Notes, Cautions, and Warnings

\[ \text{NOTE:} \quad \text{A NOTE indicates important information that helps you make better use of your product.} \]
\[ \text{CAUTION:} \quad \text{A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.} \]
\[ \text{WARNING:} \quad \text{A WARNING indicates a potential for property damage, personal injury, or death.} \]
# Contents

**About This Guide** ......................................................................................................................... 11
  - Revision History ......................................................................................................................... 11
  - Audience ..................................................................................................................................... 11
  - Contacting Dell ........................................................................................................................... 11

**1 Unisphere Overview** ................................................................................................................ 13
  - Unisphere Components .............................................................................................................. 13
  - Software and Hardware Requirements ....................................................................................... 14
  - Storage Center OS Compatibility ............................................................................................... 14
  - Data Collector Requirements .................................................................................................... 14
  - Unisphere Web Browser Requirements .................................................................................... 15
  - Server Agent Requirements ...................................................................................................... 15
  - Default Ports Used by Unisphere Central .................................................................................. 15
  - Data Collector Ports .................................................................................................................. 16
  - Client Ports ............................................................................................................................... 17
  - Server Agent Ports ................................................................................................................... 17
  - IPv6 Support ............................................................................................................................. 17
  - Unisphere Features ................................................................................................................... 18
  - Storage Center Management ..................................................................................................... 18
  - Servers ....................................................................................................................................... 18
  - SMI-S .......................................................................................................................................... 18
  - VVols .......................................................................................................................................... 18
  - Log Monitoring ......................................................................................................................... 19
  - Performance Monitoring ........................................................................................................... 19

**2 Getting Started** ......................................................................................................................... 21
  - Connect to Multiple Storage Centers Using Unisphere Central .............................................. 21
  - Connect Directly to a Storage Center Using Unisphere ............................................................ 21
  - Next Steps .................................................................................................................................. 22
    - Add Unisphere Users .............................................................................................................. 22
    - Add Storage Centers ............................................................................................................ 22
    - Configure Storage Center Volumes ....................................................................................... 22
    - Add Servers to the Storage Centers ..................................................................................... 22
    - Configure Email Notifications .............................................................................................. 22

**3 Storage Center Overview** ......................................................................................................... 23
  - Storage Center Hardware Components ...................................................................................... 23
    - Controllers ............................................................................................................................. 23
    - Switches .................................................................................................................................. 23
    - Enclosures .............................................................................................................................. 23
  - How Storage Virtualization Works ............................................................................................. 23
    - Volumes .................................................................................................................................. 24
    - Storage Types .......................................................................................................................... 24
# 4 Storage Center Administration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding and Organizing Storage Centers</td>
<td>37</td>
</tr>
<tr>
<td>User Privilege Levels</td>
<td>37</td>
</tr>
<tr>
<td>Adding and Removing Storage Centers</td>
<td>38</td>
</tr>
<tr>
<td>Organizing Storage Centers</td>
<td>39</td>
</tr>
<tr>
<td>Managing Volumes</td>
<td>41</td>
</tr>
<tr>
<td>Attributes That Determine Volume Behavior</td>
<td>41</td>
</tr>
<tr>
<td>Creating Volumes</td>
<td>41</td>
</tr>
<tr>
<td>Modifying Volumes</td>
<td>43</td>
</tr>
<tr>
<td>Copying Volumes</td>
<td>48</td>
</tr>
<tr>
<td>Creating and Managing Volume Folders</td>
<td>50</td>
</tr>
<tr>
<td>Creating and Managing Volume Snapshots</td>
<td>51</td>
</tr>
<tr>
<td>Mapping Volumes to Servers</td>
<td>53</td>
</tr>
<tr>
<td>Deleting Volumes and Volume Folders</td>
<td>56</td>
</tr>
<tr>
<td>Reset a Controller to Factory Default</td>
<td>58</td>
</tr>
<tr>
<td>Managing Virtual Volumes With Unisphere Central</td>
<td>58</td>
</tr>
<tr>
<td>Configuring VVs in Unisphere Central</td>
<td>58</td>
</tr>
<tr>
<td>VMware Virtual Volume Concepts</td>
<td>59</td>
</tr>
<tr>
<td>Setting Up VVs Operations on Unisphere Central</td>
<td>60</td>
</tr>
<tr>
<td>VASA Provider</td>
<td>61</td>
</tr>
<tr>
<td>Managing Storage Containers</td>
<td>63</td>
</tr>
<tr>
<td>Supported Hardware Platforms</td>
<td>69</td>
</tr>
<tr>
<td>Data Eligible for Data Reduction</td>
<td>69</td>
</tr>
<tr>
<td>Compression</td>
<td>70</td>
</tr>
<tr>
<td>Deduplication</td>
<td>71</td>
</tr>
<tr>
<td>View Amount of Space Saved by Data Reduction</td>
<td>71</td>
</tr>
<tr>
<td>Change the Default Data Reduction Profile</td>
<td>72</td>
</tr>
<tr>
<td>Pause or Resume Data Reduction</td>
<td>72</td>
</tr>
<tr>
<td>Disable Data Reduction for a Volume</td>
<td>73</td>
</tr>
<tr>
<td>Managing Snapshot Profiles</td>
<td>73</td>
</tr>
<tr>
<td>Default Snapshot Profiles</td>
<td>74</td>
</tr>
<tr>
<td>Consistent and Non-Consistent Snapshot Profiles</td>
<td>74</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating and Applying Snapshot Profiles</td>
<td>74</td>
</tr>
<tr>
<td>Modifying Snapshot Profiles</td>
<td>76</td>
</tr>
<tr>
<td>Managing Expiration Rules for Remote Snapshots</td>
<td>78</td>
</tr>
<tr>
<td>Managing Storage Profiles</td>
<td>79</td>
</tr>
<tr>
<td>Create a Storage Profile (Storage Center 7.2.1 and Earlier)</td>
<td>79</td>
</tr>
<tr>
<td>Create a Storage Profile (Storage Center 7.2.10 and Later)</td>
<td>79</td>
</tr>
<tr>
<td>Apply a Storage Profile to One or More Volumes</td>
<td>80</td>
</tr>
<tr>
<td>Apply a Storage Profile to a Server</td>
<td>80</td>
</tr>
<tr>
<td>Delete a Storage Profile</td>
<td>81</td>
</tr>
<tr>
<td>Managing QoS Profiles</td>
<td>81</td>
</tr>
<tr>
<td>Create a QoS Profile</td>
<td>81</td>
</tr>
<tr>
<td>Edit a QoS Profile</td>
<td>82</td>
</tr>
<tr>
<td>Delete a QoS Volume Profile</td>
<td>82</td>
</tr>
<tr>
<td>Apply a QoS Profile to a Volume</td>
<td>82</td>
</tr>
<tr>
<td>Remove a Group QoS Profile From a Volume</td>
<td>83</td>
</tr>
<tr>
<td>Importing Volumes from an External Storage Array</td>
<td>83</td>
</tr>
<tr>
<td>Connect to an External Storage Array (iSCSI)</td>
<td>83</td>
</tr>
<tr>
<td>Scan for External Devices</td>
<td>84</td>
</tr>
<tr>
<td>Rediscover an iSCSI Remote Connection</td>
<td>84</td>
</tr>
<tr>
<td>Delete a Remote Connection</td>
<td>84</td>
</tr>
<tr>
<td>Storage Center Import Requirements</td>
<td>85</td>
</tr>
<tr>
<td>Supported Server Operating Systems for Online Import</td>
<td>85</td>
</tr>
<tr>
<td>Import Data from an External Device (Offline)</td>
<td>85</td>
</tr>
<tr>
<td>Import Data from an External Device (Online)</td>
<td>86</td>
</tr>
<tr>
<td>Restart an External Device Import</td>
<td>86</td>
</tr>
<tr>
<td>5 Storage Center Server Administration</td>
<td>87</td>
</tr>
<tr>
<td>Managing Servers on a Storage Center</td>
<td>87</td>
</tr>
<tr>
<td>Creating Servers</td>
<td>87</td>
</tr>
<tr>
<td>Modifying Servers</td>
<td>87</td>
</tr>
<tr>
<td>Mapping Volumes to Servers</td>
<td>89</td>
</tr>
<tr>
<td>Creating and Managing Server Folders</td>
<td>93</td>
</tr>
<tr>
<td>Deleting Servers and Server Folders</td>
<td>95</td>
</tr>
<tr>
<td>6 Storage Center Maintenance</td>
<td>99</td>
</tr>
<tr>
<td>Managing Storage Center Settings</td>
<td>99</td>
</tr>
<tr>
<td>Viewing and Modifying Storage Center Information</td>
<td>99</td>
</tr>
<tr>
<td>Configuring Storage Center User Preferences</td>
<td>101</td>
</tr>
<tr>
<td>Configuring Storage Center Data Settings</td>
<td>105</td>
</tr>
<tr>
<td>Set Up Automated Reports for an Individual Storage Center</td>
<td>106</td>
</tr>
<tr>
<td>Set the Date and Time for a Storage Center</td>
<td>107</td>
</tr>
<tr>
<td>Configure Storage Center SMTP Server Settings</td>
<td>107</td>
</tr>
<tr>
<td>Configure SNMP Settings for a Storage Center (Storage Center 6.7)</td>
<td>108</td>
</tr>
<tr>
<td>Configure SNMP Settings for a Storage Center (Storage Center Version 7.0 and Later)</td>
<td>108</td>
</tr>
<tr>
<td>Configuring Filters to Restrict Administrative Access</td>
<td>109</td>
</tr>
<tr>
<td>Configuring Storage Center Secure Console Settings</td>
<td>111</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring a Storage Center to Inherit Settings</td>
<td>112</td>
</tr>
<tr>
<td>Managing Storage Center Users and Groups</td>
<td>113</td>
</tr>
<tr>
<td>User Privilege Levels</td>
<td>113</td>
</tr>
<tr>
<td>User Groups</td>
<td>113</td>
</tr>
<tr>
<td>User Account Management and Authentication</td>
<td>113</td>
</tr>
<tr>
<td>Managing Local Storage Center Users</td>
<td>113</td>
</tr>
<tr>
<td>Managing Local Storage Center User Groups</td>
<td>119</td>
</tr>
<tr>
<td>Managing Local Storage Center User Password Requirements</td>
<td>121</td>
</tr>
<tr>
<td>Enabling Directory Services Authentication</td>
<td>123</td>
</tr>
<tr>
<td>Managing Directory Service Users</td>
<td>126</td>
</tr>
<tr>
<td>Managing Directory User Groups</td>
<td>131</td>
</tr>
<tr>
<td>Managing Front-End I/O Ports</td>
<td>133</td>
</tr>
<tr>
<td>Front-End Connectivity Modes</td>
<td>133</td>
</tr>
<tr>
<td>About Fault Domains and Ports</td>
<td>134</td>
</tr>
<tr>
<td>Failover Behavior</td>
<td>136</td>
</tr>
<tr>
<td>Managing Front-End I/O Port Hardware</td>
<td>136</td>
</tr>
<tr>
<td>Convert Front-End Ports to Virtual Port Mode</td>
<td>138</td>
</tr>
<tr>
<td>Managing Back-End I/O Port Hardware</td>
<td>139</td>
</tr>
<tr>
<td>Configure Back-End Ports</td>
<td>139</td>
</tr>
<tr>
<td>Configure Individual Back-End I/O Ports</td>
<td>139</td>
</tr>
<tr>
<td>Rename a Back-End I/O Port</td>
<td>139</td>
</tr>
<tr>
<td>Grouping Fibre Channel I/O Ports Using Fault Domains</td>
<td>140</td>
</tr>
<tr>
<td>Create a Fibre Channel Fault Domain</td>
<td>140</td>
</tr>
<tr>
<td>Rename a Fibre Channel Fault Domain</td>
<td>140</td>
</tr>
<tr>
<td>Delete a Fibre Channel Fault Domain</td>
<td>141</td>
</tr>
<tr>
<td>Grouping iSCSI I/O Ports Using Fault Domains</td>
<td>141</td>
</tr>
<tr>
<td>iSCSI VLAN Tagging Support</td>
<td>141</td>
</tr>
<tr>
<td>Creating iSCSI Fault Domains</td>
<td>142</td>
</tr>
<tr>
<td>Modifying iSCSI Fault Domains</td>
<td>144</td>
</tr>
<tr>
<td>Configuring NAT Port Forwarding for iSCSI Fault Domains</td>
<td>148</td>
</tr>
<tr>
<td>Configuring CHAP for iSCSI Fault Domains</td>
<td>150</td>
</tr>
<tr>
<td>Grouping SAS I/O Ports Using Fault Domains</td>
<td>153</td>
</tr>
<tr>
<td>Create a SAS Fault Domain</td>
<td>153</td>
</tr>
<tr>
<td>Delete a SAS Fault Domain</td>
<td>153</td>
</tr>
<tr>
<td>Managing Disks and Disk Folders</td>
<td>153</td>
</tr>
<tr>
<td>Storage Center Disk Management</td>
<td>154</td>
</tr>
<tr>
<td>Scan for New Disks</td>
<td>154</td>
</tr>
<tr>
<td>Create a Disk Folder</td>
<td>154</td>
</tr>
<tr>
<td>Delete Disk Folder</td>
<td>155</td>
</tr>
<tr>
<td>Modify a Disk Folder</td>
<td>155</td>
</tr>
<tr>
<td>Manage Unassigned Disks</td>
<td>155</td>
</tr>
<tr>
<td>Enable or Disable the Disk Indicator Light</td>
<td>156</td>
</tr>
<tr>
<td>Release a Disk</td>
<td>156</td>
</tr>
<tr>
<td>Cancel Releasing a Disk</td>
<td>157</td>
</tr>
<tr>
<td>Delete a Disk</td>
<td>157</td>
</tr>
</tbody>
</table>
Managing Storage Center Controllers

Replace a Failed Controller ................................................................. 169
Add a Controller ............................................................................. 172
Managing Secure Data

How Secure Data Works .................................................................. 158
Configure Key Server ..................................................................... 159
Configure Rekey Interval for Disk Folder ........................................ 160
Rekey a Disk ................................................................................... 160
Copy Volumes to Disk Folder ........................................................... 161
Create Secure Data Disk Folder ....................................................... 161
Managing Data Redundancy

Redundancy Requirements ............................................................... 162
Managing RAID .............................................................................. 162
Managing Storage Types ................................................................. 163
Managing Disk Enclosures

Add an Enclosure ............................................................................ 165
Remove an Enclosure ................................................................... 166
Replace an Enclosure .................................................................... 167
Rename a Disk Enclosure ................................................................. 167
Set an Asset Tag for a Disk Enclosure ............................................ 168
Delete an Enclosure ....................................................................... 168
Mute an Enclosure Alarm ............................................................... 168
Unmute an Enclosure Alarm ............................................................ 169
Clear the Swap Status for an Enclosure Cooling Fan ...................... 169
Clear the Swap Status for an Enclosure I/O Module ......................... 169
Clear the Swap Status for an Enclosure Power Supply .................... 169
Replace a Failed Power Supply ....................................................... 170
Clear the Under Voltage Status for a Power Supply ....................... 170
Clear the Swap Status for a Temperature Sensor ............................ 170
Clear the Minimum and Maximum Recorded Values for Temperature Sensor ................................................................. 171
Replace a Failed Cooling Fan Sensor ............................................... 171
Enable or Disable the Disk Indicator Light ...................................... 171
Clear the Swap Status for a Disk ...................................................... 172
Managing Storage Center Controllers

Add a Controller ............................................................................ 172
Replace a Failed Controller ........................................................... 173
Enable or Disable a Controller Indicator Light ................................. 173
Replace a Failed Cooling Fan Sensor .............................................. 173
Managing I/O Card Changes ........................................................... 174
Add a UPS to a Storage Center ......................................................... 175
Updating Storage Center

Update Storage Center Software ..................................................... 176
Using the Storage Center Update Utility ......................................... 176
Turn On SupportAssist .................................................................. 177
Shutting Down and Restarting a Storage Center ................................. 178
7 Viewing Storage Center Information ................................................................. 181
   Summary Information....................................................................................... 181
   Storage Center Widgets.................................................................................. 181
   Rearrange Widgets on the Summary Page....................................................... 182
   Status Indicators............................................................................................. 182
   Viewing Detailed Storage Usage Information.................................................. 183
      View Storage Usage by Tier and RAID Type.................................................. 183
      View Storage Usage by Volumes................................................................... 183
      View a Data Progression Pressure Report..................................................... 183
   Viewing Historical Storage Usage Data............................................................ 184
      View Historical Storage Usage Data for a Volume......................................... 184
      View Historical Storage Usage Data for a Server......................................... 184
   Viewing Historical Performance Information................................................ 185
      View System Performance Information......................................................... 185
      View Server Performance Information......................................................... 185
      View Fault Domains Performance Information............................................. 185
      View Volume Performance Information....................................................... 185
      View Disk Performance................................................................................ 185
      View Performance Statistics for Controllers................................................. 186
      View Storage Profile Performance................................................................ 186
      View QoS Profile Performance...................................................................... 186
   Export I/O Usage Data.................................................................................... 186
   Exporting Usage and Monitoring Data............................................................ 187
      Export Storage Usage Data for a Single Storage Center................................... 187
      Export Storage Usage Data for Multiple Storage Centers.............................. 187
      Export Monitoring Data for a Single Storage Center........................................ 187
      Export Monitoring Data for Multiple Storage Centers.................................... 188

8 Storage Center Monitoring ............................................................................. 189
   Alerts.............................................................................................................. 189
      Status Levels for Alerts and Indications......................................................... 189
      View Storage Center Alerts......................................................................... 190
      Send Storage Center Alerts and Indications to the Data Collector Immediately... 192
   Data Collector Alerts..................................................................................... 192
      Data Collector Alert Types............................................................................ 193
      View Data Collector Alerts.......................................................................... 193
      Filter the Data Collector Alerts.................................................................... 193
      Select the Date Range of Data Collector Alerts to Display.......................... 194
Contents

SupportAssist Management......................................................................................................................... 237

12 SupportAssist Management......................................................................................................................... 237

Data Types that Can Be Sent Using SupportAssist....................................................................................... 237
Configure SupportAssist Settings for the Data Collector.................................................................................. 237
Configure SupportAssist Settings for a Single Storage Center........................................................................ 238
Manually Sending Diagnostic Data Using SupportAssist................................................................................ 238
    Manually Send Diagnostic Data for Multiple Storage Centers................................................................ 238
    Send Diagnostic Data for a Single Storage Center ..................................................................................... 239
Save SupportAssist Data to a File.................................................................................................................... 239
Saving SupportAssist Data to a USB Flash Drive .............................................................................................. 240
    USB Flash Drive Requirements.................................................................................................................. 240
    Prepare the USB Flash Drive...................................................................................................................... 240
    Save SupportAssist Data to the USB Flash Drive......................................................................................... 240
Troubleshooting SupportAssist USB Issues....................................................................................................... 241
Managing SupportAssist Settings.................................................................................................................... 241
    Edit SupportAssist Contact Information...................................................................................................... 241
    Configure SupportAssist to Automatically Download Updates................................................................... 242
    Configure a Proxy Server for SupportAssist................................................................................................ 242
CloudIQ.............................................................................................................................................................. 242
Controlling Data Sent to CloudIQ..................................................................................................................... 243
This guide describes how to use Unisphere and Unisphere Central for SC Series to manage and monitor your storage infrastructure.

**Revision History**

Document number: 680-122-004

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>March 2018</td>
<td>Initial release</td>
</tr>
<tr>
<td>B</td>
<td>August 2018</td>
<td>Update for Unisphere 2018 R1.10</td>
</tr>
<tr>
<td>C</td>
<td>November 2018</td>
<td>Update for Unisphere 2018 R1.20</td>
</tr>
</tbody>
</table>

**Audience**

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

**Contacting Dell**

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services might not be available in your area.

To contact Dell for sales, technical support, or customer service issues, go to [Dell.com/support](http://Dell.com/support).

- For customized support, type your system service tag on the support page and click **Submit**.
- For general support, browse the product list on the support page and select your product.
Unisphere Overview

Unisphere is a Web application that allows you to connect to a single Storage Center or multiple Storage Centers. Managing multiple Storage Centers requires the installation of a Data Collector. Unisphere allows you to monitor, manage, and analyze Storage Centers from a centralized management console.

- Unisphere for SC Series is used to connect directly to a single Storage Center.
- Unisphere Central for SC Series connects to multiple Storage Centers through a Storage Manager Data Collector. The Storage Manager Data Collector stores data it gathers from Storage Centers in a database. Unisphere Central connects to the Data Collector to perform monitoring and administrative tasks.

Topics:
- Unisphere Components
- Software and Hardware Requirements
- Default Ports Used by Unisphere Central
- IPv6 Support
- Unisphere Features

Unisphere Components

Unisphere for SC Series consists of the following components.

Table 1. Unisphere Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Setup Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Storage Manager Data Collector</td>
<td>Service that gathers reporting data and alerts from Storage Centers</td>
<td>Storage Manager Installation Guide</td>
</tr>
<tr>
<td>Unisphere Central for SC Series</td>
<td>Web application that connects to the Storage Manager Data Collector to provide a centralized management interface for one or more storage devices</td>
<td>Storage Manager Installation Guide and Unisphere and Unisphere Central for SC Series Administrator's Guide</td>
</tr>
<tr>
<td>Unisphere for SC Series</td>
<td>Web application that connects hosted on a Storage Center that provides a management interface to that storage device</td>
<td>Unisphere and Unisphere Central for SC Series Administrator's Guide</td>
</tr>
<tr>
<td>Remote Storage Manager Data Collector</td>
<td>Storage Manager Data Collector that is connected to the primary Storage Manager Data Collector and can be used to activate a disaster recovery site if the primary Storage Manager Data Collector becomes unavailable</td>
<td>Storage Manager Administrator's Guide</td>
</tr>
<tr>
<td>Storage Manager Server Agent</td>
<td>Service for Windows that allows Unisphere Central to free volume storage space from expired snapshots that would otherwise remain locked by Windows</td>
<td>Storage Manager Administrator's Guide</td>
</tr>
</tbody>
</table>
Software and Hardware Requirements

The following sections list the requirements for the Storage Center, Storage Manager Data Collector, Unisphere, and Storage Manager Server Agent.

Storage Center OS Compatibility

Unisphere is compatible with Storage Center OS versions 6.7 and later.

Data Collector Requirements

The following table lists the Storage Manager Data Collector requirements.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Any of the following 64-bit operating systems with the latest service packs:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2019</td>
</tr>
</tbody>
</table>

| NOTE: 32-bit operating systems are not supported, and Windows Server Core is not supported. |

<table>
<thead>
<tr>
<th>Windows User Group</th>
<th>Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>64-bit (x64) microprocessor with two or more cores</td>
</tr>
<tr>
<td></td>
<td>The Data Collector requires four cores for environments with 100,000 or more Active Directory members or groups.</td>
</tr>
<tr>
<td>Memory</td>
<td>Varies based on size of the storage environment:</td>
</tr>
<tr>
<td></td>
<td>• 4 GB – One to ten Storage Centers or up to 3000 total volumes</td>
</tr>
<tr>
<td></td>
<td>• 8 GB – More than ten Storage Centers, or up to 6000 total volumes</td>
</tr>
<tr>
<td></td>
<td>• 16 GB – More than ten Storage Centers, or up to 12,000 total volumes</td>
</tr>
<tr>
<td></td>
<td>• 32 GB – More than ten Storage Centers, or more than 12,000 total volumes</td>
</tr>
<tr>
<td>Disk space</td>
<td>At least 20 GB; additional space is required to manage FluidFS cluster software updates.</td>
</tr>
</tbody>
</table>

| NOTE: If you chose to use an embedded database instead of an external database, an additional 64 GB is required to store the database on the file system. However, an embedded database is not recommended for a production environment. |

| Software | Microsoft .NET Framework 4.5 Full                                                |
| Web browser | Any of the following web browsers:                      |
|          | • Internet Explorer 11                                                   |
|          | • Microsoft Edge                                                        |
|          | • Firefox                                                               |
|          | • Google Chrome                                                        |
External database

One of the following databases:

- Microsoft SQL Server 2012
- Microsoft SQL Server 2012 Express (limited to 10 GB)
- Microsoft SQL Server 2014
- Microsoft SQL Server 2014 Express (limited to 10 GB)
- Microsoft SQL Server 2016
- MySQL 5.6
- MySQL 5.7

NOTE: The embedded database stored on the file system can be used instead of an external database. However, the embedded database is limited to 64 GB and retains only the last 30 days of data. The embedded database is not recommended for a production environment.

Unisphere Web Browser Requirements

The following web browsers are supported for use with Unisphere:

- Internet Explorer 11 or later
- Firefox
- Google Chrome
- Microsoft Edge

Server Agent Requirements

The following table lists the requirements for running the Storage Manager Server Agent on Windows servers.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Any of the following 64-bit operating systems (with the latest service packs):</td>
</tr>
<tr>
<td>CPU</td>
<td>64-bit (x64) microprocessor</td>
</tr>
<tr>
<td>Software</td>
<td>Microsoft .NET Framework 4.5 Full</td>
</tr>
</tbody>
</table>

Default Ports Used by Unisphere Central

The Unisphere Central 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, Unisphere Central for SC Series, 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 ports used by the Storage Manager Data Collector:

### Inbound Data Collector Ports

The Data Collector accepts connections on the following ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3033</td>
<td>TCP</td>
<td>Web Server Port</td>
<td>Receiving:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Communication from all clients, including the Unisphere Central for SC Series, Unisphere Central, and Dell Storage Replication Adapter (SRA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Alerts from FluidFS clusters</td>
</tr>
<tr>
<td>3034</td>
<td>TCP</td>
<td>Web Server Port</td>
<td>Receiving vCenter/ESXi communication for VASA and VVol provisioning and administration</td>
</tr>
<tr>
<td>8080</td>
<td>TCP</td>
<td>Legacy Web Services Port</td>
<td>Receiving:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Storage Manager Server Agent communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Alerts forwarded from Storage Center SANs</td>
</tr>
<tr>
<td>5989</td>
<td>TCP</td>
<td>SMI-S over HTTPS</td>
<td>Receiving encrypted SMI-S communication</td>
</tr>
</tbody>
</table>

### Outbound Data Collector Ports

The Data Collector initiates connections to the following ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TCP</td>
<td>SMTP</td>
<td>Sending email notifications</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>SSL</td>
<td>• Communicating with managed Storage Centers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sending diagnostic data with SupportAssist</td>
</tr>
<tr>
<td>1199</td>
<td>TCP</td>
<td>SIMS RMI</td>
<td>Communicating with managed PS Series groups</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>Microsoft SQL Server</td>
<td>Connecting to an external Microsoft SQL Server database</td>
</tr>
<tr>
<td>3033</td>
<td>TCP</td>
<td>SSL</td>
<td>Communicating with managed Storage Centers</td>
</tr>
<tr>
<td>3306</td>
<td>TCP</td>
<td>MySQL</td>
<td>Connecting to an external MySQL database</td>
</tr>
<tr>
<td>8080</td>
<td>TCP</td>
<td>VMware SDK</td>
<td>Communicating with VMware servers</td>
</tr>
<tr>
<td>27355</td>
<td>TCP</td>
<td>Server Agent Socket</td>
<td>Storage Manager Server Agent communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Listening Port</td>
<td></td>
</tr>
<tr>
<td>35451</td>
<td>TCP</td>
<td>FluidFS</td>
<td>Communicating with managed FluidFS clusters</td>
</tr>
<tr>
<td>44421</td>
<td>TCP</td>
<td>FluidFS diagnostics</td>
<td>Retrieving diagnostics from managed FluidFS clusters</td>
</tr>
</tbody>
</table>
Client Ports
Unisphere Central clients use the following ports:

Inbound Ports
Unisphere Central does not use any inbound ports.

Outbound Ports
Unisphere Central initiates connections to the following port:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3033</td>
<td>TCP</td>
<td>Web Server Port</td>
<td>Communicating with the Storage Manager Data Collector</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>27355</td>
<td>TCP</td>
<td>Server Agent Socket Listening Port</td>
<td>Receiving communication from the Data Collector</td>
</tr>
</tbody>
</table>

Outbound Server Agent Port
The Server Agent initiates connections to the following port.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8080</td>
<td>TCP</td>
<td>Legacy Web Services Port</td>
<td>Communicating with the Data Collector</td>
</tr>
</tbody>
</table>

IPv6 Support
The Storage Manager Data Collector can use IPv6 to accept connections from Unisphere and to communicate with managed Storage Center SANs.
To use IPv6, assign IPv6 addresses as described in the following table.

<table>
<thead>
<tr>
<th>IPv6 Connection</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unisphere to Data Collector</td>
<td>• Unisphere computer must have an IPv6 address.</td>
</tr>
</tbody>
</table>
**IPv6 Connection**

**Requirements**

- Data Collector server must have both an IPv4 address and an IPv6 address.
- 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.

**Unisphere Features**

Unisphere provides the following features.

**Storage Center Management**

Unisphere 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 link**

Storage Center Administration

**Servers**

Unisphere allows you to manage the storage that is allocated to servers.

There are two ways to manage servers in Unisphere:

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

**Related link**

Storage Center Server Administration

**SMI-S**

Unisphere Central supports the Storage Management Initiative Specification (SMI-S), a standard interface specification developed by the Storage Networking Industry Association (SNIA). SMI-S allows Unisphere Central 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.

**VVols**

Unisphere Central 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 to use VVols.

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

Related link
  Storage Center Monitoring

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 link
  Viewing Storage Center Information
To manage multiple Storage Centers, open a web browser and connect to the Data Collector.
To manage a single Storage Center, open a web browser and connect directly to the Storage Center.

Topics:
- Connect to Multiple Storage Centers Using Unisphere Central
- Connect Directly to a Storage Center Using Unisphere
- Next Steps

Connect to Multiple Storage Centers Using Unisphere Central

Start a web browser and use it to connect to the Data Collector.

About this task
By default, you can log on as a local Data Collector user. If the Data Collector is configured to use an external directory service, you can log on as an Active Directory or Open LDAP user. If Kerberos authentication is configured, you can log on automatically using your Windows session credentials without typing them manually.

Steps
1. Open a web browser.
2. Type the address of the Data Collector in the following format:
   `https://Data Collector host name or IP address:3033/ui/home`
3. Type the user name and password of a Data Collector user in the **User Name** and **Password** fields.
4. Click **Log In**.
   The web browser connects to the Data Collector and displays the Unisphere Central **Home** page.

Connect Directly to a Storage Center Using Unisphere

Start a web browser and use it to connect directly to the Storage Center.

About this task
By default, you can log on as a local Storage Center user. If the Storage Center is configured to use an external directory service, you can log on as an Active Directory or Open LDAP user. If Kerberos authentication is configured, you can log on automatically using your Windows session credentials without typing them manually.

Steps
1. Open a web browser.
2. Type the address of the Storage Center in the following format:
   `https://Storage Center host name or IP address/`
3. Type the user name and password of a Storage Center user in the **User Name** and **Password** fields.
4. Click **Log In**.
   The web browser connects to the Storage Center and displays the Unisphere **Summary** page.
Next Steps

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

Add Unisphere Users

Depending on your configuration, you can add users to your system using the Data Collector or you can create local users on the Storage Center using Unisphere.

• Data Collector – The Data Collector controls user access to Unisphere Central functions and associated Storage Centers based on the privileges assigned to users: Reporter, Volume Manager, or Administrator. New users and the associated Storage Centers are created and managed only by the Data Collector. If you want to grant Storage Centers access to other members of your organization, use Unisphere Central to grant them access using either of the following methods:
  – Create local Data Collector 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.
• Unisphere – When connected directly to a Storage Center, use local user groups to control the storage objects that can be viewed by a Storage Center user. The privilege level of a Storage Center user controls what a user can do on a Storage Center.

Add Storage Centers

Add Storage Centers to the Data Collector so that they can be managed and maintained using Unisphere Central.

Related link
Adding and Organizing Storage Centers

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 links
Managing Volumes
Managing Snapshot Profiles

Add Servers to the Storage Centers

Use Unisphere to add servers that use Storage Center volumes to the associated Storage Centers.

Related link
Storage Center Server Administration

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 link
Configuring Email Alerts for Unisphere Central Events
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).

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.

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.

- **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.

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 controllers 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 2. HDD Redundancy Recommendations and Requirements**

<table>
<thead>
<tr>
<th>Disk Size</th>
<th>Level of Redundancy Recommended or Enforced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 3 TB</td>
<td>Dual redundant is the recommended level</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Non-redundant storage is not an option for SCv2000 Series Storage Centers.</td>
</tr>
<tr>
<td>3 TB and higher</td>
<td>Dual redundant is required and enforced</td>
</tr>
</tbody>
</table>

**Table 3. SSD Redundancy Recommendations and Requirements**

<table>
<thead>
<tr>
<th>Disk Size</th>
<th>Level of Redundancy Recommended or Enforced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 18 TB</td>
<td>Dual redundant is the recommended level</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Non-redundant storage is not an option for SCv2000 Series Storage Centers.</td>
</tr>
<tr>
<td>18 TB and higher</td>
<td>Dual redundant is required and enforced</td>
</tr>
</tbody>
</table>

**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 SC7020, SC5020, and SCv3000, 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) using the Storage Center Storage settings. See below for SCv2000 series disk management.

**Disk Management on SCv2000 Series Controllers**

Storage Centers with SCv2000 series controllers 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 with SCv2000 series controllers:

- 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. 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.
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 Dell Technical Support to dispatch larger capacity drives of the same disk class when the same size drive is not available, providing faster delivery times.

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: With SCv2000 series controllers, Data Progression moves data between RAID 10 and RAID 5/6 and restripes RAID, but 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, Unisphere 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.
- Prevents new volume creation.
- Volumes will 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 step**
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.

**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.

**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.

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

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.

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

**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 Virtualization for SCv2000 Series Controllers

SCv2000 series controllers manage many storage virtualization options automatically.

Disk Management on SCv2000 Series Controllers

Storage Centers with SCv2000 series controllers 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 with SCv2000 series controllers:

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

Storage Types for SCv2000 Series Controllers

SCv2000 series controllers create a storage type for each disk class, and manage storage types automatically. SCv2000 series controllers manage storage types automatically in the following ways:

- Storage types are created automatically for each disk class
- Storage types have a 2MB page size for HDD folders and a 512 MB page size for SSD folders
- Storage types cannot be modified
- Non-redundant storage types are not allowed
**RAID Tiering for SCv2000 Series Controllers**

RAID tiering for SCv2000 series controllers moves data between RAID 10 and RAID 5/6. It does not move data between storage tiers. RAID tiering happens at 7 PM every day. Data progression runs until it completes or reaches the maximum run time.

**Storage Profiles for SCv2000 Series Controllers**

The following table summarizes the storage profiles available to SCv2000 series controllers.

<table>
<thead>
<tr>
<th>Name</th>
<th>Initial Write Tier</th>
<th>Tier (T) and RAID Levels</th>
<th>RAID Tiering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balanced</td>
<td>1</td>
<td>Writes: T1 RAID 10</td>
<td>Between RAID types only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Snapshots: T1 RAID 5/6</td>
<td></td>
</tr>
<tr>
<td>Maximize Performance</td>
<td>1</td>
<td>Writes: T1 RAID 10</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Snapshots: T1 RAID 10</td>
<td></td>
</tr>
<tr>
<td>Maximize Efficiency</td>
<td>1</td>
<td>Writes: T1 RAID 5/6</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Snapshots: T1 RAID 5/6</td>
<td></td>
</tr>
</tbody>
</table>

**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 is performed from the Unisphere dashboard. The dashboard view varies slightly depending on whether you connect directly to a Storage Center or connect through the Data Collector.

**Home Page**

When connected through the Data Collector, a Home page displays an aggregate summary of all Storage Centers managed by the Data Collector.
Storage Menu

- **Storage Centers** view – Use this page to view status of all Storage Centers managed by the Data Collector and to select and individual Storage Center.
- **Volumes** view – Used to create and manage volumes and volume folders on all Storage Centers managed by the Data Collector.

Data Mobility Menu

- **Imports** view – Used to create and view connections to external devices.
- **Bandwidth Controls** view – Used to view define I/O priority for all Storage Centers.

Monitoring Menu

- **Alerts** view – Used to view and acknowledge alerts that have been issued for a single Storage Center, for all Storage Centers, or for the Data Collector.
- **Logs** view – Used to view and export logs sent from all Storage Centers.

Data Collector Menu

The Data Collector menu provides access to all Data Collector management options, including system-wide user access, SupportAssist and data collection options, and other overall system functions.

![Figure 1. Home Page for Data Collector Access](image)

Summary View

The Summary view displays a dashboard that summarizes information about the selected Storage Center. The left navigation pane provides access to the Summary view and the following menus when connected directly to a Storage Center. When you select a menu in the navigation pane, links to related pages appear.
Storage Menu

- **Volumes** view – Used to create and manage volumes and volume folders on the selected Storage Center.
- **Servers** view – Used to create and manage server mappings to the selected Storage Center.
- **Profiles** view – Used to view, modify, and create snapshot, storage, and GoS profiles for the selected Storage Center and apply them to selected volumes. GoS profile management is only available if it is enabled in the Storage Center settings.
- **Disks** view – Used to view and manage disks and disk folders, including rebalancing RAID and scanning for new disks.
- **Storage Types** view – Use this page to view information about current type usage, and add or edit types for the Storage Center.

System Menu

- **Hardware** view – Used to view hardware status and cabling information, and to configure or modify hardware settings.
- **Ports** view – Used to view status and configuration information about controller ports and fault domains.

Data Mobility Menu

- **Imports** view – Used to create and view Remote iSCSI connections to storage controllers for which you have access. This view also allows you to locate and import data from external devices.
- **Bandwidth Controls** view – Used to define I/O priority.

Monitoring Menu

- **Alerts** view – Used to view and acknowledge alerts that have been issued for the Storage Center.
- **Logs** view – Used to view logs sent from the Storage Center.
- **Performance** view – Used to view the historical I/O performance statistics for the selected Storage Center and associated storage objects.

Reports Menu

Contains the **Realtime** view used to view current volume status and statistics.
Figure 2. Summary View for Direct-Connect Access
Storage Center Administration

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

Adding and Organizing Storage Centers

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

Note the following restrictions about Unisphere Central user accounts:

- An individual Unisphere Central 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 Unisphere Central user are not necessarily visible to another user.
- When a Unisphere Central 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 Unisphere Central users, you can specify Storage Center user accounts of any privilege level.
- If your Unisphere Central user account has the Reporter privilege, you must specify a Storage Center user account that has the Reporter privilege.

**NOTE:** A Unisphere Central Administrator can also use the Data Collector to grant Storage Center access to a Unisphere Central 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 Unisphere Central user privileges share the same names, but they are not the same.

Storage Center user privileges control access to Storage Center functionality, and Unisphere Central user privileges control access to Unisphere Central functionality. A user may have a different role in Unisphere Central than in Storage Center. This role difference affects small details of that user’s access.

Related link

Unisphere Central User Privileges

**User Privilege Levels**

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

**Table 4. Storage Center User Privilege Levels**

<table>
<thead>
<tr>
<th>Privilege Level</th>
<th>Allowed Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Volume Manager</td>
<td>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.</td>
</tr>
</tbody>
</table>
Add a Storage Center

Add a Storage Center to Unisphere Central to manage and monitor the Storage Center using the Unisphere Central dashboard.

Prerequisites

- The Data Collector must have network connectivity to the Storage Center management interface.
- You must have the user name and password for a Storage Center user account.
  - The first time you add a Storage Center to the Storage Manager Data Collector, you must specify a Storage Center user account that has Administrator privileges. When the Storage Center is added for other Unisphere Central users, you can specify Storage Center user accounts of any privilege level.
  - If your Unisphere Central user account has Reporter privileges, you must specify a Storage Center user account with Reporter privileges.

  **NOTE:** Users with Reporter level privileges have limited access to Storage Centers in Unisphere Central. To grant a Reporter user access to Storage Centers, add Storage Center mappings to that user in the Data Collector. Only Unisphere Central users with Administrator privileges can set mappings for Unisphere Central users.

Steps

1. Click the **HOME** menu.
   The Unisphere Central **Home** page is displayed.
   If you are connected to a Data Collector and a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane to display to the **Home** page.
2. Click **(New)** and select **Add Storage Center**.
   The **Add Storage Center** dialog box opens.
3. Type the information needed to add the Storage Center in the following fields.
   - **Hostname or IP Address** – Type the host name or IP address of a Storage Center controller. For a dual-controller Storage Center, type the IP address or host name of the management controller.
   - **User Name** and **User 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 Unisphere Central is restricted based on the privilege and user groups assigned to the Storage Center user.

   - **Folder** – Select the parent folder for the Storage Center.
4. (Optional) Configure the Storage Center to use settings applied to another Storage Center by selecting the **Inherit settings from an existing Storage Center** checkbox. If this checkbox is selected, the **Inherit Settings** dialog box opens after the **Add Storage Center** dialog box closes.
5. Click **OK**.
   - If the **Inherit settings from existing Storage Center** checkbox was not selected, the Storage Center is added to Unisphere Central.
   - If the **Inherit settings from existing Storage Center** checkbox was selected, the Inherit Settings dialog box opens.
6. (Inherit settings only) Choose the Storage Center settings to inherit.
   a. Select the Storage Center from which you want to inherit settings.
   b. Select the checkbox for each category of settings that you want to inherit.
c Click OK.
- If passwords are not configured for the SupportAssist proxy, Secure Console proxy, or SMTP server, the dialog box closes.
- If a password is configured for the SupportAssist proxy, Secure Console proxy, or SMTP server, you are prompted to enter the required passwords.
d Type the required passwords to complete the dialog box.

Related link
Set Storage Center Mappings for a Reporter User

Reconnect to a Storage Center

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

1 If you are connected to a Data Collector and a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2 From the STORAGE menu, select Storage Centers. The Storage Centers view is displayed.
3 In the Storage Centers view, click the name of a Storage Center with a status of Down. The Reconnect to Storage Center dialog box opens.
4 Type the information needed to reconnect to the Storage Center.
   - Host or IP Address – Type the host name or IP address of a Storage Center controller. For a dual-controller Storage Center, type the IP address or host name of the management controller.
   - User Name and User 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 Unisphere Central is restricted based on the privilege and user groups 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 Unisphere Central.

1 Click the HOME menu. The Unisphere Central Home page is displayed.
   If you are connected to a Data Collector and a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane to display to the Home page.
2 From the STORAGE menu, select Storage Centers. The Storage Centers view is displayed.
3 In the Storage Centers view, select the Storage Center you want to remove.
4 Click (Delete). A confirmation dialog box opens.
5 Click Yes to remove the Storage Center.

Organizing Storage Centers

Use folders to group Storage Centers in Unisphere Central.

NOTE: For user interface reference information, click Help.
Create a Storage Center Folder

Use folders to group and organize Storage Centers.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Under the STORAGE menu, click Storage Centers. The Storage Centers view is displayed.
3. In the Storage Centers view, click +  (New), and select New Folder. The Create Folder dialog box opens.
4. In the Name field, type a name for the folder.
5. From the Parent drop-down list, select a parent folder.
6. Click OK.

Move a Storage Center Into a Folder

Storage Centers can be organized into folders.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Under the STORAGE menu, click Storage Centers. The Storage Centers view is displayed.
3. In the Storage Center view, click ... (More Actions), and then select Move. The Move to Folder dialog box opens.
4. Select the folder to which to move the Storage Center.
5. Click OK.

Rename a Storage Center Folder

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

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Under the STORAGE menu, click Storage Centers. The Storage Centers view is displayed.
3. In the Storage Centers view, select the Storage Center folder you want to modify.
4. Click / (Edit). The Edit dialog box opens.
5. In the Name field, type a name for the folder.
6. Click OK.

Delete a Storage Center Folder

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

Prerequisite
The Storage Center folder must be empty.
Steps

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Under the STORAGE menu, click Storage Centers.
   The Storage Centers view is displayed.
3. In the Storage Center view, select the Storage Center folder to delete.
4. Click (Delete).
   The Delete Folder dialog box opens.
5. Click Yes.

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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Type</td>
<td>Specifies the disk folder, tier redundancy, and data page size of the storage used by the volume.</td>
</tr>
<tr>
<td>Storage Profile</td>
<td>Controls the RAID type, storage tiers, and data progression behavior for pages used by the volume.</td>
</tr>
<tr>
<td>Snapshot Profile</td>
<td>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).</td>
</tr>
<tr>
<td>QoS Profile</td>
<td>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.</td>
</tr>
</tbody>
</table>

Related link
Managing Snapshot Profiles

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 Single Volume

Use the New Volume dialog box to create a single volume.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, click (New), and select New Volume.
The New Volume dialog box opens.

4 In the Volume Count field, type 1 to create a single volume.
5 In the Name field, type a name for the volume.
6 In the Configured Size field, type a size for the volume in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).
7 In the Volume Folder pane, select the parent folder for the volume.
8 (Optional) Configure the remaining volume attributes as needed.
   - Select the The Import To Lowest Tier checkbox to force all data written to the volume to the lowest storage tier configured for the volume. Enabling this option decreases performance for the volume.
   - To map the volume to a server, select a server from the Server drop-down list.
   - To schedule snapshot creation and expiration for the volume, apply one or more Snapshot Profiles by clicking Change across from Snapshot Profiles.
   - To enable or disable snapshot functions, select or clear the following checkboxes:
     - Pause Snapshot Creation
     - Pause Snapshot Expiration
     - Allow Snapshots to coalesce into active Snapshot

The following options are available only if the they are enabled in the Storage Center Settings dialog box:
   - To use specific disk tiers and RAID levels for volume data, select the appropriate storage profile from the Storage Profile drop-down list located in the Tiering section. 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 list located in the Tiering section.
   - To set a volume QoS profile, select a profile from the Volume QoS Profile drop-down list located in the QoS Profiles section.
   - To set a group QoS profile, select a profile from the Group QoS Profile drop-down list located in the QoS Profiles section.
   - To enable Data Compression to reduce disk space usage, select Compression from the Data Reduction Profile drop-down list.

† **NOTE:** The Data Compression setting will be applied to all volumes that share one or more snapshots with this volume. These shared volumes are referred to as siblings in the message displayed.
9 Click OK.

Create Multiple Volumes Simultaneously

You can create multiple volumes at a time.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3 In the Volumes view click + (New), and select New Volume.
   The New Volume dialog box opens.
4 In the Volume Count field, type the number of volumes to create.
5 In the Name field, type a base name for the volumes. Each volume is named with a combination of the base name and the volume number.
6 In the Configured Size field, type a size for the volumes in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).
7 In the Volume Folder pane, select the parent folder for the volumes.
8 (Optional) Configure the remaining volume attributes as needed.
   - Select the The Import To Lowest Tier checkbox to force all data written to the volume to the lowest storage tier configured for the volume. Enabling this option decreases performance for the volume.
   - To map the volume to a server, select a server from the Server drop-down list.
   - To schedule snapshot creation and expiration for the volume, apply one or more snapshot profiles by clicking Change across from Snapshot Profiles.
To enable or disable snapshot functions, select or clear the following checkboxes:

- Pause Snapshot Creation
- Pause Snapshot Expiration
- Allow Snapshots to coalesce into active Snapshot

The following options are available only if they are enabled in the Storage Center Settings dialog box:

- To use specific disk tiers and RAID levels for volume data, select the appropriate storage profile from the Storage Profile drop-down list located in the **Tiering** section. 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 from the Storage Type drop-down list located in the **Tiering** section.
- To set a volume GoS profile, select a profile from the Volume GoS Profile drop-down list located in the **GoS Profiles** section.
- To set a group GoS profile, select a profile from the Group GoS Profile drop-down list located in the **GoS Profiles** section.
- To enable Data Compression to reduce disk space usage, select **Compression** from the Data Reduction Profile drop-down list.

**NOTE:** The Data Compression setting is applied to all of the volumes that share one or more snapshots with this volume. These shared volumes are referred to as sibling volumes.

Click **OK**.

## 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**.

### Rename a Volume

A volume can be renamed without affecting its availability.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Volumes**.
   The **Volumes** view is displayed.
3. In the **Volumes** view, select the volume you want to modify,
4. Click **Edit**.
   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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Volumes**.
   The **Volumes** view is displayed.
3. In the **Volumes** view, select the volume you want to modify,
4. Click **Move**.
   The **Move to Folder** dialog box opens.
5. In the navigation pane, select a new parent volume folder.
Move Multiple Volumes to a Different Volume Folder

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

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volumes 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.
4. Click Move. The Move to Folder dialog box opens.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volume you want to expand.
4. Click (More Actions) and select 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Make sure Allow Cache Selection is enabled for volumes in the Storage Center user preferences.
   a. In the upper right corner, click (Storage Center Settings).
      The Storage Center Settings dialog box opens.
   b. Click the Preferences tab.
   c. Make sure the Allow Cache Selection checkbox is selected.
   d. Click OK.
3. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
4. In the Volumes view select the volume you want to modify.
5. Click (Edit).
   The Edit Volume dialog box opens.

Click OK.
Enable or disable the cache options as needed.

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

- Select or clear the **Write Cache** checkbox.
  
  To improve performance, disable write caching on volumes that use SSD storage for most applications.

8 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the **STORAGE** menu, select **Volumes**.
   
   The **Volumes** view is displayed.

3 From the **Volumes** view, select the volume you want to modify.

4 Select **...(More Actions)** and select **Set Snapshot Profiles**.
   
   The **Set Snapshot Profiles** dialog box opens.

5 Select the snapshot profiles to apply to the volume.

6 Click **OK**.

## Assign Snapshot Profiles to Multiple Volumes

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

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the **STORAGE** menu, select **Volumes**.
   
   The **Volumes** view is displayed.

3 In the **Volumes** view, select the volumes 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.

4 Click **...(More Actions)** and select **Set Snapshot Profiles**.
   
   The **Set Snapshot Profiles** dialog box opens.

5 Select each snapshot profile you want to assign to the volumes.

6 To remove the snapshot profiles that were previously assigned to the volume, select **Replace Existing Snapshot Profiles**.

7 Click **OK**.

## Assign a Different Storage Profile to a Volume

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

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the **STORAGE** menu, select **Volumes**.
   
   The **Volumes** view is displayed.

3 In the **Volumes** view, select the volume you want to modify.

4 Click **...(More Actions)** and select **Set Storage Profile**.
   
   The **Set Storage Profile** dialog box opens.

5 From the **Storage Profile** drop-down menu, select a storage profile.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volumes 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.
4. Click \(\text{(More Actions)}\) and select Set Storage Profile.
   The Set Storage Profile dialog box opens.
5. From the Storage Profile drop-down menu, select a storage profile.
6. 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. New writes to the volume from a host after the import is complete will follow the Storage Profile for the volume. It is important to change the Storage Profile once the import is complete to avoid potential performance degradation by writing to the lowest tier of drives.

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

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volume you want to modify.
4. Click (Edit).
   The Edit Volume dialog box opens.
5. Select the Import to lowest tier checkbox.
6. 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 controllers.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volume you want to modify.
4. Click (Edit).
   The Edit Volume dialog box opens.
5. Expand **Advanced Settings**.

6. Configure the **Space Consumption Limit** options.
   a. Select the **Space Consumption Limit** checkbox.
   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).

7. 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 might 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the **STORAGE** menu, select **Volumes**.
   The **Volumes** view is displayed.

3. On the **Volumes** view, select the volume you want to modify.

4. Click **(Edit)**.
   The **Edit Volume** dialog box opens.

5. Expand **Advanced Settings**.

6. In the **OpenVMS Unique Disk ID** field, type a new disk ID.

7. 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.

**Prerequisite**

Consult with technical support before changing these limits.

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the **STORAGE** menu, select **Volumes**.
   The **Volumes** view is displayed.

3. On the **Volumes** view, select the volume you want to modify.

4. Click **(Edit)**.
   The **Edit Volume** dialog box opens.

5. Expand **Advanced Settings**.

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. In the **Maximum Configured Volume Space** field, type the maximum combined size for all view volumes, including the original volume, that share the same snapshot history as this volume in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB). To disable this limit, select the **Unlimited** checkbox.

8. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. On the Volumes view, select the volume you want to copy.
4. Click ... (More Actions) and select 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 link
Creating Volumes

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. On the Volumes view, select the volume you want to copy.
4. Click ... (More Actions) and select 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.
(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

(Optional) Select **Schedule Start Time** to set a time for the copy to be created.

Click **OK**.

Related link
Creating Volumes

### 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Volumes**.
   The **Volumes** view is displayed.
3. On the **Volumes** view, select the volume you want to copy.
4. Click **... (More Actions)** and select **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 link
Creating Volumes

### 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.

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

**Steps**
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Volumes**.
   The **Volumes** view is displayed.
3. In the **Volumes** view, select the volume you want to view.
   The **Copy/Mirror/Migrate** area in the **Summary** tab displays information for any copy, mirror, or migrate relationship involving the selected volume.
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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, click ➕ (New) and select New Folder.
   The New 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view Select the volume folder you want to rename.
4. Click ➕ (Edit icon).
   The Edit Volume Folder 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volume folder you want to move.
4 Click Move.

The Move to Folder dialog box opens.
5 Navigate to the appropriate folder.
6 Click OK.

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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Volumes.

The Volumes view is displayed.
3 In the Volumes view, select the volume.
4 Click ... (More Actions) and select New Snapshot.

The New Snapshot 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Volumes.

The Volumes view is displayed.
3 In the Volumes view, select the volume.
4 Click the Snapshots tab.

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.

Prerequisite

QoS Profile options are shown only if Allow QoS Profile Selection has been enabled on the Storage Center Preferences dialog box (Storage Center version 7.0 or later).
Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volume.
4. Click the Snapshots tab.
5. 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.
6. (Optional) Modify default settings for the recovery volume as needed.
   - To change the volume name, modify the Name field.
   - Select Import To Lowest Tier to force all data written to the volume to the lowest storage tier configured for the volume.
   - To schedule snapshot creation and expiration for the volume, apply one or more snapshot profiles by clicking Change across from Snapshot Profiles.
   - To add a volume QoS profile to be applied to the volume, click Change across from Volume QoS Profile. When the list of defined QoS profiles opens, select a profile, then click OK. You can also apply the default QoS profile to a volume.
   - To add a group QoS profile to be applied to the volume, click Change across from Group QoS Profile. When the list of defined QoS profiles opens, select a profile, then click OK.
7. 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.

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.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volume you want to modify.
4. Click (Edit).
   The Edit Volume dialog box opens.
5. Expand the Snapshot options.
6. Select the Allow Snapshots to coalesce into active Snapshot checkbox.
7. Click OK.

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.

1. Click the Storage tab.
2. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
3. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
4. On the Volumes pane, select the volume you want to modify.
5. Click the Snapshots tab.
6. Select the snapshot you want to expire, then click Expire.
   The Expire dialog box opens.
7. Click Yes to expire the selected snapshot.

Related link
Managing Snapshot Profiles

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volume you want to modify.
4. Select the Mappings tab.
Above the Mapped Servers section click +. The Map Volume to Server wizard opens.

Select the server to which you want to map the volume, then click Next. The wizard advances to the next page.

(Optional) Expand Advanced Mapping to configure LUN settings, restrict mapping paths, or present the volume as read-only.

Click Finish.

Map Multiple Volumes to a Server

Multiple volumes can be mapped to a server in a single operation.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3 In the Volumes view, select the volumes 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.
4 Click ... (More Actions) and select Map Volume to Server.
   The Map Volume to Server wizard opens.
5 Select the server to which you want to map the volumes, then click Next. The wizard advances to the next page.
6 (Optional) Expand Advanced Mapping to configure LUN settings, restrict mapping paths, or present the volume as read-only.
7 Click Finish.

Unmap a Volume from a Server

Unmap a volume from a server if the server no longer needs to access the volume.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3 In the Volume view, click the name of the volume you want to unmap from a server to open the Volume view.
4 Click the Mappings tab.
5 Select the server(s) to unmap from the volume, then click (Delete).
   The Remove Mappings dialog box opens.
6 Click Yes to unmap the volume from the server.

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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3 In the Volume view, click the name of the volume you want to promote.
4 Click the Mappings tab.
5 Select the server for which you want to promote the mapping, then click Promote to Cluster.
   The Promote to Cluster dialog box opens.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes. The Volumes view is displayed.
3. In the Volume view, click the name of the volume you want to unmap from a server to open the Volume view.
4. Click the Mappings tab.
5. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes. The Volumes view is displayed.
3. In the Volumes view, select the volume you want to copy.
4. Click … (More Actions) and select New Boot from SAN Copy. The New 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 schedule snapshot creation and expiration for the volume, apply one or more snapshot profiles by clicking Change across from Snapshot Profiles.
6. Click OK.

Change the LUN Used by a Volume/Server Mapping

The logical unit number identifies the volume to the server operating system.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes. The Volumes view is displayed.
3. In the Volumes view, select the volume you want to modify.
4. Click the Mappings tab.
5. Select the server for which you want to modify mapping settings, then click (Edit). The Edit Volume Mapping Settings dialog box opens.
6. 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.
7. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes. The Volumes view is displayed.
3. In the Volumes view, select the volume you want to modify.
4. Click the Mappings tab.
5. Select the server for which you want to modify mapping settings, then click (Edit). The Edit Volume Mapping Settings dialog box opens.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes. The Volumes view is displayed.
3. On the Volumes view, select the volume you want to modify.
4. Click the Mappings tab.
5. Select the server for which you want to modify mapping settings, then click (Edit). The Edit Volume Mapping Settings dialog box opens.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes. The Volumes view is displayed.

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes. The Volumes view is displayed.
In the **Volumes** view, select the volume to delete.  

4 Click ![Delete](Delete).  
   The **Delete Folder** dialog box opens.  

5 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.  

6 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.  

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.  

2 From the **STORAGE** menu, select **Volumes**.  
   The **Volumes** view is displayed.  

3 Expand the **Recycle Bin**, then select the volume in the Recycle Bin that you want to restore.  

4 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.  

2 From the **STORAGE** menu, select **Volumes**.  
   The **Volumes** view is displayed.  

3 In the **Volumes** view, expand the **Recycle Bin**.  

4 Click **Empty Recycle Bin**.  
   The **Empty Recycle Bin** dialog box opens.  

5 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.  

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.  

2 From the **STORAGE** menu, select **Volumes**.  
   The **Volumes** view is displayed.  

3 In the **Volumes** view, select the volume folder you want to delete.  

4 Click ![Delete](Delete).  
   The **Delete Folder** dialog box opens.
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 controllers.
- The controller must be running Storage Center version 6.7 or later.

**About this task**

⚠️ **CAUTION:** Resetting the controller to factory defaults erases all information on the controller and all data on the drives.

**Steps**

1. In the right pane, click **Actions** → **System** → **Reset to Factory Defaults**.
   
   The **Reset Storage Center to Factory Defaults** dialog box opens.

2. In the **Factory Reset Token** field, type the text above the **Factory Reset Token** field exactly as it appears in the dialog box.

3. In the **Storage Center Administrator Username** field, type the username of a Storage Center user with administrator-level privileges.

4. In the **Storage Center Administrator Password** field, type the password of a Storage Center user with administrator-level privileges.

5. To restart the controller after the reset, select **Power on the Storage Center after resetting to factory defaults**.

6. Click **OK**.

   The Storage Center resets to the factory default settings.

Managing Virtual Volumes With Unisphere Central

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 defined the available storage capabilities, can be created for vSphere Storage Policy-Based Management.

**Related link**

VVols

Configuring VVols in Unisphere Central

Running VVols in a storage environment requires the following software and firmware:

- Storage Center 7.0 or later
- Unisphere Central 2018 R1 connected to a Data Collector.
- VMware vSphere 6 or later

**Requirements and Recommendations for Configuring VVols in Unisphere Central**

The following requirements and recommendations apply to setting up Unisphere Central to use VVols:

- Unisphere Central must be installed on a clustered hypervisor of choice with high-availability (HA) enabled.
- Fault Tolerance is recommended.
- Unisphere Central must not be deployed or moved to a VVol datastore on the managed Storage Center. Unisphere Central must be installed and remain on a traditional SAN volume.
Unisphere Central 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.

### Safeguarding VVols Data

A critical component of the total VVols solution is VVols the VM metadata. VMware's ESXi reads and writes this metadata on a per-VVol basis 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 time (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, it is conceivable that a user may 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 (by accident), 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 and intended 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 Unisphere Central when a VMware ESXi 6.0 server type is created in Unisphere Central. vSphere recognizes them as protocol endpoints after the VASA provider is registered and a Storage Container is created using Unisphere Central.
- **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 Unisphere Central (connected to Data Collector) a to create storage containers.

### Setting Up VVols Operations on Unisphere Central

To set up and run operations for virtual volumes (VVols) in Unisphere Central, you must:

- Register VMware vCenter Server in Unisphere Central.
- Register VMware vCenter Server in Storage Center either by using **Auto manage Storage Center** option in Unisphere Central 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 Unisphere Central to create datastores of type **VVOL**, which are mapped to the storage containers on the array using Unisphere Central

---

60  Storage Center Administration
• Use vCenter to create VVol-backed VMs

Unisphere Central 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.

**Virtual Volumes Restrictions**

Volume operations on virtual volumes (VVols) are restricted to specific operations.

Storage administrators use Unisphere Central 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 against 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
- 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 Unisphere Central 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 Unisphere Central 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 Unisphere Central client, select the **Register VASA Provider** checkbox.
- For a vCenter Server that is already registered in the in the Unisphere Central client, select **Edit Settings** and then select the **Register VASA Provider** checkbox.

**Unregister a VASA Provider**

Unregister a VASA provider to remove it from vCenter.

**Prerequisite**

⚠️ **CAUTION:** The VASA provider must be unregistered before you to initiate any of these tasks:

- Any action related to uninstallation, migration, upgrade, reinstalling of Unisphere Central on same host with same IP address
- Uninstalling Unisphere Central with the intention of reinstalling on another host
- Changing the Unisphere Central FQDN
- Changing the Unisphere Central 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 Unisphere Central 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 Unisphere Central 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 Unisphere Central**

If Unisphere Central is registered with a name lookup service such as DNS server or Active Directory server, Unisphere Central certificates are generated based on its FQDN. Any IP address changes do not affect certificates. If you change the FQDN, Unisphere Central 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 Unisphere Central

In Dell Unisphere Central, certificates are based on IP addresses. After an upgrade to Dell Unisphere Central, the existing certificates remain unchanged. If you need to modify the IP address of the host, the certificates would need to be updated, as described in the following table.

<table>
<thead>
<tr>
<th>IP Change</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP changes on Windows-based Unisphere Central</td>
<td>If Unisphere Central is not registered with a name lookup service such as DNS server or Active Directory, then Unisphere Central 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 Unisphere Central to regenerate certificates based on the new IP address. After the restart, you must re-register the VASA Provider.</td>
</tr>
<tr>
<td>IP changes on the Virtual Appliance</td>
<td>On a Dell Unisphere Central Virtual Appliance, network changes such as IP address happen through the Unisphere Central and hence Unisphere Central 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, Unisphere Central restarts itself to regenerate certificates based on the new IP address. You then must re-register the VASA Provider.</td>
</tr>
<tr>
<td>Switch from an IP Address to an FQDN on DellUnisphere Central</td>
<td>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 Unisphere Central host with a name lookup service. Then configure the networking properties on the host. Then follow the Dell Unisphere Central procedure for deleting existing certificates and restart the Unisphere Central. After the restart, re-register the VASA Provider.</td>
</tr>
<tr>
<td>FGDN changes on Windows or Virtual Appliance</td>
<td>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 Unisphere Central host (or both) for the new FQDN. Then follow the old procedure for deleting certificates and restart Storage Manager. Re-register VASA Provider after Unisphere Central is running.</td>
</tr>
<tr>
<td>Switching from FGDN to IP Address on DellUnisphere Central</td>
<td>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 Unisphere Central host (or both) to remove FQDN configuration. Restart Unisphere Central for the changes to take effect and register VASA Provider again.</td>
</tr>
</tbody>
</table>

**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

You can create and use storage containers to organize VMware virtual volumes (VVols) in your environment. 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 Unisphere Central, 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. Then the datastore can be used to create VVol-based VMs.

Details about storage containers and VVols shown in the **Summary** tab when you select the **Servers** node.

### How Storage Container Options Affect vCenter Advertised Capabilities

The creation of a storage container includes specifying options such as the use of compression, deduplication, encryption, and snapshots and Storage Center Storage Profiles. When the storage container creation completes, these options are advertised as capabilities to vCenter. The following VASA version 2.0 system storage capabilities are supported by Unisphere Central, and are shown on the vCenter **Summary** tab are shown 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.

### 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 Unisphere Central 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.

1. **NOTE:** The VM Storage Profile takes precedence when compatible storage exists.

1. **NOTE:** VM storage policies are applied only to data and config VVols and not to memory and swap VVols.

1. **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.

1. **NOTE:** The advertised capabilities only apply to VVols datastores and are not supported on legacy VMFS datastores.

1. **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.

1. **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>
<thead>
<tr>
<th>Storage Container Compression</th>
<th>VM Storage Policy = None Specified</th>
<th>VM Storage Policy = Compression Enabled</th>
<th>VM Storage Policy = Compression Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Volumes created with Default Data Reduction profile value from storage container</td>
<td>Volumes created with <strong>Compression</strong> Data Reduction Profile</td>
<td>Volumes created with the Data Reduction Profile set to <strong>None</strong></td>
</tr>
<tr>
<td>Disabled</td>
<td>Volumes created with Default Data Reduction profile value from storage container</td>
<td>VM creation fails because user is trying to set an unsupported capability</td>
<td>Volumes created with the Data Reduction Profile set to <strong>None</strong></td>
</tr>
</tbody>
</table>
The following table describes the expected behavior for new VM creation with the Deduplication option.

### Table 6. Expected Behavior for New VM Creation with Deduplication

<table>
<thead>
<tr>
<th>VM Storage Policy = None Specified</th>
<th>VM Storage Policy = Deduplication Enabled</th>
<th>VM Storage Policy = Deduplication Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Container Deduplication Enabled</td>
<td>Volumes created with Default Data Reduction profile value from storage container</td>
<td>Volumes created with Deduplication with Compression Data Reduction Profile</td>
</tr>
<tr>
<td>Storage Container Deduplication Disabled</td>
<td>Volumes created with Default Data Reduction profile value from storage container</td>
<td>VM creation fails because user is trying to set an unsupported capability</td>
</tr>
</tbody>
</table>

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 7. Expected Behavior for VM Storage Policy Update on Existing VMs

<table>
<thead>
<tr>
<th>Old VM Storage Policy</th>
<th>New VM Storage Policy</th>
<th>Expected Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compression Enabled</td>
<td>Compression Disabled</td>
<td>Data Reduction Profile of associated VVols changes from <strong>Compression</strong> to <strong>None</strong>. Data is uncompressed at the next data progression cycle.</td>
</tr>
<tr>
<td>Compression Disabled/ None Specified</td>
<td>Compression Enabled</td>
<td>Data Reduction Profile of associated VVols changes from <strong>None</strong> to <strong>Compression</strong>. Data is compressed at the next data progression cycle.</td>
</tr>
<tr>
<td>Deduplication Disabled</td>
<td>Deduplication Enabled</td>
<td>Data Reduction Profile of associated VVols changes to <strong>Deduplication with Compression</strong>. Data is deduplicated at the next data progression cycle.</td>
</tr>
<tr>
<td>Deduplication Enabled</td>
<td>Deduplication Disabled</td>
<td>Data Reduction Profile of associated VVols changes from <strong>Deduplication with Compression</strong> to <strong>None</strong>. Data is rehydrated at the next data progression cycle.</td>
</tr>
</tbody>
</table>

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 8. Expected Behavior for Compression and Deduplication Checkboxes on Storage Container

<table>
<thead>
<tr>
<th>Old Checkbox Value</th>
<th>New Checkbox Value</th>
<th>Expected Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compression Enabled</td>
<td>Compression Disabled</td>
<td>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 Table 5. Expected Behavior for New VM Creation with Compression and might fail if the VM Storage Policy is now noncompliant. New volumes are created with the Data Reduction Profile set to <strong>None</strong>.</td>
</tr>
<tr>
<td>Compression Disabled</td>
<td>Compression Enabled</td>
<td>Data Reduction Profile of existing volumes remains unchanged. Clone/Fast Clone of VM to the same storage container follows rules of Table 5. Expected Behavior for New VM Creation with Compression and does not fail. New volumes are created with the Data Reduction Profile according to Table 5. Expected Behavior for New VM Creation with Compression.</td>
</tr>
<tr>
<td>Deduplication Disabled</td>
<td>Deduplication Enabled</td>
<td>Data Reduction Profile of existing volumes remains unchanged.</td>
</tr>
</tbody>
</table>
Create a Storage Container

Create a storage container to define storage options for virtual volumes (VVols).

About this task

1. **NOTE:** Storage Center supports a maximum of 50 storage containers per Storage Center.
Steps

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the **Storage** menu, select **Volumes**.
   The **Volumes** view is displayed.

3. In the **Volumes** view, click **+ (New)**, and select **New Storage Container**.
   The **Create Storage Container** dialog box opens.

4. 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, select a folder from the **Volume Folder** drop-down menu.
   d. In the **Storage Type** field, select a storage type from the drop-down list.

5. 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. To specify the storage profiles to allow for new volumes created within the storage container, select profiles from the **Allowed Storage Profiles** table.

6. Specify the default settings for new volumes created within the storage container:
   a. Select the default snapshot profile setting from the **Snapshot Profile** drop-down menu.
   b. Select the default storage profile setting from the **Storage Profile** drop-down menu.
   c. Select the default data reduction profile setting from the **Data Reduction Profile** drop-down menu.
   d. Select the default data reduction input setting from the **Data Reduction Input** drop-down menu.

7. Click **OK**.

**Edit a Storage Container**

Modify a storage container to edit its settings.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the **Storage** menu, select **Volumes**.
   The **Volumes** view is displayed.

3. Click the name of the storage container to modify.

4. Click **✏️ (Edit)**.
   The **Edit Storage Container** 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**

1. **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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the **Storage** menu, select **Volumes**.
   The **Volumes** view is displayed.
Click the name of the storage container to delete.

Click (Delete).

The Delete Storage Containers dialog box opens.

Click Yes.

View Storage Container Information

Use the Volumes view to display information about storage containers and virtual volumes (VVols).

Storage containers are accessible from the Volumes view along with other 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, and Growth tabs.

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.

NOTE: Data Reduction is available in Storage Center version 7.0 or later.

Supported Hardware Platforms

The following controller series support Data Reduction:

- SCv3000 Series (Supports Compression only)
- SC4020
- SC5020
- SC5020F
- SC7020
- SC7020F
- SC8000
- SC9000

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.

Prerequisite

Data Reduction must be applied to the volume.
Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volume you want to modify.
4. Click (Edit).
   The Edit Volume dialog box opens.
5. Expand the Data Reduction menu.
6. 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
7. Click OK to close the Edit Advanced Volume Settings dialog box.
8. Click OK.

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.
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. On the Volumes view, select the volume you want to modify.
4. Click (Edit).
   The Edit Volume dialog box opens.
5. Expand Data Reduction.
6. From the Data Reduction Profile drop-down list, select Compression.
7. Click OK.

Related links
Creating Volumes
Modifying Volumes
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.

Prerequisite

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Volumes.
   The Volumes view is displayed.
3. In the Volumes view, select the volume you want to modify.
4. Click (Edit).
   The Edit Volume dialog box opens.
5. Expand Data Reduction.
6. 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 – 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 – 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Storage Types.
   The Storage Types view is displayed.
3. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the STORAGE menu, select Volumes. The Volumes view is displayed.

3. In the Volumes view, select the volume you want to view.

4. Click the Tiering tab. The amount of space saved by data reduction on that volume is displayed at the bottom of the Tiering page.

Change the Default Data Reduction Profile

The default Data Reduction profile determines what type of data reduction is applied to new volumes created by a Unisphere Central user. Allow Data Reduction Selection displays the data reduction options when creating volumes.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. Click the HOME menu. The Unisphere Central Home page is displayed.

3. In the upper right corner of the Summary view, click (Settings). The Edit Storage Center Settings dialog box opens.

4. Click the Preferences tab.

5. From the Data Reduction Profile drop-down list, select the Default Data Reduction profile.
   - Select Compression to apply compression to all new volumes.
   - In the Volume options, select Deduplication with Compression to apply deduplication and compression to all new volumes.

⚠️ **NOTE:** The setting will be applied to all volumes that share one or more snapshots with this volume. These shared volumes are referred to as siblings in the message displayed.

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the STORAGE menu, select Volumes. The Volumes view is displayed.

3. In the Volumes view, select the volume you want to modify.

4. Click (Edit). The Edit Volume dialog box opens.
5 Expand the Data Reduction option.
6 Pause or resume Data Reduction on the volume.
   • To pause Data Reduction, select the Data ReductionPaused checkbox.
   • To resume Data Reduction, clear the Data ReductionPaused 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**

1 **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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click the HOME menu.
   The Unisphere Central Home page is displayed.

3 In the Summary view, click the Settings icon.
   The Edit Storage Center Settings dialog box opens.

4 Click the Storage tab.

5 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.

6 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the STORAGE menu, select Volumes.
   The Volumes view is displayed.

3 In the Volumes view, select the volume you want to modify.

4 Click (Edit).
   The Edit Volume dialog box opens.

5 Expand the Data Reduction option.

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.

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.

<table>
<thead>
<tr>
<th>Consistent Snapshot Profile</th>
<th>Non-Consistent Snapshot Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Halts I/O across all volumes as a group</td>
<td>Halts I/O for each volume independently of other volumes.</td>
</tr>
<tr>
<td>Resource intensive</td>
<td>Less resource intensive — depends on the amount of data written since the previous snapshot</td>
</tr>
<tr>
<td>Number of volumes limited based on storage controller.</td>
<td>No limit to the number of volumes to which the snapshot profile is attached</td>
</tr>
<tr>
<td>SC8000, SC9000, SC7020, and SC7020F: 100</td>
<td></td>
</tr>
<tr>
<td>SC5020 and SC5020F: 50</td>
<td></td>
</tr>
<tr>
<td>SC4020: 40</td>
<td></td>
</tr>
<tr>
<td>SCv2000 and SCv3000 series: 25</td>
<td></td>
</tr>
<tr>
<td>Snapshots are taken of all volumes simultaneously</td>
<td>Choose between standard (one volume at a time) or parallel (all volumes simultaneously)</td>
</tr>
<tr>
<td>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.)</td>
<td>All snapshots are taken</td>
</tr>
<tr>
<td>Can delete incomplete group of snapshots</td>
<td>All snapshots are taken</td>
</tr>
<tr>
<td>Can be converted to Non-Consistent snapshot profile</td>
<td>Can be converted to Consistent snapshot profile</td>
</tr>
</tbody>
</table>

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click Snapshot Profiles.
4. Click ➕ New and select New Snapshot Profile from the menu.
   The New 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click Snapshot Profiles.
4. Select the profile to use from the Snapshot Profile section.
5. Click Apply to Volumes. The Apply to Volumes dialog box opens.
6. 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.
7. (Optional) To remove existing snapshot profiles from the selected volumes, select Replace existing Snapshot Profiles.
8. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
In the Profiles view, click **Snapshot Profiles**.

Select the profile to use from the **Snapshot Profile** section.

Click **Apply to Server**.

The **Apply to Server** dialog box opens.

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.

(Optional) To remove existing Snapshot Profiles from the selected server, select **Replace existing Snapshot Profiles**.

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the **STORAGE** menu, select **Profiles**.

   The Profiles view is displayed.

3. In the Profiles view, click **Snapshot Profiles**.

4. Click + and select **New Snapshot Profile** from the menu.

   The **New Snapshot Profile** dialog box opens.

5. 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**.

6. (Optional) In the **Description** field, type a description of the snapshot. The default descriptive text is "Manually Created."

7. 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 snapshot profile.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the **STORAGE** menu, select **Profiles**.

   The Profiles view is displayed.

3. In the Profiles view, click **Snapshot Profiles**.

4. Select the profile to rename in the Snapshot section.

5. Click **(Edit)**.

   The **Edit Snapshot Profile** dialog box opens.

6. In the **Name** field, type a new name for the snapshot profile.

7. Click **OK**.
**Modify Rules for a Snapshot Profile**

Snapshot Profile rules determine when snapshots are created and expired.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the `STORAGE` menu, select `Profiles`.
   - The `Profiles` view is displayed.
3. In the `Profiles` view, click `Snapshot Profiles`.
4. Select the profile to modify in the Snapshot section.
5. Click `Edit`.
   - The `Edit Snapshot Profile` dialog box opens.
6. (Optional) Add a rule to the snapshot profile.
   a. Click `+` under the Rules heading.
   - The `Add Rule` dialog box opens.
   b. In the `Expiration` field, type the length of time to keep snapshots before deleting them.
   c. Select the `Schedule Type` to set the frequency at which the rule runs.
   d. Configure the dates and times at which you want snapshots to be created.
   e. Click `OK`.
7. (Optional) Modify the existing rules as needed.
   - To modify a rule, select the rule, then click `Edit`.
   - To remove a rule, select the rule, then click `Delete`.
8. Click `OK`.

**Change the Snapshot Creation Method for a Snapshot Profile**

The snapshot creation method controls how snapshots triggered by the snapshot profile are created.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the `STORAGE` menu, select `Profiles`.
   - The `Profiles` view is displayed.
3. In the `Profiles` view, click `Snapshot Profiles`.
4. Select the profile to modify in the Snapshot section.
5. Click `Edit`.
   - The `Edit Snapshot Profile` dialog box opens.
6. 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.
7. Click `OK`. 
Delete a Snapshot Profile

A snapshot profile cannot be deleted if it is being used by any volumes.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click Snapshot Profiles.
4. Select the snapshot profile to delete.
5. Make sure the snapshot profile is not in use by any volumes.
6. Click (Delete).
   A confirmation dialog box is displayed.
7. Click Yes.

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. Remote Snapshots are applicable only to Storage Centers that are managed by a Data Collector.

| 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view click the Snapshot Profiles tab.
4. Click Rules subtab.
5. Click Edit Remote Snapshot Expiration.
   The Edit Remote Snapshot Expiration dialog box opens.
6. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
In the Profiles view, click the Snapshot Profiles tab.

Click the Remote Expiration Rules subtab.

Select the remote expiration rule to modify and click (Edit Remote Snapshot Expiration).

The Edit Remote Snapshot Expiration dialog box opens.

Configure the remote snapshot expiration rule.

- In the Remote Expiration field, specify the number of minutes, hours, days, or weeks to keep the remote snapshot before deleting it.
- 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.

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.

Prerequisite

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   
The Profiles view is displayed.
3. In the Profiles view, click the Storage Profiles tab.
4. Click (New).
   
The New Storage Profile dialog box opens.
5. Configure the storage profile.
   
   - Type a name for the storage profile in the Name field.
   - Select the RAID levels to use for volumes associated with the storage profile from the RAID Type Used drop-down menu.
   - In the Tiers Used 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.

Prerequisite

In the Storage Center User Volume Defaults area, the Allow Storage Profile selection checkbox must be selected.

About this task

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click the Storage Profiles tab.
4. Click + (New).
   The New 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 drop-down menu.
   e. Select the RAID level to use for snapshot data in tier 2 from the Tier 2 drop-down menu.
   f. Select the RAID level to use for snapshot data in tier 3 from the Tier 3 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.
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click the Storage Profiles tab.
4. Select the storage profile to apply to a volume.
5. Click Apply to Volumes.
   The Apply to Volumes dialog box opens.
6. Select the volumes to which you want to apply the storage profile.
7. 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.
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click the Storage Profiles tab.
4. Select the storage profile to apply to a server.
5. Click Apply to Server Volumes.
   The Apply to Server Volumes dialog box opens.
6. Select the server to which you want to apply the storage profile.
7. 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click Storage Profiles.
4. In the Storage Profile section, select the storage profile to delete.
5. Click (Delete).
   A confirmation dialog box is displayed.
6. Click Yes.

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.

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click QoS Profiles.
4. In the Qos Profiles area, select the type of profile to create.
   - Volume
   - Group
5. Click + (New).
   The New QoS Profile dialog box opens.
6. Configure the QoS profile.
a In the Name field, type a name for the QoS profile.
b (Optional for volume QoS profiles only) In the Relative Priority field, select the priority of profile in relation to other QoS profiles. To specify a custom relative priority, select Custom and type a number in the Priority Value field.
c (Optional for volume QoS profiles only) Select Enable Latency Threshold Alert, then type a value in milliseconds for the latency alert threshold.
d (Optional) Select Limit by IOPS, then type a value for the maximum I/O per second allowed.
e (Optional) Select Limit by Bandwidth, then type a value for the maximum MB per second allowed.

7 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Profiles. The Profiles view is displayed.
3 In the Profiles view, click Qos Profiles.
4 In the QoS Profile section select the QoS profile you want to modify.
5 Click (Edit). The Edit QoS Profile dialog box opens.
6 Where allowed, modify the values. The profile type field cannot be modified.
7 Click OK.

Delete a QoS Volume Profile

Delete a QoS profile for a volume.

Prerequisite
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 In the Storage tab navigation tab, expand QoS Profiles and select the profile to be deleted.
2 Right-click the profile and select Delete. A confirmation dialog box opens to request approval for the deletion.
3 Click OK.
4 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
5 From the STORAGE menu, select Profiles. The Profiles view is displayed.
6 In the Profiles view, click Qos Profiles.
7 Select the QoS profile to delete and click (Delete).

Apply a QoS Profile to a Volume

Apply a previously defined QoS profile to a volume.

Prerequisite
The QoS profile must already exist.
Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click QoS Profiles.
4. In the QoS Profiles section select the profile to apply.
5. Select Apply to Volumes.
   The Apply to Volumes dialog box opens.
6. Select the checkbox next to each volume to which you want to apply the QoS profile.
7. Click OK.

Remove a Group QoS Profile From a Volume
Remove a Group QoS profile previously associated with one or more volumes.
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Profiles.
   The Profiles view is displayed.
3. In the Profiles view, click QoS Profiles.
4. Select the Group QoS profile to be removed and click Remove Group Profile from Volume.
5. Select the checkbox next to each volume from which you want to remove the QoS profile.
6. 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.

Prerequisite
The external device must be connected to the controller using iSCSI.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the DATA MOBILITY menu, select Imports.
   The Imports view is displayed.
3. Click the Connections tab.
4. Click Create iSCSI Remote Connection.
   The Create iSCSI Remote 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 OK.
Scan for External Devices

After connecting an external device to the controller, use Unisphere to locate the device and add it to the system.

Prerequisite
The external device must be connected to the controller using iSCSI.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the DATA MOBILITY menu, select Imports.
   The Imports view is displayed.
3. Click the External Devices tab.
4. Click Scan for External Devices.
   A confirmation dialog box is displayed.
5. Click Yes.
   Unisphere identifies external devices connected to the system and adds them to the External Devices view.

Rediscover an iSCSI Remote Connection

If a remote connection is lost, you can rediscover and reconnect to the external device.

Prerequisite
The external device must be connected to the controller using iSCSI.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the DATA MOBILITY menu, select Imports.
   The Imports view is displayed.
3. Click the Connections tab.
4. Click Rediscover iSCSI Remote Connections.
   A confirmation dialog box is displayed.
5. Click Yes.
   Unisphere identifies external devices connected to the system that allow discovery, and adds them to the Connections view.

Delete a Remote Connection

Use the Data Mobility menu to remove a remote connection when it is no longer needed.

Prerequisite
The external device must be connected to the controller using iSCSI.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the DATA MOBILITY menu, select Imports.
   The Imports view is displayed.
3. Click the Connections tab.
4. Select the connection to remove.
5. Click Delete iSCSI Remote Connection.
   A confirmation dialog box is displayed.
6. Click Yes.
Storage Center Import Requirements

A Storage Center storage system must meet the following requirements to import data from a PS Series storage array.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Center OS version</td>
<td>Version 6.7 or later</td>
</tr>
<tr>
<td>Connectivity</td>
<td>iSCSI</td>
</tr>
<tr>
<td>Network</td>
<td>Low-Latency, High-Bandwidth</td>
</tr>
</tbody>
</table>

Supported Server Operating Systems for Online Import

Performing an online import of volumes from an EqualLogic 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](https://www.dell.com/support/kbdoc) located in the Dell Knowledge Base.

Steps

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the ![DATA MOBILITY](https://www.dell.com/support) menu, select **Imports**.
   
   The **Imports** view is displayed.
3. Click the **External Devices** tab.
4. Click **Offline Import From External Device**.
   
   The **Offline Import From External Device** dialog box opens.
5. Modify the import settings as needed.
6. Click **OK**.
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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **DATA MOBILITY** menu, select **Imports**.
   - The **Imports** view is displayed.
3. Click the **External Devices** tab.
4. From the **Server** drop down box select the server to map to the destination volume.
5. Click **Online Import from External Device**.
   - The **Online Import from External Device** dialog box opens.
6. Modify the import settings as needed.
7. Click **OK**.

Restart an External Device Import

If an external device import becomes unresponsive, use this procedure to restart the process.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **DATA MOBILITY** menu, select **Imports**.
   - The **Imports** view is displayed.
3. Click the **External Devices** tab.
4. Click **Restart External Device Import**.
   - A confirmation dialog box is displayed.
5. Click **Yes**.
Storage Center Server Administration

Unisphere allows you to allocate storage on a Storage Center to the servers in your SAN environment. To present storage to a server, a server object must be added to the Storage Center.

Managing Servers on a Storage Center

Use the **Servers** view to create and manage server objects for a Storage Center.

![Unisphere Servers View](Image)

**Figure 3. Unisphere Servers View**

1 | **NOTE:** Server Agent features are not supported on the Data Collector.

Related links
- Creating Servers
- Modifying Servers
- Mapping Volumes to Servers
- Creating and Managing Server Folders
- Deleting Servers and Server Folders

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.

1 | **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.

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

3 From the STORAGE menu, select Servers.
   The Servers view is displayed.

4 Click ➕(New), then select New Server.
   The New Server dialog box opens.

5 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. Select a server folder from the Server Folder drop-down menu.
   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 HBAs table.
      - If a server HBA is not visible to the Storage Center, click ➕(New) 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.

6 Click OK.

Related links
   Configure Front-End I/O Ports (Fibre Channel and SAS)
   Configure Front-End I/O Ports (iSCSI)

Create a Virtual Server

Create a virtual server object to represent a virtual machine in your environment.

Prerequisite
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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

3 From the STORAGE menu, select Servers.
   The Servers view is displayed.

4 Select the server that hosts the virtual server in the Server view.

5 Click ➕(New) and select New Virtual Server.
   The New Virtual Server dialog box opens.

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. Select the operating system for the server from the Operating System drop-down menu.
c. To generate Storage Center alerts when connectivity is lost between the Storage Center and the server, select Alert On Lost Connectivity.
d. 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 HBAs table.
   • If a server HBA is not visible to the Storage Center, click + (New) 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 links
Configure Front-End I/O Ports (Fibre Channel and SAS)
Configure Front-End I/O Ports (iSCSI)

Create a Server Cluster

Create a server cluster object to represent a cluster of servers in your environment.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   The Servers view is displayed.
3. Click + (New), then select New Server Cluster.
   The New Server Cluster dialog box opens.
4. 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. Select a server folder from the Server Folder drop-down menu.
   c. From the Operating System drop-down menu, select the operating system for the cluster.
   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.
5. Add servers to the server cluster.
   • To add existing servers to the cluster, select the checkboxes of the servers to add from the Servers table.
   • To define a new server, click + (New), configure the server attributes, and then click OK.
6. Click OK.

Modifying Servers

Modify a server to change its attributes, apply a Snapshot Profile, and add or remove HBAs.
**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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   - The Servers view is displayed.
3. Select the server.
4. Click (Edit).
   - The Edit Server dialog box opens.
5. Type a name for the server in the Name field.
6. Click OK.

**Move a Server to a Different Server Folder**

For convenience, server objects can be organized by folders.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   - The Servers view is displayed.
3. Select the server.
4. Click Move.
   - The Move to Folder dialog box opens.
5. Select the folder to which to move the server.
6. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   - The Servers view is displayed.
3. Select the server.
4. Click (Edit).
   - The Edit Server dialog box opens.
5. Select the operating system for the server from the Operating System drop-down list.
6. Click OK.

**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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
Add a Server to a Server Cluster

You can add a server to a server cluster.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   The Servers view is displayed.
3. Select the server to add to the cluster.
4. Click (More Actions), then select Add 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   The Servers view is displayed.
3. Expand the server cluster.
4. Select the server to remove from the server cluster.
5. Click (More Actions), then select Remove from Cluster.
   The Remove Server from Cluster dialog box opens.
6. Click Yes.

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   The Servers view is displayed.
3. Select the physical server to convert to a virtual server.
4. Click (More Actions), then select 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   The Servers view is displayed.
3. Select the virtual server to convert to a physical server.
4. Click ...(More Actions), then select Convert to Physical Server.
   The Convert to Physical Server dialog box opens.
5. 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.

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
3. From the STORAGE menu, select Servers.
   The Servers view is displayed.
4. Select the server.
5. Click ...(More Actions), then select Add HBAs.
   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.
   - 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 links
Configure Front-End I/O Ports (Fibre Channel and SAS)
Configure Front-End I/O Ports (iSCSI)

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   The Servers view is displayed.
3. Select the server.
4. Click ...(More Actions), then select Remove HBAs.
   The Remove HBAs from Server dialog box opens.
5. Select the checkboxes of the HBAs to remove from the server.
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.
- If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
- From the STORAGE menu, select Servers.
- The Servers view is displayed.
- Select the server.
- Click Map Volume to Server.
- The Map Volume to Server wizard opens.
- In the Volume area, select the volume you want to map to the server.
- Click Next.
- The Map Volume to Server wizard advances to the next page.
- (Optional) Configure LUN settings, restrict mapping paths, or present the volume as read-only.
- 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.

- If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
- From the STORAGE menu, select Servers.
- The Servers view is displayed.
- Select the server.
- Click (More Actions), then select Remove Volume Mappings.
- The Remove Mappings dialog box opens.
- Select the checkboxes of the volumes to unmap from the server.
- 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.

- If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
- From the STORAGE menu, select Servers.
- The Servers view is displayed.
- Select the server to which to map a new volume.
- Click (New), then select New Volume.
- The New Volume select box opens.
- Leave the Volume Count field set to 1.
Type a name for the volume in the **Name** field.

Select a unit of storage from the drop-down menu and enter the size for the volume in the **Configured Size** field. The available storage units are bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), and terabytes (TB).

Select a parent folder for the volume from the **Volume Folder** drop-down menu.

To force all data written to the volume to the lowest tier, select the **Import to Lowest Tier** checkbox.

(Optional) Configure the remaining volume attributes as needed.

- To allocate storage to the volume before the volume is mapped to the server, select the **Preallocate Storage** checkbox.

  **NOTE:** When a volume is preallocated, the Storage Center allocates all of the space on the volume to 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.

- To schedule snapshot creation and expiration for the volume, apply one or more Snapshot Profiles by clicking **Change** located to the right of **Snapshot Profiles**. The default Snapshot Profile is Daily.

- To configure LUN settings, restrict mapping paths, configure multipathing, or present the volume as read-only, click **Advanced Mapping**.

- To prevent snapshots from being created by a Snapshot Profile, select the **Pause Snapshot Creation** checkbox.

- To temporarily stop snapshot expiration, select the **Pause Snapshot Expiration** checkbox.

- To allow space management snapshots to be combined into the next scheduled or manual snapshot, select the **Allow Snapshots to coalesce into active Snapshot** checkbox.

- To use specific disk tiers and RAID levels for volume data, select the appropriate Storage Profile from the **Storage Profile** drop-down menu.

  **NOTE:** 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 change the volume QoS profile for the volume, select a profile from the **Volume QoS Profile** drop-down menu.

- To change the group QoS profile for the volume, select a profile from the **Group QoS Profile** drop-down menu.

- To enable Data Reduction, select the **Compression** checkbox and select either **Compression** or **Deduplication with Compression** from the **Data Reduction Profile** drop-down menu.

Click **OK**.

**Related link**

**Modifying Volumes**

**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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the **STORAGE** menu, select **Servers**.

   The **Servers** view is displayed.

3. Select the server to which to map new volumes.

4. Click **+** (**New**), then select **New Volume**.

   The **New Volume** 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 **Configured Size** field. The available storage units are bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), and terabytes (TB).

8. Select a parent folder for the volume from the **Volume Folder** drop-down menu.

9. To force all data written to the to the lowest tier, select the **Import to Lowest Tier** checkbox.
Configure the remaining volume attributes as needed.

- To allocate storage to the volume before the volume is mapped to the server, select the **Preallocate Storage** checkbox.

**NOTE:** When a volume is preallocated, the Storage Center allocates all of the space on the volume to the server. The Free Space of the volume is 0 MB and the Used/Active Space of the volume is 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.

- To schedule snapshot creation and expiration for the volume, apply one or more Snapshot Profiles by clicking **Change** located to the right of **Snapshot Profiles**. The default Snapshot Profile is Daily.

- To configure LUN settings, restrict mapping paths, configure multipathing, or present the volume as read-only, click **Advanced Mapping**.

- To prevent snapshots from being created by a Snapshot Profile, select the **Pause Snapshot Creation** checkbox.

- To allow space management snapshots to be combined into the next scheduled or manual snapshot, select the **Allow Snapshots to coalesce into active Snapshot** checkbox.

- To use specific disk tiers and RAID levels for volume data, select the appropriate Storage Profile from the **Storage Profile** drop-down menu.

**NOTE:** 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 change the volume QoS profile for the volume, select a profile from the **Volume QoS Profile** drop-down menu.

- To change the group QoS profile for the volume, select a profile from the **Group QoS Profile** drop-down menu.

- To enable Data Reduction, select the **Compression** checkbox and select either **Compression** or **Deduplication with Compression** from the **Data Reduction Profile** drop-down menu.

Click **OK**.

Related link
Modifying Volumes

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Servers**. The **Servers** view is displayed.
3. Click **+ (New)**, then select **New Server Folder**. The **New Server Folder** dialog box opens.
4. Type a name for the folder in the **Name** field.
5. (Optional) Type information about the server folder in the **Notes** field.
6. Select a parent folder for the new folder from the **Parent** drop-down menu.
7. Click **OK**.
Rename a Server Folder

Select a different name for a server folder.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   The Servers view is displayed.
3. Select the server folder to rename.
4. Click (Edit).
   The Edit Server Folder 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   The Servers view is displayed.
3. Select the server folder to move.
4. Click (Edit).
   The Edit Server Folder dialog box opens.
5. Select a new parent folder from the Parent drop-down menu.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Servers.
   The Servers view is displayed.
3. Select the server to delete.
4. Click (Delete).
   The Delete Servers dialog box opens.
5. Click OK.
Delete a Server Folder

Delete a server folder if it is no longer needed.

**Prerequisite**
The server folder must be empty.

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the STORAGE menu, select Servers.
   The Servers view is displayed.

3. Select the server folder to delete.

4. Click ![Delete](delete_icon).  
The Delete Server Folder dialog box opens.

5. Click Yes.
Storage Center Maintenance

Unisphere can manage Storage Center settings, users and user groups, and apply settings to multiple Storage Centers. Storage Center maintenance includes operations performed on a production system such as changing the operation mode, updating software, and managing hardware.

Managing Storage Center Settings

This section describes how to configure general Storage Center settings.

Related links
- Viewing and Modifying Storage Center Information
- Configuring Storage Center User Preferences
- Configuring Storage Center Data Settings
- Configuring Storage Center Secure Console Settings
- Configuring Filters to Restrict Administrative Access

Viewing and Modifying Storage Center Information

Unisphere Central provides options for changing default properties for each individual Storage Center that is managed by Unisphere Central. You can change the Storage Center name, change the operation mode, modify network settings, and view or change license information using the Storage Center Settings dialog box.

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the General tab.
5. In the Name field, type a new name.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
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.

About this task

1. **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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click **Summary.**
   The **Summary** view is displayed.
3. Click **(Settings).**
   The **Storage Center Settings** dialog box opens.
4. Click the **Network** tab.
5. In the **Management IPv4 Settings** area, type the IPv4 addresses for the management IP.
6. (Optional) In the **Management IPv6 Settings** area, type the IPv6 addresses for the management IP.
7. (Optional) In the **Network Settings** area, type the server addresses and domain name.
8. Click **OK.**

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click **Summary.**
   The **Summary** view is displayed.
3. Click **(Settings).**
   The **Storage Center Settings** dialog box opens.
4. Click the **Storage Center License** tab to display license information.
5. 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.

**Prerequisite**

- You must be able to access a Storage Center license file from the computer from which you are running Unisphere.
About this task

1 | **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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click **Summary**.
   The Summary view is displayed.
3. Click **(Settings)**.
   The Storage Center Settings dialog box opens.
4. Click the Storage Center License tab.
5. Click **Submit License File**.
   The Submit License File dialog box opens.
6. Click **Browse**.
   The Choose File to Upload dialog box opens.
7. Browse to and select a Storage Center license file, then click **Open**.
   The Choose File to Upload dialog box closes.
8. Click **Apply**.
9. 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 Unisphere. Unisphere honors these preferences.

1 | **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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click **Summary**.
   The Summary view is displayed.
3. Click **(Settings)**.
   The Storage Center Settings dialog box opens.
4. Click the Preferences tab.
5. In the Volume Size field, type a default size for new volumes in bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).
6. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click **Summary**.
The Summary view is displayed.

3. Click 🛠️ (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Preferences tab.
5. In the Base Volume Name field, type a name to use as a base for new volumes. The default base is New Volume.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click 🛠️ (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Preferences tab.
5. Select or clear the Read Cache Enabled and Write Cache Enabled checkboxes to set the default cache settings for new volumes.
6. Select or clear the Allow Cache Selection Enabled checkbox to allow or prevent users from configuring cache settings when creating volumes.
7. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click 🛠️ (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Preferences tab.
5. Configure data reduction defaults.
   • In the Data Reduction Profile drop-down menu, set the data reduction profile default for new volumes.
   • Select the Allow Data Reduction Selection checkbox to allow users to enable or disable data reduction 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click 🛠️ (Settings).
   The Storage Center Settings dialog box opens.
4 Click the Preferences tab.
5 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.
6 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.
7 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.
1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click Summary.
   The Summary view is displayed.
3 Click (Settings).
   The Storage Center Settings dialog box opens.
4 Click the Preferences tab.
5 Select or clear the Allow Advanced Mapping Enabled checkbox to enable or disable advanced volume mapping options.
6 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.
1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click Summary.
   The Summary view is displayed.
3 Click (Settings).
   The Storage Center Settings dialog box opens.
4 Click the Preferences tab.
5 From the Operating System drop-down menu, select the default operating system for new servers.
6 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.
1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click Summary.
   The Summary view is displayed.
3 Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Preferences tab.
5. From the Storage Profile drop-down menu, select the Storage Profile to use as the default for new volumes.
6. To allow users to select a Storage Profile when creating a volume, select Allow Storage Profile Selection.
7. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Preferences tab.
5. From the Storage Type drop-down menu, select the Storage Type to use as the default for new volumes.
6. To allow users to select a Storage Type when creating a volume, select Allow Storage Type Selection.
7. Click OK.

**Set Default Volume QoS Profile**

Specify the default Volume QoS Profiles to be used for new volumes.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Preferences tab.
5. In the Quality of Service Profile area, click Change.
   The Select Volume QoS Profile dialog box opens, which shows all QoS profiles that have been defined.
6. Select one of the profiles by clicking its name.
7. Click OK.

**Allow QoS Profile Selection**

To enable users to select QoS Profiles, set the option to enabled.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Preferences tab.
5. In the Quality of Service Profiles area, select the Allow QoS Profile Selection checkbox.
6. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Storage tab.
5. Select or clear the Read Cache Enabled and Write Cache Enabled checkboxes.
6. Click OK.

Schedule or Limit Data Progression

Schedule when Data Progression runs and limit how long it is allowed to run.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Storage tab.
5. In the Data Progression Start Time field, select or type the time at which Data Progression starts running daily.
6. From the Data Progression Max Run Time drop-down menu, select the maximum time period that Data Progression is allowed to run.
7. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Storage tab.
5. From the RAID 5 Stripe Width drop-down menu, select a stripe width of 5 or 9 disks.
6  From the **RAID 6 Stripe Width** drop-down menu, select a stripe width of 6 or 10 disks.
7  Click **OK**.

**Configure an iSNS Server**

Set the host name or IP address of the Internet Storage Name Service (iSNS) server on your network.

1  If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2  Click **Summary**.
   The **Summary** view is displayed.
3  Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4  Click the **Storage** tab.
5  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.
6  Click **OK**.

**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.

1  If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2  Click **Summary**.
   The **Summary** view is displayed.
3  Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4  Click the **Automated Reports** tab.
5  Deselect the **Use global settings** checkbox.
6  Select the checkboxes in the **Automated Report Settings** area to specify which reports to generate and how often to generate them.
7  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.

8  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.

   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:** Unisphere Central 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.
9  Click **OK**.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click ➔ Summary.
   The Summary view is displayed.
3. Click ⚙ (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Time Settings tab.
5. From the Region drop-down menu, select the region where the Storage Center is located.
6. From the Time Zone drop-down menu, select the time zone where the Storage Center is located.
7. 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 Current 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.
8. Click OK.

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click ➔ Summary.
   The Summary view is displayed.
3. Click ⚙ (Settings).
   The Storage Center Settings dialog box opens.
4. Click the SMTP Server tab.
5. Configure the SMTP server settings.
   a. Select the Enable SMTP Email checkbox.
   b. In the SMTP Mail Server field, type the IP address or fully qualified domain name of the SMTP email server. Click Test Server to verify connectivity to the SMTP server.
   c. (Optional) In the Backup SMTP Server field, type the IP address or fully qualified domain name of a backup SMTP email server. Click Test Server to verify connectivity to the SMTP server.
   d. If the SMTP server requires emails to contain a MAIL FROM address, specify an email address in the Sender Email Address field.
   e. (Optional) In the Common Subject Line field, type a subject line to use for all emails sent by the Storage Center.
   f. 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) checkbox, then type the Storage Center fully qualified domain name in the Extended Hello Message (EHLO) field.
6. Click OK.
Configure SNMP Settings for a Storage Center (Storage Center 6.7)

Configure SNMP if you want to monitor the Storage Center with a network management system.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. Click \(\text{Summary}\). The Summary view is displayed.

3. Click \(\text{Settings}\). The Storage Center Settings dialog box opens.

4. Click the SNMP Server tab.

5. 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.

6. If the Agent Running status is Not Running, click Start Agent.

7. If the Storage Center supports SNMP v1 or v2, specify settings for the network management system to which Storage Center will send SNMP traps.
   a. In the Trap Community String field, type a password used to allow the Storage Center SNMP agent to communicate with the Network Management System.
   b. In the Trap Destination field, type host name or IP address of the Network Management System that is collecting trap information.
   c. From the Trap Type drop-down menu, select the trap type to use.
   d. Click Start Trap.

8. Click OK.

Configure SNMP Settings for a Storage Center (Storage Center Version 7.0 and Later)

Configure SNMP if you want to monitor the Storage Center with a network management system.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. Click \(\text{Summary}\). The Summary view is displayed.

3. Click \(\text{Settings}\). The Storage Center Settings dialog box opens.

4. Click the SNMP Server tab.

5. From the SNMP Version drop-down menu, select the version of SNMP to be configured.

6. Click Apply. The contents of the dialog box change depending on the version selected.

7. If you selected SNMP v1 or v2, 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.
If you selected SNMP v3, specify the users of SNMP v3 by selecting an existing user or creating a new one. 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.

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 notification type and the SNMP version of the trap or inform to be sent.

d. In the **Port** field, type the port number of the network management system.

e. To create an SNMP v1 or v2 trap, in the **Community String** field, type a password used to allow the Storage Center SNMP agent to communicate with the network management system.

f. To create an SNMP v3 trap, select a user from the **SNMP v3 User** drop-down menu.

g. If you selected SNMP v1 or v2, to apply the changes to SNMP settings to other Storage Centers, check **Apply these settings to other Storage Centers**.

h. Click **OK**.

If the **SNMP Running** status is **No**, click **Start SNMP**.

10. 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.

- Unisphere 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. Click **Summary**. The **Summary** view is displayed.

3. Click **(Settings)**. The **Storage Center Settings** dialog box opens.

4. Click the **IP Filtering** tab.

5. Click **Create Filter**. The **Create IP Filter** dialog box opens.

6. 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.

7 Specify which source IP addresses to allow.

   ![NOTE](image)
   **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**.

### Modify an Access Filter for a Storage Center

Modify an access filter to change the users or IP addresses it allows.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click **Summary**.
   The **Summary** view is displayed.
3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4 Click the **IP Filtering** tab.
5 Select the access filter that you want to modify, then click **Modify Filter**.
   The **Modify IP Filter** dialog box opens.
6 Modify the access filter settings as needed. For user interface reference information, click **Help**.
7 (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.
8 (Optional) Modify the allowed source IP addresses.
   ![NOTE](image)
   **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.
9 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click **Summary**.
   The **Summary** view is displayed.
3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4 Click the **IP Filtering** tab.
5 Select the access filter that you want to delete, then click **Delete Filter**. The **Delete IP Filter** dialog box opens.

6 Click **OK** to confirm.

7 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click **Summary**. The **Summary** view is displayed.

3 Click **(Settings)**. The **Storage Center Settings** dialog box opens.

4 Click the **IP Filtering** tab.

5 Click **Show Access Violations**. The **Show Access Violations** dialog box opens.

6 (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 **Yes**. The confirmation dialog box closes.
   d Click **Close**. The **Show Access Violations** dialog box closes.

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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click **Summary**. The **Summary** view is displayed.

3 Click **(Settings)**. The **Storage Center Settings** dialog box opens.

4 Click the **Secure Console** tab.

5 Select the **Enable secure console access** checkbox.

6 In the **Reservation Server Host or IP Address** field, type the host name or IP address of a secure console server provided by technical support.

7 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.

8 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.
9 Click OK.

Restart the Storage Center Secure Console Server

Troubleshooting an issue may require restarting the secure console server.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click Summary.
   The Summary view is displayed.
3 Click (Settings).
   The Storage Center Settings dialog box opens.
4 Click the Secure Console tab.
5 Click Restart Server.
   A confirmation dialog box opens.
6 Click OK to confirm.
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.

About this task

NOTE: This function applies to Unisphere Central connected to a Data Collector only.

NOTE: For user interface reference information, click Help

Steps

1 Select a Storage Center from the drop-down list in the left navigation pane.
2 Click Summary.
   The Summary view is displayed.
3 Click ... (More Actions) and select Inherit Settings from the drop-down menu.
   The Inherit Settings dialog box opens.
4 Select the Storage Center from which you want to inherit settings, then select the checkbox for each category of settings that you want to inherit.
5 Click OK.
   • 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>
<thead>
<tr>
<th>Privilege Level</th>
<th>Allowed Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Volume Manager</td>
<td>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.</td>
</tr>
<tr>
<td>Reporter</td>
<td>Read-only access to the folders associated with the assigned user groups.</td>
</tr>
</tbody>
</table>

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click **Summary**.
   - The **Summary** view is displayed.
3 Click ☰ (Settings).
   The Storage Center Settings dialog box opens.
4 Click the Users and User Groups tab.
5 On the Local Users subtab, click New User.
   The Create Local User dialog box opens.
6 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.
7 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.
8 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.
9 From the Preferred Language drop-down menu, select a language. That language will be used for email alerts.
10 (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 New 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.
11 Specify and confirm a password for the user in the Password and Confirm Password fields.
12 (Optional) Specify more information about the user in the Details area.
13 Click OK.
   The Create Local User dialog box closes.
14 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click ☰ Summary.
   The Summary view is displayed.
3 Click ☰ (Settings).
   The Storage Center Settings dialog box opens.
4 Click the Users and User Groups tab.
5 On the Local Users subtab, click More Actions > Default User Preferences.
   The Configure Default 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 Configure Default User Preferences dialog box closes.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary. The Summary view is displayed.
3. Click (Settings). The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
5. On the Local Users subtab, select the user, then click Settings. The Edit Local User Settings dialog box opens.
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 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.
7. Click OK. The local user Edit Local User Settings dialog box closes.
8. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary. The Summary view is displayed.
3. Click (Settings). The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
5. On the Local Users subtab, select the user, then click Settings. The Edit Local User Settings dialog box opens.
6. 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.
7. Click OK. The Edit Settings dialog box closes.
8. 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 from the Storage Center.

**Prerequisite**
The Storage Center must support the preferred language.

**Steps**
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click 📊 Summary.
   The **Summary** view is displayed.
3. Click ⚙️ (Settings).
   The **Storage Center Settings** dialog box opens.
4. Click the **Users and User Groups** tab.
5. On the **Local Users** subtab, select the user, then click **Settings**.
   The **Edit Local User Settings** dialog box opens.
6. From the **Preferred Language** drop-down menu, select a language.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click 📊 Summary.
   The **Summary** view is displayed.
3. Click ⚙️ (Settings).
   The **Storage Center Settings** dialog box opens.
4. Click the **Users and User Groups** tab.
5. On the **Local Users** subtab, select the user, then click **Settings**.
   The **Edit Local User Settings** dialog box opens.
6. 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.
7. Click **OK**.
   The local user **Edit Settings** dialog box closes.
8. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click 📊 Summary.
   The **Summary** view is displayed.
3. Click ⚙️ (Settings).
   The **Storage Center Settings** dialog box opens.
4. Click the **Users and User Groups** tab.
On the Local Users subtab, select the user, then click Settings. The Edit Local User Settings dialog box opens.

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 New 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.

Click OK.
The Edit Local User Settings dialog box closes.

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.

If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

Click Summary. The Summary view is displayed.

Click (Settings). The Storage Center Settings dialog box opens.

Click the Users and User Groups tab.

On the Local Users subtab, select the user, then click Settings. The Edit Local User Settings dialog box opens.

Click Configure User Preferences. The Configure User Preferences dialog box opens.

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

Click OK.
The Edit Local User Settings dialog box closes.

Click OK.

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.

If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

Click Summary. The Summary view is displayed.

Click (Settings). The Storage Center Settings dialog box opens.
4 Click the **Users and User Groups** tab.
5 On the **Local Users** subtab, select the user, then click **Settings**.
   The **Edit Local User Settings** 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 **Edit Local User Settings** dialog box closes.
9 Click **OK**.

### Change the Password for a Local Storage Center User

Changing the password for a local Storage Center user through Unisphere Central automatically updates any Storage Center mappings that were made using the user’s credentials.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click **Summary**.
   The **Summary** view is displayed.
3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4 Click the **Users and User Groups** tab.
5 On the **Local Users** subtab, select the user, then click **Change Password**.
   The **Change Password** dialog box opens.
6 Type the old password.
7 Type and confirm a new password for the local user, then click **OK**.
8 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 Unisphere cannot be deleted. The last user with the Administrator privilege cannot be deleted because Storage Center requires at least one Administrator.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click **Summary**.
   The **Summary** view is displayed.
3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4 Click the **Users and User Groups** tab.
5 On the **Local Users** subtab, select the user, then click **Delete**.
   The **Delete** dialog box opens.
6 Click **OK** to confirm.
7 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
5. On the Local Users subtab, click More Actions > Restore User.
   The Restore Deleted User wizard opens.
6. Select the local user that you want to restore, then click Next.
   The wizard advances to the next page.
7. (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.
8. Type and confirm a new password for the local user in the New Password and Confirm Password fields.
9. Modify the remaining user settings as needed.

   **NOTE:** For user interface reference information, click Help.
10. Click Finish.
11. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
   The Create Local User Group wizard opens.
6 In the **Name** field, type a name for the local user group, then click **Next**.

7 Add volume folders to the local user group.
   a If you need to create a volume folder, click **New Volume Folder**, then complete the fields in the **New Volume Folder** dialog box.
   b Click **OK** to create the volume folder.
   c Click **Next**.
     The wizard advances to the next page.

8 Add server folders to the local user group.
   a If you need to create a server folder, click **New Server Folder**, then complete the fields in the **New Server Folder** dialog box.
   b Click **OK** to create the server folder.
   c Click **Next**.
     The wizard advances to the next page.

9 Add disk folders to the local user group.
   a Select the disk folders you want to add to the local user group.
   b Click **Finish**.

10 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click **Summary**.
   The **Summary** view is displayed.

3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.

4 Click the **Users and User Groups** tab.

5 On the **Local User Groups** subtab, select the local user group, then click **Edit > Users**.
   The **Manage Users** dialog box opens.

6 Manage user membership for the user group.
   - Place a check next to the names of users you want to add.
   - Remove the check next to the names of users you want to remove.

7 Click **OK**.
   The **Manage Users** dialog box closes.

8 Click **OK**.

### 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click **Summary**.
   The **Summary** view is displayed.

3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.

4 Click the **Users and User Groups** tab.

5 On the **Local User Groups** subtab, select the local user group, then click **Edit > Folders**.
   The **Manage Folders** wizard opens.
6 Manage volume folders for the local user group.
   a If you need to create a volume folder, click **New Volume Folder**, then complete the fields in the **New Volume Folder** dialog box.
   b Click **OK**.
   c Click **Next**.
      The wizard advances to the next page.

7 Manage server folders for the local user group.
   a If you need to create a server folder, click **New Server Folder**, then complete the fields in the **New Server Folder** dialog box.
   b Click **OK**.
   c Click **Next**.
      The wizard advances to the next page.

8 Manage disk folders for the local user group.
   a Select the disk folders you want to add.
   b Click **Finish**.
      The wizard closes.

9 Click **OK**.

### Delete a Local Storage Center User Group

Delete a local Storage Center user group if it is no longer needed.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click **Summary**.
   The **Summary** view is displayed.
3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4 Click the **Users and User Groups** tab.
5 On the **Local User Groups** subtab, select the local user group, then click **Delete**.
   The **Delete** dialog box opens.
6 Click **Yes** to confirm.
7 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click **Summary**.
   The **Summary** view is displayed.
3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4 Click the **Password Configuration** tab.
5 Select the **Enabled** checkbox.
6 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.
7 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.

**Prerequisite**
Password Configuration must be enabled.

**Steps**
1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click **Summary**.
   The **Summary** view is displayed.
3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4 Click the **Password Configuration** tab.
5 Select the **Enabled** checkbox.
6 Select the **Reset Aging Clock** checkbox.
7 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.

**Prerequisite**
Password Configuration must be enabled.
Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Password Configuration tab.
5. Select the Enabled checkbox.
6. Select the Requires Password Change checkbox.
7. 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).

- 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Directory Services tab.
5. Click Configure Directory Services Automatic Discovery.
   The Storage Center automatically discovers directory server settings and displays the settings in the Directory Services Auto Configuration Wizard.
6. Type a new value into the field of any setting you want to change.
   - 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.

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**.
   b 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.
   c Click **OK** to upload the certificate.

9 Click **Next**.

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**.

13 Type the user name and password of a domain administrator.

14 Click **Next**.

15 If you want to change any setting, click **Back** to return to the previous page.

16 Click **Finish**.

17 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click Summary.
The Summary view is displayed.

3 Click (Settings).
   The Storage Center Settings dialog box opens.

4 Click the Directory Services tab.

5 Click Configure Directory Services Manually.

6 From the Directory Type drop-down menu, select Active Directory or OpenLDAP.

7 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:**
   (No escapes necessary)

   **Relative Base:**
   (The plus character is escaped)

   **Relative Base:**
   (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.

8 (Optional) Click **Test Server** to verify that the Storage Center can communicate with the specified directory servers using the selected protocol.

9 (Optional) If Transport Layer Security (TLS) is enabled, upload a Certificate Authority PEM file.
   a Click **Upload Certificate**.
   b Browse to the location of the PEM file, select the file, and click **Open**. The **Upload TLS Certificate** dialog box opens.
   c **NOTE**: If you select the wrong PEM file, click **Upload Certificate** in the **Upload TLS Certificate** dialog box to select a new file.

10 Click **Next**. The **Kerberos Settings** page opens.

11 (Optional) Select the **Enabled** checkbox to enable Kerberos authentication.

12 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.

13 Click **Next**.
   The **Join Domain** page opens.

14 Type the user name and password of a domain administrator.

15 Click **Next**.
   The **Summary** page opens.

16 If you want to change any setting, click **Back** to return to the previous page.

17 Click **Finish**.

18 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 his or her directory credentials.

**Prerequisite**
- The Storage Center must be configured to authenticate users with an external directory service.

**Steps**
1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click **Summary**.
   The **Summary** view is displayed.

3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.

4 Click the **Users and User Groups** tab.

5 On the **Directory Users** subtab, click **Add User**.
   The **Grant Access to Directory User** dialog box opens.
In the **User Principal Name** field, type the directory user name assigned to the user. The following formats are supported:

- `username@domain`
- `domain\username`

In the **Distinguished Name** field, type the distinguished name for the user.

Example: `CN=Firstname Lastname,CN=Users,DC=example,DC=com`

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.

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.

(Optional) 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 **New 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.

(Optional) Specify more information about the user in the **Details** area. For user interface reference information, click **Help**.

Click **OK**.

The **Grant Access to Directory User** dialog box closes.

### 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. Click **Summary**.

   The **Summary** view is displayed.

3. Click **(Settings)**.

   The **Storage Center Settings** dialog box opens.

4. Click the **Users and User Groups** tab.

5. On the **Directory Users** subtab, select the user, then click **Settings**.

   The **Edit Settings** dialog box opens.

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 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.

7. Click **OK**.

   The local user **Edit Settings** dialog box closes.

8. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
5. On the Directory Users subtab, select the user, then click Settings.
   The Edit Settings dialog box opens.
6. 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.
7. Click OK.
   The Edit Settings dialog box closes.
8. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
5. On the Directory Users subtab, select the user, then click Settings.
   The Edit Settings dialog box opens.
6. Enable or disable access for the directory service user.
   • To enable access, select the Enabled checkbox.
   • To disable access, clear the Enabled checkbox.
7. Click OK.
   The local user Edit Settings dialog box closes.
8. 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.

Prerequisite

• 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
5. On the Directory Users subtab, select the user, then click Settings.
   The Edit Settings dialog box opens.
6. 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.
7. Click OK.
   The local user Edit Settings dialog box closes.
8. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
5. On the Directory Users subtab, select the user, then click Settings.
   The Edit Settings dialog box opens.
6. Click Configure User Preferences. The Configure User Preferences dialog box opens.
7. Modify the user preferences as needed, 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.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
5. On the Directory Users subtab, select the user, then click Settings.
   The Edit Settings dialog box opens.
6. Click Configure User Preferences.
   The Configure User Preferences dialog box opens.
7. Modify the Real Name field as necessary.
8. Modify the fields in the Details area as necessary, then click OK.

   NOTE: For user interface reference information, click Help.
9. Click OK.
   The local user Edit Settings dialog box closes.
10. 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 Unisphere cannot be deleted. The last user with the Administrator privilege cannot be deleted because Storage Center requires at least one Administrator.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the Users and User Groups tab.
5. On the Directory Users subtab, select the user, then click Delete.
   The Delete dialog box opens.
6. Click Yes to confirm.
7. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3 Click (Settings).
The Storage Center Settings dialog box opens.
4 Click the Users and User Groups tab.
The Restore Deleted User wizard opens.
6 Select the directory service user that you want to restore, then click Next.
The wizard advances to the next page.
7 (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.
8 Modify the remaining user settings as needed.
   ⚠️ NOTE: For user interface reference information, click Help.
9 Click Finish.
The Restore Deleted User wizard closes.
10 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.

Prerequisite

- The Storage Center must be configured to authenticate users with an external directory service.

Steps

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click Summary.
The Summary view is displayed.
3 Click (Settings).
The Storage Center Settings dialog box opens.
4 Click the Users and User Groups tab.
The Grant Access to Directory User Groups dialog box opens.
6 In the Display Name field, type a name to identify the directory user group.
7 In the Distinguished Name field, type the distinguished name for the directory user group.
   Example: CN=Groupname,CN=Users,DC=example,DC=com
8 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.

9 (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.

10 Click **OK**.
   The **Grant Access to Directory User Groups** dialog box closes.

11 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click **Summary**.
   The **Summary** view is displayed.

3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.

4 Click the **Users and User Groups** tab.

5 On the **Directory User Groups** subtab, select the directory user group, then click **Edit Settings**.
   The **Edit Settings** dialog box opens.

6 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.

7 Click **OK**.
   The **Edit Settings** dialog box closes.

8 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click **Summary**.
   The **Summary** view is displayed.

3 Click **(Settings)**.
   The **Storage Center Settings** dialog box opens.
4 Click the Users and User Groups tab.
5 On the Directory User Groups subtab, select the directory user group, then click Edit Settings.
The Edit Settings dialog box opens.
6 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.
7 Click OK.
The Edit Settings dialog box closes.
8 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.
1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 Click Summary.
The Summary view is displayed.
3 Click (Settings).
The Storage Center Settings dialog box opens.
4 Click the Users and User Groups tab.
5 On the Directory User Groups subtab, select the directory user group, then click Delete.
The Delete dialog box opens.
6 Click OK to confirm.
7 Click OK.

Managing Front-End I/O Ports
Front-end ports connect an Storage Center directly to a server using SAS connections or to the Ethernet networks and Fibre Channel (FC) fabrics that contain servers that use storage. iSCSI, FC, or SAS I/O ports can be designated for use as front-end ports.

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. In 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 Centers

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 storage systems. 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 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 11. Front-End I/O Ports Failover Behavior

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Virtual Port Mode</th>
<th>Legacy Mode</th>
<th>ALUA Port Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal operating conditions</td>
<td>All ports are active and pass I/O.</td>
<td>• Primary ports pass I/O.</td>
<td>• Active/Optimized ports pass I/O.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reserved ports remain in a standby mode until a controller failure.</td>
<td>• Standby ports remain in a standby mode until a controller or port failure.</td>
</tr>
<tr>
<td>A controller fails in a dual-controller Storage Center</td>
<td>Virtual ports on the failed controller move to physical ports on the functioning controller.</td>
<td>Primary ports on the failed controller fail over to reserved ports on the functioning controller.</td>
<td>Active/Optimized ports on the failed controller fail over to the Standby ports on the functioning controller.</td>
</tr>
<tr>
<td>A single port fails (single- or dual-controller Storage Center)</td>
<td>An individual port fails over to another port on the same controller in the same fault domain.</td>
<td>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.</td>
<td>The port fails over to the Standby port on the functioning controller.</td>
</tr>
</tbody>
</table>

**NOTE:** 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.

## 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.

**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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the ✨SYSTEM menu, select Ports.
   The Ports view is displayed.
3. Click the Front End Ports tab.
4. Select the I/O port, then click ✏️ (Edit).
   The Edit Port dialog box opens.
In the Name field, type a descriptive name for the I/O port.

Click OK.

The Edit Port dialog box closes.

Set or Modify the IP Address for a Single iSCSI Port

Servers target the iSCSI port IP address to initiate iSCSI connections to the Storage Center.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3. Click the Front End Ports tab.
4. Select the I/O port, then click (Edit).
   The Edit Port dialog box opens.
5. In the IPv4 Address field, type the new IPv4 address for the iSCSI I/O port.
6. Click OK.
   The Edit Port 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3. Click the Front End Ports tab.
4. Select the I/O port, then click ... (More Actions) and select Ping from the drop-down menu.
   The Ping dialog box opens.
5. 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.
6. 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.
7. Click OK. A message displays the results of the test.
8. Click OK.

Related link

Test Network Connectivity for an iSCSI Port in a Fault Domain

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3. Click the Front End Ports tab.
4. 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the **SYSTEM** menu, select **Ports**. 
   The Ports view is displayed.
3 Click the **Front End Ports** tab.
4 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the **SYSTEM** menu, select **Ports**. 
   The Ports view is displayed.
3 Click the **Front End Ports** tab.
4 Select a down I/O port and click **Unconfigure Port**.
   The **Unconfigure Port** confirmation dialog box opens.
5 Click **OK**.

**Convert Front-End Ports to Virtual Port Mode**

Use Unisphere to convert all front-end iSCSI or Fibre Channel I/O ports to virtual port mode. After the conversion is complete, the ports cannot be converted back to legacy mode.

**Prerequisite**
The ports must be in legacy port mode.

1 | **NOTE:** This operation cannot be undone. After the ports are converted to virtual port mode, they cannot be converted back.

**Steps**

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the **SYSTEM** menu, select **Ports**. 
   The Ports view is displayed.
3 Click the **Front End Ports** tab, and then click the **Fault Domain** link. 
   The Fault Domain view opens.
4 Click **Convert**. 
   The **Convert** drop-down menu opens.
5 Select a conversion option.
   - iSCSI to Virtual Port Mode.
   - Fibre Channel to Virtual Port Mode.
   The **Convert to Virtual Port Mode** confirmation dialog box opens.
6 If converting an iSCSI port that is currently in a fault domain, type a new IP address to be used for the primary port of each iSCSI fault domain.

7 Click OK.

Managing Back-End I/O Port Hardware

Back-end SAS 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 on CT-SC040, SC8000, or SC9000 controllers. After configuring the ports, they can be used to connect enclosures.

Prerequisites

- Supports only CT-SC040, SC8000, or SC9000 controllers.
- Back-end ports have not been previously configured during Storage Center configuration.
- An enclosure must be connected to the ports.

Steps

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3 Click + (New) and select Default Storage Port Configuration.
   The Generate Default Back End Port Configuration dialog box opens and displays the status of all SAS ports.
4 Select the ports and click OK to configure the SAS ports with a status of Up as back-end ports.

Configure Individual Back-End I/O Ports

On CT-SC040, SC8000, or SC9000 controllers, a back-end port must be configured before the port can be used for back-end connectivity.

Steps

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3 Click the Back End Ports tab.
4 Select a SAS I/O port from the Unconfigured Ports table, then click Configure as Back End.
   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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3 Click the Back End Ports tab.
4 Select the I/O port, then click Edit (Edit).
   The Edit Port dialog box opens.
5 In the Name field, type a descriptive name for the I/O port.
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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3. Click the Front End Ports tab and select Fibre Channel.
4. Click + (New) and select Create Fibre Channel Fault Domain.
   The Create Fault Domain dialog box opens.
5. In the Name field, type a name for the fault domain.
6. 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.
7. Click OK.

Rename a Fibre Channel Fault Domain

The fault domain name allows administrators to identify the fault domain.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3. Click the Front End Ports tab.
4. Expand Fibre Channel and click the fault domain link.
   The Fault Domain view is displayed.
On the Summary tab, click (Edit).
The Edit Fibre Channel Fault Domain dialog box opens.

In the Name field, type a name for the fault domain.

Click OK.

Delete a Fibre Channel Fault Domain

Delete a Fibre Channel fault domain if all ports have been removed and it is no longer needed.

**Prerequisites**

- The Storage Center Fibre Channel front-end I/O ports must be configured for legacy mode. In virtual port mode, fault domains cannot be deleted.
- The fault domain must contain no FC ports.

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3. Click the Front End Ports tab.
4. Expand Fibre Channel and click the fault domain link.
   The FC Fault Domain view is displayed.
5. On the Summary tab, click (More Actions) and select Delete FC Fault Domain from the drop-down menu.
   The Delete FC Fault Domain dialog box opens.
6. 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 Unisphere.
**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.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Center controller model</td>
<td>Multi-VLAN Tagging is not supported on SCv3000 or SCv2000 storage systems.</td>
</tr>
<tr>
<td>Storage Center iSCSI I/O card</td>
<td>Chelsio T3, T5, or T6 iSCSI cards must be installed in the Storage Center.</td>
</tr>
<tr>
<td>hardware</td>
<td></td>
</tr>
<tr>
<td>Storage Center front-end</td>
<td>The Storage Center iSCSI ports must be configured for virtual port mode.</td>
</tr>
<tr>
<td>connectivity mode</td>
<td>Legacy mode is not supported.</td>
</tr>
</tbody>
</table>

**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 an iSCSI Fault Domain**

Create an 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.

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Ports**.
The Ports view is displayed.

3 Click **(New)** and select **Create iSCSI Fault Domain**.
   The **Create iSCSI Fault Domain** dialog box opens.

4 In the **Name** field, type a name for the fault domain.

5 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.

6 In the **Ports** table, select the iSCSI ports to add to the fault domain.

   **NOTE:** On Scv2000 series and Scv3000 series storage systems, the iSCSI fault domains (iSCSI Fault Domain 1 and iSCSI Fault Domain 2) are predefined and the iSCSI ports are automatically assigned to the correct fault domains.

   **NOTE:** On Scv2000 or Scv3000 series storage systems, the iSCSI fault domains (iSCSI Fault Domain 1 and iSCSI Fault Domain 2) are predefined and the iSCSI ports are automatically assigned to the correct fault domains.

7 Click **OK**.

**Related links**
- Set or Modify the IP Address for a Single iSCSI Port
- Add a VLAN ID to a Physical iSCSI Fault Domain
- iSCSI VLAN Tagging Support

### Create a VLAN Copy of an 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the **SYSTEM** menu, select **Ports**.
   The **Ports** view is displayed.

3 Click the **Front End Ports** tab.

4 Expand **iSCSI** and click the fault domain link.
   The **Fault Domain** view is displayed.

5 In the **Summary** tab, click **... (More Actions)** and select **Create VLAN Copy**.
   The **Create VLAN Copy** dialog box opens.

6 In the **Name** field, type a name for the fault domain.

7 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.

8 Configure VLAN tagging.
   a In the **VLAN ID** field, type the VLAN ID for the fault domain. Allowed values are 1–4096.
   b 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 Click **OK**.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports. The Ports view is displayed.
3. Click the Front End Ports tab.
4. Expand iSCSI and click the fault domain link. The Fault Domain view is displayed.
5. On the Summary tab, click (Edit). The Edit iSCSI Fault Domain dialog box opens.
6. In the Name field, type a name for the fault domain.
7. 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.

Prerequisite
The Storage Center iSCSI ports must be configured for virtual port mode.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports. The Ports view is displayed.
3. Click the Front End Ports tab.
4. Expand iSCSI and click the fault domain link. The Fault Domain view is displayed.
5. On the Summary tab, click (Edit). The Edit iSCSI Fault Domain dialog box opens.
6. In the Target IPv4 Address field, type an IP address to assign to the iSCSI control port.
7. In the Subnet Mask field, type the subnet mask for the well-known IP address.
8. In the Gateway IPv4 Address field, type the IP address for the iSCSI network default gateway.
9. (Optional) If IPv6 is supported, in the Target IPv6 Address field, type an IP address to assign to the iSCSI control port.
10. 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.

**Prerequisite**
The Storage Center iSCSI ports must be configured for virtual port mode.

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select **Ports**. The Ports view is displayed.
3. Click the **Front End Ports** tab.
4. Expand **iSCSI** and click the fault domain link. The Fault Domain view is displayed.
5. On the **Summary** tab, click **(Edit)**. The Edit iSCSI Fault Domain dialog box opens.
6. Select the **VLAN Tagged** checkbox.
7. In the **VLAN ID** field, type a VLAN ID for the fault domain. Allowed values are 1–4096.
8. (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. Click **OK**.

**Related link**
iSCSI VLAN Tagging Support

**Modify the MTU for an iSCSI Fault Domain**

The Maximum Transmission Unit (MTU) specifies the largest packet size supported by the iSCSI network.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select **Ports**. The Ports view is displayed.
3. Click the **Front End Ports** tab.
4. Expand **iSCSI** and click the fault domain link. The Fault Domain view is displayed.
5. On the **Summary** tab, click **(Edit)**. The Edit iSCSI Fault Domain dialog box opens.
6. From the **MTU** drop-down menu, select the largest packet size supported by the iSCSI network.
7. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select **Ports**. The Ports view is displayed.
3. Click the **Front End Ports** tab.
4 Expand iSCSI and click the fault domain link.
The Fault Domain view is displayed.
5 On the Summary tab, click \(\text{EDIT}\).
The Edit iSCSI Fault Domain dialog box opens.
6 Expand Advanced Port Settings.
7 In the Port Number field, type the TCP port to use for iSCSI traffic.
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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Ports.
The Ports view is displayed.
3 Click the Front End Ports tab.
4 Expand iSCSI and click the fault domain link.
The Fault Domain view is displayed.
5 On the Summary tab, click \(\text{EDIT}\).
The Edit iSCSI Fault Domain dialog box opens.
6 Expand Advanced Port Settings.
7 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.
8 Click OK.

Modify Digest Settings for an iSCSI Fault Domain

The iSCSI digest settings determine whether iSCSI error detection processing is performed.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Ports.
The Ports view is displayed.
3 Click the Front End Ports tab.
4 Expand iSCSI and click the fault domain link.
The Fault Domain view is displayed.
5 On the Summary tab, click \(\text{EDIT}\).
The Edit iSCSI Fault Domain dialog box opens.
6 Expand Advanced Port Settings.
7 In the Ports area, select or clear the Enable Immediate Data Write checkbox as needed.
8 Click OK.

Modify Timeout Settings for an iSCSI Fault Domain

iSCSI timeout settings determine how the Storage Center handles idle connections.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Ports.
The Ports view is displayed.
3 Click the Front End Ports tab.
4 Expand iSCSI and click the fault domain link.
The Fault Domain view is displayed.
5 On the Summary tab, click (Edit).
The Edit iSCSI Fault Domain dialog box opens.
6 Expand Advanced Port Settings.
7 In the Timeout Settings area, modify the timeout values as needed. These options are described in the online help.
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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Ports. The Ports view is displayed.
3 Click the Front End Ports tab.
4 Expand iSCSI and click the fault domain link.
The Fault Domain view is displayed.
5 On the Summary tab, click (Edit).
The Edit iSCSI Fault Domain dialog box opens.
6 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.
7 Click OK.

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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Ports. The Ports view is displayed.
3 Click the Front End Ports tab.
4 Expand iSCSI, then select the physical port for which you want to test connectivity.
5 Click ... (More Actions) and select Ping. The Ping dialog box opens.
6 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.
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 appear depending on the hardware I/O cards used by the Storage Center.

Click OK. A message displays the results of the test.

Click OK.

Related link
Test Network Connectivity for an iSCSI Port

## Remove Ports from an iSCSI Fault Domain

Before you repurpose one or more front-end iSCSI ports, remove them from the fault domains to which they belong.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3. Click the Front End Ports tab.
4. Expand iSCSI and click the fault domain link.
   The Fault Domain view is displayed.
5. On the Summary tab, click (Edit).
   The Edit iSCSI Fault Domain dialog box opens.
6. In the Ports table, deselect the iSCSI ports to remove from the fault domain.
7. 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...
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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports.
   - The Ports view is displayed.
3. Click the Front End Ports tab.
4. Expand iSCSI and click the fault domain link.
   - The Fault Domain view is displayed.
5. On the Summary tab, click *(More Actions)* and select Configure NAT Port Forwarding.
   - The Configure NAT Port Forwarding dialog box opens.
6. 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 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.
7. Repeat the preceding steps for each additional iSCSI control port and physical port in the fault domain.
8 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.

9 Repeat the preceding steps for each additional iSCSI initiator IP address or subnet that requires port forwarding.

10 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the **SYSTEM** menu, select **Ports**.
   The **Ports** view is displayed.
3 Click the **Front End Ports** tab.
4 Expand **iSCSI** and click the fault domain link.
   The **Fault Domain** view is displayed.
5 On the **Summary** tab, click **(More Actions)** and select **Configure NAT Port Forwarding**.
   The **Configure NAT Port Forwarding** dialog box opens.
6 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**.
7 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**.
8 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Ports.
   The Ports view is displayed.
3. Click the Front End Ports tab.
4. Expand iSCSI and click the fault domain link.
   The Fault Domain view is displayed.
5. On the Summary tab, click ... (More Actions) and select Configure CHAP.
   The Configure CHAP dialog box opens.
6. Select the CHAP Enabled checkbox.
7. (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.
8. 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. (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.
   e. In the Remote CHAP Secret field, type the shared secret that the remote initiator must provide when challenged by the Storage Center (target).
   f. Click OK.
      The Add Remote CHAP Initiator dialog box closes.
9. Click OK.
   The Configure CHAP dialog box closes.
10. 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Ports**.
   The **Ports** view is displayed.
3. Click the **Front End Ports** tab.
4. Expand **iSCSI** and click the fault domain link.
   The **Fault Domain** view is displayed.
5. On the **Summary** tab, click **(More Actions)** and select **Configure CHAP**.
   The **Configure CHAP** dialog box opens.
6. In the **Remote CHAP Configuration** table, select a CHAP configuration, then click **Edit**.
   The **Edit Remote CHAP Initiator** dialog box opens.
7. Modify the options as needed, then click **OK**.
   The **Edit Remote CHAP Initiator** dialog box closes.
8. 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.
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Ports**.
   The **Ports** view is displayed.
3. Click the **Front End Ports** tab.
4. Expand **iSCSI** and click the fault domain link.
   The **Fault Domain** view is displayed.
5. On the **Summary** tab, click **(More Actions)** and select **Configure CHAP**.
   The **Configure CHAP** dialog box opens.
6. In the **Remote CHAP Configuration** table, select a CHAP configuration, then click **Remove**.
   The CHAP configuration is removed from the table.
7. Click **OK**.

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.

**Prerequisite**
CHAP must be enabled for the fault domain.

**Steps**
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Ports**.
   The **Ports** view is displayed.
3. Click the **Front End Ports** tab.
4. Expand **iSCSI** and click the fault domain link.
   The **Fault Domain** view is displayed.
5. On the **Summary** tab, click **(More Actions)** and select **Configure CHAP**.
   The **Configure CHAP** dialog box opens.
6. Type a shared secret in the **Bidirectional CHAP Secret** field.
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 ports for failover purposes on SC4020 controllers.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Ports**. The **Ports** view is displayed.
3. Click + (New) and select **Create SAS Fault Domain**. The **Create SAS 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Ports**. The **Ports** view is displayed.
3. Click the **Front End Ports** tab.
4. Expand **SAS** and right-click the fault domain, then select **Delete**. The **Delete SAS 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 Unisphere 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 Unisphere 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 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 Centers (except

Disk Management on SCv2000 Series Controllers

Storage Centers with SCv2000 series controllers 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 with SCv2000 series controllers:

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

Scan for New Disks

Scanning for disks recognizes new disks and allows them to be assigned to a disk folder.

1  If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2  From the STORAGE menu, select Disks.
   The Disks view is displayed.
3  Click Scan For Disks.
   The Scan For Disks dialog box opens.
4  Click Yes.

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2  From the STORAGE menu, select Disks.
   The Disks view is displayed.
3 Click + (New).
   The New Disk Folder dialog box opens.
4 Type a name in the Name field.
5 Select the disks to be included in the disk folder.
6 Click OK.

Delete Disk Folder

Delete a disk folder if all disks have been released from the folder and the folder is not needed.

Prerequisite
The disk folder does not contain disks.

Steps
1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Disks.
   The Disks view is displayed.
3 Select a disk folder, then click (Delete).
   The Delete Disk Folder dialog box opens.
4 Click Yes.

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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Disks.
   The Disks view is displayed.
3 Expand Disks, then select a disk folder and click (Edit).
   The Edit Disk Folder dialog box opens.
4 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.
5 Click OK.

Manage Unassigned Disks

Manage Unassigned Disks assigns disks to an existing disk folder. A RAID rebalance is required to complete managing disks.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the STORAGE menu, select Disks.
   The Disks view is displayed.
3 Expand Disks and select an unassigned disk folder.
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 Select Unassigned Disks to Manage 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Hardware. The Hardware view is displayed.
3 Click the System tab.
4 In the System tab navigation pane, click Disks. The Disks view is displayed.
5 In the right pane, select a disk and click Toggle Indicator. The Toggle Indicator dialog box opens.
6 Click OK.

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the SYSTEM menu, select Hardware. The Hardware view is displayed.
3 Click the System tab.
4 In the System tab navigation pane, expand the Storage Center and select Disks. The Disks view is displayed.
5 In the disks table, select a disk and click Release Disk. The Release Disks dialog box opens.
6 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.
7 To skip the RAID rebalance, select I will start RAID rebalance later.
8 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, expand the Storage Center and select Disks.
   The Disks view is displayed.
5. In the disks table, select a disk marked for release and click Cancel Release Disk.
   The Cancel Release Disks dialog box opens.
6. 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, expand the Storage Center and select Disks.
   The Disks view is displayed.
5. In the disks table, select the disk and click (Delete).
   The Delete Disks dialog box opens.
6. Click Yes.

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.

Prerequisite
The disk must be down, removed from the enclosure, and deleted from Storage Center.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3 Click the **System** tab.
4 In the **System** tab navigation pane, expand the Storage Center and select **Disks**.

   The **Disks** view is displayed.
5 In the disks table, select the disk and click **Restore Disk**.

   The **Restore Disks** dialog box opens.
6 Click **Yes**.

   Storage Center restores the disk and adds it to a disk folder.

### Replace a Failed Disk

The Replace Failed Disk wizard identifies a disk and provides steps to replace the disk.

**Prerequisite**

The disk must be down

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Hardware**.

   The **Hardware** view is displayed.
3. Click the **System** tab.
4. In the **System** tab navigation pane, expand the Storage Center and select **Disks**.

   The **Disks** view is displayed.
5. In the disks table, select the failed disk and click **Replace Disk**.

   The **Replace Disk** wizard opens.
6. Locate the failed disk and click **Next**.
7. Follow the instructions to physically remove the failed disk from the enclosure. Click **Next**.
8. Insert the new disk into the enclosure, following all instructions. Click **Next**.

   Storage Center attempts to recognize the replacement disk.
9. If the disk replacement succeeds, Storage Center confirms this. It also displays information about the new disk.
10. 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.

**Prerequisite**

The Storage Center must have the Self-Encrypting Drives license.

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary. The Summary view is displayed.
3. Click (Settings). The Storage Center Settings dialog box opens.
4. Click the Secure Data tab.
5. In the Hostname field, type the host name or IP address of the key management server.
6. In the Port field, type the number of a port with open communication with the key management server.
7. 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.
8. 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.

9. If the key management server requires a user name to validate the Storage Center certificate, type the name in the Username field.
10. If the key management server requires a password to validate the Storage Center certificate, type the password in the Password field.
11. 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.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Disks.
   The Disks view is displayed.
3. Select the name of a Secure Disk folder and click (Edit).
   The Edit Disk Folder dialog box opens.
4. If the Rekey option is not enabled, select the checkbox to enable it.
5. 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.
6. Click OK.

Rekey a Disk Folder

Perform an on-demand rekey of a Secure Disk folder.

Prerequisite
The disk or disk folder must be enabled as Secure Disk.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Disks.
   The Disks view is displayed.
3. Select the name of a Secure Disk folder and click Rekey Disk Folder.
   The Rekey Disk Folder dialog box opens.
4. Click Yes.

Rekey a Disk

Perform an on-demand rekey of a Secure Disk.

Prerequisite
The disk or disk folder must be enabled as Secure Disk.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Disks.
   The Disks view is displayed.
3. Select the name of a Secure Disk disk and click Rekey Disk.
   The Rekey Disk dialog box opens.
4. Click Yes.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Disks.
   The Disks view is displayed.
3. Click ... (More Actions) and select Copy Volumes to Disk Folder.
   The Copy Volumes to Disk Folder dialog box opens.
4. Choose the source volume by selecting the checkbox next to the name of the disk folder.
5. Use the drop-down menu to select the destination disk folder.
6. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Disks.
   The Disks view is displayed.
3. In the right pane, right-click Disks and select New Disk Folder from the drop-down menu.
   The New Disk Folder dialog box opens. The dialog box displays all unmanaged disks and designates spare disks.
4. 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.
5. Type a name in the Name field.
6. Select the disks to be managed and click OK.
   The Secure Data Disk folder is created.
7. 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.)
8. 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 12. HDD Redundancy Recommendations and Requirements

<table>
<thead>
<tr>
<th>Disk Size</th>
<th>Level of Redundancy Recommended or Enforced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 3 TB</td>
<td>Dual redundant is the recommended level</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Non-redundant storage is not an option for SCv2000 Series Storage Centers.</td>
</tr>
<tr>
<td>3 TB and higher</td>
<td>Dual redundant is required and enforced</td>
</tr>
</tbody>
</table>

### Table 13. SSD Redundancy Recommendations and Requirements

<table>
<thead>
<tr>
<th>Disk Size</th>
<th>Level of Redundancy Recommended or Enforced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 18 TB</td>
<td>Dual redundant is the recommended level</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Non-redundant storage is not an option for SCv2000 Series Storage Centers.</td>
</tr>
<tr>
<td>18 TB and higher</td>
<td>Dual redundant is required and enforced</td>
</tr>
</tbody>
</table>

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Disks.
   The Disks view is displayed.
3. Click Rebalance RAID.
   The RAID Rebalance dialog box opens. If a RAID rebalance is needed, the dialog box shows RAID rebalance options.
4. Select Perform RAID Rebalance immediately.
5. 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Disks.
   The Disks view is displayed.
3. Click Rebalance RAID.
   The RAID Rebalance dialog box opens.
4. Click Stop Rebalancing. After rebalance stops, a confirmation dialog box opens.
5. Click OK.

Schedule a RAID Rebalance

Schedule a RAID rebalance to rebuild the data on all of the disks at a later date.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Disks.
   The Disks view is displayed.
3. 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.
4. Select Schedule RAID rebalance.
5. Select a date and time.
6. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Disks.
   The Disks view is displayed.
3. Click Rebalance RAID.
   The RAID Rebalance dialog box shows the status of a RAID rebalance.
4. 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.

Prerequisite
SCv2000 does 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Storage Types. The Storage Types view is displayed.
3. Click + (New). The New 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. Select a Page 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.
8. Drive Addition is selected by default. Leave this option selected.
9. 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the STORAGE menu, select Storage Types. The Storage Types view is displayed.
3. In the Storage Type area, select the Storage Type to modify, then click (Edit). The Modify Tier Redundancy dialog box opens.
4. 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.
5. 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.)
6. Drive Addition is selected by default. Leave this option selected.
7. 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.

**Prerequisite**

This wizard is available only for SCv2000 series and SCv3000 series arrays. This procedure can be performed without a controller outage.

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
The Hardware view is displayed.

1. Click the System tab.
2. In the System tab navigation pane, click Enclosure.
The Enclosure view is displayed.
3. Click Add Enclosure.
The Add New Enclosure wizard opens.
4. 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.
5. If prompted, select the enclosure type and click Next.
6. Follow the instructions to insert disks into the new enclosure and turn on the enclosure. Click Next when finished.
7. If displayed, follow the instructions to disconnect the A side chain cable from an existing enclosure.
8. Click Next.
9. 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.
10. Click Next.
11. Connect the B side chain cables to the new enclosure by following the displayed instructions.
12. 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.
13. 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the System menu, select Hardware.
The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, click Enclosure.
The Enclosure view is displayed.
5. Select the enclosure you want to remove and click Remove Enclosure.
The Remove Enclosure wizard opens.
6. Confirm the details of your current install, and click Next.
7. Locate the enclosure in the Storage Center and click Next.
8. Follow the directions to disconnect the A side chain cables connecting the enclosure to the Storage Center, Click Next.
9. Reconnect the A side chain cables by following the directions to exclude the enclosure. Click Next.
10. Follow the directions to disconnect the B side chain cables connecting the enclosure to the Storage Center. Click Next.
11. 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.
12. 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, click Enclosure.
   The Enclosure view is displayed.
5. Select the enclosure you want to replace and click Replace Enclosure.
   The Replace Enclosure wizard opens.
6. Click Next to accept the warning of service interruption.
7. Follow the instruction for locating the enclosure in the rack.
8. Click Next.
9. Follow all instructions to remove disks from the enclosure.
10. Click Next.
11. Disconnect the enclosure from the Storage Center.
12. Click Next.
13. Add disks to your enclosure by following the instructions.
14. Click Next.
15. Follow the instructions to connect the A-side chain.
16. Click Next.
   The wizard checks that the enclosure is connected.
17. Follow the instructions to connect the B-side chain.
18. Click Next.
   The wizard validates the cabling.
19. 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, click Enclosure.
   The Enclosure view is displayed.
5. In the right pane, select an enclosure and click Edit Settings.
   The Edit Settings dialog box opens.
6 In the **Name** field, type a new name for the enclosure.
7 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the **SYSTEM** menu, select **Hardware**.
   - The **Hardware** view is displayed.
3 Click the **System** tab.
4 In the **System** tab navigation pane, click **Enclosure**.
   - The **Enclosure** view is displayed.
5 In the right pane, select an enclosure and click **Edit Settings**.
   - The **Edit Settings** dialog box opens.
6 In the **Asset Tag** field, type an asset tag for the enclosure.
7 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the **SYSTEM** menu, select **Hardware**.
   - The **Hardware** view is displayed.
3 Click the **System** tab.
4 In the **System** tab navigation pane, click **Enclosure**.
   - The **Enclosure** view is displayed.
5 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.
6 Click **OK**.

**Mute an Enclosure Alarm**

Mute an enclosure alarm to prevent it from sounding.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2 From the **SYSTEM** menu, select **Hardware**.
   - The **Hardware** view is displayed.
3 Click the **System** tab.
4 In the **System** tab navigation pane, click **Enclosure**.
The Enclosure view is displayed.

5. In the right pane, select an enclosure.
6. Click Audible Alarms, then select Request Mute.

**Unmute an Enclosure Alarm**

Unmute an enclosure alarm to allow it to sound.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, click Enclosure.
   The Enclosure view is displayed.
5. In the right pane, select an enclosure.
6. Click Audible Alarms, 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, click Fan Sensors.
   The 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
The **Hardware** view is displayed.

3 Click the **System** tab.

4 In the **System** tab navigation pane, 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.

**Prerequisite**
This wizard is only available for the SCv2000 series, and can be completed without a controller outage.

**Steps**

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the **SYSTEM** menu, select **Hardware**.
   The **Hardware** view is displayed.

3 Click the **System** tab.

4 In the **System** tab navigation pane, 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the **SYSTEM** menu, select **Hardware**.
   The **Hardware** view is displayed.

3 Click the **System** tab.

4 In the **System** tab navigation pane, 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the **SYSTEM** menu, select **Hardware**.
   The **Hardware** view is displayed.

3 Click the **System** tab.
4. In the **System** tab navigation pane, click **Temp. Sensors**.
   The **Temp. Sensors** 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Hardware**.
   The **Hardware** view is displayed.
3. Click the **System** tab.
4. In the **System** tab navigation pane, click **Temp. Sensors**.
   The **Temp. 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.

**Prerequisite**
This wizard is only available for the SCv2000 series and SCv3000 series Storage Centers.

**Steps**
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Hardware**.
   The **Hardware** view is displayed.
3. Click the **System** tab.
4. In the **System** tab navigation pane, 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **SYSTEM** menu, select **Hardware**.
   The **Hardware** view is displayed.
3. Click the **System** tab.
4. In the **System** tab navigation pane, click **Disks**.
The Disks view is displayed.

5 In the right pane, select a disk and click **Toggle Indicator**.
   The **Toggle Indicator** dialog box opens.

6 Click **OK**.

### Clear the Swap Status for a Disk

Clear the swap status for a disk to acknowledge that it has been replaced.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the **SYSTEM** menu, select **Hardware**.
   The **Hardware** view is displayed.

3 Click the **System** tab.

4 In the **System** tab navigation pane, click **Disks**.
   The **Disks** view is displayed.

5 In the right pane, select a disk, then click **Request Swap Clear**.

### Managing Storage Center Controllers

Unisphere 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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the **SYSTEM** menu, select **Hardware**.
   The **Hardware** view is displayed.

3 Click the **System** tab.

4 In the **System** tab navigation pane, click **Controllers**.
   The **Controllers** view is displayed.

5 Click **Add Controller**.
   The **Add New Controller** wizard opens.

6 Confirm the details of your current install, and click **Next**.

7 Insert the controller into the existing enclosure. Click **Next** to validate the install.

8 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.

**Prerequisite**
This wizard is only available for the SCv2000 series controllers.

**Steps**
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the `SYSTEM` menu, select `Hardware`. The `Hardware` view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, click Controllers. The Controllers view is displayed.
5. In the right pane, select the controller you want to replace and click Replace Controller. The Replace Controller wizard opens.
6. Refer to the graphic in the wizard to located the failed controller. Click Next.
7. Follow the instructions to remove the battery from the failed controller. Click Next.
8. Follow the instructions to remove the failed controller from the Storage Center. Click Next.
9. Insert the battery from the failed controller into the new controller. Click Next.
10. 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.
11. 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.

**Prerequisite**
The controller indicator light is visible only on SC8000 or SC9000 storage controllers.

**Steps**
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the `SYSTEM` menu, select `Hardware`. The `Hardware` view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, click Controllers. The Controllers view is displayed.
5. In the right pane, select a controller and click Toggle Indicator. The Toggle Indicator dialog box opens.
6. Click OK.

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.

**Prerequisite**
This wizard is only available for the SCv2000 series and SCv3000 series Storage Centers.
Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, 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.

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 controllers have 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:

- 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.

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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   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 uninterruptable 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 Unisphere.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the SYSTEM menu, select Hardware.
   The Hardware view is displayed.
3. Click the System tab.
4. In the System tab navigation pane, click UPS.
   The UPS view is displayed.
5. Click + (New).
   The Register UPS dialog box opens.
6. In the Community String field, type the community string configured on the UPS. The default is Public.
7. In the IPv4 Address field, type the IP address of the UPS.
8. In the Type field, select the brand of the UPS.
9. 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.

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.

Prerequisite
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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary. The Summary view is displayed.
3. Click ... (More Actions) and select Check for Update. The Update Storage Center dialog box opens and checks for an update.
4. (Optional) Click Release Notes for information about the update.
5. Select an Update Action:
   - Select Download Update and click Download Update to download the update right away.
   - Select Download and Install Now to download and apply the update immediately.
6. 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.
7. Click Install Update.
8. (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.
9. 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.

Prerequisite
The Storage Center Update Utility must be setup and running.

Steps
1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the SupportAssist tab.
5. Disable SupportAssist. Click Turn Off.
6. Under Use Update Utility, select the Enabled checkbox.
7. In the Update Utility Host or IP Address field, type the IP address of the Storage Center Update Utility.
8. In the Update Utility Port field, type the port of the Storage Center Update Utility.
9. Click OK.

Turn On SupportAssist

If SupportAssist is disabled to use the Storage Center Update Utility, it must be enabled.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary.
   The Summary view is displayed.
3. Click (Settings).
   The Storage Center Settings dialog box opens.
4. Click the SupportAssist tab.
5. Click Turn On.
   The Turn On SupportAssist wizard opens.
6. Read the SupportAssist agreement, and click Next to accept the agreement.
7. Review and update the contact information if necessary, and click Next.
8. Review and update the on site address information if necessary, and click Next.
   A confirmation dialog box opens.
9. Click Yes.
   The SupportAssist connection is validated.
10. Click Finish.
11. Click OK.
12. (Optional) Apply the settings to other Storage Centers.
Shutting Down and Restarting a Storage Center

Shutting down or restarting a Storage Center affects all controllers.

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 you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click **Summary**.
   The **Summary** view is displayed.
3. Click **(More Actions)** and select **Shutdown/Restart**.
   The **Shutdown/Restart** dialog box opens.
4. From the first drop-down menu, select **Shutdown**.
5. Click **OK**.
6. After the controllers have shut down, shut down the disk enclosures by physically turning off the power supplies.

**Next step**
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.

Restart All Controllers in a Storage Center

If the Storage Center has dual-controllers, the controllers can be restarted in sequence or simultaneously.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click **Summary**.
   The **Summary** view is displayed.
3. Click **(More Actions)** and select **Shutdown/Restart**.
   The **Shutdown/Restart** dialog box opens.
4. From the first drop-down menu, select **Restart**.
5. (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**.
6. 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.

1. From the **SYSTEM** menu, select **Hardware**.
The Hardware view is displayed.

2 Click the System tab.

3 In the System tab navigation pane, click Controllers.
The Controller view is displayed.

4 In the right pane, select the controller and click Shut Down/Restart Controller.
The Shut Down/Restart Controller dialog box opens.

5 From the drop-down menu, select Shut down.

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.

1 From the SYSTEM menu, select Hardware.
The Hardware view is displayed.

2 Click the System tab.

3 In the System tab navigation pane, click Controllers.
The Controller view is displayed.

4 In the right pane, select the controller and 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 controllers.
- The controller must be running Storage Center version 6.7 or later.

**About this task**

⚠️ **CAUTION:** Resetting the controller to factory defaults erases all information on the controller and all data on the drives.

**Steps**

1 In the right pane, click Actions → System → Reset to Factory Defaults.
The Reset Storage Center to Factory Defaults dialog box opens.

2 In the Factory Reset Token field, type the text above the Factory Reset Token field exactly as it appears in the dialog box.

3 In the Storage Center Administrator Username field type the username of a Storage Center user with administrator-level privileges.

4 In the Storage Center Administrator Password field type the password of a Storage Center user with administrator-level privileges.

5 To restart the controller after the reset, select Power on the Storage Center after resetting to factory defaults.

6 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. Unisphere 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

Unisphere can display information on FRU tickets, and can also close FRU tickets.

**NOTE:** If FRUs and FRU Manager are not enabled, Unisphere 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.

1. From the **MONITORING** menu, select **Alerts**.
   
   The **Alerts** view is displayed.
2. Select a FRU ticket.
3. Click **View FRU Ticket**.
   
   The **FRU Ticket Information** dialog opens.
4. Click **OK**.

### Close a FRU Ticket

Close a FRU ticket if the FRU ticket is not needed.

1. From the **MONITORING** menu, select **Alerts**.
   
   The **Alerts** view is displayed.
2. Select a FRU ticket.
3. Click **Close FRU Ticket**.
   
   The **Close FRU Ticket** dialog opens.
4. Click **OK**.
Viewing Storage Center Information

Unisphere provides access to summary information about managed Storage Centers, including I/O performance and hardware status. Use this information to monitor the status of your Storage Centers.

Summary Information

Unisphere connected directly to a Storage Center provides summary information for that single Storage Center. To view summary information for the Storage Center, use the Storage Center SUMMARY page.

Unisphere Central connected through a Data Collector provides summary information for all of the Storage Centers managed by the Data Collector. To view summary information for all of the Storage Centers, use the Unisphere Central HOME dashboard.

Storage Center Widgets

The following widgets provide summary information for an individual Storage Center or multiple Storage Centers, depending on your configuration. The Storage Center widgets can be rearranged on the page.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
<th>Home Page (Multiple Storage Centers)</th>
<th>Storage Center Summary Page (Single Storage Center)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Summary information about the objects associated with the Storage Center or Storage Centers. Information includes numeric totals and graphical status indicators for each object.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Alerts</td>
<td>Summary of the most recent alerts detected by the Storage Center or Storage Centers. Alert information includes numeric totals and graphical status indicators for each alert. Clicking View All opens the Alerts View, which provides a list and description of all alerts.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Volumes Percent Full</td>
<td>A graphical representation of the amount of disk space being used in each volume.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Volumes Full Forecast</td>
<td>Volumes that are estimated to be full within 7 days, 14 days, and 28 days.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Capacity</td>
<td>Graphical representation showing used disk space versus available disk space.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Top Used Disk Folders</td>
<td>Graphical representation showing used disk space versus available disk space by disk folder, including the threshold level. The threshold level is the percent of space remaining before a warning is triggered.</td>
<td>N/A</td>
<td>x</td>
</tr>
<tr>
<td>Hardware</td>
<td>Image of the hardware and identifying information such as IP addresses and firmware version. Clicking 🎨 (Settings) opens the Storage Center settings dialog box.</td>
<td>N/A</td>
<td>x</td>
</tr>
<tr>
<td>Front End IOPS</td>
<td>Transfer rate of read and write operations between the Storage Center and the host for the selected time frame. The arrow in the upper-right corner brings you to a page that provides more detailed information about IOPS.</td>
<td>N/A</td>
<td>x</td>
</tr>
<tr>
<td>Widget</td>
<td>Description</td>
<td>Home Page (Multiple Storage Centers)</td>
<td>Storage Center Summary Page (Single Storage Center)</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>Back End IOPS</td>
<td>Transfer rate of read and write operations between the Storage Center and the drives attached to the system. The arrow in the upper-right corner brings you to a page that provides more detailed information about IOPS.</td>
<td>N/A</td>
<td>x</td>
</tr>
<tr>
<td>Front End Bandwidth</td>
<td>Communications bandwidth between the Storage Center and the host. The arrow in the upper-right corner brings you to a page that provides more detailed information about bandwidths.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Back End Bandwidth</td>
<td>Communications bandwidth between the Storage Center and the drives attached to the system. The arrow in the upper-right corner brings you to a page that provides more detailed information about bandwidths.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>I/O Pending</td>
<td>Number of I/O operations that are pending.</td>
<td>N/A</td>
<td>x</td>
</tr>
</tbody>
</table>

**Rearrange Widgets on the Summary Page**

Rearrange the widgets on the *Summary* page to view the widgets in the order you want.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click *Summary*.
   The *Summary* view is displayed.
3. Locate the widget you want to move.
4. Move the mouse cursor on the widget until the pointer appears as a four-sided arrow.
5. Drag and drop the widget to the new location.
6. Repeat these steps with any other widgets you want to move.

**Status Indicators**

Unisphere uses the following icons and alerts to indicate system status.

**Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>Object is up and functioning normally.</td>
</tr>
<tr>
<td>⚠</td>
<td>Object is in a degraded state and should be investigated.</td>
</tr>
<tr>
<td>⚠</td>
<td>Object is down and requires attention.</td>
</tr>
</tbody>
</table>

**Alerts**

<table>
<thead>
<tr>
<th>Alert</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>The object is in a critical state and may be nearing failure.</td>
</tr>
</tbody>
</table>
Alert | Meaning
--- | ---
Warning | A condition on the Storage Center is affecting performance and can become critical if it is not corrected.
Informational | Information regarding an operation that is occurring or has occurred on the Storage Center.

**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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Storage Types**. The **Storage Types** view is displayed.
3. Click the **Tiers** subtab to view storage usage by tier and RAID type.

**View Storage Usage by Volumes**

Storage usage by volume is displayed for each Storage Type.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Storage Types**. The **Storage Types** view is displayed.
3. Click the **Volumes** subtab to view storage usage by volume.

**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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Storage Types**. The **Storage Types** view is displayed.
3. 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.
4. (Optional) 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.
Viewing Historical Storage Usage Data

Use the **Growth** tab to view and monitor historical usage statistics for a volume or server.

View Historical Storage Usage Data for a Volume

Use the **Growth** tab in the **Volume** view to view historical storage usage data for a volume.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Volumes**.
   The **Volumes** view is displayed.
3. Select a volume and then click the **Growth** tab.
   The historical storage usage data for the volume is displayed.
4. (Optional) Select the period of the storage usage data to display from the **Display** drop-down menu.
   - **Last Day** – Displays the past 24 hours of storage usage data.
   - **Last 3 Days** – Displays the past 72 hours of storage usage data.
   - **Last 5 Days** – Displays the past 120 hours of storage usage data.
   - **Last Week** – Displays the past 168 hours of storage usage data.
   - **Last Month** – Displays storage usage data for the past month.
   - **Custom** – Displays options that allow you to specify the start time and the end time of the storage usage data to display.

View Historical Storage Usage Data for a Server

Use the **Growth** tab in the **Server** view to view historical storage usage data for a server.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **STORAGE** menu, select **Servers**.
   The **Servers** view is displayed.
3. Select a server and then click the **Growth** tab.
   The historical storage usage data for the server is displayed.
4. (Optional) Select the period of the storage usage data to display from the **Display** drop-down menu.
   - **Last Day** – Displays the past 24 hours of storage usage data.
   - **Last 3 Days** – Displays the past 72 hours of storage usage data.
   - **Last 5 Days** – Displays the past 120 hours of storage usage data.
   - **Last Week** – Displays the past 168 hours of storage usage data.
   - **Last Month** – Displays storage usage data for the past month.
   - **Custom** – Displays options that allow you to specify the start time and the end time of the storage usage data to display.
Viewing Historical Performance Information

Use the Performance tab to view and monitor historical I/O performance statistics for a Storage Center and associated storage objects.

View System Performance Information

Use the Performance view to display I/O usage data for a Storage Center.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the MONITORING menu, click Performance.
3. Click the System tab.
4. Click Open to view more details about each statistic.

View Server Performance Information

Use the Performance tab to view historical I/O usage data for a server.

1. From the MONITORING view, click Performance.
2. Click the Servers tab.
3. Click Open to view more details about each statistic.

View Fault Domains Performance Information

Use the Performance tab to view historical I/O usage data for a fault domain.

1. From the MONITORING view, click Performance.
2. Click the Ports tab.
3. Click Open to view more details about each statistic.
4. Select a fault domain to view I/O usage data specific to that fault domain.

View Volume Performance Information

Use the Performance tab to view historical I/O usage data for a Storage Center volume.

1. From the MONITORING view, click Performance.
2. Click the Volumes tab.
3. Click Open to view more details about each statistic.

View Disk Performance

The Disks tab displays MB/s, IOPS, latency, average I/O size, and I/O pending statistics.

1. From the MONITORING view, click Performance.
2. Click the Disks tab.
View Performance Statistics for Controllers

The Controllers tab displays MB/s, IOPS, latency and average I/O size statistics.

1. From the **MONITORING** menu, click **Performance**.
2. Click the **Controllers** tab.
3. Click **Open** to view more details about each statistic.

View Storage Profile Performance

The **Storage Profiles** tab displays MB/s, IOPS, latency, average I/O size, and I/O pending statistics.

1. From the **MONITORING** view, click **Performance**.
2. Click the **Storage Profiles** tab.
3. Click **Open** to view more details about each statistic.

View QoS Profile Performance

The QoS Profiles tab displays MB/s, IOPS, latency and average I/O size statistics.

1. From the **MONITORING** view, click **Performance**.
2. Click the **QoS Profiles** tab.
3. Click **Open** to view more details about each statistic.

Export I/O Usage Data

You can export I/O usage data for systems, servers, ports, volumes, disks, controllers, storage profiles, and QoS profiles.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **MONITORING** menu, select **Performance**. The **Performance** view is displayed.
3. Click the tab that contains the I/O usage data to export.
4. Click **Export I/O Usage**. The **Export I/O Usage Data** dialog box opens.
5. Select the file type for the I/O usage data from the **Output Type** drop-down menu:
   - Comma Separated Values (CSV)
   - HyperText Markup Language (HTML)
   - Portable Document Format (PDF)
   - Microsoft Excel Format
6. Select the items that contain the I/O data to export in the **IO Usage Options** area.
7. Click **OK**.

Viewing Storage Center Information
Exporting Usage and Monitoring Data

You can export Storage Usage and Monitoring data to CSV, Text, Excel, HTML, XML, or PDF.

Export Storage Usage Data for a Single Storage Center

You can export storage usage data for an individual Storage Center and the volumes, and servers associated with the Storage Center.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. In the Storage Center Summary view, click \( \text{(More Actions)} \) and then select Export Storage Usage.
   The Export Storage Usage Data dialog box opens.
3. Select the Output Type: CSV (\.csv), HTML (\.htm), PDF (\.pdf), or Excel (\.xls).
4. Select or clear the Convert Size Data into Units (bytes by default) checkbox. Selecting this checkbox displays size data using the units that are the most appropriate for the displayed values. For example, 2097152 megabytes is displayed as 2 TB.
5. Select the storage usage data to export by selecting or clearing the checkboxes in the Storage Center, Volume, and Server tabs. By default, all of the storage usage data is selected to be exported.
6. Click OK.

Export Storage Usage Data for Multiple Storage Centers

Use Unisphere Central to export storage usage data for multiple Storage Centers and the volumes, and servers associated with each Storage Center.

1. If a Storage Center is selected from the drop-down list, click \( \text{(Home)} \) in the left navigation pane.
2. Click Export and select Export Storage Usage from the drop-down list.
   The Export Storage Usage Data dialog box opens.
3. Select the Output Type: CSV (\.csv), HTML (\.htm), PDF (\.pdf), or Excel (\.xls).
4. Select or clear the Convert Size Data into Units (bytes by default) checkbox. Selecting this checkbox displays size data using the units that are the most appropriate for the displayed values. For example, 2097152 megabytes is displayed as 2 TB.
5. Select the Storage Centers for which to export storage data.
6. Select the storage usage data to export by selecting or clearing the checkboxes in the Storage Center, Volume, and Server tabs. By default, all of the storage usage data is selected to be exported.
7. Click OK.

Export Monitoring Data for a Single Storage Center

You can export storage usage data for an individual Storage Center and the volumes, and servers associated with the Storage Center.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. In the Storage Center Summary view, click \( \text{(More Actions)} \) and then select Export Monitoring Data.
   The Export Monitoring Data dialog box opens.
3. Select the Output Type: CSV (\.csv), HTML (\.htm), PDF (\.pdf), or Excel (\.xls).
4. Select the alerts and log data to export by selecting or clearing the checkboxes in the Monitoring Data Options area.
5. Click OK.
Export Monitoring Data for Multiple Storage Centers

Use Unisphere Central to export monitoring data such as alerts and log, for multiple Storage Centers.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Export and select Export Monitoring Data from the drop-down list. The Export Monitoring Data dialog box opens.
3. Select the Output Type: CSV (.csv), HTML (.htm), PDF (.pdf), or Excel (.xls).
4. Select the Storage Centers for which to export monitoring data.
5. Select the alerts and log data to export by selecting or clearing the checkboxes in the Monitoring Data Options area.
6. Click OK.
Storage Center Monitoring

Unisphere provides a centralized location to view Storage Center alerts, indications, and logs collected by the Storage Center. System events logged by the Storage Center can also be viewed.

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 14. Alert and Indication Status Levels

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Okay/Inform</td>
<td>Provide information regarding some operation that is occurring or has occurred on the Storage Center.</td>
</tr>
<tr>
<td>Degraded</td>
<td>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.</td>
</tr>
<tr>
<td>Down</td>
<td>Indicates an item on the Storage Center is down and not currently operational.</td>
</tr>
<tr>
<td>Critical</td>
<td>Indicates an item on the Storage Center is in a critical state and may be nearing failure.</td>
</tr>
<tr>
<td>Complete</td>
<td>Indicates that an operation on the Storage Center has completed.</td>
</tr>
<tr>
<td>Emergency</td>
<td>Indicates an item on the Storage Center requires immediate attention in order to remain operational.</td>
</tr>
<tr>
<td>Deleting</td>
<td>Indicates that an item on the Storage Center has been deleted.</td>
</tr>
<tr>
<td>Unavailable</td>
<td>Indicates that an item on the Storage Center that is expected to be present cannot currently be found for use.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Indicates a condition on the Storage Center that is not defined by one of the other categories.</td>
</tr>
<tr>
<td>Warning</td>
<td>Indicates a condition on the Storage Center that decreases performance or can become critical if it is not corrected.</td>
</tr>
</tbody>
</table>
View Storage Center Alerts

Alerts represent current issues present on a Storage Center.

Display Alerts for Multiple Storage Centers

View Alerts for multiple Storage Centers using Unisphere Central connected to a Data Collector.

1. If you are connected to a Data Collector and a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.

2. From the MONITORING menu, select Alerts.
   The Alerts view is displayed.

3. Select the checkboxes of the Storage Centers to display and clear the checkboxes of the Storage Centers to hide.
   The Alerts view displays alerts for the selected Storage Centers.

4. To refresh the alert data, click (Refresh).

5. To view more information about an alert, select the alert and click More Information.
   A knowledge base article with information about the alert is displayed.

Related links
- Acknowledge Storage Center Alerts
- Export Storage Center Alerts
- Delete Storage Center Alerts
- Select the Columns to Display

---

Display Alerts for a Single Storage Center

View Alerts for a single Storage Center in the Alerts view.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. From the MONITORING menu, select Alerts.
   The Alerts view is displayed.

3. To refresh the alert data, click (Refresh).

4. To view more information about an alert, select the alert and click More Information.
   A knowledge base article with information about the alert is displayed.

Related links
- Acknowledge Storage Center Alerts
- Export Storage Center Alerts
- Delete Storage Center Alerts
- Filter the Storage Center Alerts
- Select the Columns to Display
**Acknowledge Storage Center Alerts**

Acknowledge alerts to indicate to the Storage Center that you have read the alert message and are aware of the problem.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **MONITORING** menu, select **Alerts**.
   The **Alerts** view is displayed.
3. Select the alerts to acknowledge.
   
   **NOTE:** The option to acknowledge an alert does not appear if an alert has already been acknowledged.
4. Click **Acknowledge**.
   The **Acknowledge** dialog box opens.
5. Click **Yes**.

**Export Storage Center Alerts**

To export alerts from the **Alerts** view:

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **MONITORING** menu, select **Alerts**.
   The **Alerts** view is displayed.
3. Click **Export**.
   The **Export** dialog box opens.
4. Select an output type from the **Output Type** drop-down list.
5. Click **OK**.

**Delete Storage Center Alerts**

Delete alerts to remove them from the **Alerts** view.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **MONITORING** menu, select **Alerts**.
   The **Alerts** view is displayed.
3. Select the alert to delete.
   
   **NOTE:** Some types of alerts cannot be deleted.
4. Click **Delete**.
   The **Delete** dialog box opens.
5. Click **Yes**.

**Filter the Storage Center Alerts**

The **Alerts** view displays all unacknowledged Storage Center alerts by default. You can customize the view by filtering the alerts.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the **MONITORING** menu, select **Alerts**.
The Alerts view is displayed.

3 Click \( \text{Column Filters} \).
The Filters dialog box opens.

4 Select one or more of the following filter categories:
   - Severity
   - Status
   - Date & Time
   - Message
   - Source Name
   - Category
   - Type
   - Acknowledged

5 Select one or more filter values for the selected categories.

6 Click Apply.

7 Click X to close the Filters dialog box.

---

**Select the Columns to Display**

Show or hide columns to customize the view.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the MONITORING menu, select Alerts.
The Alerts view is displayed.

3 Click (Show/Hide Columns).
The Columns dialog box opens.

4 Select the checkboxes of the columns to show and clear the checkboxes of the columns to hide.

5 Click X to close the Columns 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 Unisphere Central immediately when they are triggered, configure a Storage Center to send them to the Data Collector.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 From the Summary tab, click (Settings).
The Storage Center Settings dialog box opens.

3 Click the Alerts and Logs tab.

4 Select the Send Alerts to Data Collector checkbox.

5 Click OK.

---

**Data Collector Alerts**

Data Collector alerts are a collection of messages that have been generated by events in Unisphere Central. You can view alerts on the Data Collector tab or configure Unisphere Central to email you when events occur.
Data Collector Alert Types

Unisphere Central alerts are categorized by severity.

Table 15. Data Collector Alert Types

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inform</td>
<td>Provides information regarding an event that is occurring or has occurred on the Storage Center.</td>
</tr>
<tr>
<td>Warning</td>
<td>Indicates a condition on the Storage Center that decreases performance or can become critical if it is not corrected.</td>
</tr>
<tr>
<td>Error</td>
<td>Indicates an error has occurred on the Storage Center.</td>
</tr>
<tr>
<td>Exception</td>
<td>Indicates an exception occurred on the Storage Center.</td>
</tr>
</tbody>
</table>

View Data Collector Alerts

View Data Collector alerts from the Alerts tab.

1. If you are connected to a Data Collector and a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. From the MONITORING menu, select Alerts. The Alerts view is displayed.
3. Click Data Collector.
4. To refresh the alert data, click Refresh.
5. To export Data Collector alerts, click Export and enter an output type.

Filter the Data Collector Alerts

The Alerts view displays all unacknowledged Storage Center alerts by default. Click the Data Collector tab to view Data Collector alerts.

1. If you are connected to a Data Collector and a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. From the MONITORING menu, select Alerts. The Alerts view is displayed.
3. Click Data Collector tab from the Alerts view.
4. Click (Column Filters). The Filters dialog box opens.
5. Select one or more of the following filter categories:
   • Severity
   • Last Occurrence
   • Date & Time
   • Message
   • Type
6. Select one or more filter values for the selected categories.
Select the Date Range of Data Collector Alerts to Display

You can view Data Collector alerts for a specific time period.

1. If you are connected to a Data Collector and a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. From the MONITORING menu, select Alerts.
   The Alerts view is displayed.
3. Click the Data Collector tab from the Alerts view.
4. Click (Column Filters).
   The Filters dialog box opens.
5. Specify a start date and time in the Last Occurrence field.
   a. Click the calendar icon and select a start date from the calendar.
   b. Click the clock icon and select a start time from the drop-down list.
6. Specify an end date and time in the Last Occurrence field.
   a. Click the calendar icon and select an end date from the calendar.
   b. Click the clock icon and select an end time from the drop-down list.
7. Click Apply.
8. Click X to close the Filters dialog box.

Configuring Email Alerts for Unisphere Central Events

To receive email notifications for Unisphere Central events, configure SMTP server settings for the Data Collector, add an email address to your user account, and enable notification emails for the events.

Configure SMTP Server Settings

The SMTP server settings must be configured to allow Unisphere Central to send notification emails.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Environment tab and, then click the SMTP Server subtab.
4. Click Edit.
   The SMTP Server Configuration dialog box opens.
5. 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.
6. Click OK.
Configure an Email Address for Your User Account

To receive email notifications, you must specify an email address for your account.

**Prerequisite**
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 Unisphere Central, click your user name and select Edit User Settings. The Edit User Settings dialog box opens.
2. Type the email address of the current user 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 link**
Configure SMTP Server Settings

Configure Email Notification Settings for Your User Account

Make sure that Unisphere Central 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 Unisphere Central, click your user name, then select User Preferences. 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 links**
Configure SMTP Server Settings
Configure an Email Address for Your User Account
Logs

Logs are records of event activity on the managed Storage Centers. Use the Logs tab to display and search for events in storage system logs.

View Storage Logs for Multiple Storage Centers

View Storage logs for multiple Storage Centers using Unisphere Central connected to a Data Collector.

1. If you are connected to a Data Collector and a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.

2. From the MONITORING menu, select Logs.
   The Logs view is displayed.

3. Select the checkboxes of the Storage Centers to display and clear the checkboxes of the Storage Centers to hide.
   The Logs view displays storage logs for the selected Storage Centers.

4. To refresh the log data, click C (Refresh).

View Storage Logs for a Single Storage Center

Storage logs for a single Storage Center are displayed in the Logs view.

1. If you are connected to a Data Collector and a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.

2. From the MONITORING menu, select Logs.
   The Logs view is displayed.

3. To refresh the log data, click C (Refresh).

Select the Date Range of Log Events to Display

You can view log events for a specific time period.

1. From the MONITORING menu, select Logs.
   The Logs view is displayed.

2. Click ▼ (Column Filters).
   The Filters dialog box opens.

3. Select the Date & Time checkbox.

4. Specify a start date and time.
   a. Click the calendar icon and select a start date from the calendar.
   b. Click the clock icon and select a start time from the drop-down list.

5. Specify an end date and time.
   a. Click the calendar icon and select an end date from the calendar.
   b. Click the clock icon and select an end time from the drop-down list.

6. Click Apply.

7. Click X to close the Filters dialog box.
Export Storage Center Logs

To export Storage Center logs from the Logs view:

1. From the MONITORING menu, select Logs.
   The Logs view is displayed.
2. Click Export.
   The Export dialog box opens.
3. Select an output type from the Output Type drop-down list.
4. Click OK.

Send Storage Center Logs to a Syslog Server

Modify the Storage Center to send logs to a syslog server.

1. In the Storage Center Summary view, click (Storage Center Settings).
2. Click the Alerts and Logs tab.
3. Select Send Logs to Syslog Server.
4. In the Host or IP Address field, type the host name or IP address of the syslog server.
5. Click OK.

Stop Sending Logs To a Syslog Server

Modify Storage Center settings to stop sending logs to a Syslog server.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Storage Center Settings.
3. Select Alerts and Logs from the Storage Center Settings menu.
4. Click the Do Not Send Logs checkbox.
5. Click OK.
Storage Center Realtime Reports

Unisphere displays preconfigured Storage Center realtime reports. You can select usage reports or unmapped volumes reports.

View Storage Center Usage Report

You can view Storage Center usage reports by volumes, servers, or disks in either tabular or chart views.

**About this task**

Usage reports display the following information:

- **Volumes** – Volume name, Path, % Full, Size on Disk, as well as Configured, Free, Used, and Snapshot space.
- **Servers** – Server name, Status, Path, as well as Configured, Free, Used, Snapshot space and RAID information
- **Disks** – Disk name, Status, % Allocated, as well as Total, Allocated, and Unallocated space.

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the REPORTS menu, select **Realtime**.
   The Reports view is displayed.
3. In the Reports view, select **Usage**.
4. From the Types drop-down box, select Volumes, Servers, or Disks.
5. Click **(Column Filters)**.
   The Filters dialog box opens.
6. Select one or more of the filter categories and filter values.
7. Click **Apply**.
8. (Optional) Click **(Show/Hide Columns)** and select the columns to display.

View Storage Center Unmapped Volumes Report

Unmapped Volumes report displays the following information: Volume Name, Size on Disk as well as Configured, Free, and Used space.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. From the REPORTS menu, select **Realtime**.
   The Reports view is displayed.
3. In the Reports view, select Unmapped Volumes.
4. Click **(Column Filters)**.
   The Filters dialog box opens.
5. Select one or more of the filter categories and filter values.
6. Click **Apply**.
7. (Optional) Click **(Show/Hide Columns)** and select the columns to display.
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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. 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 to stop and restart the Data Collector.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the General tab, and then select the Summary subtab.
4. Click OK.
The Data Collector Restart dialog box opens.

5 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.

1 If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.

2 Click Data Collector.
The Data Collector view is displayed.

3 Click the General tab, and then click the Summary subtab.

4 In the License Information section, click Submit License.
The License information dialog box opens.

5 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.

6 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

1 | NOTE: The Data Collector must be restarted to apply timeout setting changes.

Steps

1 If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.

2 Click Data Collector.
The Data Collector view is displayed.

3 Click the General tab, and then click the Summary subtab.

4 Expand the Advanced area located below the License Information section.

5 Click Edit.
The Edit Advanced Settings dialog box opens.

6 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.

7 Click OK.
The Data Collector Restart dialog box opens.
8. Click **Yes**.
   The Data Collector service stops and restarts.

## Set the Maximum Server Memory Usage

Use the **Edit Advanced Settings** dialog to set the maximum amount of memory that the Data Collector may use.

### About this task

**NOTE:** The Data Collector must be restarted to save server memory changes.

### Steps

1. If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.

2. Click **Data Collector**.
   The Data Collector view is displayed.

3. Click the **General** tab, and then click the **Summary** subtab.

4. Expand the **Advanced** area located below the **License Information** section.

5. Click **Edit**.
   The **Edit Advanced Settings** dialog box opens.

6. Type the amount of memory in MB to allocate for the Data Collector in the **Maximum Server Memory Usage** box.

7. Click **OK**.
   The **Data Collector Restart** dialog box opens.

8. Click **Yes**.
   The Data Collector service stops and restarts.

## 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.

### Prerequisite

The network adapter must have connectivity to the devices managed by Unisphere Central for SC Series.

**NOTE:** The Data Collector must be restarted to save network adapter changes.

### Steps

1. If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.

2. Click **Data Collector**.
   The Data Collector view is displayed.

3. Click the **General** tab, and then click the **Summary** subtab.

4. Expand the **Advanced** area located below the **License Information** section.

5. Click **Edit**.
   The **Edit Advanced Settings** dialog box opens.

6. 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.

7. Click **OK**.
   The **Data Collector Restart** dialog box opens.

8. 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 website. An SSL certificate is also required to communicate with a directory service using LDAP with the StartTLS extension or the LDAPS protocol.

Prerequisites

- The custom certificate must be signed by a Certificate Authority (CA) that is trusted by the hosts in your network.
- The certificate public key file must use DER or PEM encoding.
- The certificate private key file must be in PKCS #12 format.
- You must know the alias and password for the private key.

About this task

Certificates are generated on the Storage Center in the following locations:

- /mnt/root/cacert.pem
- /mnt/root/cakey.pem
- /mnt/root/server.pem

**NOTE:** The Data Collector must be restarted to apply SSL certificate 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, click **(Home)** in the left navigation pane.

3. Click **Data Collector**.
   The **Data Collector** view is displayed.

4. Click the **General** tab, and then click the **Security** subtab.

5. In the Registered Certificate section, click **Edit**.
   The **Registered Certificate** dialog box opens.

6. Upload the 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.

7. 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.

8. Type the name of the entry in the PKCS #12 private key file to use as the private key in the **Alias** field.

9. Type the password for the private key file in the **Password** field.

10. Click **OK**.
    The **Data Collector Restart** dialog box opens.
11. 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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click **Data Collector**.
   The Data Collector view is displayed.
3. Click the **General** tab, and then click the **Security** subtab.
4. In the Login Message section, click **Edit**.
   The Login Message dialog box opens.
5. Type a message to display on the login screen in the Login Banner Message field.
6. 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. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
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 the name of the service to edit.
   - Web Server Service (cannot be disabled)
   - Server Agent Service
   - SMI-S Service (Windows installations only)
   - VASA Service
6. Select or clear the **Enabled** checkbox to enable or disable a port.
7. If the port is enabled, type a port number in the **Port** field.
8. Click **OK**.
   The Data Collector Restart dialog box opens.
9. 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 Unisphere Central 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. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.

2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the General tab, and then click the Database subtab.
4. Click Change Data Source.
   The Change Data Source dialog box opens.
5. Select the type of database from the Database Type drop-down menu.
6. Type the host name or IP address of the database server in the Hostname or IP Address field.
7. Type the port number of the database server in the 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. 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 fields.
10. 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.
11. Click OK.

Change the Database Connection

Use this procedure to change the host name, IP address, or port for the database server.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the General tab, and then click the Database subtab.
4. Click Change Connection.
   The Change Data Connection dialog box opens.
5. Type the host name or IP address of the database server in the Database Server field.
6. Type port number of the database server in the Database Port field.
7. Type the user name and password of a user account that has database administrator rights in the User Name and Password fields.
8. Click OK.
   The Data Collector Restart dialog box opens.
9. 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 Unisphere Central to view the settings and status.

Prerequisite
Remote Data Collector has been configured for the system.

Steps
1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. 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 Unisphere Central to access the Remote Data Collector.

Prerequisite
Remote Data Collector has been configured for the system.

Steps
1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Environment tab, and then click the Remote Data Collector subtab.
   The settings and status of the Remote Data Collector are displayed.
4. 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 Unisphere Central to send notification emails.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Environment tab and, then click the SMTP Server subtab.
4. Click Edit.
   The SMTP Server Configuration dialog box opens.
5. 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.
Configure Server Usage Data Update Frequency

Configure the Server Agent to update usage data every 30 minutes.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Environment tab, and then click the Server Agent subtab.
4. Click Edit.
   The Server Agent dialog box opens.
5. Select the Periodically Update Usage Data checkbox.
   When selected, server usage data is updated every 30 minutes.
6. Type the number of days of usage data to include in the Usage Data Range field
7. 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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Monitoring tab, and then click the SupportAssist subtab.
4. Expand the Proxy Server area.
5. Click Edit in the Proxy Server area.
   The Network Proxy Configuration dialog box opens.
6. Select the Enabled checkbox to enable the proxy server.
7. Type the host name or IP address of the proxy server in the Host or IP Address field.
8. Type the port number of the proxy server in the Port field.
9. If the proxy server requires a user name and password, type a user name and password in the User Name and Password fields.
10. Click OK.
    The Change Values dialog box opens, which states that the Data Collector service must be stopped and restarted.
11. 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:

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Reports</td>
<td>Generates a report for the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Storage Center Summary</strong>: Displays information about storage space and</td>
</tr>
<tr>
<td></td>
<td>the number of storage objects on the Storage Center.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disk Class</strong>: Displays information about storage space on each disk class.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disk Power On Time</strong>: Displays information about how long each disk has</td>
</tr>
<tr>
<td></td>
<td>been powered on.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alerts</strong>: Displays Storage Center alerts.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Volume Storage</strong>: Displays volume storage statistics.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Replications</strong>: Displays information about volume replications.</td>
</tr>
<tr>
<td>Automated Table Reports</td>
<td>Generates a report for the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>I/O</strong>: Displays I/O information about the most active volumes, servers,</td>
</tr>
<tr>
<td></td>
<td>and disks.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Storage</strong>: Displays detailed information about the following:</td>
</tr>
<tr>
<td></td>
<td>– Volume, volume folder, and volume growth</td>
</tr>
<tr>
<td></td>
<td>– Disk, disk folder, disk class, and disk tier</td>
</tr>
<tr>
<td></td>
<td>– Server, and server folder</td>
</tr>
</tbody>
</table>

Set Up Automated Reports for All Storage Centers (Global Settings)

Configure automated report settings for 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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector. The Data Collector view is displayed.
3. Click the Monitoring tab and then select the Automated Reports subtab.
4. Select the checkboxes in the Automated Report Settings area to specify which reports to generate and how often to generate them.
5. 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.

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.
   b. To configure the Data Collector to email the reports when they are generated:
      i. 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:** Unisphere Central sends emails to the email address specified in the User Properties.

Select the file format for exported and emailed **Table Reports** from the **File Type for Table Reports** drop-down box.

7 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, Unisphere Central generates reports into a folder named for the day when the report was generated.

1 If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.

2 Click **Data Collector**.

The **Data Collector** view is displayed.

3 Click the **Monitoring** tab, and then click the **Automated Reports** subtab.

4 Review the current report settings:

   a. If the settings are acceptable, click **Run Now**.
   b. To change the report settings, click **Edit**, adjust the settings, and click **Run Now**.

The **Generate Reports Now** dialog box opens.

5 Select the checkboxes of the reports to generate.

6 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.

7 Click **OK**.

**Configure Data Collection Schedules**

Configure the interval at which the Data Collector collects monitoring data from Storage Centers.

1 If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.

2 Click **Data Collector**.

The **Data Collector** view is displayed.

3 Click the **Monitoring** tab, and then click the **Data Collection** subtab.

4 Click **Edit**.

The **Data Collection** dialog box opens.

5 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.

6 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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Monitoring tab, and then click the Support subtab.
4. Click Edit.
   The Edit Support dialog box opens.
5. Select the checkboxes of the debug logs to enable.
6. Click OK.

Configure Log File Limits

Configure the size limits for the log files.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Monitoring tab, and then click the Support subtab.
4. Click Edit.
   The Edit Support dialog box opens.
5. To modify the maximum file size of the Data Collector debug logs, change value in the Maximum Log File Size field.
6. 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.
7. To modify the number of days after which a log file is expired, change the period of time in the Log File Lifetime field.
8. Click OK.

Clear Debug Logs

Clear the debug log files to delete all Unisphere Central debug log files.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Monitoring tab, and then click the Support subtab.
4. Click Clear All Debug Logfiles.
   A confirmation dialog box opens.
5. 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.

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, click (Home) in the left navigation pane.

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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.

2. Click Data Collector.
   The Data Collector view is displayed.

3. Click the Virtual Appliance tab, and then click the Network subtab.

4. Click Edit.
   The Network Configuration dialog box opens.

5. In the Hostname field, type the host name of the Virtual Appliance.

6. In the Domain field, type the domain name of the Virtual Appliance.

7. To enable the Secure Shell (SSH), select the Enable SSH checkbox.

8. Select the network configuration type from the Configuration drop-down menu.
- **DHCP** - Dynamic IP address
- **Static** - Static IP address

9 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.

10 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.

1 If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.

2 Click **Data Collector**.

   The **Data Collector** view is displayed.

3 Click the **Virtual Appliance** tab, and then click the **Time** subtab.

4 Click **Edit**. The **Time Configuration** dialog box opens.

5 Select a time zone for the Virtual Appliance from the **Timezone** drop-down menu.

6 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.

7 To sync the time on the Virtual Appliance with the ESX host select **Sync with ESX Host**.

8 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 Unisphere Central users.

### 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.

1 If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.

2 Click **Data Collector**.

   The **Data Collector** view is displayed.

3 Click the **Users & System** tab, and then select the **Storage Centers** subtab.

4 Select the Storage Center to delete.

5 Click **Delete Storage Center**.

   A warning message is displayed.

6 Click **Yes**.
Clear All Data for a Storage Center

Clear data for a Storage Center to remove historical data from Unisphere Central.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, and then select the Storage Centers subtab.
4. Select the Storage Center for which you want to clear all data.
5. Click Clear Storage Center Data.
   A warning message is displayed.
6. Click Yes.

Remove a Storage Center from a Data Collector User Account

Remove a Storage Center from a user account to prevent the user from viewing and managing the Storage Center.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, and then select the Storage Centers subtab.
4. Select the Storage Center from which you want to delete a User/Storage Center map.
5. In the User/Storage Center Maps pane, select the user to unmap from the Storage Center.
6. Click (Delete).
   A warning message is displayed.
7. Click Yes.

Managing Available PS Series Groups

Use the PS Groups subtab to manage available PS Series groups that have been mapped to a Unisphere Central user.

Delete an Available PS Series Group

Remove a PS Series group when you no longer want to manage it from Unisphere Central.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the PS Groups subtab.
4. Select the PS Series group to delete.
5. Click Delete PS Group.
6. Click Yes.
Remove a PS Series Group from a Unisphere Central User

To prevent a user from managing a PS Series group, remove the group from the Unisphere Central user.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the PS Groups subtab.
4. In the User/PS Groups Maps pane, select the user to unmap from the PS Series group.
5. Click (Delete User/PS Group Map).
6. 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 Unisphere Central.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the FluidFS Clusters subtab.
4. Select the FluidFS cluster to delete.
5. Click (Delete System).
   A confirmation dialog box is displayed.
6. Click Yes.

Remove a FluidFS Cluster from a Unisphere Central User Account

Remove a FluidFS cluster from a user account to prevent the user from viewing and managing the cluster.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the FluidFS Clusters subtab.
4. Select the FluidFS cluster for which you want to delete a User/FluidFS cluster map.
5. In the User/FluidFS Cluster Maps pane, select the user you want to unmnap from the FluidFS cluster.
6. Click (Delete User/FluidFS Cluster Map).
   A confirmation dialog box is displayed.
7. 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

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.

**Prerequisite**
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.

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.
To modify the domain name used by the Storage Manager Virtual Appliance, type a new domain name, and then press Enter.

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.

Press 1 to confirm the changes and press Enter.

Press Enter to complete the configuration.

**Configure IPv6 Settings**

Use the Storage Manager Virtual Appliance console to modify the IPv6 network settings.

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.

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.

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. Right-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.

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.

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.

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 2008, 2012, or 2014, the Data Collector database can be migrated to a new Microsoft SQL Server.

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`. Do not assign the user to a schema at this time.
   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`:
   ```sql
   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 Unisphere Central data from the MySQL database and reinstall the Data Collector.

1. Enter the following SQL commands as an Admin user:
   ```sql
   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 Unisphere Central data from the database and reinstall the Data Collector.
1. Enter the following SQL commands as an Admin user:
   - Drop Database compmsadb;
   - EXEC SP_DropLogin 'compmsauser';
2. Reinstall the Storage Manager Data Collector.

Clean an Embedded Database on the File System

Reinstall the Storage Manager Data Collector. The embedded database on the file system is automatically cleaned up during the reinstallation process.
Data Collector User Management

Use the Data Collector to add users to and manage existing users on Unisphere Central.

Unisphere Central User Privileges

The Data Collector controls user access to Unisphere Central functions and associated Storage Centers based on the privileges assigned to users: Reporter, Volume Manager, or Administrator. The following tables define Unisphere Central user level privileges with the following categories.

NOTE: Unisphere Central 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 Unisphere Central users control access to Unisphere Central functionality.

Administrator Privileges

The Administrator privilege level is the most powerful user profile in Unisphere Central.

An Administrator user has full access to all of the Unisphere Central features.

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 Unisphere Central. However, a Volume Manager user does not have access to Data Collector properties.

Reporter Privileges

The Reporter privilege level is the most limited type of user in Unisphere Central.

A Reporter user can view most features of Unisphere Central. However, a Reporter user is not able to manage, create, or edit any feature. In addition, a Reporter user cannot view SupportAssist properties, Data Collector properties, or Storage Profiles.

NOTE: A Unisphere Central Reporter user can map Storage Centers to other Reporter users if they have Unisphere Central Reporter credentials.

Authenticating Users with an External Directory Service

The Data Collector can be configured to authenticate Unisphere Central 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.

Unisphere Central 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. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Environment tab and then select the Directory Service subtab.
4. Click Edit.
   The Service Settings dialog box opens.
5. Configure LDAP settings.
   a. Select the Enabled checkbox.
   b. In the Domain field, type the name of the domain to search.
   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.
6. (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.
To verify that the Data Collector can communicate with the specified directory server(s) using the selected protocol, click Test.

In the Base DN field, type the base Distinguished Name for the LDAP server. This name is the starting point when searching for users.

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.

(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.

Select the Kerberos Enabled checkbox.

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.

(OpenLDAP only) Type the host name or IP address of the Key Distribution Center (KDC) in the KDC Host Name or IP Address field.

In the Data Collector Host Name field, type the fully qualified domain name (FQDN) of the server that hosts the Data Collector.

(Optional — Open LDAP only) If Transport Layer Security (TLS) is enabled, upload a Certificate Authority PEM file...

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.

Click OK to upload the certificate.

(Active Directory Only) To register the Data Collector on the domain, select Register the Data Collector on the domain.

Type the user name and password of a domain administrator.

The user name Administrator is not allowed. These credentials are used only to register the Data Collector and are not saved.

Click OK.

To use an existing service account, select Use an existing service account for joining the domain.

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.

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.

On the server that hosts the Data Collector, use a text editor to open the file C:\Program Files (x86)\Compellent Technologies\Compellent Enterprise Manager\msaservice\directory_settings.txt.

Confirm that the values listed in the directory_settings.txt file match the network environment.

If the file contains incorrect values, make configuration changes to correct the issue.

Confirm that the server that hosts the Data Collector is joined to the correct Domain.

Make sure that DNS SRV records are correctly configured.

Use Data Collector to discover the directory service again.

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.

Prerequisite
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. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Environment tab and then select the Directory Service subtab.
4. Click Rescan. A message appears to inform you that scanning succeeded or failed.
5. Click OK.

Grant Access to Directory Service Users and Groups

To allow directory users to log in to Unisphere Central, add directory service users and/or user groups to Data Collector user groups.

Add Directory Groups to a Data Collector User Group

Add a directory group to a Data Collector user group to allow all users in the directory group to access Unisphere Central. 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.

Prerequisite
The Data Collector must be configured to authenticate users with an external directory service.

Steps
1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab and then select the Users & User Groups subtab.
4. Select the Data Collector user group to which you want to add directory groups.
5. Click Add Directory User Groups.
   The Add Directory User Groups dialog box opens.
6. (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.
7. Select each directory group that you want to add to the Unisphere Central user group.
8. When you are finished, click OK. The directory groups that are associated with the Data Collector group appear on the User Groups subtab.
Add a Directory User to a Data Collector User Group

Add a directory user to a Data Collector user group to allow the directory user to access Unisphere Central. 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.

**Prerequisite**
The Data Collector must be configured to authenticate users with an external directory service.

**Steps**
1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
The Data Collector view is displayed.
3. Click the Users & System tab and then select the Users & User Groups subtab.
4. Select the Data Collector user group to which you want to add a directory user.
5. Click Add Directory Users.
The Add Directory Users dialog box opens.
6. 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.
7. 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.
8. Click OK to close the message.
9. If any of the specified directory user names could not be verified, correct the names and then click Check Names again.
10. When you are finished, click OK. The Add Directory Users dialog box closes, and the directory users that are associated with the selected Data Collector user group appear on the User Groups subtab.

Revoke Access for Directory Service Users and Groups

To revoke access to Unisphere Central for a directory service user or group, remove the directory group or user from Data Collector user groups.

Remove a Directory Service Group from a Data Collector User Group

Remove a directory service group from a Data Collector user group to prevent directory users in the group from accessing Unisphere Central.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
The Data Collector view is displayed.
3. Click the Users & System tab and then select the Users & User Groups subtab.
4. Click the User Groups tab.
5. Select the Data Collector user group to which the directory group is added.
6. Click the Directory Groups subtab.
Select the directory service group for which you want to revoke access, then click **Delete**.

The **Delete Directory User Group** dialog box opens.

Click **Yes**.

### Remove a Directory Service User from a Data Collector User Group

Remove a directory service user from a Data Collector user group to prevent the directory user from accessing Unisphere Central.

1. If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.
2. Click **Data Collector**.
   
The **Data Collector** view is displayed.
3. Click the **Users & System** tab and then select the **Users & User Groups** subtab.
4. Click the **User Groups** tab.
5. Select the Data Collector user group to which the directory group is added.
6. Click the **Users** subtab.
7. Select the directory service group user for which you want to revoke access, then click **Delete User**. The **Delete Directory User** dialog box opens.
8. 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 Unisphere Central. If you choose to re-enable directory service authentication at a later time, all directory users and user groups must be granted access again.

**Steps**

1. If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.
2. Click **Data Collector**.
   
The **Data Collector** view is displayed.
3. Click the **Environment** tab and then select the **Directory Service** subtab.
4. Click **Edit**.
   
The **Service Settings** dialog box opens.
5. Clear the **Enabled** checkbox.
6. Click **OK**.

### Managing Local Users Through the Data Collector

Unisphere Central users and mappings to Storage Center can be configured on the **Users** tab on the Data Collector view.

### Create a User

Create a user account to allow a person access to Unisphere Central.

1. If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.
2. Click **Data Collector**.
   
The **Data Collector** view is displayed.
3. Click the **Users & System** tab, then select the **Users & User Groups** subtab.

4. Click **+ (New User)**. The **Create User** dialog box opens.

5. 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.

6. Click **OK**.

**Related link**

Unisphere Central User Privileges

### Configure or Modify the Email Address of a User

An email address must be configured if you want Unisphere Central to send email notifications to the user.

1. If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.

2. Click **Data Collector**. The **Data Collector** view is displayed.

3. Click the **Users & System** tab, then select the **Users & User Groups** subtab.

4. Select the user to modify and click **(Edit Settings)**. The **User Settings** dialog box opens.

5. Enter the email address of the user in the **Email Address** field.

6. Click **OK**.

### Change the Privileges Assigned to a User

You can change the privileges for a user account by changing the user role.

1. If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.

2. Click **Data Collector**. The **Data Collector** view is displayed.

3. Click the **Users & System** tab, then select the **Users & User Groups** subtab.

4. Select the user to modify and click **(Edit Settings)**. The **User Settings** dialog box opens.

5. Select the role to assign to the user from the **Role** drop-down menu.

6. Click **OK**.

**Related link**

Unisphere Central User Privileges
Change the Preferred Language for a Unisphere Central User

The preferred language for a Unisphere Central 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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the Users & User Groups subtab.
4. Select the user to modify and click (Edit Settings).
   The User Settings dialog box opens.
5. From the Preferred Language drop-down menu, select a language.
6. 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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the Users & User Groups subtab.
4. Select the user to modify and click (Edit Settings).
   The User Settings dialog box opens.
5. Select the Requires Password Change checkbox.
6. Click OK.

Change the Password for a User

You can change the password for any user account using Unisphere Central.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the Users & User Groups subtab.
4. Select the user to modify and click Change User Password.
   The Change User Password dialog box opens.
5. Type the admin password in the Authorization Password field.
6. Enter a new password for the user in the New Password and Confirm Password fields.
7. 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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the Users subtab.
4. Select the Reporter user to modify.
5. In the lower pane on the Storage Centers tab, click + (Select Storage Center Mappings).
   The Select Storage Center Mappings dialog box opens.
6. Select the checkbox of each Storage Center to map to the user.
   Clear the checkbox of each Storage Center to unmap from the user.
7. Click OK.

Delete a User

Delete a user account to prevent the user from viewing and managing the Storage Center.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the Users & User Groups subtab.
4. Select the user you want to delete.
5. Click (Delete User).
   A confirmation dialog box opens.
6. 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.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the Users & User Groups subtab.
4. Select the user for which you want to delete a Storage Center mapping.
5. Select the Storage Center to unmap from the user on the Storage Center pane.
6. Click (Delete Storage Center Map).
   A confirmation dialog box opens.
7. 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 Unisphere Central to unlock the account.

**Prerequisites**
- Password Configuration is enabled.
- A user account is locked.

**Steps**
1. If a Storage Center is selected from the drop-down list, click 🏡 (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the Users & User Groups subtab.
4. Select the locked user account.
5. Click Unlock User.
   A confirmation dialog box opens.
6. Click Yes.

Managing Local User Password Requirements

Manage the password expiration and complexity requirements for Unisphere from the Data Collector view.

Configure Local Unisphere Central User Password Requirements

Set local user password requirements to increase the complexity of local user passwords and improve the security of Unisphere Central.

1. If a Storage Center is selected from the drop-down list, click 🏡 (Home) in the left navigation pane.
2. Click Data Collector.
   The Data Collector view is displayed.
3. Click the Users & System tab, then select the Password Configuration subtab.
4. Click Edit.
   The Password Configuration dialog box opens.
5. Select Enabled.
6. Set the password requirements.

   🔄 **NOTE:** For user interface reference information, click Help.
7. Click OK.

Apply Password Requirements to Storage Center Users

Unisphere Central local user password requirements can be applied to Storage Center users.

**Prerequisite**
Password Configuration must be enabled.
Steps

1. If a Storage Center is selected from the drop-down list, click [Home] in the left navigation pane.

2. Click [Data Collector].
   The Data Collector view is displayed.

3. Click the [Users & System] tab, then select the [Password Configuration] subtab.

4. Click [Edit]. The Password Configuration dialog box opens.

5. Select the Storage Centers to which to apply the password requirements.

6. Click [OK].

Related link
Configure Local Unisphere Central User Password Requirements

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.

Prerequisite
Password Configuration must be enabled.

Steps

1. If a Storage Center is selected from the drop-down list, click [Home] in the left navigation pane.

2. Click [Data Collector].
   The Data Collector view is displayed.

3. Click the [Users & System] tab, then select the [Password Configuration] subtab.

4. Click [Edit]. The Password Configuration dialog box opens.

5. Select the [Reset Aging Clock] checkbox.

6. Click [OK].

Related link
Configure Local Unisphere Central User Password Requirements

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.

Prerequisite
Password Configuration must be enabled.

Steps

1. If a Storage Center is selected from the drop-down list, click [Home] in the left navigation pane.

2. Click [Data Collector].
   The Data Collector view is displayed.

3. Click the [Users & System] tab, then select the [Password Configuration] subtab.

4. Click [Edit]. The Password Configuration dialog box opens.

5. Select the [Requires Password Change] checkbox.

6. Click [OK].
Managing User Settings with Unisphere

Use Unisphere 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.

1. In the top pane of Unisphere, click your user name, then select User Preferences.
   The Edit User Settings dialog box opens.
2. On the User Information tab, click Change Password.
   The Change Password dialog box opens.
3. Type the current password of the user in the Current Password field.
4. Type a new password in the New Password and Confirm New 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.

1. In the top pane of Unisphere, click your user name, then select User Preferences.
   The Edit User Settings dialog box opens.
2. 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.
3. Click OK.

Configure Client Options

The alert display settings and formatting of storage units can be configured for the current user in the Edit User Settings dialog box.

Configure Alert Display Settings

The alert display settings for the current user are located in the Edit User Settings dialog box.

1. In the top pane of Unisphere, click your user name, then select User Preferences.
   The Edit User Settings dialog box opens.
2. On the Client Options tab, configure alert settings by selecting or clearing the following checkboxes:
   - Show Threshold Alert levels on charts – Displays a horizontal line parallel to the X axis on charts, showing the relationship between the reported data and the threshold level.
   - Show Storage Center alerts on charts – Displays a vertical line parallel to the Y axis, showing the relationship between reported data and Storage Center Alerts for failed controllers and down Remote Storage Centers.
3. Click OK.
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.

1. In the top pane of Unisphere, click your user name, then select User Preferences. The Edit User Settings dialog box opens.
2. On the Client Options 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.
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.

Data Types that Can Be Sent Using SupportAssist

Unisphere 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.

<table>
<thead>
<tr>
<th>SupportAssist Data Type</th>
<th>Description</th>
<th>SupportAssist Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O Usage report</td>
<td>Summarizes read and write I/O performance for one or more Storage Centers</td>
<td>Automatic or manual</td>
</tr>
<tr>
<td>Storage Usage report</td>
<td>Summarizes storage use and growth for one or more Storage Centers</td>
<td>Automatic or manual</td>
</tr>
<tr>
<td>Replication report</td>
<td>Summarizes the status of replications</td>
<td>Automatic or manual</td>
</tr>
<tr>
<td>Storage Center configuration</td>
<td>Sends all Storage Center configuration information</td>
<td>Manual</td>
</tr>
<tr>
<td>Storage Center logs</td>
<td>Sends Storage Center logs</td>
<td>Manual</td>
</tr>
<tr>
<td>FluidFS cluster summary</td>
<td>Summarizes all FluidFS cluster configuration information</td>
<td>Automatic</td>
</tr>
<tr>
<td>FluidFS cluster events</td>
<td>Sends FluidFS cluster events</td>
<td>Automatic</td>
</tr>
<tr>
<td>FluidFS cluster diagnostics</td>
<td>Sends full system diagnostics, including summary information for the FluidFS cluster configuration, services, and logs</td>
<td>Automatically triggered on critical events. Manually triggered when an administrator runs the FluidFS cluster diagnostics</td>
</tr>
</tbody>
</table>

Configure SupportAssist Settings for the Data Collector

Modify the SupportAssist settings for the Data Collector.

1. If a Storage Center is selected from the drop-down list, click (Home) in the left navigation pane.
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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click ➡️ Summary.
   The Summary view is displayed.
3. In the Summary tab, click ⚙️ (Settings).
   The Edit Storage Center Settings dialog box opens.
4. Click the SupportAssist tab.
   The SupportAssist settings dialog box opens.
5. Click Change global settings.
6. Select the frequency to send data from the Send Interval drop-down box.
7. 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.
8. Select your preference for receiving software updates from the Software Update Mode drop-down menu.
9. 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.
10. 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.

Manually Send Diagnostic Data for Multiple Storage Centers

You can send diagnostic data for multiple Storage Centers from the Data Collector.

1. If a Storage Center is selected from the drop-down list, click 🏡 (Home) in the left navigation pane.
2. Click 🔄 Data Collector.
   The Data Collector view is displayed.
3. Click the Monitoring tab, and then click the SupportAssist subtab.
4. Click Send SupportAssist Data Now.
   The Send SupportAssist Data Now dialog box opens.
5. In the Storage Centers area, select the checkboxes of the Storage Centers for which you want to send SupportAssist data to technical support.
6. In the Reports area, select the checkboxes of the Storage Center reports to send.
7. 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.

8 Click **OK**.

### Send Diagnostic Data for a Single Storage Center

You can send Storage Center diagnostic data using SupportAssist from the Storage Center settings.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
   The Storage Center must be added to Unisphere Central using a Storage Center user with the Administrator privilege.

2 Click **Summary**.
   The **Summary** view is displayed.

3 In the **Summary** tab, click **(Settings)**.
   The **Storage Center Settings** dialog box opens.

4 Click the **SupportAssist** tab.

5 Click **Send Data Now**.
   The **Send SupportAssist Data 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**.

10 Click **OK** to close the **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.

1 If a Storage Center is selected from the drop-down list, click **(Home)** in the left navigation pane.

2 Click **Data Collector**.
   The **Data Collector** view is displayed.

3 Click the **Monitoring** tab, and then click the **SupportAssist** subtab.

4 Click **Export Historical Data**.
   The **Export Historical Data** dialog box opens.

5 In the **Storage Center** table, select the Storage Center for which you want to export data.

6 In the **Reports** section, select the type of data that you want to export.

7 In the **Time Range** section, specify the time period for which you want to export data.

8 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.
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 Unisphere 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.
- Storage Center must recognize the USB flash drive.
- SupportAssist must be turned off.

**Steps**

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.
2. Click Summary. The Summary view is displayed.
3. In the Summary view, click (Settings).
The **Edit Storage Center Settings** dialog box opens.

4. Click **Send Information to USB**.
   The **Send SupportAssist Information to USB** dialog box opens.

5. Review the License Agreement 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:** Unisphere Central 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**.
   d. Save SupportAssist data to the USB flash drive following the instructions in **Save SupportAssist Data to the USB Flash Drive**.

### 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.

1. If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2. Click **Summary**.
   The **Summary** view is displayed.

3. In the **Summary** tab, click **(Settings)**.
   The **Storage Center Settings** dialog box opens.

4. Click the **SupportAssist** tab.

5. Click **Edit Contact Information**.
The **Edit 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.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click **Summary**.

   The **Summary** view is displayed.

3 In the **Summary** view, click **(Settings)**.

   The **Storage Center Settings** dialog box opens.

4 Click the **SupportAssist** tab.

5 In the **Server** area, select **Notify me of updates and automatically download them** from the **Software Update Mode** drop-down menu.

6 Click **OK**.

### Configure a Proxy Server for SupportAssist

Use the Storage Center settings to configure a proxy server for SupportAssist.

1 If you are connected to a Data Collector, select a Storage Center from the drop-down list in the left navigation pane.

2 Click **Summary**.

   The **Summary** view is displayed.

3 In the **Summary** view, click **(Settings)**.

   The **Storage Center Settings** dialog box opens.

4 Click the **SupportAssist** tab.

5 Select the **Use Web Proxy** checkbox.

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.

1. In the Summary tab, click (Settings). The Edit Storage Center Settings dialog box opens.
2. Click the SupportAssist tab.
3. Select or clear the CloudIQ Enabled checkbox.
4. Click OK.

**NOTE:** It may take up to four hours for changes made to this checkbox to take effect.