Authentication Bind Password** field, type the password for the auth bind Distinguished Name.
   e. If you modified the **Domain** field, click **Discover** to locate the directory service for the specified domain.
7. (Optional) Manually configure the directory service settings.
   a. From the **Type** drop-down menu, select **Active Directory** or **OpenLDAP**.
   b. In the **Directory Servers** field, type the fully qualified domain name (FQDN) of each directory server on a separate line.

      NOTE: To verify that the Data Collector can communicate with the specified directory server(s) using the selected protocol, click **Test**.

   c. In the **Base DN** field, type the base Distinguished Name for the LDAP server. This name is the starting point when searching for users.
   d. In the **Connection Timeout** field, type the maximum time (in minutes) that the Data Collector will wait while attempting to connect to an LDAP server.
8. (Optional) Configure Kerberos authentication. To allow users to log in with the Client automatically using his or her Windows session credentials, Kerberos authentication must be configured.
   a. Select the **Kerberos Enabled** checkbox.
   b. In the **Kerberos Domain Realm** field, type the Kerberos realm to authenticate against. In Windows networks, this realm is usually the Windows domain name in uppercase characters.
   c. (OpenLDAP only) Type the host name or IP address of the Key Distribution Center (KDC) in the **KDC Host Name or IP Address** field.
   d. In the **Data Collector Host Name** field, type the fully qualified domain name (FQDN) of the server that hosts the Data Collector.
9. (Optional — Open LDAP only) If Transport Layer Security (TLS) is enabled, upload a Certificate Authority PEM file...
   a. Browse to the location of the PEM file, select the file, and click Open. .
      The **Upload TLS Certificate** dialog box opens.

      NOTE: If you select the wrong PEM file, click **Upload Certificate** in the **Upload TLS Certificate** dialog box to select a new file

   b. c. Click **OK** to upload the certificate.
10. (Active Directory Only) To register the Data Collector on the domain, select **Register the Data Collector on the domain**.
    a. Type the user name and password of a domain administrator.
       These credentials are used only to register the Data Collector and are not saved.
    b. Click **OK**.
11. To use an existing service account, select **Use an existing service account for joining the domain**.
    a. Type the user name and password for the service account.

       NOTE: The existing service account must include a *servicePrincipalName* attribute with the following values in the form:

       HTTP/<host name>dc.<domain>@<realm>

       HTTP/<host name>dc.<domain>

       These values can be set using the Microsoft setspn.exe tool or the equivalent.

    b. Click **OK**.

Troubleshoot Directory Service Discovery

The Data Collector attempts to automatically discover the closest directory service based on the network environment configuration. Discovered settings are written to a text file for troubleshooting purposes. If discovery fails, confirm that the text file contains values that are correct for the network environment.

Steps

1. On the server that hosts the Data Collector, use a text editor to open the file `C:\Program Files\Dell EMC\Storage Manager\msaservice\directory_settings.txt`.
2. Confirm that the values listed in the `directory_settings.txt` file match the network environment.
3. If the file contains incorrect values, make configuration changes to correct the issue.
   a. Confirm that the server that hosts the Data Collector is joined to the correct Domain.
   b. Make sure that DNS SRV records are correctly configured.
   c. Use Data Collector to discover the directory service again.
4. If the previous step did not correct the issue, select the **Enable Manual Configuration** checkbox and manually configure directory service settings. If necessary, contact technical support for assistance.

Scan for Domains in Local and Trusted Forests

If domains are added or removed from the local forest, or if two-way forest trusts between the local forest and one or more remote forests are added or removed, use the Data Collector to scan for domains.

Prerequisites

The Data Collector must be configured to authenticate users with an Active Directory directory service and Kerberos.

NOTE: Authentication attempts for Active Directory users may fail while a rescan operation is in progress.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Environment** tab and then select the **Directory Service** subtab.
5. Click **Rescan**. A message appears to inform you that scanning succeeded or failed.
6. Click **OK**.

Related tasks

Troubleshoot Directory Service Discovery on page 654

Grant Access to Directory Service Users and Groups

To allow directory users to log in to Storage Manager, add directory service users and/or user groups to Storage Manager user groups.

Add Directory Groups to a Storage Manager User Group

Add a directory group to a Storage Manager user group to allow all users in the directory group to access Storage Manager. Access can be granted to groups that belong to the domain to which the Data Collector is joined, domains in the same forest, and domains that belong to forests for which two-way forest trusts are configured. Directory service groups are not supported for one-way trust domains.

Prerequisites

The Data Collector must be configured to authenticate users with an external directory service.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab and then select the **Users & User Groups** subtab.
5. Select the Storage Manager user group to which you want to add directory groups.
6. Click **Add Directory User Groups**.
   The **Add Directory User Groups** dialog box opens.
7. (Multi-domain environments only) From the **Domain** drop-down menu, select the domain that contains the directory groups to which you want to grant access.
8. Select each directory group that you want to add to the Storage Manager user group.
9. When you are finished, click **OK**. The directory groups that are associated with the Storage Manager group appear on the **User Groups** subtab.

Related tasks

Configure the Data Collector to Use a Directory Service on page 652

Add a Directory User to a Storage Manager User Group

Add a directory user to a Storage Manager user group to allow the directory user to access Storage Manager. Access can be granted to users that belong to the domain to which the Data Collector is joined, domains in the same forest, and domains that belong to forests for which one-way or two-way trusts are configured.

Prerequisites

The Data Collector must be configured to authenticate users with an external directory service.

Steps

1. Connect to the Data Collector.

a. Open a web browser.
b. Type the address of the Data Collector in the web browser using the following format:
https://*data_collector_host_name_or_IP_address*:3033/
c. Press Enter.
The Unisphere Central login page is displayed.
d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Users & System** tab and then select the **Users & User Groups** subtab.
5. Select the Storage Manager user group to which you want to add a directory user.
6. Click **Add Directory Users**.
The **Add Directory Users** dialog box opens.
7. In the **Directory Users** field, type the name of each directory user that you want to add.
   - For OpenLDAP, the user name format is supported (example: *user*).
   - For Active Directory, the following user name formats are supported:
     - User name (example: *user*)
     - User Principal Name (example: *user*@*domain*)

     NOTE: To add users that belong to a domain other than the domain for which the Data Collector is configured, use the User Principal Name format.
8. Click **Check Names** to verify that the specified users exist in the directory service. A message appears.

   NOTE: Checking names is not supported on domains for which a one-way trust is configured.

9. Click **OK** to close the message.
10. If any of the specified directory user names could not be verified, correct the names and then click **Check Names** again.
11. When you are finished, click **OK**. The **Add Directory Users** dialog box closes, and the directory users that are associated with the selected Storage Manager user group appear on the **User Groups** subtab.

Related tasks

Configure the Data Collector to Use a Directory Service on page 652

Revoke Access for Directory Service Users and Groups

To revoke access to Storage Manager for a directory service user or group, remove the directory group or user from Storage Manager user groups.

Remove a Directory Service Group from a Storage Manager User Group

Remove a directory service group from a Storage Manager user group to prevent directory users in the group from accessing Storage Manager.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.

e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab and then select the **Users & User Groups** subtab.
5. Click the **User Groups** tab.
6. Select the Storage Manager user group to which the directory group is added.
7. Click the **Directory Groups** subtab.
8. Select the directory service group for which you want to revoke access, then click **Delete**.
   The **Delete Directory User Group** dialog box opens.
9. Click **Yes**.

Remove a Directory Service User from a Storage Manager User Group

Remove a directory service user from a Storage Manager user group to prevent the directory user from accessing Storage Manager.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab and then select the **Users & User Groups** subtab.
5. Click the **User Groups** tab.
6. Select the Storage Manager user group to which the directory group is added.
7. Click the **Users** subtab.
8. Select the directory service group user for which you want to revoke access, then click **Delete User**. The **Delete Directory User** dialog box opens.
9. Click **Yes**.

Disable External Directory Service Authentication

Disable external directory service authentication to prevent directory users from authenticating.

About this task

CAUTION: Disabling directory service authentication removes all directory service users and groups from Storage Manager. If you choose to reenable directory service authentication at a later time, all directory users and user groups must be granted access again.

Steps

1. Connect to the Data Collector.

a. Open a web browser.
b. Type the address of the Data Collector in the web browser using the following format:
https://*data_collector_host_name_or_IP_address*:3033/
c. Press Enter.
The Unisphere Central login page is displayed.
d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Environment** tab and then select the **Directory Service** subtab.
5. Click **Edit**.
The **Service Settings** dialog box opens.
6. Clear the **Enabled** checkbox.
7. Click **OK**.

Managing Local Users Through the Data Collector

Storage Manager users and mappings to Storage Center can be configured on the **Users** tab on the Data Collector view.

Update the Information Displayed on the Users & System Tab

Refresh the **Users & System** tab to display changes to user accounts and user/Storage Center maps.

Steps

1. In the Data Collector, click the **Users** tab.
2. Click **Refresh**. The **Users & System** tab reappears after the data is refreshed.

Create a User

Create a user account to allow a person access to Storage Manager.

Steps

1. Connect to the Data Collector.
a. Open a web browser.
b. Type the address of the Data Collector in the web browser using the following format:
https://*data_collector_host_name_or_IP_address*:3033/
c. Press Enter.
The Unisphere Central login page is displayed.
d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.
5. Click **+(New User)**.
The **Create User** dialog box opens.

6. Enter information for the new user.
   a. Type the user name of the user in the **User Name** field.
   b. (Optional) Type the email address of the user in the **Email Address** field.
   c. Select the role to assign to the user from the **Role** drop-down menu.
   d. Select a language from the **Preferred Language** drop-down menu.
   e. Enter a password for the user in the **Password** and **Confirm Password** fields.
   f. To force the user to change the password after the first login, select the **Requires Password Change** checkbox.
7. Click **OK**.

Related concepts

Storage Manager User Privileges on page 651

Configure or Modify the Email Address of a User

An email address must be configured if you want Storage Manager to send email notifications to the user.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.
5. Select the user to modify and click **(Edit Settings)**.
   The **User Settings** dialog box opens.
6. Enter the email address of the user in the **Email Address** field.
7. Click **OK**.

Change the Privileges Assigned to a User

You can change the privileges for a user account by changing the user role.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.

3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.
5. Select the user to modify and click **(Edit Settings)**.
   The **User Settings** dialog box opens.
6. Select the role to assign to the user from the **Role** drop-down menu.

Related concepts

Storage Manager User Privileges on page 651

Change the Preferred Language for a Storage Manager User

The preferred language for a Storage Manager user determines the language displayed in automated reports and email alerts from the Data Collector. Reports displayed in the UI and generated by a user request will not use the preferred language.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.
5. Select the user to modify and click **(Edit Settings)**.
   The **User Settings** dialog box opens.
6. From the **Preferred Language** drop-down menu, select a language.
7. Click **OK**.

Force the User to Change the Password

You can force a user to change the password the next time he or she logs in.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.

3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.
5. Select the user to modify and click **(Edit Settings)**.
   The **User Settings** dialog box opens.
6. Select the **Requires Password Change** checkbox.
7. Click **OK**.

Change the Password for a User

You can change the password for any user account using Storage Manager.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.
5. Select the user to modify and click **Change User Password**.
   The **Change User Password** dialog box opens.
6. Type the admin password in the **Authorization Password** field
7. Enter a new password for the user in the **New Password** and **Confirm Password** fields.
8. Click **OK**.

Set Storage Center Mappings for a Reporter User

Storage Center mappings can be set only for users that have Reporter privileges. Users that have Administrator or Volume Manager privileges manage their own Storage Center mappings using Unisphere Central.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.

4. Click the **Users & System** tab, then select the **Users** subtab.
5. Select the Reporter user to modify.
6. In the lower pane on the **Storage Centers** tab, click + (Select Storage Center Mappings).
   The **Select Storage Center Mappings** dialog box opens.
7. Select the checkbox of each Storage Center to map to the user.

   Clear the checkbox of each Storage Center to unmap from the user.
8. Click **OK**.

Delete a User

Delete a user account to prevent the user from viewing and managing the Storage Center.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.
5. Select the user you want to delete.
6. Click **(Delete User)**.
   A confirmation dialog box opens.
7. Click **Yes**.

Delete a Storage Center Mapping for a User

Remove a Storage Center map from a user account to prevent the user from viewing and managing the Storage Center.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.

5. Select the user for which you want to delete a Storage Center mapping.
6. Select the Storage Center to unmap from the user on the **Storage Center** pane.
7. Click **(Delete Storage Center Map)**.
   A confirmation dialog box opens.
8. Click **Yes**.

Unlock a Local User Account

After a user enters an incorrect password beyond the Account Lockout threshold, that user account is locked. Use Storage Manager to unlock the account.

Prerequisites

- Password Configuration is enabled.
- A user account is locked.

NOTE: If the locked account is a Storage Manager administrator account, contact technical support for assistance in unlocking the account.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Users & User Groups** subtab.
5. Select the locked user account.
6. Click **Unlock User**.
   A confirmation dialog box opens.
7. Click **Yes**.

Related tasks

Configure Local Storage Manager User Password Requirements on page 663

Managing Local User Password Requirements

Manage the password expiration and complexity requirements for Unisphere from the Data Collector view.

Configure Local Storage Manager User Password Requirements

Set local user password requirements to increase the complexity of local user passwords and improve the security of Storage Manager.

Steps

1. Connect to the Data Collector.

a. Open a web browser.
b. Type the address of the Data Collector in the web browser using the following format:
https://*data_collector_host_name_or_IP_address*:3033/
c. Press Enter.
The Unisphere Central login page is displayed.
d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.

2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Password Configuration** subtab.
5. Click **Edit**.
The **Password Configuration** dialog box opens.
6. Select **Enabled**.
7. Set the password requirements.

NOTE: For user interface reference information, click Help.

8. Click **OK**.

Apply Password Requirements to Storage Center Users

Storage Manager local user password requirements can be applied to Storage Center users.

Prerequisites

Password Configuration must be enabled.

Steps

1. Connect to the Data Collector.
a. Open a web browser.
b. Type the address of the Data Collector in the web browser using the following format:
https://*data_collector_host_name_or_IP_address*:3033/
c. Press Enter.
The Unisphere Central login page is displayed.
d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Password Configuration** subtab.
5. Click **Edit**. The **Password Configuration** dialog box opens.
6. Select the Storage Centers to which to apply the password requirements.
7. Click **OK**.

Related tasks

Configure Local Storage Manager User Password Requirements on page 663

Reset Password Aging Clock

The password aging clock determines when a password expires based on the minimum and maximum age requirements. Reset the password aging clock to start the password aging clock from the current date and time.

Prerequisites

Password Configuration must be enabled.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Users & System** tab, then select the **Password Configuration** subtab.
5. Click **Edit**. The **Password Configuration** dialog box opens.
6. Select the **Reset Aging Clock** checkbox.
7. Click **OK**.

Related tasks

Configure Local Storage Manager User Password Requirements on page 663

Require Users to Change Passwords

The new password requirements apply to new user passwords only. Existing user passwords may not follow the password requirements. Require users to change passwords at next login so that the password complies with the password requirements.

Prerequisites

Password Configuration must be enabled.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.

4. Click the **Users & System** tab, then select the **Password Configuration** subtab.
5. Click **Edit**. The **Password Configuration** dialog box opens.
6. Select the **Requires Password Change** checkbox.
7. Click **OK**.

Related tasks

Configure Local Storage Manager User Password Requirements on page 663

Managing User Settings with the Storage Manager Client

Use the Storage Manager Client to change preferences for your user account.

Change User Password

The password for the current user can be changed from the **Edit User Settings** dialog box.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**.
   The **Edit User Settings** dialog box opens.
2. On the **General** tab, click **Change Password**.
   The **Change Password** dialog box opens.
3. Type the current password of the user in the **Authorization Password** field.
4. Type a new password in the **New Password** and **Confirm Password** fields.
5. Click **OK** to save changes to the password and close the **Change Password** dialog box.
6. Click **OK** to close the **Edit User Settings** dialog box.

Configure Email Settings

The email settings for the current user can be changed from the **Edit User Settings** dialog box.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**.
   The **Edit User Settings** dialog box opens.
2. Select the **General** tab.
3. Edit the email settings.
   - **Email Address** – Type the email address for the current user.
   - **Email Format** – Select Plain text or HTML.
   - (Optional) **Test Email** – Click to send an email message to the address entered in the Email Address field.
4. Click **OK**.

Change the Preferred Language

The preferred language for a Storage Manager user determines the language displayed in automated reports and email alerts from the Data Collector. Reports displayed in the UI and generated by a user request will not use the preferred language.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box appears.
2. From the **Preferred Language** drop-down menu, select a language.
3. Click **OK**.

Configure Charting Options

Threshold alert levels and Storage Center alerts can be configured to appear on charts for the current user, and chart colors can be changed for the current user on the **Charting Options** section of the **General** tab.

Related concepts

Configuring User Settings for Charts on page 316

Configure Client Options

The default view, formatting of storage units , and warning/error threshold percentages can be configured for the current user on the **Client Options** section of the **General** tab.

Specify the Default View to Display in the Storage Manager Client

You can choose the view that is first displayed after you log in to the Client.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box opens.
2. On the **General** tab, select the view to display by default from the **Default View** drop-down.
3. Click **OK** to save changes and close the **Edit User Settings** dialog box.

Specify the Preferred Wizard Style

You can choose the style of creation wizard you see when creating a volume. The guided multi-step wizard provides a detailed, step by step method of creating new volumes.

About this task

The default for the SCv2000 series controller is the guided multiple-step wizard. The default for all other devices is the unguided single-step wizard.

Steps

1. In the top pane of the Dell Storage Manager Client, click **Edit User Settings**.
   The **Edit User Settings** dialog box appears.
2. On the **General** tab, select your preferred wizard style from the **Preferred Wizard Style** drop-down.
3. Click **OK** to save changes and close the **Edit User Settings** dialog box.

Configure the Units for Display

Storage units can be shown in megabytes, gigabytes, terabytes, or an automatically chosen unit of measure that best fits the data.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**.
   The **Edit User Settings** dialog box opens.
2. On the **General** tab, select how to display the storage units from the **Storage Units Formatting** drop-down menu:
   - **Automatic** – The units that are most appropriate for the displayed values are automatically selected.
   - **Always show in MB** – All storage units are displayed in megabytes.
   - **Always show in GB** – All storage units are displayed in gigabytes.
   - **Always show in TB** – All storage units are displayed in terabytes.
3. Click **OK**.

Change the Warning Percentage Threshold

The warning percentage threshold specifies the utilization percentage at which storage objects indicate a warning.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box opens.
2. On the **General** tab, enter a new utilization percentage at which storage objects indicate a warning in the **Warning Percentage Threshold** field.
3. Click **OK** to save changes and close the **Edit User Settings** dialog box.

Change the Error Percentage Threshold

The error percentage threshold specifies the utilization percentage at which storage objects indicate an error.

Steps

1. In the top pane of the Storage Manager Client, click **Edit User Settings**. The **Edit User Settings** dialog box opens.
2. On the **General** tab, enter a new utilization percentage at which storage objects indicate an error in the **Error Percentage Threshold** field.
3. Click **OK** to save changes and close the **Edit User Settings** dialog box.

24

SupportAssist Management

SupportAssist sends data to technical support for monitoring and troubleshooting purposes. You can configure SupportAssist to send diagnostic data automatically, or you can send diagnostic data manually using SupportAssist when needed. SupportAssist settings can be configured for all managed Storage Centers or individually for each Storage Center.

Topics:

- Data Types that Can Be Sent Using SupportAssist
- Configure SupportAssist Settings for the Data Collector
- Configure SupportAssist Settings for a Single Storage Center
- Manually Sending Diagnostic Data Using SupportAssist
- Saving SupportAssist Data to a USB Flash Drive
- Managing SupportAssist Settings
- CloudIQ

Data Types that Can Be Sent Using SupportAssist

Storage Manager can send reports, Storage Center data, and FluidFS cluster data to technical support.

The following table summarizes the types of data that can be sent using SupportAssist.

SupportAssist Data Type	Description	SupportAssist Method
I/O Usage report	Summarizes read and write I/O performance for one or more Storage Centers	Automatic or manual
Storage Usage report	Summarizes storage use and growth for one or more Storage Centers	Automatic or manual
Replication report	Summarizes the status of replications	Automatic or manual
Storage Center configuration	Sends all Storage Center configuration information	Manual
Storage Center logs	Sends Storage Center logs	Manual
FluidFS cluster summary	Summarizes all FluidFS cluster configuration information	Automatic
FluidFS cluster events	Sends FluidFS cluster events	Automatic
FluidFS cluster diagnostics	Sends full system diagnostics, including summary information for the FluidFS cluster configuration, services, and logs	Automatically triggered on critical events. Manually triggered when an administrator runs the FluidFS cluster diagnostics

Configure SupportAssist Settings for the Data Collector

Modify the SupportAssist settings for the Data Collector.

Steps

1. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
2. Click **Data Collector**.
   The **Data Collector** view is displayed.
3. Click the **Monitoring** tab, and then click the **SupportAssist** subtab.
4. Click **Edit**. The **SupportAssist** dialog box opens.
   a. Select the frequency to send usage data from the **Send Interval** drop-down menu.
   b. Select usage reports to send from the **Global Reporting SupportAssist Settings** area.

   NOTE: The **Send Interval** setting is ignored for **Storage Usage** reports. Instead, **Storage Usage** reports are sent to technical support on a daily basis.
5. Click **OK**.

Configure SupportAssist Settings for a Single Storage Center

Modify SupportAssist Settings for a single Storage Center.

Steps

1. Click the **Storage** view.
2. In the **Storage** view navigation pane, select a Storage Center.
3. In the top pane of the Storage Manager Client, click **Edit Settings**.
   The **Edit Data Collector Settings** dialog box opens.
4. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane of Unisphere Central.
5. Click **Summary**.
   The **Summary** view is displayed.
6. Click the **SupportAssist** tab.
   The SupportAssist settings dialog box opens.
7. Select the frequency to send data from the **Frequency** drop-down box.
8. Select usage reports to send in the **Global Reporting SupportAssist Settings**.

   NOTE: The default collection schedule for **Storage Usage** data is daily at midnight. Therefore, the default **Send Interval** setting of **4 Hours** is ignored for **Storage Usage** reports. Instead, **Storage Usage** reports are sent to technical support on a daily basis by default.
9. Select your preference for receiving software updates from the **Software Update Mode** drop-down menu.
10. If your network requires hosts to use a proxy server to reach the Internet, configure a proxy server for SupportAssist:
    a. Select the **Enabled** checkbox next to **Web Proxy Settings** to enable a proxy server.
    b. Specify the IP address and port for the proxy server.
    c. If the proxy server requires authentication, type valid credentials in the **User Name** and **Password** fields.
11. Click **OK**.

Manually Sending Diagnostic Data Using SupportAssist

You can send diagnostic data manually using SupportAssist for multiple Storage Centers or for a specific Storage Center. If a Storage Center does not have Internet connectivity or cannot communicate with the SupportAssist servers, you can export the data to a file and send it to technical support manually.

Manually Send Diagnostic Data for Multiple Storage Centers

You can send diagnostic data for multiple Storage Centers from the Data Collector.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
   https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
   The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **SupportAssist** subtab.
5. Click **Send SupportAssist Data Now**.
   The **Send SupportAssist Data Now** dialog box opens.
6. In the **Storage Centers** area, select the checkboxes of the Storage Centers for which you want to send SupportAssist data to technical support.
7. In the **Reports** area, select the checkboxes of the Storage Center reports to send.
8. In the **Time Range** area, choose the period of time for which you want to send data.
   a. In the **Start Date** fields, specify the start date and time.
   b. To specify an end date, clear the **Use Current Time For End Date** checkbox and specify a date and time in the **End Date** fields.
   To use the current date and time as the end date, select the **Use Current Time For End Date** checkbox.
9. Click **OK**.

Send Diagnostic Data for a Single Storage Center

You can send Storage Center diagnostic data using SupportAssist from the Storage Center settings.

Prerequisites

The Storage Center must be added to Storage Manager using a Storage Center user with the Administrator privilege.

Steps

1. Click the **Storage** view.
2. In the **Storage** view navigation pane, select a Storage Center.
3. In the right pane, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
4. Click the **SupportAssist** tab.

5. Click **Send SupportAssist Information Now**.
   The **Send SupportAssist Information Now** dialog box opens.
6. In the **Reports** area, select the checkboxes of the Storage Center reports to send.
7. In the **Time Range** area, specify the period of time for which you want to send data.
   a. In the **Start Date** fields, specify the start date and time.
   b. To specify an end date, clear the **Use Current Time For End Date** checkbox and specify a date and time in the **End Date** fields.
      To use the current date and time as the end date, select the **Use Current Time For End Date** checkbox.
8. In the **Storage Center** area, select the checkboxes for the types of Storage Center data to send.
9. Click **OK**.
   The dialog box displays SupportAssist progress and closes when the process is complete.
10. Click **OK** to close the **Edit Storage Center Settings** dialog box.

Save SupportAssist Data to a File

If your site does not have connectivity to SupportAssist servers, you can use the **Export Historical Data** option to save SupportAssist data to a file or email the data to technical support.

Steps

1. Connect to the Data Collector.
   a. Open a web browser.
   b. Type the address of the Data Collector in the web browser using the following format:
      https://*data_collector_host_name_or_IP_address*:3033/
   c. Press Enter.
      The Unisphere Central login page is displayed.
   d. Type the user name and password of a Data Collector user with Administrator privileges in the **User Name** and **Password** field.
   e. Click **Log In**.
2. If a Storage Center is selected from the drop-down list in Unisphere Central, click **(Home)**.
   The Unisphere Central **Home** page is displayed.
3. Click **Data Collector**.
   The **Data Collector** view is displayed.
4. Click the **Monitoring** tab, and then click the **SupportAssist** subtab.
5. Click **Export Historical Data**.
   The **Export Historical Data** dialog box opens.
6. In the **Storage Center** table, select the Storage Center for which you want to export data.
7. In the **Reports** section, select the type of data that you want to export.
8. In the **Time Range** section, specify the time period for which you want to export data.
9. Select whether to export the data to a file or to send the data via email.
   - To export the data to a file, select **Export historical data to file system**.
   - To export the data and send view email, select **Export historical data via email** and type the recipient email address in the **Email Address** field.

     NOTE: An SMTP server must be configured on the Data Collector to export historical data via email.
10. Click **OK**.

Saving SupportAssist Data to a USB Flash Drive

If the Storage Center is not configured to send, or is unable to send SupportAssist data to the SupportAssist server, you can save the SupportAssist data to a USB flash drive and then send the data to technical support.

USB Flash Drive Requirements

The flash drive must meet the following requirements to be used to save SupportAssist data:

- USB 2.0
- Minimum size of 4 GB

Prepare the USB Flash Drive

When the USB flash drive contains a file named **`phonehome.phy`**, the Storage Center recognizes that the drive will be used to save SupportAssist data.

Prerequisites

- This procedure requires a USB flash drive that contains a partition table with one partition formatted with an MSDOS/FAT32 filesystem. USB devices may come from the vendor formatted with or without partitions. Use Windows disk management or other third-party tools to create a partition if the flash drive does not have an MSDOS/FAT32 partition.
- The USB flash drive cannot contain any other .phy marker files.

About this task

NOTE: To save SupportAssist data from both controllers, you must use two separate USB flash drives.

Steps

1. Create a text file and name it: **`phonehome.phy`** changing the file type from .txt to .phy.
2. Save the file to the root of the MSDOS/FAT32 filesystem on the flash drive.
3. Insert the USB drive into a port on the lead controller.
4. To save SupportAssist data from both controllers, insert a second USB flash drive into the peer controller.
5. Wait five minutes to allow the controllers to recognize the USB flash drive.
6. Check the Storage Center logs in Storage Manager to verify that Storage Center recognized the USB flash drive.

Save SupportAssist Data to the USB Flash Drive

Use the Send SupportAssist Information to USB dialog box to save data to the USB flash drive.

Prerequisites

- Prepare the USB flash drive according to Prepare the USB Flash Drive on page 673.
- Storage Center must recognize the USB flash drive.
- SupportAssist must be turned off.

Steps

1. Click the **Storage** view.
2. From the **Storage** navigation pane, select the Storage Center for which to save SupportAssist data .
3. In the **Summary** tab, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
4. Click **Send SupportAssist Information to USB**.
   The **Send SupportAssist Information to USB** dialog box opens.
5. Review the SupportAssist System State Information Collection and Storage terms.

6. Place a check next to **By checking this box, you accept the above terms** to accept the terms.
7. Click **Next**.
8. Place a check next to **Detailed Logs** to save this information to the USB flash drive.

   NOTE: Storage Manager saves the Storage Center configuration data to the USB flash drive automatically.

9. Click **Finish**. The dialog box displays SupportAssist progress and closes when the process is complete.

   NOTE: Do not remove the drive from the port on the controller until SupportAssist has completed saving data. This process may take up to five minutes.

10. When SupportAssist has completed successfully, remove the drive from the controller port and send the SupportAssist data to technical support.

Troubleshooting SupportAssist USB Issues

Follow one of the following procedures to resolve issues sending SupportAssist data to a USB flash drive. Before sending the USB flash drive to SupportAssist, verify that Storage Center successfully wrote SupportAssist data to the drive.

After sending SupportAssist data to the USB flash drive, the drive should contain multiple files.

1. Verify that the USB flash drive contains the SupportAssist data.
   a. Insert the USB flash drive into a computer.
   b. Verify that the drive contains files.

      NOTE: The timestamp on the files must match the time that the SupportAssist data was sent.
2. If the USB flash drive does not contain new SupportAssist files:
   a. Verify that the USB flash drive meets the minimum requirements.
   b. Reformat the USB drive using MSDOS/FAT32 file system.
   c. Prepare the USB flash drive following the instructions in Prepare the USB Flash Drive on page 673.
   d. Save SupportAssist data to the USB flash drive following the instructions in Save SupportAssist Data to the USB Flash Drive on page 673.

Managing SupportAssist Settings

SupportAssist settings can be configured individually for each Storage Center or applied to multiple Storage Centers.

Edit SupportAssist Contact Information

Use the Storage Center settings to edit SupportAssist contact information.

Steps

1. Click the **Storage** view.
2. In the **Storage** view navigation pane, select a Storage Center.
3. In the right pane, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens
4. Click the **SupportAssist** tab.
5. Click **Edit SupportAssist Contact Information**.
   The **Edit SupportAssist Contact Information** dialog box opens.
6. Enter the name, email, and phone number of the onsite contact in the **General** area.
7. Specify contact preferences in the **Contact Preferences** area.
   a. Select the **Send me emails from SupportAssist...** checkbox to notify the onsite contact when a support alert is sent to technical support.
   b. Select a preferred contact method from the **Type** drop-down menu.
   c. Select a preferred language for emails from the **Email Language** drop-down menu.
   d. Specify the working hours of the onsite contact in the **Time** fields.

e. Select the time zone for the onsite contact from the **Time Zone** drop-down menu.

8. Specify the site address in the **Onsite Address** area.
9. Click **OK**.

Configure SupportAssist to Automatically Download Updates

Configure SupportAssist to automatically download updates to the Storage Center.

Steps

1. Click the **Storage** view.
2. In the **Storage** view navigation pane, select a Storage Center.
3. In the right pane , click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens.
4. Click the **SupportAssist** tab.
5. In the Server Settings area, select **Notify me of updates and automatically download them** from the **Update Option** drop-down menu.
6. Click **OK**.

Configure a Proxy Server for SupportAssist

Use the Storage Center settings to configure a proxy server for SupportAssist.

Steps

1. Click the **Storage** view.
2. In the **Storage** view navigation pane, select a Storage Center.
3. In the right pane, click **Edit Settings**.
   The **Edit Storage Center Settings** dialog box opens
4. Click the **SupportAssist** tab.
5. Select the **Enabled** checkbox under **Web Proxy Settings**.
6. Specify the IP address for the proxy server in the **IPv4 Address** field.
7. Specify the port number for the proxy server in the **Port** field.
8. If the proxy server requires authentication, type the user name and password for the proxy server in the **User Name** and **Password** fields.
9. Click **OK**.

CloudIQ

CloudIQ provides storage monitoring and proactive service, giving you information tailored to your needs, access to near real-time analytics, and the ability to monitor storage systems from anywhere at any time. CloudIQ simplifies storage monitoring and service by providing:

- Proactive serviceability that informs you about issues before they impact your environment.
- Centralized monitoring across your environment, using a dashboard that aggregates key information such as system health scores, performance metrics, and current capacity and trends.

CloudIQ requires the following:

- Storage Centers must be running software version 7.3 or later.
- SupportAssist must be enabled on Storage Center.
- Each Storage Center must be connected to CloudIQ and initialized using the CloudIQ process referred to as onboarding. To onboard a Storage Center, you need the serial number, service tag, and Storage Center software version.
- Each user must be registered with support.emc.com for access to the Dell EMC support portal, which also includes access to CloudIQ.

For more information about CloudIQ, contact technical support or visit the Dell EMC CloudIQ Home Page.

Controlling Data Sent to CloudIQ

When a Storage Center has been onboarded to CloudIQ and SupportAssist is enabled, the **CloudIQ Enabled** option appears in the SupportAssist settings tab and is selected by default. When the **CloudIQ Enabled** checkbox is selected, the Storage Center sends data to CloudIQ more frequently than, and independent of, the SupportAssist schedule. You can remain connected to CloudIQ, but stop sending data by clearing the checkbox.

Steps

1. Click the **Storage** view.
2. In the **Storage** view navigation pane, select a Storage Center.
3. In the **Summary** tab, click **Edit Settings**. The **Edit Storage Center Settings** dialog box opens.
4. Click the **SupportAssist** tab.
5. Select or clear the **CloudIQ Enabled** checkbox.
6. Click **OK**.

   NOTE: It may take up to four hours for changes made to this checkbox to take effect.