



ONTAP® 9

# Cluster Management Using OnCommand® System Manager

December 2016 | [215-11634\_B0]  
[doccomments@netapp.com](mailto:doccomments@netapp.com)

Updated for ONTAP 9.1  
Release Candidate Documentation - Contents Subject To Change



# Contents

<b>Welcome to OnCommand System Manager Help .....</b>	<b>16</b>
Access to your favorite topics .....	16
<b>Understanding System Manager .....</b>	<b>17</b>
<b>Icons used in the application interface .....</b>	<b>18</b>
<b>Window layout customization .....</b>	<b>19</b>
<b>Supportability Dashboard .....</b>	<b>20</b>
<b>Where to find additional ONTAP information .....</b>	<b>21</b>
<b>Setting up your cluster environment .....</b>	<b>22</b>
Setting up the cluster by using OnCommand System Manager .....	22
Setting up a cluster by using the template file .....	22
Setting up the cluster manually .....	24
Accessing a cluster by using OnCommand System Manager browser-based graphic interface .....	28
Configuring System Manager options .....	28
Viewing OnCommand System Manager log files .....	29
How system logging works .....	29
Configuring a cluster by using System Manager .....	30
Accessing a cluster by using OnCommand System Manager browser- based graphic interface .....	30
Setting up the cluster .....	30
Setting up the network .....	36
Setting up physical storage .....	37
Setting up logical storage .....	42
<b>Managing clusters .....</b>	<b>56</b>
What a cluster is .....	56
Understanding quorum and epsilon .....	56
What a node in the cluster is .....	57
Dashboard window .....	57
Monitoring a cluster using the dashboard .....	59
Configuration update .....	59
Configuring the administration details of an SVM .....	59
Configuration Updates window .....	60
Service Processors .....	61
Assigning IP addresses to Service Processors .....	61
Editing Service Processor settings .....	62
Understanding the Service Processor .....	62
Service Processors window .....	62
Cluster peers .....	63
Prerequisites for cluster peering .....	63
Creating cluster peer relationships .....	65
Modifying the cluster peer passphrase .....	66

Modifying the peer network parameters .....	66
Deleting cluster peer relationships .....	66
What a cluster peer is .....	67
What cluster peer intercluster connectivity is .....	67
Connecting one cluster to another cluster in a peer relationship .....	67
Peers window .....	67
High availability .....	68
Understanding HA pairs .....	68
High Availability window .....	68
Licenses .....	69
Deleting licenses .....	69
Managing licenses .....	70
License types and entitlement risk .....	71
Licenses window .....	73
Cluster update .....	74
Updating the cluster nondisruptively .....	75
How you update a cluster nondisruptively .....	77
Cluster Update window .....	78
Date and time .....	79
Managing the cluster time .....	79
Date and Time window .....	80
SNMP .....	81
Enabling or disabling SNMP .....	81
Setting SNMP information .....	81
Enabling or disabling SNMP traps .....	81
Testing the trap host configuration .....	82
Options to use when configuring SNMP .....	82
Managing SNMP on the cluster .....	82
SNMP window .....	83
LDAP .....	84
Viewing the LDAP client configuration .....	84
Using LDAP services .....	84
LDAP window .....	84
Users .....	85
Adding a cluster user account .....	85
Editing a cluster user account .....	85
Changing passwords for cluster user accounts .....	85
Locking or unlocking cluster user accounts .....	86
User accounts (cluster administrators only) .....	86
Roles .....	86
Users window .....	86
Roles .....	87
Adding roles .....	87
Editing roles .....	88
Roles and permissions .....	88

Predefined roles for cluster administrators .....	88
Roles window .....	89
<b>Managing the network .....</b>	<b>90</b>
IPspaces .....	90
Editing IPspaces .....	90
Deleting IPspaces .....	90
Configuring IPspaces .....	91
Standard properties of IPspaces .....	91
Broadcast domains .....	92
Editing broadcast domains .....	92
Deleting broadcast domains .....	92
Configuring broadcast domains .....	93
Subnets .....	93
Editing subnets .....	93
Deleting subnets .....	94
Network interfaces .....	94
Creating network interfaces .....	94
Editing network interfaces .....	96
Deleting network interfaces .....	96
Migrating a LIF .....	97
What LIFs are .....	97
Roles for LIFs .....	98
Guidelines for creating LIFs .....	99
Ethernet ports .....	100
Creating interface groups .....	100
Creating VLAN interfaces .....	100
Editing Ethernet port settings .....	101
Editing interface group settings .....	101
Editing the MTU size of a VLAN .....	101
Deleting VLANs .....	102
Ports and adapters .....	102
Types of network ports .....	102
How VLANs work .....	103
FC/FCoE adapters .....	104
Editing the FC/FCoE adapter speed .....	104
Configuring subnets .....	104
Network window .....	104
<b>Managing physical storage .....</b>	<b>112</b>
Aggregates .....	112
Editing aggregates .....	112
Deleting aggregates .....	113
Changing the RAID configuration when creating an aggregate .....	113
Provisioning cache by adding SSDs .....	114
Adding capacity disks .....	116
Changing the RAID group when adding capacity disks .....	117

Moving FlexVol volumes .....	118
Mirroring aggregates .....	118
Viewing aggregate information .....	119
What aggregates are .....	119
How RAID groups are named .....	119
How moving a FlexVol volume works .....	119
How Flash Pool aggregates work .....	120
How you can use effective ONTAP disk type for mixing HDDs .....	120
What compatible spare disks are .....	121
How System Manager works with hot spares .....	121
Rules for displaying disk types and disk RPM .....	122
Aggregate requirements for Infinite Volumes .....	122
How mirrored aggregates work .....	123
Aggregates window .....	124
Storage pools .....	127
Creating a storage pool .....	127
Adding disks to a storage pool .....	128
Deleting storage pools .....	128
How you use SSD storage pools .....	129
How Flash Pool SSD partitioning increases cache allocation flexibility for Flash Pool aggregates .....	129
Requirements and best practices for using SSD storage pools .....	130
Considerations for when to use SSD storage pools .....	131
Considerations for adding SSDs to an existing storage pool versus creating a new one .....	132
Why you add disks to storage pools .....	132
How storage pool works .....	132
Storage Pools window .....	132
Disks .....	134
Reassigning disks to nodes .....	134
Viewing disk information .....	134
Understanding RAID drive types .....	135
How ONTAP reports disk types .....	135
How hot spare disks work .....	136
RAID protection for array LUNs .....	137
Minimum number of hot spares you should have .....	137
Spare requirements for multi-disk carrier disks .....	138
Shelf configuration requirements for multi-disk carrier storage shelves ....	138
How to determine when it is safe to remove a multi-disk carrier .....	138
Considerations for sizing RAID groups .....	138
Considerations for ONTAP RAID groups for array LUNs .....	139
Disks window .....	140
Array LUNs .....	142
Assigning array LUNs .....	142
Reassigning spare array LUNs to nodes .....	143

Zeroing spare array LUNs .....	143
About disks and array LUNs .....	144
How disks and array LUNs become available for use .....	144
Rules for mixing array LUNs in an aggregate .....	145
Array LUNs window .....	145
Nodes .....	146
Initializing the ComplianceClock time .....	146
Nodes window .....	147
Flash Cache .....	148
Enabling or disabling Flash Cache .....	148
How Flash Cache works .....	148
Flash Cache window .....	148
Events .....	149
Events window .....	149
System alerts .....	150
Monitoring the health of your system .....	150
Acknowledging system health alerts .....	150
Suppressing system health alerts .....	151
Deleting system health alerts .....	151
Available cluster health monitors .....	151
Ways to respond to system health alerts .....	152
System Alerts window .....	153
AutoSupport notifications .....	154
Setting up AutoSupport notifications .....	154
Enabling or disabling AutoSupport settings .....	154
Adding AutoSupport email recipients .....	154
Testing AutoSupport settings .....	155
Generating AutoSupport data .....	155
Viewing AutoSupport summary .....	155
AutoSupport severity types .....	156
AutoSupport window .....	156
Jobs .....	157
Jobs .....	157
Job window .....	157
Flash Pool statistics .....	158
Flash Pool aggregate Statistics window .....	158
<b>Managing logical storage .....</b>	<b>159</b>
Storage Virtual Machines .....	159
SVM Dashboard window .....	159
Monitoring SVMs .....	159
Editing SVM settings .....	160
Deleting SVMs .....	161
Starting SVMs .....	162
Stopping SVMs .....	162
What SVMs are .....	162

Managing SVMs .....	164
Types of SVMs .....	164
Why you use SVMs .....	165
How ONTAP name service switch configuration works .....	165
Storage Virtual Machines window .....	166
Volumes .....	168
Editing the volume properties .....	169
Editing data protection volumes .....	171
Deleting volumes .....	171
Creating FlexClone volumes .....	172
Creating FlexClone files .....	173
Splitting a FlexClone volume from its parent volume .....	173
Viewing the FlexClone volume hierarchy .....	174
Changing the status of a volume .....	174
Viewing the Snapshot copies .....	175
Creating Snapshot copies .....	175
Setting the Snapshot copy reserve .....	176
Hiding the Snapshot copy directory .....	177
Scheduling automatic Snapshot copies .....	177
Restoring a volume from a Snapshot copy .....	177
Extending the expiry date of Snapshot copies .....	178
Renaming Snapshot copies .....	179
Deleting Snapshot copies .....	179
Resizing volumes .....	180
Enabling storage efficiency on a volume .....	181
Changing the deduplication schedule .....	182
Running deduplication operations .....	183
Moving FlexVol volumes between aggregates or nodes .....	183
Assigning volumes to Storage QoS .....	184
Creating a mirror relationship from a source SVM .....	185
Creating a vault relationship from a source SVM .....	188
Creating a mirror and vault relationship from a source SVM .....	190
Creating an NFS datastore for VMware .....	193
Creating FlexGroup volumes .....	193
Editing FlexGroup volumes .....	194
Resizing FlexGroup volumes .....	194
Changing the status of a FlexGroup volume .....	195
Deleting FlexGroup volumes .....	195
Viewing FlexGroup volume information .....	196
What volume granular encryption is .....	196
How FlexVol volumes work .....	196
What an Infinite Volume is .....	197
Considerations for creating a FlexClone volume from a SnapMirror	
source or destination volume .....	197
Snapshot configuration .....	197



Guidelines for working with Snapshot copies of Infinite Volumes .....	197
When Snapshot copies of Infinite Volumes are accessible .....	198
How volume guarantees work for FlexVol volumes .....	199
How incremental tape backup uses SnapDiff and Snapshot copies .....	200
FlexClone volumes and space guarantees .....	200
Thin provisioning for greater efficiencies using FlexVol volumes .....	200
Using space reservations with FlexVol volumes .....	201
Considerations when using thin provisioning with Infinite Volumes .....	201
Benefits of storage efficiency .....	203
Data compression and deduplication .....	204
Guidelines for using deduplication .....	204
Options for resizing volumes .....	205
Considerations when moving volumes .....	205
How moving a FlexVol volume works .....	206
Volumes window .....	206
Application Provisioning .....	214
Provisioning storage for Oracle application type over NFS .....	214
Namespace .....	217
Mounting volumes .....	217
Unmounting FlexVol volumes .....	218
Changing export policies .....	218
Namespace window .....	219
Shares .....	219
Creating a CIFS share .....	219
Stopping share access .....	220
Creating home directory shares .....	221
Editing share settings .....	221
How ONTAP enables dynamic home directories .....	222
Shares window .....	223
LUNs .....	225
Creating FC SAN optimized LUNs .....	225
Application-specific LUN settings .....	226
Creating LUNs .....	229
Deleting LUNs .....	231
Creating initiator groups .....	231
Deleting initiator groups .....	231
Adding initiators .....	232
Deleting initiators from an initiator group .....	232
Creating port sets .....	232
Deleting port sets .....	233
Cloning LUNs .....	233
Editing LUNs .....	233
Bringing LUNs online .....	234
Taking LUNs offline .....	234
Moving LUNs .....	234

Assigning LUNs to Storage QoS .....	236
Editing initiator groups .....	237
Editing initiators .....	237
Editing port sets .....	237
Viewing LUN information .....	238
Viewing initiator groups .....	238
Guidelines for working with FlexVol volumes that contain LUNs .....	238
LUN size and type .....	239
Understanding space reservations for LUNs .....	239
Guidelines for using LUN multiprotocol type .....	239
Understanding LUN clones .....	241
Resizing a LUN .....	241
Initiator hosts .....	241
VMware RDM .....	241
What igroups are .....	241
Required information for creating igroups .....	242
igroup name .....	242
igroup type .....	242
igroup ostype .....	242
Ways to limit LUN access with port sets and igroups .....	242
LUNs window .....	243
Qtrees .....	246
Creating qtrees .....	246
Deleting qtrees .....	247
Editing qtrees .....	247
Assigning export policies to qtrees .....	248
Viewing qtree information .....	248
What a qtree is .....	248
Qtree options .....	249
Security styles .....	249
Qtrees window .....	250
Quotas .....	251
Creating quotas .....	251
Deleting quotas .....	252
Editing quota limits .....	252
Activating or deactivating quotas .....	253
Resizing quotas .....	253
Viewing quota information .....	253
Types of quotas .....	254
Quota limits .....	254
Quota management .....	255
How qtree changes affect quotas .....	255
How changing the security style of a qtree affects user quotas .....	255
How quotas work with users and groups .....	256
Quotas window .....	256

CIFS protocol .....	257
Setting up CIFS .....	258
Editing the general properties for CIFS .....	259
Adding home directory paths .....	259
Deleting home directory paths .....	260
Resetting CIFS domain controllers .....	260
Updating the CIFS group policy configuration .....	260
Enabling or disabling a CIFS group policy configuration .....	261
Reloading CIFS group policy .....	261
Setting up BranchCache .....	261
Modifying the BranchCache settings .....	262
Deleting the BranchCache configuration .....	263
Adding preferred domain controllers .....	263
Editing preferred domain controllers .....	264
Deleting preferred domain controllers .....	264
Viewing CIFS domain information .....	264
SMB concepts .....	264
How ONTAP enables you to provide SMB client access to UNIX symbolic links .....	265
Using BranchCache to cache SMB share content at a branch office .....	266
What happens when you delete the BranchCache configuration .....	266
CIFS window .....	266
NFS protocol .....	268
Editing NFS settings .....	268
How ONTAP handles NFS client authentication .....	269
NFS window .....	269
iSCSI protocol .....	269
Creating iSCSI aliases .....	270
Enabling or disabling the iSCSI service on storage system interfaces .....	270
Adding the security method for iSCSI initiators .....	271
Editing default security settings .....	271
Editing initiator security .....	272
Changing the default iSCSI initiator authentication method .....	272
Setting the default security for iSCSI initiators .....	273
Starting or stopping the iSCSI service .....	273
Viewing initiator security information .....	273
What iSCSI is .....	274
What iSCSI nodes are .....	274
Initiator security .....	274
What CHAP authentication is .....	274
iSCSI window .....	275
FC/FCoE protocol .....	275
Starting or stopping the FC or FCoE service .....	275
Changing an FC or FCoE node name .....	276
What FC is .....	276

What FC nodes are .....	276
The FCoE protocol .....	277
FC/FCoE window .....	277
Export policies .....	277
Creating an export policy .....	277
Renaming export policies .....	278
Deleting export policies .....	278
Adding rules to an export policy .....	278
Modifying export policy rules .....	279
Deleting export policy rules .....	280
How export policies control client access to volumes or qtrees .....	280
Export Policies window .....	281
Efficiency policies .....	282
Adding efficiency policies .....	282
Editing efficiency policies .....	283
Deleting efficiency policies .....	283
Enabling or disabling efficiency policies .....	283
What an efficiency policy is .....	284
Understanding predefined efficiency policies .....	284
Efficiency Policies window .....	284
Protection policies .....	285
Creating protection policies .....	285
Deleting protection policies .....	286
Editing protection policies .....	286
Managing data protection using SnapMirror policies .....	287
Protection Policies window .....	287
QoS policy groups .....	288
Creating QoS policy groups .....	288
Deleting QoS policy groups .....	288
Editing QoS policy groups .....	289
Managing workload performance by using Storage QoS .....	289
How Storage QoS works .....	290
How the maximum throughput limit works .....	290
Rules for assigning storage objects to policy groups .....	291
QoS Policy Groups window .....	292
NIS services .....	293
Adding NIS domains .....	293
Editing NIS domains .....	293
Managing NIS domains .....	293
NIS window .....	294
LDAP client services .....	294
Adding an LDAP client configuration .....	294
Deleting an LDAP client configuration .....	295
Editing an LDAP client configuration .....	295
LDAP Client window .....	296

LDAP configuration services .....	296
Editing active LDAP clients .....	296
Deleting active LDAP clients .....	297
LDAP Configuration window .....	297
Kerberos realm services .....	298
Creating a Kerberos realm configuration .....	298
Editing a Kerberos realm configuration .....	299
Deleting Kerberos realm configurations .....	299
Using Kerberos with NFS for strong security .....	300
Kerberos authentication for CIFS .....	300
Kerberos Realm window .....	300
Kerberos interface services .....	301
Editing Kerberos configuration .....	301
Kerberos Interface window .....	301
DNS/DDNS Services .....	302
Enabling or disabling DNS and DDNS .....	302
Editing DNS and DDNS settings .....	303
DNS/DDNS Services window .....	303
Users .....	304
Adding SVM user accounts .....	304
Changing the password for SVM user accounts .....	304
Editing SVM user accounts .....	305
Locking or unlocking SVM user accounts .....	305
Users window .....	305
Roles .....	306
Adding roles .....	306
Editing roles .....	307
Predefined roles for SVM administrators .....	307
Roles window .....	308
UNIX .....	309
UNIX window .....	309
Windows .....	310
Creating a local Windows group .....	310
Editing local Windows group properties .....	312
Adding user accounts to a Windows local group .....	312
Renaming a local Windows group .....	313
Deleting a local Windows group .....	314
Creating a local Windows user account .....	315
Editing the local Windows user properties .....	316
Assigning group memberships to a user account .....	316
Renaming a local Windows user .....	317
Resetting the password of a Windows local user .....	318
Deleting a local Windows user account .....	318
Using local users and groups for authentication and authorization .....	319
Local users and groups concepts .....	319

Reasons for creating local users and local groups .....	320
What local privileges are .....	320
List of supported privileges .....	320
Predefined BUILTIN groups and default privileges .....	321
Windows window .....	322
Name mapping .....	324
How name mappings are used .....	325
How name mapping works .....	325
Name mapping conversion rules .....	326
How group mapping supports multiprotocol access to Infinite Volumes ....	327
Name Mapping window .....	328
<b>Managing data protection .....</b>	<b>330</b>
Mirror relationships .....	330
Creating a mirror relationship from a destination SVM .....	330
Deleting mirror relationships .....	333
Editing mirror relationships .....	333
Initializing mirror relationships .....	334
Updating mirror relationships .....	335
Quiescing mirror relationships .....	336
Resuming mirror relationships .....	336
Breaking SnapMirror relationships .....	337
Resynchronizing mirror relationships .....	337
Reverse resynchronizing mirror relationships .....	338
Aborting a mirror transfer .....	339
Restoring a volume in a mirror relationship .....	339
Components of a mirror relationship .....	341
How SnapMirror works .....	341
Uses for data protection mirror copies .....	341
Providing disaster recovery on Infinite Volumes using mirroring technology .....	341
Vault relationships .....	342
Creating a vault relationship from a destination SVM .....	342
Deleting vault relationships .....	345
Editing vault relationships .....	345
Initializing a vault relationship .....	346
Updating a vault relationship .....	347
Quiescing a vault relationship .....	347
Resuming a vault relationship .....	348
Aborting a Snapshot copy transfer .....	348
Restoring a volume in a vault relationship .....	349
What a SnapVault backup is .....	350
How a SnapVault backup works .....	351
Which data gets backed up and restored from a SnapVault backup .....	352
How SnapVault backups work with data compression .....	352
SnapVault backup limitations .....	352

Guidelines for planning Snapshot copy schedule and retention for SnapVault backups .....	352
Data protection for SVM namespace and root information .....	353
Mirror and vault relationships .....	354
Creating a mirror and vault relationship from a destination SVM .....	354
Deleting mirror and vault relationships .....	356
Editing mirror and vault relationships .....	357
Initializing mirror and vault relationships .....	358
Updating mirror and vault relationships .....	358
Quiescing mirror and vault relationships .....	359
Resuming mirror and vault relationships .....	359
Breaking mirror and vault relationships .....	360
Resynchronizing mirror and vault relationships .....	360
Reverse resynchronizing mirror and vault relationships .....	361
Aborting mirror and vault relationships .....	361
Restoring a volume in a mirror and vault relationship .....	362
What lag time is .....	363
Types of data protection relationships .....	363
Protection window .....	364
Snapshot policies .....	366
Creating Snapshot policies .....	366
Editing Snapshot policies .....	366
Deleting Snapshot policies .....	367
About Snapshot policies .....	367
Snapshot Policies window .....	367
Schedules .....	368
Creating schedules .....	368
Editing schedules .....	369
Deleting schedules .....	369
Schedules .....	369
Schedules window .....	370
<b>Copyright information .....</b>	<b>371</b>
<b>Trademark information .....</b>	<b>372</b>
<b>How to send comments about documentation and receive update     notifications .....</b>	<b>373</b>
<b>Index .....</b>	<b>374</b>

## **Welcome to OnCommand System Manager Help**

---

The Help includes information about how to configure, manage, and monitor storage objects and storage systems running Data ONTAP by using OnCommand System Manager (abbreviated to System Manager).

The table of contents, search, index, and favorites in the Help system help you find the relevant information required to achieve your goals.

The structure of the Help is similar to what you see on the UI. You can click **Help > OnCommand System Manager Help** to access the contextual help.

### **Access to your favorite topics**

You can quickly access a particular subject that you often look up by bookmarking topics in the **Favorites** tab of the Help system.



## Understanding System Manager

---

System Manager is a graphical management interface that enables you to manage storage systems and storage objects (such as disks, volumes, and aggregates) and perform common management tasks related to storage systems from a web browser. As a cluster administrator, you can use System Manager to administer the entire cluster and its resources.

**Important:** System Manager is no longer available as an executable file and is now included with ONTAP software as a web service, enabled by default, and accessible by using a browser.

System Manager enables you to perform many common tasks such as the following:

- Create a cluster, configure a network, and set up support details for the cluster.
- Configure and manage storage objects such as disks, aggregates, volumes, qtrees, and quotas.
- Configure protocols such as CIFS and NFS, and provision file sharing.
- Configure protocols such as FC, FCoE, and iSCSI for block access.
- Create and configure network components such as subnets, broadcast domains, data and management interfaces, and interface groups.
- Set up and manage mirroring and vaulting relationships.
- Perform cluster management, storage node management, and Storage Virtual Machine (SVM, formerly known as Vserver) management operations.
- Create and configure SVMs, manage storage objects associated with SVMs, and manage SVM services.
- Monitor and manage HA configurations in a cluster.
- Configure Service Processors to remotely log in, manage, monitor, and administer the node, regardless of the state of the node.





## Icons used in the application interface

---

You can view the icons in the interface to get quick information about systems and operations.

### Dashboard window icons

You might see the following icons when viewing the dashboard for the storage system:



Icon	Name	Description
	Warning	There are minor issues, but none that require immediate attention.
	Error	Problems that might eventually result in downtime and therefore require attention.
	Critical	The storage system is not serving data or cannot be contacted. Immediate attention is required.
	Link arrow	If this is displayed next to a line item in a dashboard pane, clicking it links to another page from which you can get more information about the line item or make changes to the line item.

## Window layout customization


---

System Manager enables you to customize the window layout. By customizing the windows, you can control which data is viewable or how it is displayed.

### Sorting

You can click the column header to change the sort order of the column entries. When you click the column header, the sort arrows (  and  ) appear for that column.

### Filtering

You can click the filter icon (  ) to display only those entries that match the conditions that are provided. You can then use the character filter (?) or string filter (\*) to narrow your search. The filter icon is displayed when you move the pointer over the column headings.

You can apply filters to one or more columns.

**Note:** When you apply filters to the physical size field or the usable size field, any value that you enter without the unit suffix in these fields is considered to be in bytes. For example, if you enter a value of 1000 without specifying the unit in the physical size field, the value is automatically considered as 1000 bytes.

### Hiding or redisplaying the columns

You can click the column display icon (  ) to select which columns you want to display.

### Customizing the layout

You can drag the bottom of the list of objects area up or down to resize the main areas of the window. You can also display or hide the list of related objects and list of views panels. You can drag the vertical dividers to resize the width of the columns or other areas of the window.

### Searching

You can use the search box to search for volumes, LUNs, qtrees, network interfaces, Storage Virtual Machines (SVMs), aggregates, disks, or Ethernet ports, or all of these objects. You can click the results to navigate to the exact location of the object.

#### Notes:

- When you search for objects that contain one or more of the { \ ? ^ > | characters, the results are displayed correctly, but they do not navigate to the correct row in the page.
- You must not use the question mark (?) character to search for an object.

## Supportability Dashboard

---

You can use the Supportability Dashboard to access product documentation and AutoSupport tools, download software, and visit sites such as the Community and NetApp University for additional information.

The Supportability Dashboard contains the following sources of information.

### **Community**

Provides access to online collaborative resources on a range of NetApp products.

### **NetApp Support Site**

Provides access to technical assistance, troubleshooting tools, and the Interoperability Matrix Tool.

### **NetApp University**

Provides course material for learning about NetApp products.

### **Downloads**

Provides access to NetApp firmware and software that you can download.

### **Documentation**

Provides access to NetApp product documentation.

### **My AutoSupport**

Provides access to the MyAutoSupport portal and the Manual AutoSupport Upload tool.

## Where to find additional ONTAP information

---

System Manager Help provides basic ONTAP conceptual information to help you perform tasks using System Manager. For in-depth conceptual information to help you configure, monitor, and manage storage objects and storage systems, you can see the ONTAP documentation available on the NetApp Support Site.

### Related information

*[NetApp Documentation: ONTAP 9](#)*

## Setting up your cluster environment

---

You can create a cluster by using System Manager or the command-line interface (CLI). To create a cluster using System Manager, you must set up the node management IP address on any node in the cluster network. If you have created a cluster using the CLI, you can configure the cluster using System Manager.

### Setting up the cluster by using OnCommand System Manager

Beginning with ONTAP 9.1, you can use OnCommand System Manager to setup up a cluster by creating a cluster, setting up the node management and cluster management networks, and setting up the AutoSupport messages and event notifications.

#### Before you begin

- You must have configured the node management IP addresses for at least one node.
- Nodes must be in the default mode of HA.
- Nodes must be running ONTAP 9.1 or later.
- Nodes must be of the same model.
- All of the nodes must be healthy and cabling for the nodes must be set up.
- Ensure that the cabling and connectivity are in place for your cluster configuration.
- You must have sufficient cluster management, node management, Service Processor IP addresses, and gateway and netmask details.
- If the cluster interface is present on a port, then that port must be present in the cluster IPspace.

#### About this task

To create a cluster, you have to log in through the console, and configure the node management IP address on any node in the cluster network. After you have configured the node management IP address on a node, you can add other nodes and create a cluster by using OnCommand System Manager.

Cluster setup is not supported on MetroCluster configurations for ONTAP software.

You can set up the cluster by using a template file or by manually entering the values in the guided setup.

#### Choices

- [Setting up a cluster by using the template file](#) on page 22
- [Setting up the cluster manually](#) on page 24

### Setting up a cluster by using the template file

You can use the template file that is provided in System Manager to set up a cluster by creating a cluster, setting up the node management and cluster management networks, and then setting up the

AutoSupport messages and event notifications. You can download the template file in `.xlsx` format or `.csv` format.

### About this task

- If the cluster supports ONTAP 9.1 or later, you can add only storage systems that are running ONTAP 9.1 or later.
- All fields are not auto populated when you upload the file.  
You must manually enter the value of some fields such as password and cluster management port.

### Steps

1. Open the web browser, and then enter the node management IP address that you have configured:  
`https://node-management-IP`
  - If you have set up the credentials for the cluster, the Login page is displayed.  
You must enter the credentials to log in.
  - If you have not set up the credentials for the cluster, the Guided Setup page is displayed.
2. Download the `.xlsx` template file or the `.csv` template file.
3. Provide all the required values in the template file, and save the file.
 

**Note:**

  - Do not edit any other column in the template other than Value.
  - Do not change the version of the template file.
4. Click **Browse**, and select the updated template file.
  - You can upload the template file only in the `.csv` format. If you have downloaded the template file in `.xlsx` format, you must save the file as a `.csv` file, and then upload the file.
  - You must ensure that the encoding used for this file is UTF8. If not, the values will not be read.
5. Click **Upload**.  
The details that you have provided in the template file are used to complete the guided setup process.
6. Click the **Guided Setup** icon to view the details for the cluster.
7. Verify the details in the **Cluster** window, and then click **Submit**.  
You can edit the cluster details, if required.  
  
If you log in to the Cluster window for the second time, the **Feature Licenses** field is enabled by default. You can add new feature license keys or retain the pre-populated license keys.
8. Verify the details in the **Network** window, and then click **Submit**.  
You can edit the network details, if required.
9. Verify the details in the **Support** window, and then click **Submit**.  
You can edit the support details, if required.
10. Verify all the details in the **Summary** page, and then click **Manage your cluster** to complete the cluster setup process and launch System Manager.

## Setting up the cluster manually

You can use System Manager to manually setup the cluster by creating a cluster, setting up the node management and cluster management networks, and setting up the AutoSupport messages and event notifications.

### Creating a cluster

You can use OnCommand System Manager to create and set up a cluster in your data center.

#### About this task

If the cluster supports ONTAP 9.1 or later, you can add only those storage systems that are running ONTAP 9.1 or later.

#### Steps

1. Open the web browser, and then enter the node management IP address that you have configured:  
`https://node-management-IP`
  - If you have set up the credentials for the cluster, the Login page is displayed.  
You must enter the credentials to log in.
  - If you have not set up the credentials for the cluster, the Guided Setup page is displayed.  
Click the **Guided Setup** icon to set up a cluster.
2. In the **Cluster** page, enter a name for the cluster.  
**Note:** If all the nodes are not discovered, click **Refresh**.  
  
The nodes in that cluster network are displayed in the Nodes field.
3. Optional: If desired, update the node names in the **Nodes** field.
4. For a two-node cluster configuration, select switched or switchless cluster based on your hardware connectivity or cabling.
5. Enter the password for the cluster.
6. Optional: Enter the cluster base license keys.  
**Note:** The cluster base license keys are mandatory if you want to enter the feature license keys.
7. Optional: Enter the feature license keys.
8. Click **Submit**.

#### After you finish

Enter the network details in the Network page to continue with the cluster setup.

#### Related references

[Licenses window](#) on page 73

[Configuration Updates window](#) on page 60



## Setting up a network

By setting up a network, you can manage your cluster, nodes, and Service Processors. You can also set up DNS and NTP details by using the network window.

### Before you begin

You must have set up the cluster.

### About this task

- Only those nodes that are up and running are listed for cluster creation. You can create LIFs for those nodes.
- You can disable IP address range and enter individual IP addresses for cluster management, node management, and Service Processor management networks.

## Setting up a network when an IP address range is enabled

You can set up a network by enabling an IP address range. The IP address range enables you to enter IP addresses that are in the same netmask range or in the different netmask range.

### Steps

1. Enter a range of IP addresses in the **IP Address Range** field, and then click **Apply**.

Option	Description
You have a range of IP addresses in the same netmask	Enter the IP address range, and then click <b>Apply</b> . IP addresses are applied to cluster management, node management, and Service Processor management networks sequentially.
You have a range of IP addresses in different netmasks	Enter the IP address range in rows, and then click <b>Apply</b> . The first IP address applied to cluster management and other IP addresses are applied to node management and Service Processor management networks sequentially.

**Note:** After entering the IP address range for cluster management, node management, and Service Processor management, you must not manually modify the IP address values in these fields. You must ensure that all the IP addresses are IPv4 addresses.

2. Enter the netmask and gateway details.
3. Select the port for cluster management in the **Port** field.
4. If the **Port** field in the node management is not populated with **e0M**, enter the port details.  
**Note:** By default, the Port field displays e0M.
5. For Service Processor management, if you are overriding the default values, ensure that you have entered the mandatory gateway details.
6. If you have enabled the **DNS Details** field, enter the DNS server details.
7. If you have enabled the **NTP Details** field, enter the NTP server details.  
**Note:** Providing alternative NTP server details is optional.
8. Click **Submit**.

**After you finish**

Enter AutoSupport message details and event notifications in the Support page to continue with the cluster setup.

**Related information**

[NetApp KB Article 3012997: What is a Service Processor and how do I use it?](#)

[NetApp KB Article 1014787: How to configure and troubleshoot NTP on clustered Data ONTAP 8.2 and later using CLI](#)

[NetApp Documentation: ONTAP 9](#)

**Setting up a network when an IP address range is disabled**

You can set up a network by disabling an IP address range and entering individual IP addresses for cluster management, node management, and service provider networks.

**About this task**

In the Networks page, if the **IP Address Range** is disabled, enter individual IP addresses for cluster management, node management, and service processor networks.

**Steps**

1. Enter the cluster management IP address in the **Cluster Management IP Address** field.
2. Enter the netmask details for cluster management.
3. Optional: Enter the gateway details for cluster management.
4. Select the port for cluster management in the **Port** field.
5. If you want to provide netmask and gateway details to manage your nodes, clear the **Retain Netmask and Gateway configuration of the Cluster Management** check box, and then enter the netmask and gateway details.
6. Enter the node management IP addresses in the **Node Management** field.
7. If the **Port** field in the node management is not populated with **e0M**, enter the port details.  
**Note:** By default, the Port field displays e0M.
8. Enter the Service Processor management netmask and gateway details.
9. Enter the Service Processor IP management addresses in the **Service Processor Management** field.
10. If you have enabled the **DNS Details** field, enter the DNS server details.
11. If you have enabled the **NTP Details** field, enter the NTP server details.  
**Note:** Providing alternative NTP server details is optional.
12. Click **Submit**.

**After you finish**

Enter AutoSupport message details and event notifications in the Support page to continue with the cluster setup.

**Related references**

[Network window](#) on page 104

[Configuration Updates window](#) on page 60

[Date and Time window](#) on page 80

[Service Processors window](#) on page 62

#### Related information

[NetApp KB Article 3012997: What is a Service Processor and how do I use it?](#)

[NetApp KB Article 1014787: How to configure and troubleshoot NTP on clustered Data ONTAP 8.2 and later using CLI](#)

[NetApp Documentation: ONTAP 9](#)

### Setting up a support page

Setting up the support page completes the cluster setup, and involves setting up the AutoSupport messages and event notifications, and for single-node clusters, configuring system backup.

#### Before you begin

You must have set up the cluster and network.

#### About this task

If you have enabled the AutoSupport button, all the nodes in that cluster are enabled to send AutoSupport messages. If you have disabled the AutoSupport button, then all the nodes in that cluster are disabled to send AutoSupport messages.

#### Steps

1. If you have enabled the AutoSupport button, set up the AutoSupport messages by entering the proxy URL in the **Proxy URL** field.

**Note:** The format of the proxy URL must be `username:password@proxyUrl:port`.

2. Set up the event notifications by using the mailhost, or SNMP trap host, or Syslog server.

**Note:** You must set up at least one event notification system.

3. If you have a single-node cluster, configure a system backup on an FTP server or on an HTTP server.

**Note:** System backup is applicable only for single-node clusters.

4. Click **Submit**.

#### After you finish

You must verify the details that you have provided in the Summary page, and then click **Manage your cluster** to launch System Manager.

#### Related references

[AutoSupport window](#) on page 156

#### Related information

[NetApp AutoSupport](#)

## Accessing a cluster by using OnCommand System Manager browser-based graphic interface

If you prefer to use a graphic interface instead of the command-line interface for accessing and managing a cluster, you can do so by using OnCommand System Manager, which is included with ONTAP as a web service, enabled by default, and accessible by using a browser.

### Before you begin

You must have a cluster user account configured with the **admin** role and the **http**, **ontapi**, and **console** application types.

### About this task

You can use a cluster management LIF or node management LIF to access OnCommand System Manager. However, you should use the cluster management LIF for an uninterrupted access to OnCommand System Manager.

### Steps

1. Point the web browser to the cluster management LIF in one of the following formats:

- **https://cluster-mgmt-LIF** (if using IPv4)
- **https://[cluster-mgmt-LIF]** (if using IPv6)

*cluster-mgmt-LIF* is the IP address of the cluster management LIF.

Only HTTPS is supported for the browser access of OnCommand System Manager.

If the cluster uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a Certificate Authority (CA) signed digital certificate on the cluster for server authentication.

2. Log in to OnCommand System Manager by using your cluster administrator credential.

### Related information

[NetApp Documentation: ONTAP 9](#)

## Configuring System Manager options

You can enable logging and specify the inactivity timeout value for the System Manager application.

### About this task

You can also configure the options from the System Manager login window. However, you must log in to the application to specify the inactivity timeout value.

### Steps

1. In the System Manager application window, click **Administration > Settings**.
2. In the **Settings** dialog box, select the required log level.
3. Specify the inactivity timeout value, in minutes.

4. Click **OK**.

## Viewing OnCommand System Manager log files

If you encounter any issues when using System Manager, you can send the log files to technical support to help troubleshoot the issues. The System Manager log files are located in the `mlog` directory along with the Data ONTAP log files.

### Before you begin

You must be aware of the node that hosts the cluster-management LIF.

### Steps

1. Enter the following URL in a web browser:  
`https://cluster-mgmt-LIF/spi`  
*cluster-mgmt-LIF* is the IP address of the cluster-management LIF.
2. Enter your cluster administrator credentials, and then click **OK**.
3. In the **Clustered Data ONTAP - Root Volume File Access** window, click the **logs** link for the node that hosts the cluster-management LIF.
4. Navigate to the `mlog` directory to access the System Manager log files.

You might require the following log files, depending on the type of issue:

- `sysmgr.log`  
This file contains the latest logs for System Manager.
- `mgwd.log`
- `php.log`
- `apache_access.log`
- `messages.log`

## How system logging works

System logging is an essential tool for application troubleshooting. You should enable system logging so that if there is a problem with an application, the problem can be located. You can enable System Manager logging at runtime without modifying the application binary.

Log output can be voluminous and therefore can become difficult to manage. System Manager enables you to refine the logging output by selecting which type of log statements are output. By default, system logging is set to INFO. You can choose one of the following log levels:

- OFF
- ERROR
- WARN
- INFO
- DEBUG

These levels function hierarchically. A log level set to OFF indicates no logging of messages.

## Configuring a cluster by using System Manager

Certain prerequisites must be met before you configure a cluster using System Manager.

- You must have created a cluster.
- You must have not configured the cluster.

## Accessing a cluster by using OnCommand System Manager browser-based graphic interface

If you prefer to use a graphic interface instead of the command-line interface for accessing and managing a cluster, you can do so by using OnCommand System Manager, which is included with ONTAP as a web service, enabled by default, and accessible by using a browser.

### Before you begin

You must have a cluster user account configured with the **admin** role and the **http**, **ontapi**, and **console** application types.

### About this task

You can use a cluster management LIF or node management LIF to access OnCommand System Manager. However, you should use the cluster management LIF for an uninterrupted access to OnCommand System Manager.

### Steps

1. Point the web browser to the cluster management LIF in one of the following formats:
  - **https://cluster-mgmt-LIF** (if using IPv4)
  - **https://[cluster-mgmt-LIF]** (if using IPv6)

*cluster-mgmt-LIF* is the IP address of the cluster management LIF.

Only HTTPS is supported for the browser access of OnCommand System Manager.

If the cluster uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a Certificate Authority (CA) signed digital certificate on the cluster for server authentication.

2. Log in to OnCommand System Manager by using your cluster administrator credential.

### Related information

[NetApp Documentation: ONTAP 9](#)

## Setting up the cluster

Setting up the cluster involves gathering the configuration information, creating cluster-management and node-management interfaces, adding licenses, setting up the cluster time, and monitoring HA pairs.

## Updating the cluster name

You can use System Manager to modify the cluster name when required.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Configuration Updates**.
3. Click **Update Cluster Name**.
4. In the **Update Cluster Name** dialog box, type the new cluster name, and then click **Submit**.

## Changing the cluster password

You can use System Manager to reset the password of the cluster.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Configuration Updates**.
3. Click **Change Password**.
4. In the **Change Password** dialog box, specify the new password, confirm the new password, and then click **Change**.

## Editing DNS configurations

You can use System Manager to add host information to centrally manage DNS. You can modify the DNS details when you want to change the domain names or IP addresses.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Configuration Updates**.
3. Click **Edit DNS Configuration**.
4. In the **Edit DNS Settings** dialog box, select the **DNS service** check box to enable DNS.
5. In the DNS Domains area, add or modify the DNS domain names.
6. In the Name Servers area, add or modify the IP addresses.
7. Click **OK**.

## Creating a cluster-management interface

You can use System Manager to create a cluster-management interface or LIF to provide a single management interface for the entire cluster. You can use this LIF to manage all the activities of the entire cluster.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Configuration Updates**.
3. Click **Create Cluster-management LIF**.

4. In the **Create Cluster-Management LIF** dialog box, specify a name for the cluster-management LIF.
5. Assign the IP address by choosing one of the following options:

If you want to...	Then...
Specify the IP address using a subnet	<ol style="list-style-type: none"> <li>a. Select <b>Using a subnet</b>.</li> <li>b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For an intercluster LIF, only the subnets that are associated with the selected IPspace are displayed.</li> <li>c. If you want to assign a specific IP address to the interface, select <b>Use a specific IP address</b>, and then type the IP address. The IP address you specify is added to the subnet if it is not already present in the subnet range.</li> <li>d. Click <b>OK</b>.</li> </ol>
Specify the IP address manually without using a subnet	<ol style="list-style-type: none"> <li>a. Select <b>Without a subnet</b>.</li> <li>b. In the Add Details dialog box, perform the following steps:               <ol style="list-style-type: none"> <li>i. Specify the IP address and network mask or prefix.</li> <li>ii. Optional: Specify the gateway. The destination field is populated with the default value based on the family of the IP address.</li> <li>iii. If you do not want the default value, specify the new destination value.  If a route does not exist, a new route is automatically created based on the gateway and destination.</li> </ol> </li> <li>c. Click <b>OK</b>.</li> </ol>

6. Select the required ports from the ports details area.
7. Click **Create**.

#### After you finish

If you have an existing cluster-management interface or LIF and if you want to delete it, you must use the command-line interface (CLI).

### Editing the node name

You can use System Manager to modify the node name when required.

#### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Configuration Updates**.
3. In the **Nodes** tab, select the node, and then click **Edit Node Name**.
4. In the **Edit Node Name** dialog box, type the new node name, and then click **Submit**.



## Creating a node-management interface

You can use System Manager to create a dedicated IP address for managing a particular node in a cluster. You can use this LIF to manage the system maintenance activities of the particular node.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Configuration Updates**.
3. In the **Nodes** tab, select the node, and then click **Create Node-management LIF**.
4. In the **Create Node-Management LIF** dialog box, specify a name for the node-management LIF.
5. Assign the IP address by choosing one of the following options:

If you want to...	Then...
Specify the IP address using a subnet	<ol style="list-style-type: none"> <li>a. Select <b>Using a subnet</b>.</li> <li>b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For an intercluster LIF, only the subnets that are associated with the selected IPspace are displayed.</li> <li>c. If you want to assign a specific IP address to the interface, select <b>Use a specific IP address</b>, and then type the IP address. The IP address you specify is added to the subnet if it is not already present in the subnet range.</li> <li>d. Click <b>OK</b>.</li> </ol>
Specify the IP address manually without using a subnet	<ol style="list-style-type: none"> <li>a. Select <b>Without a subnet</b>.</li> <li>b. In the Add Details dialog box, perform the following steps:               <ol style="list-style-type: none"> <li>i. Specify the IP address and network mask or prefix.</li> <li>ii. Optional: Specify the gateway. The destination field is populated with the default value based on the family of the IP address.</li> <li>iii. If you do not want the default value, specify the new destination value.  If a route does not exist, a new route is automatically created based on the gateway and destination.</li> </ol> </li> <li>c. Click <b>OK</b>.</li> </ol>

6. Select the required ports from the ports details area.
7. Click **Create**.

### After you finish

If you have an existing node-management interface or LIF and if you want to delete it, you must use the command-line interface (CLI).

## Editing AutoSupport settings

You can use System Manager to modify your AutoSupport settings to specify an email address from which email notifications are sent and add multiple email host names.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Configuration Updates**.
3. In the **Nodes** tab, select the node, and then click **Edit AutoSupport**.
4. In the **Email Recipient** tab, type the email address from which email notifications are sent, specify the email recipients and the message content for each email recipient, and then add the mail hosts.  
  
You can add up to five email addresses of the host names.
5. In the **Others** tab, select a transport protocol for delivering the email messages, and then specify the HTTP or HTTPS proxy server details.
6. Click **OK**.

## Adding licenses

If your storage system software was installed at the factory, System Manager automatically adds the software to its list of licenses. If the software was not installed at the factory or if you want to add additional software licenses, you can add the software license by using System Manager.

### Before you begin

The software license code for the specific Data ONTAP service must be available.

### About this task

- When you add a new license in a MetroCluster configuration, it is a best practice to add the license on the surviving site cluster as well.
- You cannot use System Manager to add the cloud license.  
The cloud license is not listed in the license page. System Manager does not raise any alert about the entitlement risk status of the cloud license.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Licenses**.
3. In the **Licenses** window, click **Add**.
4. In the **Add License** dialog box, enter the software license key, and then click **Add**.  
  
You can add multiple licenses by entering the software license keys, separated by commas.  
  
The new license is added.  
  
The Add License Status dialog box displays the list of licenses that were added successfully. The window also displays the license keys of the licenses that were not added and the reason.
5. Click **Close**.

**Result**

The software license is added to your storage system and is displayed in the list of licenses in the Licenses window.

**Related references**

[Licenses window](#) on page 73

**Setting the time for a cluster**

You can manually set or modify the time zone for your cluster by using the Edit Date and Time dialog box in System Manager. You can also add time servers to the cluster.

**About this task**

Network Time Protocol (NTP) is always enabled on the cluster. You can disable NTP by contacting technical support. However, disabling NTP is not recommended.

You can add the IP addresses of the NTP server at your site. This server is used to synchronize the time across the cluster.

You can specify either an IPv4 address or an IPv6 address for the time server.

**Steps**

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Date and Time**.
3. Click **Edit**.
4. In the **Edit Date and Time** dialog box, select the time zone.
5. Specify the IP address of the time servers, and then click **Add**.
6. Click **OK**.
7. Verify the changes you made to the date and time settings in the **Date and Time** window.

**Related tasks**

[Creating a Kerberos realm configuration](#) on page 298

**Related references**

[Date and Time window](#) on page 80

**Monitoring HA pairs**

You can use System Manager to monitor the state and interconnect status of all the HA pairs in a cluster. You can verify whether takeover or giveback is enabled or has occurred, and view reasons why takeover or giveback is not currently possible.

**Steps**

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **High Availability**.
3. In the **High Availability** window, click the HA pair image to view details such as the cluster HA status, node status, interconnect status, and hardware model of each node.

If the cluster management LIF or the data LIFs of a node are not in their home node, a warning message is displayed indicating that the node has some LIFs that are not in the home node.

#### Related references

[High Availability window](#) on page 68

## Setting up the network

Setting up the network consists of creating IPspaces, a broadcast domain, and subnets.

### Creating IPspaces

You can create an IPspace by using System Manager to configure a single Data ONTAP cluster for client access from more than one administratively separate network domain, even when the clients use the same IP address subnet range. This enables you to separate client traffic for privacy and security.

#### About this task

All IPspace names must be unique within a cluster and must not consist of names reserved by the system, such as local or localhost.

#### Steps

1. Click the **Network** tab.
2. In the **IPspaces** tab, click **Create**.
3. In the **Create IPspaces** dialog box, specify a name for the IPspace that you want to create.
4. Click **Create**.

### Creating broadcast domains

You can create a broadcast domain by using System Manager to provide a logical division of a computer network. In a broadcast domain, all associated nodes can be reached through broadcast at the datalink layer.

#### Steps

1. Click the **Network** tab.
2. In the **Broadcast Domains** tab, click **Create**.
3. In the **Create Broadcast Domain** dialog box, specify the name, MTU size, IPspace, and ports for the broadcast domain that you want to create.
4. Click **Create**.

#### Related references

[Network window](#) on page 104

## Creating subnets

You can create a subnet by using System Manager to provide a logical subdivision of an IP network to pre-allocate the IP addresses. A subnet enables you to create interfaces more easily by specifying a subnet instead of an IP address and network mask values for each new interface.

### Before you begin

You must have created the broadcast domain on which the subnet is used.

### About this task

If you specify a gateway when creating a subnet, a default route to the gateway is added automatically to the SVM when a LIF is created using that subnet.

### Steps

1. Click the **Network** tab.
2. In the **Subnets** tab, click **Create**.
3. In the **Create Subnet** dialog box, specify subnet details, such as the name, subnet IP address or subnet mask, range of IP addresses, gateway address, and broadcast domain.  
  
You can specify the IP addresses as a range, as comma-separated multiple addresses, or as a mix of both.
4. Click **Create**.

### Related references

[Network window](#) on page 104

## Setting up physical storage

Setting up the physical storage consists of assigning disks to nodes, zeroing the spare disks, and creating aggregates.

### Assigning disks to nodes

You can use System Manager to assign ownership of an unassigned disk to a specific node to increase the capacity of an aggregate or storage pool.

### About this task

- You can assign disks if the following conditions are true:
  - The container type of the selected disks must be “unassigned”.
  - The disks must be connected to nodes in an HA pair.
  - The disks must be visible to the node.
- For MetroCluster configurations, you cannot use System Manager to assign disks. You must use the command-line interface instead.

### Steps

1. Click **Hardware and Diagnostics > Disks**.
2. In the **Disks** window, select the **Inventory** tab.

3. Select the disks that you want to assign, and then click **Assign**.
4. In the **Assign Disks** dialog box, select the node to which you want to assign the disks.
5. Click **Assign**.

### Zeroing spare disks

You can use System Manager to erase all the data and to format the spare disks by writing zeros to the disk. These disks can then be used in new aggregates.

#### About this task

When you zero the spare disks, all the spares in the cluster, including array LUNs, are zeroed. You can zero the spare disks for a specific node or for the entire cluster.

#### Steps

1. Click **Hardware and Diagnostics > Disks**.
2. In the **Disks** window, select the **Inventory** tab.
3. Click **Zero Spares**.
4. In the **Zero Spares** dialog box, select a node or “All nodes” from which you want to zero the disks.
5. Select the **Zero all non-zeroed spares** check box to confirm the zeroing operation.
6. Click **Zero Spares**.

### Provisioning storage through aggregates

You can create an aggregate or a Flash Pool aggregate to provide storage for one or more volumes by using System Manager.

#### Before you begin

You must have enough spare disks to create an aggregate.

#### About this task

You cannot perform the following actions by using System Manager:

- Combine disks of different sizes even if there are enough spare disks of different sizes.  
You can initially create an aggregate with disks of the same size and add disks of a different size later.
- Combine disks with different checksum types.  
You can initially create an aggregate with a single checksum type and add storage of a different checksum type later.

#### Related references

[Aggregates window](#) on page 124

### Provisioning storage by creating an aggregate

You can create an aggregate that consists of only HDDs or only SSDs by using System Manager.

#### Before you begin

All disks must be of the same size.

### About this task

- If you are creating an aggregate on a four-node cluster in ONTAP Select, the mirrored aggregate option is selected by default.
- Starting with ONTAP 9.0, you can create aggregates with disk size equal to or larger than 10 TB.
- If the disk type of the aggregate disks is FSAS or MSATA, and the disk size is equal to or larger than 10 TB, then RAID-TEC is the only option available for RAID type.

### Steps

1. Click **Hardware and Diagnostics > Aggregates**.
2. Click **Create**.
3. In the **Create Aggregate** dialog box, perform the following steps:
  - a. Specify the name of the aggregate, the disk type, and the number of disks or partitions to include in the aggregate.  
The minimum hot spare rule is applied to the disk group that has the largest disk size.
  - b. Optional: Modify the RAID configuration of the aggregate:
    - i. Click **Change**.
    - ii. In the Change RAID Configuration dialog box, specify the RAID type and the RAID group size.  
RAID-DP is the only supported RAID type for shared disks.
    - iii. Click **Save**.
  - c. If you want to mirror the aggregate, select the **Mirror this aggregate** check box.  
For MetroCluster configurations, creating unmirrored aggregates is restricted; therefore, the mirroring option is enabled by default.
4. Click **Create**.

### Result

The aggregate is created with the specified configuration, and is added to the list of aggregates in the Aggregates window.

## Provisioning storage by creating a Flash Pool aggregate

You can use System Manager to create a Flash Pool aggregate, or to convert an existing HDD aggregate to a Flash Pool aggregate by adding SSDs. When you create a new HDD aggregate, you can provision an SSD cache to it and create a Flash Pool aggregate.

### Before you begin

- You must be aware of platform-specific and workload-specific best practices for the Flash Pool aggregate SSD tier size and configuration.
- All HDDs must be in zeroed state.
- If you want to add SSDs to the aggregate, you must ensure that all the existing and dedicated SSDs are of the same size.

**About this task**

- You cannot use partitioned SSDs while creating the Flash Pool aggregate.
- You cannot mirror the aggregates if the cache source is storage pools.
- If you are creating an aggregate on a four-node cluster in ONTAP Select, the mirrored aggregate option is selected by default.
- Starting with ONTAP 9.0, you can create aggregates with disk size equal to or larger than 10 TB.
- If the disk type of the aggregate disks is FSAS or MSATA, and the disk size is equal to or larger than 10 TB, then RAID-TEC is the only option available for RAID type.

**Steps**

1. Click **Hardware and Diagnostics > Aggregates**.
2. Click **Create**.
3. In the **Create Aggregate** dialog box, specify the name of the aggregate, the disk type, and the number of HDD disks or partitions to include in the aggregate.
4. If you want to mirror the aggregate, select the **Mirror this aggregate** check box.  
For MetroCluster configurations, creating unmirrored aggregates is restricted; therefore, the mirroring option is enabled by default.
5. Click **Use Flash Pool Cache with this aggregate**.
6. Specify the cache source by choosing one of the following actions:

If you want to select the cache source as...	Then...
Storage pools	<ol style="list-style-type: none"> <li>a. Select <b>Storage pools</b> as the Cache Source.</li> <li>b. Select the storage pool from which the cache can be obtained, and then specify the cache size.</li> <li>c. Modify the RAID type, if required.</li> </ol>
Dedicated SSDs	<ol style="list-style-type: none"> <li>a. Select <b>Dedicated SSDs</b> as the Cache Source.</li> <li>b. Select the SSD size and the number of SSDs to include in the aggregate.</li> <li>c. Modify the RAID configuration, if required: <ol style="list-style-type: none"> <li>i. Click <b>Change</b>.</li> <li>ii. In the Change RAID Configuration dialog box, specify the RAID type and the RAID group size.</li> <li>iii. Click <b>Save</b>.</li> </ol> </li> </ol>

7. Click **Create**.

**Result**

The Flash Pool aggregate is created with the specified configuration, and is added to the list of aggregates in the Aggregates window.



**Related concepts**

[How storage pool works](#) on page 132

**Related information**

[NetApp Technical Report 4070: Flash Pool Design and Implementation Guide](#)

**Provisioning storage by creating a SnapLock aggregate**

You can use System Manager to create a SnapLock Compliance aggregate or a SnapLock Enterprise aggregate. You can create SnapLock volumes on these aggregates, which provide “write once, read many” (WORM) capabilities.

**Before you begin**

The SnapLock license must have been added.

**About this task**

- In MetroCluster configurations, you can create only SnapLock Enterprise aggregates.
- For array LUNs, only SnapLock Enterprise is supported.
- If you are creating a Snaplock Enterprise aggregate on a four-node cluster in ONTAP Select, the mirrored aggregate option is selected by default.
- Starting with ONTAP 9.0, you can create aggregates with disk size equal to or larger than 10 TB.
- If the disk type of the aggregate disks is FSAS or MSATA, and the disk size is equal to or larger than 10 TB, then RAID-TEC is the only option available for RAID type.
- Starting with ONTAP 9.1, you can create a SnapLock aggregate on an All Flash FAS platform.

**Steps**

1. Click **Hardware and Diagnostics > Aggregates**.
2. Click **Create**.
3. In the **Create Aggregate** dialog box, perform the following steps:
  - a. Specify the name of the aggregate, the disk type, and the number of disks or partitions to include in the aggregate.  
 You cannot change the name of a SnapLock Compliance aggregate after you create it.  
 The minimum hot spare rule is applied to the disk group that has the largest disk size.
  - b. Optional: Modify the RAID configuration of the aggregate:
    - i. Click **Change**.
    - ii. In the Change RAID Configuration dialog box, specify the RAID type and the RAID group size.  
 Shared disks support two RAID types: RAID-DP and RAID-TEC.
    - iii. Click **Save**.
  - c. Specify the SnapLock type.
  - d. If you have not initialized the system ComplianceClock, select the **Initialize ComplianceClock** check box.  
 This option is not displayed if the ComplianceClock is already initialized on the node.

**Note:** Ensure that the current system time is correct. The ComplianceClock is set based on the system clock, and once it is set, you cannot modify or stop the ComplianceClock.

- e. Optional: If you want to mirror the aggregate, select the **Mirror this aggregate** check box.

For MetroCluster configurations, creating unmirrored aggregates is restricted; therefore, the mirroring option is enabled by default.

The mirroring option is disabled for SnapLock Compliance aggregates.

4. Click **Create**.

## Setting up logical storage

Setting up the logical storage consists of creating Storage Virtual Machines (SVMs) and volumes.

### Creating SVMs

You can use System Manager to create fully configured Storage Virtual Machines (SVMs) that can serve data immediately. A cluster can have one or more SVMs with FlexVol volumes and SVMs with Infinite Volume.

#### Before you begin

- The cluster must have at least one non-root aggregate in the online state.
- The aggregate must have sufficient space for the SVM root volume.
- You must have synchronized the time across the cluster by configuring and enabling NTP to prevent CIFS creation and authentication failures.
- Protocols that you want to configure on the SVM must be licensed.
- You must have configured the CIFS protocol for secure DDNS to work.

#### About this task

- While creating SVMs, you can perform the following tasks:
  - Create and fully configure SVMs.
  - Configure the volume type allowed on SVMs.
  - Create and configure SVMs with minimal network configuration.
  - Delegate the administration to SVM administrators.
- To name the SVM, you can use alphanumeric characters and the following special characters: “.” (period), “-” (hyphen), and “\_” (underscore).  
The SVM name should start with an alphabet or “\_” (underscore) and must not contain more than 47 characters.

**Note:** You should use unique fully qualified domain names (FQDNs) for the SVM name such as vs0.example.com.

- You can establish SnapMirror relationships only between volumes that have the same language settings.  
The language of the SVM determines the character set that is used to display file names and data for all NAS volumes in the SVM.
- You cannot use a SnapLock aggregate as the root aggregate of SVMs.

## Steps

1. Click the **SVMs** tab.
2. Click **Create**.
3. In the **Storage Virtual Machine (SVM) Setup** window, specify details such as the following:
  - SVM name
  - IPspace allocated to the SVM
  - Volume type allowed
  - Protocols allowed
  - SVM language
  - Security style of the root volume
  - Root aggregate

The default language setting for any SVM is C.UTF-8.

By default, the aggregate with the maximum free space is selected as the container for root volume of the SVM. Based on the protocols selected, the default security style and the root aggregate are selected.

The security style is set to NTFS if you select CIFS protocol or a combination of CIFS protocol with the other protocols. The security style is set to UNIX if you select NFS, iSCSI, or FC/FCoE or a combination of these protocols.

In a MetroCluster configuration, only the aggregates that are contained in the cluster are displayed.

4. Specify the DNS domain names and the name server IP addresses to configure the DNS services. The default values are selected from the existing SVM configurations.
5. Optional: When configuring a data LIF to access data using a protocol, specify the target alias, subnets, and the number of LIFs per node details.

You can select the **Review or Modify LIFs configuration (Advanced Settings)** check box to modify the number of portsets in the LIF.

You can edit the details of the portset in a particular node by selecting the node from the nodes list in the details area.

6. Optional: Enable host-side applications such as SnapDrive and SnapManager for the SVM administrator by providing the SVM credentials.
7. Optional: Create a new LIF for SVM management by clicking **Create a new LIF for SVM management**, and then specify the portsets and the IP address with or without a subnet for the new management LIF.
 

For CIFS and NFS protocols, data LIFs have management access by default. You must create a new management LIF only if required. For iSCSI and FC protocols, a dedicated SVM management LIF is required because data and management protocols cannot share the same LIF.
8. Click **Submit & Continue**.

The SVM is created with the specified configuration.

## Result

The SVM that you created is started automatically. The root volume name is automatically generated as *SVM\_name\_root*. By default, the *vsadmin* user account is created and is in the locked state.

**After you finish**

- You must configure at least one protocol on the SVM to allow data access.
- After you create an SVM with Infinite Volume, you must create an Infinite Volume for the SVM.

**Configuring CIFS and NFS protocols on an SVM**

You can use System Manager to configure CIFS and NFS protocols on the Storage Virtual Machine (SVM) to provide file-level data access for NAS clients. To enable CIFS protocol, you must create the data LIFs and the CIFS server. To enable NFS protocol, you can specify the NIS details and the data LIFs.

**Before you begin**

- Protocols that you want to configure or allow on the SVM must be licensed.  
If the protocol is not allowed on the SVM, you can use the Edit Storage Virtual Machine window to enable the protocol for the SVM.
- You must have the Active Directory, organizational unit, and administrative account credentials for configuring the CIFS protocol.

**About this task**

SnapLock aggregates are not considered for automatically creating volumes.

**Steps**

1. If you have not configured the protocols while creating the SVM, click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click the protocol that you want to configure.
5. In the Data LIF Configuration section, if you want to retain the same data LIF configuration for both CIFS and NFS, select the **Retain the CIFS data LIF's configuration for NFS client** check box.  
  
If you do not retain the same data LIF configuration for both CIFS and NFS, you must specify the IP address and ports separately for both CIFS and NFS.
6. Specify the IP address by choosing one of the following options:

If you want to...	Then...
Specify the IP address using a subnet	<ol style="list-style-type: none"> <li>a. Select <b>Using a subnet</b>.</li> <li>b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIF, only the subnets that are associated with the selected IPspace are displayed.</li> <li>c. If you want to assign a specific IP address to the interface, select <b>Use a specific IP address</b>, and then type the IP address. The IP address you specify is added to the subnet if it is not already present in the subnet range.</li> <li>d. Click <b>OK</b>.</li> </ol>

If you want to...	Then...
Specify the IP address manually without using a subnet	<p><b>a.</b> Select <b>Without a subnet</b>.</p> <p><b>b.</b> In the Add Details dialog box, perform the following steps:</p> <ul style="list-style-type: none"> <li><b>i.</b> Specify the IP address and network mask or prefix.</li> <li><b>ii.</b> Optional: Specify the gateway. The destination field is populated with the default value based on the family of the IP address.</li> <li><b>iii.</b> If you do not want the default value, specify the new destination value.  If a route does not exist, a new route is automatically created based on the gateway and destination.</li> </ul> <p><b>c.</b> Click <b>OK</b>.</p>

7. Specify a port to create a data LIF:
  - a. Click **Browse**.
  - b. In the **Select Network Port or Adapter** dialog box, select a port.
  - c. Click **OK**.
8. Configure the CIFS server by performing the following steps:
  - a. Specify the following information to create a CIFS server:
    - CIFS server name
    - Active Directory to associate with the CIFS server
    - Organizational unit (OU) within the Active Directory domain to associate with the CIFS server  
By default, this parameter is set to CN=Computers.
    - Credentials of an administrative account that has sufficient privileges to add the CIFS server to the OU
  - b. Optional: Select **Encrypt Data while accessing all shares of this SVM** to enable SMB 3.0 encryption for all the shares of the SVM.
  - c. Provision a volume for CIFS storage when configuring the protocol by providing the share name, size of the share, and access permissions.
  - d. Optional: Select **Encrypt Data while accessing this share** to enable SMB 3.0 encryption for a particular share.
9. Optional: Configure the NIS services:
  - a. Specify the IP addresses of the NIS servers and NIS domain name to configure NIS services on the SVM.
  - b. Select the appropriate database type for which you want to add the “nis” name service source.
  - c. Provision a volume for NFS storage by specifying export name, size, and permission.
10. Click **Submit & Continue**.

## Result

The CIFS server and NIS domain are configured with the specified configuration, and data LIFs are created. By default, the data LIFs have management access. You can view the configuration details on the Summary page.

## Configuring iSCSI protocol on SVMs

You can configure the iSCSI protocol on the Storage Virtual Machine (SVM) to provide block-level data access by using System Manager. You can create iSCSI LIFs and portsets and add the LIFs to the portsets. LIFs are created on the most suitable adapters and assigned to portsets to ensure data path redundancy.

### Before you begin

- The iSCSI license must be enabled on the cluster.  
If the protocol is not allowed on the SVM, you can use the Edit Storage Virtual Machine window to enable the protocol for the SVM.
- All the nodes in the cluster must be healthy.
- Each node must have at least two data ports and the port state must be **up**.

### About this task

- You can configure the iSCSI protocol while creating the SVM or you can do so at a later time.
- SnapLock aggregates are not considered for automatically creating volumes.

### Steps

1. If you have not configured the protocols while creating the SVM, click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. Optional: In the Network Access section, specify an alias for the iSCSI target.  
The maximum number of characters for an alias name is 128. If you do not specify a target alias, the SVM name is used as an alias.
6. Specify the number of iSCSI LIFs that can be assigned to a single node.  
The minimum number of LIFs per node is one. The maximum number is the minimum of all the ports in the **up** state across the nodes. If the maximum value is an odd number, the previous even number is considered as the maximum value. You can choose any even number in the minimum and maximum value range.

### Example

A 4-node cluster has node1, node2, and node3 with 6 ports each in the **up** state, and node4 with 7 ports in the **up** state. The effective maximum value for the cluster is 6.

If the number of LIFs that you want to assign to the node is more than 2, you must assign at least one portset to each LIF.

7. Specify the network details, including the subnet details, to create iSCSI LIFs:

If you want to...	Then...
Specify the IP address using a subnet	<ol style="list-style-type: none"> <li>a. Select <b>Using a subnet</b>.</li> <li>b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIF, only the subnets that are associated with the selected IPspace are displayed.</li> <li>c. If you want to assign a specific IP address to the interface, select <b>Use a specific IP address</b>, and then type the IP address. The IP address you specify is added to the subnet if it is not already present in the subnet range.</li> <li>d. Click <b>OK</b>.</li> </ol>
Specify the IP address manually without using a subnet	<ol style="list-style-type: none"> <li>a. Select <b>Without a subnet</b>.</li> <li>b. In the Add Details dialog box, perform the following steps: <ol style="list-style-type: none"> <li>i. Specify the IP address and network mask or prefix.</li> <li>ii. Optional: Specify the gateway. The destination field is populated with the default value based on the family of the IP address.</li> <li>iii. If you do not want the default value, specify the new destination value.  If a route does not exist, a new route is automatically created based on the gateway and destination.</li> </ol> </li> <li>c. Click <b>OK</b>.</li> </ol>

8. Select the broadcast domain.
9. Optional: Provision a LUN for iSCSI storage when configuring the iSCSI protocol by providing the LUN size, OS type for the LUN, and host initiator details.
10. If you want to verify or modify the automatically generated iSCSI LIFs configuration, select **Review or Modify LIFs configuration (Advanced Settings)**.  
  
You can modify only the LIF name and the home port. By default, the portsets are set to the minimum value. You must ensure that you specify unique entries. If you specify duplicate LIF names, System Manager appends numeric values to the duplicate LIF name.  
  
Based on the selected portset, the LIFs are distributed across the portsets using a round-robin method to ensure redundancy in case of node or port failure.
11. Click **Submit & Continue**.

### Result

The iSCSI LIFs and portsets are created with the specified configuration. The LIFs are distributed accordingly among the portsets. The iSCSI service is started if all the LIFs are successfully created.

If the LIF creation fails, you can use the Network Interfaces window to create the LIFs, attach the LIFs to the portsets by using the LUNs window, and start the iSCSI service by using the iSCSI window.

## Configuring FC and FCoE protocols on SVMs

You can configure the FC and the FCoE protocols on the SVM for SAN hosts. LIFs are created on the most suitable adapters and assigned to port sets to ensure data path redundancy. Based on your requirements, you can configure either FC, FCoE, or both the protocols by using System Manager.

### Before you begin

- The FCP license must be enabled on the cluster.
- All the nodes in the cluster must be healthy.
- Each node must have at least two correctly configured ports for each protocol (FC and FCoE).

### About this task

- You can configure the FC and FCoE protocols while creating the SVM or you can do so at a later time. If the protocols are not allowed on the SVM, you can use the Edit Storage Virtual Machine window to enable the protocols for the SVM.
- SnapLock aggregates are not considered for automatically creating volumes.

### Steps

1. If you have not configured the protocols while creating the SVM, click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **FC/FCoE**.
5. In the Data Interface Configuration section, select the corresponding option to configure data LIFs for FC and FCoE protocols.
6. Specify the number of data LIFs per node for each protocol.

The minimum number of LIFs per node is one. The maximum number is the minimum of all the ports in the **up** state across the nodes. If the maximum value is an odd number, the previous even number is considered as the maximum value. You can choose any even number in the minimum and maximum value range.

### Example

A 4-node cluster has node1, node2, and node3 with 6 ports each in the **up** state, and node4 with 7 ports in the **up** state. The effective maximum value for the cluster is 6.

If the number of LIFs that you want to assign to the node is more than 2, you must assign at least one portset to each LIF.

7. If you want to verify or modify the automatically generated LIFs configuration, select **Review or Edit the Interface Association**.

You can modify only the LIF name and home port. You must ensure that you do not specify duplicate entries.

8. Optional: Provision a LUN for the FC or FCoE storage when configuring the protocol by providing the LUN size, OS type for the LUN, and host initiator details.
9. Click **Submit & Continue**.



## Result

The data LIFs and port sets are created with the specified configuration. The LIFs are distributed accordingly among the port sets. FCP service is started if all the LIFs are successfully created for at least one protocol.

If the LIF creation fails, you can create the LIFs and start the FCP service from the FC/FCoE window.

## Related information

*[NetApp Documentation: ONTAP 9](#)*

## Delegating administration to SVM administrators

After setting up a functional Storage Virtual Machine (SVM) or SVMs with basic network configuration, you can optionally delegate the administration of the SVM to SVM administrators.

### About this task

SVM administrators cannot use System Manager to manage delegated SVMs. You can only manage them by using the command-line interface (CLI).

### Steps

1. In the Administrator Details section, set up a password for the `vsadmin` user account.
2. If you want a dedicated LIF for SVM management, select **Create a LIF for SVM management**, and then specify the network details.  
  
A dedicated SVM management LIF is required for SAN protocols, where data and management protocols cannot share the same LIF. SVM management LIFs can be created only on data ports.
3. Specify the network details, including subnet details, to create iSCSI LIFs:

If you want to...	Then...
Specify the IP address using a subnet	<ol style="list-style-type: none"> <li>a. Select <b>Using a subnet</b>.</li> <li>b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIF, only the subnets that are associated with the selected IPspace are displayed.</li> <li>c. If you want to assign a specific IP address to the interface, select <b>Use a specific IP address</b>, and then type the IP address. The IP address you specify is added to the subnet if it is not already present in the subnet range.</li> <li>d. Click <b>OK</b>.</li> </ol>

If you want to...	Then...
Specify the IP address manually without using a subnet	<ol style="list-style-type: none"> <li>a. Select <b>Without a subnet</b>.</li> <li>b. In the Add Details dialog box, perform the following steps: <ol style="list-style-type: none"> <li>i. Specify the IP address and network mask or prefix.</li> <li>ii. Optional: Specify the gateway. The destination field is populated with the default value based on the family of the IP address.</li> <li>iii. If you do not want the default value, specify the new destination value.  If a route does not exist, a new route is automatically created based on the gateway and destination.</li> </ol> </li> <li>c. Click <b>OK</b>.</li> </ol>

4. Specify a port to create a data LIF:
  - a. Click **Browse**.
  - b. Select a port from the Select Network Port or Adapter dialog box.
  - c. Click **OK**.

### Result

The `vsadmin` account is unlocked and configured with the password.

The default access methods for the `vsadmin` account are Data ONTAP API (`ontapi`) and SSH (`ssh`). The SVM administrator can log in to the storage system using the management IP address.

### After you finish

You must assign aggregates to the SVM by using the Edit Storage Virtual Machine dialog box.

**Note:** If the SVM does not have any assigned aggregates, the SVM administrator cannot create volumes.

## Assigning aggregates to SVMs

After creating an SVM for an Infinite Volume, you should assign specific aggregates to it so that the Infinite Volume that you create will use those specific aggregates and not use all the aggregates in the cluster.

### Before you begin

You should have reviewed the available aggregates and decided which aggregates the SVM will use.

### About this task

You identify which aggregates the Infinite Volume will use by assigning aggregates to its containing SVM with Infinite Volume. If you do not specify the aggregate list for the SVM with Infinite Volume, the Infinite Volume can potentially use all the aggregates in the cluster.

### Steps

1. In the **Select aggregates** section, select the aggregates to assign to the SVM.

By default, the node root aggregates are not selected. You should not provision volumes on root aggregates because it might cause performance or stability issues.

2. Click **Submit & Continue**.

## Creating FlexVol volumes

You can create a FlexVol volume for your data by using the Create Volume dialog box in System Manager. You should always create a separate volume for your data rather than storing data in the root volume.

### Before you begin

- The cluster must contain a non-root aggregate and a Storage Virtual Machine (SVM).
- If you want to create read/write (rw) volumes, you must have configured the protocols for the SVM, and you must have installed either the SnapMirror or the SnapVault license.  
If you have not configured the protocols but have installed any one of these licenses, you can create only data protection (DP) volumes.

### About this task

- You can enable storage Quality of Service (QoS) only for a read/write (rw) volume.
- When you create a DP volume on the sync-source SVM in a MetroCluster configuration, the volume is not replicated on the sync-destination SVM.
- When you create a DP volume in a MetroCluster configuration, the source volume is not replicated (mirrored or vaulted) in the destination SVM.
- In a MetroCluster configuration, System Manager displays only the following aggregates for creating volumes:
  - In normal mode, when you create volumes on sync-source SVMs or data-serving SVMs in the primary site, only those aggregates that belong to the cluster in the primary site are displayed.
  - In switched-over mode, when you create volumes on sync-destination SVMs or data-serving SVMs in the surviving site, only switched-over aggregates are displayed.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM and click **Manage**.
3. Click the **Volumes** tab.
4. Click **Create**.
5. In the **Create Volume** dialog box, specify a new name if you want to change the default name.
6. Select the containing aggregate for the volume.
7. Select the type of storage for which you are creating this volume.

You have to select **Data Protection** if you are creating a SnapMirror destination volume. You are provided read-only access to this volume.

8. Specify the size of the volume and the percentage of the total volume size that you want to reserve for Snapshot copies.

The default space reserved for Snapshot copies is zero percent for SAN and VMware volumes. For NAS volumes, the default is five percent.

9. Select **Default**, **Thin provisioned** or **Thick provisioned** for the volume.

When thin provisioning is enabled, space is allocated to the volume from the aggregate only when data is written to it.

**Note:** For All Flash FAS(AFF) storage systems, the value of thin provisioning is “Default ” and for other storage systems, the value of thick provisioning is “Default”.

10. If you want to enable deduplication on this volume, make the necessary changes in the **Storage Efficiency** tab.

System Manager uses the default deduplication schedule. If the specified volume size exceeds the limit required for running deduplication, the volume is created and deduplication is not enabled.

For All Flash Optimized personality systems, inline compression is enabled by default.

11. If you want to enable storage QoS for the FlexVol volume to manage workload performance, select the **Manage Storage Quality of Service** check box in the **Quality of Service** tab.
12. Create a new storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the FlexVol volume:

If you want to...	Do this...
Create a new policy group	<p>a. Specify the policy group name.</p> <p>b. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group do not exceed the specified throughput limit.</p> <p>If you do not specify the maximum throughput limit, the value is set to Unlimited and the unit that you specify does not affect the maximum throughput.</p>
Select an existing policy group	<p>Select <b>Existing Policy Group</b>, and then click <b>Choose</b> to select an existing policy group from the Select Policy Group dialog box.</p> <p>You can also choose to modify the maximum throughput for the selected policy group.</p> <p>If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.</p>

13. Click **Create**.
14. Verify that the volume you created is included in the list of volumes in the **Volume** window.
- The volume is created with UNIX style security and UNIX 700 “read write execute” permissions for the owner.

#### Related references

[Volumes window](#) on page 206

### Creating an Infinite Volume

You can create Infinite Volumes to provide a large, scalable data container with a single namespace and a single mount point by using System Manager. You can use Infinite Volumes to store large unstructured repositories of primary data that is written once and seldom used.

#### Before you begin

- You must have created aggregates according to the aggregate requirements for Infinite Volumes.
- You must have created the SVM that can contain the Infinite Volume.

- If you want to create read/write (rw) volumes, you must have configured the protocols for the SVM and must have installed either the SnapMirror or the SnapVault license.  
If you have not configured the protocols but have installed any one of these licenses, you can create only data protection (DP) volumes.

### About this task

You can create only Infinite Volumes without storage classes by using System Manager. If you want to create Infinite Volumes with storage classes, you cannot use System Manager; you must use OnCommand Workflow Automation instead.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Click **Create**.
5. If you want to change the default name, specify a new name.
6. Specify a junction path to mount the volume.
7. Select **Data Protection** if you are creating a SnapMirror destination volume.  
You are provided read-only access to this volume.  
The number of aggregates that the volume spans is displayed.
8. Click **Edit** to modify the list of aggregates that are available to the Infinite Volume.
9. Specify the size of the volume and the percentage of the total volume size that you want to reserve for Snapshot copies.  
The minimum size of the volume is 1.33 TB for each node used. The default space reserved for Snapshot copies is five percent.
10. Optional: Select **Enable SnapDiff** to enable incremental tape backup of the volume.  
You can enable SnapDiff only on read/write volumes.
11. If you want to enable deduplication on the volume, make the necessary changes in the **Storage Efficiency** tab.  
You can enable storage efficiency settings only on read/write volumes.  
System Manager uses the default deduplication schedule. If the specified volume size exceeds the limit required for running deduplication, the volume is created and deduplication is not enabled.
12. Click **Create**.
13. Verify that the volume you created is displayed in the **Infinite Volume** window.  
The volume is created with unified style security and UNIX 700 “read write execute” permissions for the Owner.

### Related concepts

[Aggregate requirements for Infinite Volumes](#) on page 122

## Creating SnapLock volumes

You can use System Manager to create a SnapLock Compliance volume or a SnapLock Enterprise volume. When you create a volume, you can also set retention times, and choose whether to automate setting the WORM state on data in the volume.

### Before you begin

- The SnapLock license must have been installed.
- The SnapLock aggregate must be online.

### About this task

- You can delete a complete SnapLock Enterprise volume or a file in a SnapLock Enterprise volume; however, you cannot delete only the data within a file in a SnapLock Enterprise volume.
- You cannot delete a SnapLock Compliance volume if data is committed to the volume.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Click **Create**.
5. In the **Create Volume** dialog box, specify a new name if you want to change the default name of the volume.

You cannot change the name of a SnapLock Compliance volume after you create it.

6. Select the containing aggregate for the volume.  
You must select a SnapLock Compliance aggregate or SnapLock Enterprise aggregate to create a SnapLock volume. The volume inherits the SnapLock type from the aggregate, and the SnapLock type cannot be changed after the volume is created; therefore, you must select the correct aggregate.

7. Select the type of storage for which you are creating this volume.

If you are creating a SnapMirror destination volume, you must select **Data Protection**. You are provided read-only access to this volume.

8. Specify the size of the volume and the percentage of the total volume size that you want to reserve for Snapshot copies.

The default space that is reserved for Snapshot copies is zero percent for SAN and VMware volumes. For NAS volumes, the default is 5 percent.

9. Optional: Select **Thin Provisioned** to enable thin provisioning for the volume.

When thin provisioning is enabled, space is allocated to the volume from the aggregate only when data is written to the volume.

10. Optional: Make the necessary changes in the **Storage Efficiency** tab to enable deduplication on the volume.

System Manager uses the default deduplication schedule. If the specified volume size exceeds the limit required for running deduplication, the volume is created, and deduplication is not enabled.

11. Select the **SnapLock** tab, and then perform the following steps:
  - a. Optional: Specify the autocommit period.  
The file in the volume must remain unchanged for the period that you specify before it is committed to the WORM state. To set files to the WORM state manually, you must choose **Not specified** as the autocommit setting.
  - b. Specify the minimum retention period and maximum retention period.  
The values must be in the range of 1 day through 70 years or Infinite.
  - c. Select the default retention period.  
The default retention period must be within the specified minimum retention period and maximum retention period.
12. Optional: Select the **Manage Storage Quality of Service** check box in the **Quality of Service** tab to enable storage QoS for the FlexVol volume in order to manage workload performance.
13. Create a new storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the FlexVol volume:

If you want to...	Do this...
Create a new policy group	<ol style="list-style-type: none"> <li>a. Specify the policy group name.</li> <li>b. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. If you do not specify the maximum throughput limit, the value is set to Unlimited, and the unit that you specify does not affect the maximum throughput.</li> </ol>
Select an existing policy group	<p>Select <b>Existing Policy Group</b>, and then click <b>Choose</b> to select an existing policy group from the Select Policy Group dialog box.</p> <p>You can also choose to modify the maximum throughput for the selected policy group.</p> <p>If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.</p>

14. Click **Create**.
15. Verify that the volume that you created is included in the list of volumes in the **Volume** window.

### Result

The volume is created with UNIX-style security and UNIX 700 “read write execute” permissions for the owner.

## Managing clusters

---

You can use System Manager to manage clusters.

### What a cluster is

A cluster consists of one or more nodes grouped together as (HA pairs) to form a scalable cluster. Creating a cluster enables the nodes to pool their resources and distribute work across the cluster, while presenting administrators with a single entity to manage. Clustering also enables continuous service to end users if individual nodes go offline.

- The maximum number of nodes within a cluster depends on the platform model and licensed protocols.
- Each node in the cluster can view and manage the same volumes as any other node in the cluster. The total file-system namespace, which comprises all of the volumes and their resultant paths, spans the cluster.
- The nodes in a cluster communicate over a dedicated, physically isolated and secure Ethernet network. The cluster logical interfaces (LIFs) on each node in the cluster must be on the same subnet.
- When new nodes are added to a cluster, there is no need to update clients to point to the new nodes. The existence of the new nodes is transparent to the clients.
- If you have a two-node cluster (a single HA pair), you must configure cluster high availability (HA).
- You can create a cluster on a stand-alone node, called a single-node cluster. This configuration does not require a cluster network, and enables you to use the cluster ports to serve data traffic. However, nondisruptive operations are not supported on single-node clusters.

### Understanding quorum and epsilon

Quorum and epsilon are important measures of cluster health and function that together indicate how clusters address potential communications and connectivity challenges.

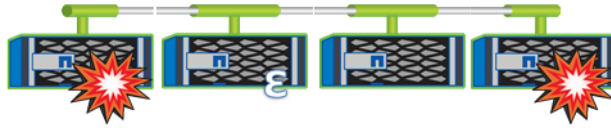
*Quorum* is a precondition for a fully functioning cluster. When a cluster is in quorum, a simple majority of nodes are healthy and can communicate with each other. When quorum is lost, the cluster loses the ability to accomplish normal cluster operations. Only one collection of nodes can have quorum at any one time because all of the nodes collectively share a single view of the data. Therefore, if two non-communicating nodes are permitted to modify the data in divergent ways, it is no longer possible to reconcile the data into a single data view.

Each node in the cluster participates in a voting protocol that elects one node *master*; each remaining node is a *secondary*. The master node is responsible for synchronizing information across the cluster. When quorum is formed, it is maintained by continual voting. If the master node goes offline and the cluster is still in quorum, a new master is elected by the nodes that remain online.

Because there is the possibility of a tie in a cluster that has an even number of nodes, one node has an extra fractional voting weight called *epsilon*. If the connectivity between two equal portions of a large cluster fails, the group of nodes containing epsilon maintains quorum, assuming that all of the nodes are healthy. For example, the following illustration shows a four-node cluster in which two of the



nodes have failed. However, because one of the surviving nodes holds epsilon, the cluster remains in quorum even though there is not a simple majority of healthy nodes.



Epsilon is automatically assigned to the first node when the cluster is created. If the node that holds epsilon becomes unhealthy, takes over its high-availability partner, or is taken over by its high-availability partner, then epsilon is automatically reassigned to a healthy node in a different HA pair.

Taking a node offline can affect the ability of the cluster to remain in quorum. Therefore, Data ONTAP issues a warning message if you attempt an operation that will either take the cluster out of quorum or else put it one outage away from a loss of quorum. You can disable the quorum warning messages by using the `cluster quorum-service options modify` command at the advanced privilege level.

In general, assuming reliable connectivity among the nodes of the cluster, a larger cluster is more stable than a smaller cluster. The quorum requirement of a simple majority of half the nodes plus epsilon is easier to maintain in a cluster of 24 nodes than in a cluster of two nodes.

A two-node cluster presents some unique challenges for maintaining quorum. Two-node clusters use *cluster HA*, in which neither node holds epsilon; instead, both nodes are continuously polled to ensure that if one node fails, the other has full read-write access to data, as well as access to logical interfaces and management functions.

## What a node in the cluster is

A *node* is a controller in a cluster. It is connected to other nodes in the cluster over a private management cluster network. It is also connected to the disk shelves that provide physical storage for the Data ONTAP system or to third-party storage arrays that provide array LUNs for Data ONTAP use.

A *node Storage Virtual Machine (SVM)* represents a node in the cluster. The cluster setup process automatically creates a node SVM for each node in the cluster.

## Dashboard window

The Dashboard window contains multiple panels that provide cumulative at-a-glance information about your system and its performance.

You can use the Dashboard window to view information about important alerts and notifications, efficiency and capacity of aggregates and volumes, the nodes that are available in a cluster, the status of the nodes in a high-availability (HA) pair, the most active objects, and the performance metrics of the cluster or a node.

### Alerts and Notifications

Displays all alerts in red, such as emergency EMS events, offline node details, broken disk details, license entitlements that are in high risk, and offline network port details. Displays all notifications in yellow, such as health monitor notifications that occurred in the past 24 hours at the cluster level, license entitlements that are in medium risk, unassigned disk details, the number of migrated LIFs, volume move operations that failed, and volume move operations that required administrative intervention in the past 24 hours.

The panel displays up to three alerts and notifications beyond which a View-All link is displayed. You can click the View-All link to view more information about the alerts and notifications.

The refresh interval for this panel is one minute.

### Efficiency and Capacity

Displays the aggregates and volumes that are nearing capacity, and the storage efficiency of the cluster or a node.

The Efficiency tab displays the storage efficiency savings for the cluster or a node. You can view the total logical space used, total physical space used, overall savings from storage efficiency, volume data reduction ratio, aggregate data reduction ratio, and ratio of FlexClone volumes and Snapshot copies. You can select the cluster or a specific node to view the storage efficiency savings.

**Note:** During a takeover operation or giveback operation, the storage efficiency data may not be fully reported. In such cases, the reported storage efficiency data of these operations is corrected after some time, depending on the number of Snapshot copies across all the volumes in the nodes.

In the Aggregates tab, the graph displays the top five online aggregates that are nearing capacity, in descending order of used space. You can click the View All link to navigate to the Aggregates inventory page.

The Volumes tab displays the top three SVMs—including destination SVMs for disaster recovery and SVMs in a locked state—that contain the volumes with the highest capacity utilized when you enter a valid value in the “Volumes exceeding used capacity of” field. You can click the View All link to view the Volumes dialog box, and then navigate to the Volumes page.

The refresh interval for this panel is 15 minutes.

### Nodes

Displays a pictorial representation of the number and names of the nodes that are available in the cluster, and the status of the nodes that are in an HA pair. You must position the cursor over the pictorial representation of the nodes to view the status of the nodes in an HA pair.

You can view more information about all the nodes by using the Nodes link. You can also click the pictorial representation to view the model of the nodes and the number of aggregates, storage pools, shelves, and disks that are available in the nodes. You can manage the nodes by using the Manage Nodes link. You can manage the nodes in an HA pair by using the Manage HA link.

The refresh interval for this panel is 15 minutes.

### Top Objects

Provides information about the top five active clients and files in the cluster. You can view the top five active clients and files based on IOPS or throughput.

The refresh interval for this panel is one minute.

### Performance

Displays the average performance metrics, read performance metrics, and write performance metrics of the cluster based on latency, IOPS, and throughput. The average performance metrics is displayed by default. You can click Read or Write to view the read or write performance metrics, respectively. You can view the performance metrics of the cluster or a node.

If the information about cluster performance cannot be retrieved from ONTAP, you cannot view the respective graph. In such cases, System Manager displays the specific error message.

The refresh interval for the charts in this tab is 15 seconds.

## Monitoring a cluster using the dashboard

The dashboard in System Manager enables you to monitor the health and performance of a cluster. You can also identify hardware problems and storage configuration issues by using the dashboard.

### Step

1. Click the **Dashboard** tab to view the health and performance dashboard panels.

## Configuration update

You can use System Manager to configure the administration details of Storage Virtual Machines (SVMs).

## Configuring the administration details of an SVM

You can use System Manager to quickly configure the administration details of an SVM. You can optionally delegate the administration of the SVM to SVM administrators.

### About this task

As an SVM administrator, you cannot use System Manager to manage delegated SVMs. You can manage them only by using the command-line interface (CLI).

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Configuration Updates**.
3. In the **SVMs** tab, select the node, and then click **Configure Administration Details**.
4. In the Administrator Details section, set up a password for the `vsadmin` user account.
5. If you want a dedicated LIF for SVM management, select **Create a LIF for SVM management**, and then specify the network details.

A dedicated SVM management LIF is required for SAN protocols, where data and management protocols cannot share the same LIF. SVM management LIFs can be created only on data ports.

6. Specify the network details:

If you want to...	Then...
Specify the IP address using a subnet	<ol style="list-style-type: none"> <li>Select <b>Using a subnet</b>.</li> <li>In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIF, only the subnets that are associated with the selected IPspace are displayed.</li> <li>If you want to assign a specific IP address to the interface, select <b>Use a specific IP address</b>, and then type the IP address. The IP address you specify is added to the subnet if it is not already present in the subnet range.</li> <li>Click <b>OK</b>.</li> </ol>
Specify the IP address manually without using a subnet	<ol style="list-style-type: none"> <li>Select <b>Without a subnet</b>.</li> <li>In the Add Details dialog box, perform the following steps: <ol style="list-style-type: none"> <li>Specify the IP address and network mask or prefix.</li> <li>Optional: Specify the gateway. The destination field is populated with the default value based on the family of the IP address.</li> <li>If you do not want the default value, specify the new destination value.  If a route does not exist, a new route is automatically created based on the gateway and destination.</li> </ol> </li> <li>Click <b>OK</b>.</li> </ol>

7. Specify a port to create a data LIF:

- Click **Browse**.
- In the **Select Network Port or Adapter** dialog box, select a port, and then click **OK**.

## Configuration Updates window

You can use the Configuration Updates window to update the configuration details of the cluster, Storage Virtual Machine (SVM), and nodes.

### Tabs

#### Nodes

Enables you to configure details of the node.

#### SVMs

Enables you to configure details of the SVM.

### Nodes tab

#### Command buttons

##### Edit Node Name

Opens the Edit Node Name dialog box, which enables you to modify the name of the node.

**Create Node-management LIF**

Opens the Create Node-management LIF dialog box, which enables you to create a node-management LIF for managing a specific node.

**Edit AutoSupport**

Opens the Edit AutoSupport Settings dialog box, which enables you to specify an email address from which email notifications are sent and to add multiple email addresses of the host names.

**SVMs tab****Command button****Configure Administration Details**

Opens the Configure Administration Details dialog box, which enables you configure the administration details of the SVM.

**Related tasks**

[Creating a cluster](#) on page 24

[Setting up a network when an IP address range is disabled](#) on page 26

## Service Processors

You can use a Services Processor to monitor and manage your storage system parameters such as temperature, voltage, current, and fan speeds through System Manager.

### Assigning IP addresses to Service Processors

You can use System Manager to assign IP addresses to all your Service Processors at the same time and use these Service Processors to monitor and manage various system parameters of your storage systems.

**Steps**

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Service Processor**.
3. In the **Service Processor** window, click **Global Settings**.
4. In the **Global Settings** dialog box, choose the source to assign the IP addresses:

If you want to...	Select the option...
Assign IP addresses automatically from a DHCP server	DHCP
Assign IP addresses from a subnet	Subnet
Manually provide IP addresses	Manual Assignment

5. Click **Save**.

## Editing Service Processor settings

You can modify Service Processor attributes, such as the IP address, the network mask or the prefix-length, and the gateway address by using System Manager. You can also allocate IP addresses to Service Processors that do not have any IP addresses assigned.

### About this task

- You can edit the settings of a Service Processor that was assigned IP addresses manually.
- You cannot edit the settings of a Service Processor that was assigned IP addresses through a DHCP server or through a subnet.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Service Processor**.
3. In the **Service Processor** window, select the Service Processor, and then click **Edit**.
4. In the **Edit Service Processor** dialog box, make the necessary changes, and then click **Save and Close**.

## Understanding the Service Processor

A Service Processor is a system-independent resource in the storage system that helps you to monitor and manage storage system parameters such as the temperature, voltage, current, and fan speeds.

When the service processor detects an abnormal condition in any of the storage system parameters, it logs an event, notifies Data ONTAP of the issue, and generates AutoSupport messages through email or through SNMP traps.

The Service Processor monitors Data ONTAP through a watchdog mechanism and can facilitate a quick failover to the partner node. The Service Processor also tracks numerous system events and saves them in a log file. The events include boot progress, field-replaceable unit (FRU) changes, Data ONTAP generated events, and a user transaction history.

The Service Processor can remotely log in and administer the storage system and can diagnose, shut down, power cycle, or reboot the system, regardless of the state of the storage system. In addition, the Service Processor provides remote diagnostic features.

The combined monitoring and managing capabilities of the Service Processor enables you to evaluate the storage system in the event of an issue, and you can immediately perform effective service actions.

## Service Processors window

You can use the Service Processors window to view and modify Service Processors attributes, such as the IP address, network mask (IPv4) or prefix-length (IPv6), and gateway, and to configure the IP source for a Service Processor.

- [Command buttons](#) on page 63
- [Service processors list](#) on page 63
- [Details area](#) on page 63

## Command buttons

### Edit

Opens the Edit Service Processor dialog box, which enables you to modify the IP address, network mask (IPv4) or prefix-length (IPv6), and gateway information of a Service Processor.

### Global Settings

Opens the Global Settings dialog box, which allows you to configure the source of IP address for all your Service Processors as one of the following: DHCP, subnet, or manual.

### Refresh

Updates the information in the window.

## Service processors list

### Node

Specifies the node on which the Service Processor is located.

### IP Address

Specifies the IP addresses of the Service Processor.

### Status

Specifies the status the Service Processor, which can be online, offline, daemon offline, node offline, degraded, rebooted, or unknown.

### MAC Address

Specifies the MAC address of the Service Processor.

## Details area

The area below the Service Processor list displays detailed information about the Service Processor, including network details, such as the IP address, network mask (IPv4) or prefix-length (IPv6), gateway, IP source, and MAC address, as well as general details, such as the firmware version and whether automatic update of the firmware is enabled.

## Related tasks

[Setting up a network when an IP address range is disabled](#) on page 26

# Cluster peers

You can use System Manager to peer two clusters so that the peered clusters can coordinate and share resources between them.

## Prerequisites for cluster peering

Before you set up cluster peering, you should confirm that the connectivity, port, IP address, subnet, firewall, and cluster-naming requirements are met.

### Connectivity requirements

The subnet used in each cluster for intercluster communication must meet the following requirements:

- The subnet must belong to the broadcast domain that contains the ports that are used for intercluster communication.

- The IP addresses that are used for intercluster LIFs do not need to be in the same subnet, but having them in the same subnet is a simpler configuration.
- You must have decided whether the subnet is dedicated to intercluster communication or is shared with data communication.

Each node must have an intercluster LIF with an IP address on the intercluster network.

The intercluster network must be configured so that cluster peers have *pair-wise full-mesh connectivity* within the applicable IPspace, which means that each pair of clusters in a cluster peer relationship has connectivity among all of their intercluster LIFs.

A cluster's intercluster LIFs have an IPv4 address or an IPv6 address.

### Port requirements

The ports that are used for intercluster communication must meet the following requirements:

- All ports that are used to communicate with a given remote cluster must be in the same IPspace. You can use multiple IPspaces to peer with multiple clusters. *Pair-wise full-mesh connectivity* is required only within an IPspace.
- The broadcast domain that is used for intercluster communication must include at least two ports per node so that intercluster communication can fail over from one port to another port. Ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).
- All ports must be cabled.
- All ports must be in a healthy state.
- The MTU settings of the ports must be consistent.
- You must decide whether the ports that are used for intercluster communication are shared with data communication.

### Firewall requirements

Firewalls and the intercluster firewall policy must allow the following protocols:

- ICMP service
- TCP to the IP addresses of all the intercluster LIFs over the ports 10000, 11104, and 11105
- HTTPS

The default **intercluster** firewall policy allows access through the HTTPS protocol and from all IP addresses (0.0.0.0/0), but the policy can be altered or replaced.

### Cluster requirements

Clusters must meet the following requirements:

- The time on the clusters in a cluster peering relationship must be synchronized within 300 seconds (5 minutes).  
Cluster peers can be in different time zones.

### Related information

[NetApp Documentation: ONTAP 9](#)



## Creating cluster peer relationships

You can create an authenticated cluster peer relationship to connect clusters so that the clusters in the relationship can communicate securely with each other. You can use System Manager to configure an intercluster interface for the local cluster if the intercluster interface is not configured.

### Before you begin

You must have reviewed the requirements to perform this task.

*Prerequisites for cluster peering* on page 63

### About this task

- If you want to create a peer relationship with a cluster running Data ONTAP 8.2.2 or earlier, you must use the command-line interface (CLI).
- In a MetroCluster configuration, when you create a peer relationship between the primary cluster and an external cluster, it is a best practice to create a peer relationship between the surviving site cluster and the external cluster as well.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Cluster Peers**.
3. Click **Create**.
4. In the **Details of the local cluster** area, select the IPspace for the cluster peer relationship.  
The operational intercluster interface for the selected IPspace is displayed.
5. Optional: If the node does not contain an operational intercluster interface, click **Create intercluster interface** to configure the LIF for the node.
6. In the **Details of the remote cluster to be peered** area, specify a passphrase for the cluster peer relationship.  
  
The passphrase that you enter will be validated against the passphrase of the peered cluster to ensure an authenticated cluster peer relationship.  
  
The minimum default length of the passphrase is eight characters.  
  
If the name of the local cluster and remote cluster are identical, an alias is created for the remote cluster.  
  
If the name of the local cluster and remote cluster are identical, or if the local cluster is in a peer relationship with another remote cluster of the same name, an Enter Cluster Alias Name dialog box is displayed.
7. Enter an alias name for the remote cluster.
8. Enter the intercluster interface IP addresses for the remote cluster.
9. Click **Create**.
10. Log in to the remote cluster and perform the above steps to create a peer relationship between the local and remote clusters.

## Modifying the cluster peer passphrase

For security reasons, you can modify the passphrase that is provided during cluster peer creation by using System Manager.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Cluster Peers**.
3. Select the peer cluster, and click **Modify Passphrase**.
4. In the **Modify Passphrase** dialog box, enter the new passphrase, and then click **Modify**.  
**Note:** The minimum default length of the passphrase is eight characters.
5. Log in to the remote cluster and perform steps 1 through 4 to modify the passphrase in the remote cluster.

The authentication status for the local cluster is displayed as **ok\_and\_offer** until you modify the passphrase in the remote cluster.

## Modifying the peer network parameters

You can use System Manager to modify the IPspace and intercluster logical interfaces (LIFs) that are configured for the remote cluster. You can add new intercluster IP addresses or remove existing IP addresses.

### Before you begin

You must have at least one intercluster IP address to create the cluster peer relationship.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Cluster Peers**.
3. Select a peer cluster, and then click **Modify Peer Network Parameters**.
4. In the **Modify Peer Network Parameters** dialog box, select the IPspace, and then add or remove the intercluster IP addresses.  
You can add multiple IP addresses by using comma separators.
5. Click **Modify**.
6. Verify the changes that you made in the **Peers** window.

## Deleting cluster peer relationships

You can use System Manager to delete a cluster peer relationship if the relationship is no longer required. You must delete the cluster peering relationship from each of the clusters in the peer relationship.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Cluster Peers**.

3. Select the cluster peer that you want to delete, and then click **Delete**.
4. Select the confirmation check box, and then click **Delete**.
5. Log in to the remote cluster and perform steps 1 through 4 to delete the peer relationship between the local and remote clusters.

The status of the peer relationship is displayed as “unhealthy” until the relationship is deleted from both the local and remote clusters.

## What a cluster peer is

The cluster peer feature allows two clusters to coordinate and share resources between them.

## What cluster peer intercluster connectivity is

You should know about the interfaces and ports that you put together to create a cluster peer intercluster connection and how they are used. Knowing this information might reduce the amount of time you use to create the cluster peer intercluster connectivity.

Cluster peer intercluster connectivity consists of intercluster logical interfaces (LIFs) that are assigned to network ports. The intercluster connection on which replication occurs between two different clusters is defined when the intercluster LIFs are created. Replication between two clusters can occur on the intercluster connection only; this is true regardless of whether the intercluster connectivity is on the same subnet as a data network in the same cluster.

The IP addresses assigned to intercluster LIFs can reside in the same subnet as data LIFs or in a different subnet. When an intercluster LIF is created, it uses routes that belong to the System SVM that the intercluster LIF is in.

System Manager enables you to create an authenticated cluster peer relationship between clusters that are running Data ONTAP 8.3 or later. An authenticated peer relationship uses passphrases to provide secure intercluster communication.

## Connecting one cluster to another cluster in a peer relationship

You connect clusters together in a cluster peer relationship to share information and to provide access to operations on the peer cluster.

### About this task

Connecting clusters together requires network ports, network interfaces configured with the intercluster role, and creating the cluster peer relationship.

## Peers window

You can use the Peers window to manage peer relationships, which enable you to move data from one cluster to another.

### Command buttons

#### Create

Opens the Create Cluster Peering dialog box, which enables you to create a relationship with a remote cluster.

#### Modify Passphrase

Opens the Modify Passphrase dialog box, which enables you to enter a new passphrase for the local cluster.

#### Modify Peer Network Parameters

Opens the Modify Peer Network Parameters dialog box, which enables you to modify the IPspace, add new intercluster IP addresses, or remove existing IP addresses.

You can add multiple IP addresses, separated by commas.

#### **Delete**

Opens the Delete Cluster Peer Relationship dialog box, which enables you to delete the selected peer cluster relationship.

#### **Refresh**

Updates the information in the window.

#### **Peer cluster list**

##### **Peer Cluster**

Specifies the name of the peer cluster in the relationship.

##### **Availability**

Specifies whether the peer cluster is available for communication.

##### **Authentication Status**

Specifies whether the peer cluster is authenticated or not.

##### **IPspace**

Displays IPspace associated to the cluster peer relation.

#### **Details area**

The details area displays detailed information about the selected peer cluster relationship, including the active IP addresses discovered by the system to set up the intercluster network and the last updated time.

## **High availability**

You can use System Manager to create high availability (HA) pairs that provide hardware redundancy that is required for nondisruptive operations and fault tolerance.

### **Understanding HA pairs**

HA pairs provide hardware redundancy that is required for nondisruptive operations and fault tolerance and give each node in the pair the software functionality to *take over* its partner's storage and subsequently *give back* the storage.

### **High Availability window**

The High Availability window provides a pictorial representation of the HA state, interconnect status, and takeover or giveback status of all the HA pairs in clustered Data ONTAP. You can also manually initiate a takeover or giveback operation.

You can view details such as the takeover or giveback status and interconnect status by clicking the HA pair image.

The color indicates the HA pair status:

- **Green:** Indicates that the HA pair and the interconnect are optimally configured and available for takeover or giveback. It also indicates takeover in progress, giveback in progress, and waiting for giveback states.
- **Red:** Indicates a downgraded state such as a takeover failure.
- **Yellow:** Indicates that the interconnect status is down.

When multiple HA pairs in a cluster are simultaneously involved in storage failover operations, the cluster status that is displayed is based on the status and severity of the HA pair. The following order of severity is considered while displaying the cluster status: Takeover in progress, Giveback in progress, Waiting for giveback.

## Actions

You can perform tasks such as takeover or giveback based on the status of the nodes in the HA pair.

- **Takeover** *node\_name*  
Enables you to perform a takeover operation when maintenance is required on the partner node.
- **Giveback** *node\_name*  
Enables you to perform a giveback operation when the partner node that has been taken over is waiting for giveback or is in a partial giveback state.
- **Enable or Disable automatic giveback**  
Enables or disables the automatic giveback operation.

**Note:** Automatic giveback is enabled by default.

## Command buttons

### Refresh

Updates the information in the window.

**Note:** Information displayed in the High Availability window is automatically refreshed every 60 seconds.

## Related tasks

[Monitoring HA pairs](#) on page 35

# Licenses

You can use System Manager to view, manage, or delete any software licenses installed on a cluster or node.

## Deleting licenses

You can use the Licenses window in System Manager to delete any software license installed on a cluster or a node.

### Before you begin

The software license you want to delete must not be used by any service or feature.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Licenses**.
3. In the **Licenses** window, perform the appropriate action:

If you want to...	Do this...
Delete a specific license package on a node or a master license	Click the <b>Details</b> tab.
Delete a specific license package across all the nodes in the cluster	Click the <b>Packages</b> tab.

4. Select the software license package that you want to delete, and then click **Delete**.

You can delete only one license package at a time.

5. Select the confirmation check box, and then click **Delete**.

### Result

The software license is deleted from your storage system. The deleted license is also removed from the list of licenses in the Licenses window.

### Related references

[Licenses window](#) on page 73

## Managing licenses (cluster administrators only)

A license is a record of one or more software entitlements. Installing license keys, also known as *license codes*, enables you to use certain features or services on your cluster. Data ONTAP enables you to manage feature licenses and monitor feature usage and license entitlement risk.

Each cluster requires a cluster base license key, which you can install either during or after the cluster setup. Some features require additional licenses. Data ONTAP feature licenses are issued as *packages*, each of which contains multiple features or a single feature. A package requires a license key, and installing the key enables you to access all features in the package. Data ONTAP prevents you from installing a feature license before a cluster base license key is installed.

Starting with Data ONTAP 8.2, all license keys are 28 characters in length. Licenses installed prior to Data ONTAP 8.2 continue to work in Data ONTAP 8.2 and later releases. However, if you need to reinstall a license (for example, you deleted a previously installed license and want to reinstall it in Data ONTAP 8.2 or later, or you perform a controller replacement procedure for a node in a cluster running Data ONTAP 8.2 or later), Data ONTAP requires that you enter the license key in the 28-character format.

You can find license keys for your initial or add-on software orders at the NetApp Support Site under **My Support > Software Licenses** (login required). If you cannot locate your license keys from the Software Licenses page, contact your sales or support representative.

Data ONTAP enables you to manage feature licenses in the following ways:

- Add one or more license keys (`system license add`)
  - Display information about installed licenses (`system license show`)
  - Display the packages that require licenses and their current license status on the cluster (`system license status show`)
  - Delete a license from the cluster or a node whose serial number you specify (`system license delete`)
- The cluster base license is required for the cluster to operate. Data ONTAP does not enable you to delete it.
- Display or remove expired or unused licenses (`system license clean-up`)

Data ONTAP enables you to monitor feature usage and license entitlement risk in the following ways:

- Display a summary of feature usage in the cluster on a per-node basis (`system feature-usage show-summary`)  
The summary includes counter information such as the number of weeks a feature was in use and the last date and time the feature was used.
- Display feature usage status in the cluster on a per-node and per-week basis (`system feature-usage show-history`)  
The feature usage status can be **not-used**, **configured**, or **in-use**. If the usage information is not available, the status shows **not-available**.
- Display the status of license entitlement risk for each license package (`system license entitlement-risk show`)  
The risk status can be **low**, **medium**, **high**, **unlicensed**, or **unknown**. The risk status is also included in the AutoSupport message. License entitlement risk does not apply to the base license package.  
The license entitlement risk is evaluated by using a number of factors, which might include but are not limited to the following:
  - Each package's licensing state
  - The type of each license, its expiry status, and the uniformity of the licenses across the cluster
  - Usage for the features associated with the license package

If the evaluation process determines that the cluster has a license entitlement risk, the command output also suggests a corrective action.

#### Related information

[NetApp KB Article 3013749: Data ONTAP 8.2 and 8.3 Licensing Overview and References](#)  
[NetApp KB Article 1014509: How to verify Data ONTAP Software Entitlements and related License Keys using the Support Site](#)  
[NetApp: Data ONTAP Entitlement Risk Status](#)

## License types and entitlement risk

Understanding license types and entitlement risk helps you manage the risk associated with the licenses in a cluster.

### License types

A package can have one or more of the following types of licenses installed in the cluster:

- Node-locked license or standard license  
A node-locked license is issued for a node with a specific system serial number (also known as a *controller serial number*). This license is valid only for the node that has the matching serial number.  
Installing a node-locked license entitles a node to the licensed functionality. For the cluster to use the licensed functionality, at least one node must be licensed for the functionality. It might be out of compliance to use the licensed functionality on a node that does not have an entitlement for the functionality.  
Data ONTAP 8.2 and later releases treat a license that was installed prior to Data ONTAP 8.2 as a standard license. Therefore, in Data ONTAP 8.2 and later releases, all nodes in the cluster automatically have the standard license for the package that the previously licensed functionality is part of.

- Master or site license

A master or site license is not tied to a specific system serial number. When you install a site license, all nodes in the cluster are entitled to the licensed functionality.

If your cluster has a master license and you remove a node from the cluster, the node does not carry the site license with it, and it is no longer entitled to the licensed functionality. If you add a node to a cluster that has a master license, the node is automatically entitled to the functionality granted by the site license.

- Demo or temporary license

A demo or temporary license expires after a certain period of time. This license enables you to try certain software functionality without purchasing an entitlement. A temporary license is a cluster-wide license, and is not tied to a specific serial number of a node.

If your cluster has a temporary license for a package and you remove a node from the cluster, the node does not carry the evaluation license with it.

- Capacity license

A capacity license is issued based on the total amount of storage currently attached to the ONTAP Select instance. A capacity license can be purchased based on your data requirements. The maximum capacity of storage that can be attached to one ONTAP Select instance is 2 TB, for one capacity license. You need to purchase another capacity license if you storage exceeds the maximum capacity.

### Entitlement risk

An entitlement risk arises because of the non-uniform installation of a node-locked license. If the node-locked license is installed on all the nodes, there is no entitlement risk.

An entitlement risk can be a high risk, medium risk, no risk, or an unknown risk depending on certain conditions:

- High risk

- If there is usage on a particular node, but the node-locked license is not installed on that node
- If the demo license that was installed on the cluster expires, and there is usage on any node

**Note:** If a master license is installed on a cluster, the entitlement risk is never high.

- Medium risk

- If there is usage on the nodes, and only the site license is installed on the cluster
- If there is usage on the nodes, but the node-locked license is not installed on these nodes
- If the site license is not installed, and the node-locked license is non-uniformly installed on the nodes in a cluster

- No risk

There is no entitlement risk if a node-locked license is installed on all the nodes, irrespective of the usage.

- Unknown

The risk is unknown if the API is sometimes unable to retrieve the data related to entitlement risk that is associated with the cluster or the nodes in the cluster.



## Licenses window

Your storage system arrives from the factory with pre-installed software. If you want to add or remove a software license after you receive the storage system, you can use the Licenses window.

**Note:** System Manager does not monitor evaluation licenses and does not provide any warning when an evaluation license is nearing expiry. An evaluation license is a temporary license that expires after a certain period of time.

- [Command buttons](#) on page 73
- [Packages tab](#) on page 73
- [Packages details area](#) on page 73
- [Details tab](#) on page 73

### Command buttons

#### Add

Opens the Add License window, which enables you to add new software licenses.

#### Delete

Deletes the software license that you select from the software license list.

#### Refresh

Updates the information in the window.





### Packages tab

Displays information about the license packages that are installed on your storage system.

#### Package

Displays the name of the license package.

#### Entitlement Risk

Indicates the level of risk as a result of license entitlement issues for a cluster. The entitlement risk level can be high risk () , medium risk () , no risk () , unknown () , or unlicensed (-).

#### Description

Displays the level of risk as a result of license entitlement issues for a cluster.

### License Package details area

The area below the license packages list displays additional information about the selected license package. This area includes information about the cluster or node on which the license is installed, the serial number of the license, usage in the previous week, whether the license is installed, the expiration date of the license, and whether the license is a legacy one.

### Details tab

Displays additional information about the license packages that are installed on your storage system.

#### Package

Displays the name of the license package.

#### Cluster/Node

Displays the cluster or node on which the license package is installed.

**Serial Number**

Displays the serial number of the license package that is installed on the cluster or node.

**Type**

Displays the type of the license package, which can be the following:

- **Temporary:** Specifies that the license is a temporary license, which is valid only during the demonstration period.
- **Master:** Specifies that the license is a master license, which is installed on all the nodes in the cluster.
- **Node Locked:** Specifies that the license is a node-locked license, which is installed on a single node in the cluster.
- **Capacity:** Specifies that the license is a capacity license, which is issued based on the total amount of storage attached to the ONTAP Select instance.

**State**

Displays the state of the license package, which can be the following:

- **Evaluation:** Specifies that the installed license is an evaluation license.
- **Installed:** Specifies that the installed license is a valid purchased license.
- **Warning:** Specifies that the installed license is a valid purchased license and is approaching maximum capacity.
- **Enforcement:** Specifies that the installed license is a valid purchased license and has exceeded the expiry date.
- **Waiting for License:** Specifies that the license has not yet been installed.

**Legacy**

Displays whether the license is a legacy license.

**Maximum Capacity**

Displays the maximum amount of storage that can be attached to the ONTAP Select instance.

**Current Capacity**

Displays the total amount of storage that is currently attached to the ONTAP Select instance.

**Expiration Date**

Displays the expiration date of the software license package.

**Related tasks**

[Adding licenses](#) on page 34

[Deleting licenses](#) on page 69

[Creating a cluster](#) on page 24

## Cluster update

You can use System Manager to update a cluster or individual nodes in HA pairs.

## Updating the cluster nondisruptively

You can use System Manager to update a cluster or individual nodes in HA pairs that are running Data ONTAP 8.3.1 to a specific version of ONTAP software without disrupting access to client data.

### Before you begin

- All the nodes must be in HA pairs.  
You cannot update a single-node cluster.
- All the nodes must be healthy.
- The clusters must be running Data ONTAP 8.3.1.  
You can update only to versions later than Data ONTAP 8.3.1 by using System Manager.
- You must have copied the software image from the NetApp Support Site to an HTTP server or FTP server on your network so that the nodes can access the image.

[Obtaining Data ONTAP software images](#) on page 77

### About this task

- If you try to perform other tasks from System Manager while updating the node that hosts the cluster-management LIF, an error message might be displayed.  
You must wait for the update to finish before performing any operations.
- If the cluster consists of less than eight nodes, a rolling update is performed; if there are eight or more nodes in the cluster, a batch update is performed.  
In a rolling update, the nodes in the cluster are updated one at a time. In a batch update, multiple nodes are updated in parallel.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster Settings** pane, click **Cluster Update**.
3. In the **Cluster Update** tab, perform one of the following operations:

If you want to...	Then...
Add a new software image	<ol style="list-style-type: none"> <li>a. Click <b>Add</b>.</li> <li>b. In the Add a New Software Image dialog box, enter the URL of the HTTP server or FTP server on which you have saved the image that was downloaded from the NetApp Support Site. For anonymous FTP, enter the URL in the <code>ftp://anonymous@ftpserver</code> format.</li> <li>c. Click <b>Add</b>.</li> </ol>
Select an available image	Choose one of the listed images.

4. Click **Validate** to run the pre-update validation checks to verify whether the cluster is ready for an update.

The validation operation checks the cluster components to validate that the update can be completed nondisruptively, and then displays any errors or warnings, along with any required remedial action that you must perform before updating the software.

**Important:** You must perform all the required remedial actions for the errors before proceeding with the update. Although you can ignore the remedial actions for the warnings, the recommended practice is to perform them before proceeding with the update.

5. Click **Next**.

6. Optional: Click **Advanced Options**, and perform the following steps:

- a. In the **Advanced Options** area, perform one of the following operations:

If you want to...	Then...
Update the entire cluster	Select the <b>Update the entire cluster</b> check box. By default, this check box is selected.
Update particular HA pairs	Clear the <b>Update the entire cluster</b> check box, and then select the HA pair that you want to update.

- b. Specify a different stabilization time if your environment requires more or less time for client stabilization.

Stabilization time specifies the time period for which the update process should wait after completing a task to enable client applications to recover. It should be in the range of 1 through 60 minutes; it is set to 8 minutes by default.

- c. Select the **Pause after every step (not recommended)** check box if you want to automatically pause the update after every major step.

Pausing an update after every major step enables you to review the status of the update and then manually resume the update. This option is disabled by default, and the update is not paused unless an error occurs or you manually pause the update.

- d. Select the **Force Rolling Update** check box to perform a rolling update.

This check box is displayed only if your cluster consists of eight or more nodes.

You can enable this option if the entire cluster is selected or if there are four or more HA pairs for update.

7. Click **Update**.

Validation is performed again.

- When the validation is complete, a table is displayed, which shows the errors and warnings, if any, along with the required remedial action that you have to perform before proceeding.
- If the validation is completed with warnings, you can select the **Continue update with warnings** check box, and then click **Continue**.

When the validation is complete and the update is in progress, the update might be paused because of errors. You can click the error to view the details, and then perform the remedial actions before resuming the update.

After the update is completed successfully, you are redirected to the login page of System Manager.

8. Verify that the cluster is successfully updated to the selected version by clicking **Cluster > Cluster Update > Update History** and viewing the details.

### Related concepts

[How you update a cluster nondisruptively](#) on page 77

## Obtaining ONTAP software images

You must copy a software image from the NetApp Support Site to an HTTP server or FTP server on your network so that nodes can access the image.

### About this task

To upgrade the cluster to the target release of ONTAP, you need access to software images. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site. Note the following important information:

- Software images are specific to platform models.  
You must be sure to obtain the correct image for your cluster.
- Software images include the latest version of system firmware that was available when a given version of ONTAP was released.

### Steps

1. Locate the target ONTAP software in the **Software Downloads** area of the NetApp Support Site.
2. Copy the software image (for example, `900_q_image.tgz` for an upgrade or `832_q_image.tgz` for a revert) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served.

## How you update a cluster nondisruptively

You can use System Manager to update a cluster nondisruptively to a specific Data ONTAP version. In a nondisruptive update, you have to select a Data ONTAP image, validate that your cluster is ready for the update, and then perform the update.

During the nondisruptive update, the cluster remains online and continues to serve data during the update.

### Planning and preparing for the update

As part of planning and preparing for the cluster update, you have to obtain the version of Data ONTAP image to which you want to update the cluster from the NetApp Support Site, select the software image, and then perform a validation. The pre-update validation verifies whether the cluster is ready for an update to the selected version.

If validation finishes with errors and warnings, you have to resolve them by performing the remedial actions and ensure that the cluster components are ready for the update. For example, during the pre-update check, if a warning is displayed that there are offline aggregates present in the cluster, you must navigate to the aggregate page and change the status of all the offline aggregates to online.

### Performing an update

When you update the cluster, either the entire cluster is updated or nodes in an HA pair are updated. As part of the update, a validation is run again to verify that the cluster is ready for the update.

A rolling or batch update is performed, depending on the number of nodes in the cluster.

#### Rolling update

One of the nodes is taken offline and updated while the partner node takes over its storage.

A rolling update is performed for a cluster that consists of two or more nodes. This is the default and only method of update for clusters with less than eight nodes.

#### Batch update

The cluster is separated into two batches, each of which contains multiple HA pairs.

A batch update is performed for a cluster that consists of eight or more nodes. In such clusters, you can perform either a batch update or a rolling update. By default, a batch update is performed.

#### Related tasks

[Updating the cluster nondisruptively](#) on page 75

## Cluster Update window

You can use the Cluster Update window to perform an automated cluster upgrade without disrupting access to client data.

- [Tabs](#) on page 78
- [Cluster Update tab](#) on page 78
- [Update History tab](#) on page 79

### Tabs

#### Cluster Update

Enables you to perform a nondisruptive upgrade (NDU) of a cluster.

#### Update History

Displays the details of previous cluster updates.

### Cluster Update tab

#### Command buttons

##### Refresh

Updates the information in the window.

##### Select

You can select the version of the software image for the update.

- **Cluster Version Details:** Displays the current cluster version in use and the version details of the nodes or HA pairs.
- **Available Software Images:** Enables you to select an already available software image for the update. Alternatively, you can download a software image from the NetApp Support Site and add it for the update.

##### Validate

You can view and validate the cluster against the software image version for the update. A pre-update validation checks whether the cluster is in a state that is ready for an update. If the validation is completed with errors, a table displays the status of the various components and the required corrective action for the errors.

You can perform the update only when the validation is completed successfully.

##### Update

You can update all the nodes in the cluster or an HA pair in the cluster to the selected version of the software image. While the update is in progress, you can choose to pause and then either cancel or resume the update.

If an error occurs, the update is paused and an error message is displayed with the remedial steps. You can choose to either resume the update after performing the remedial steps or cancel the update. You can view the table with the node name, uptime, state, and Data ONTAP version when the update is successfully completed.

## Update History tab

### Update History list

#### Image Version

Specifies the version of Data ONTAP image that the node will be updated to.

#### Software Updates Installed on

Specifies the type of disk on which the updates are installed.

#### Status

Specifies the status of the software image update, whether it is successful or cancelled.

#### Start Time

Specifies the time when the update was started.

#### Completion Time

Specifies the time when the update was completed.

This field is hidden by default.

#### Time Taken for the Update

Specifies the time taken for the update to complete.

#### Previous Version

Specifies the Data ONTAP version of the node before the update.

#### Updated Version

Specifies the Data ONTAP version of the node after the update.

## Date and time

You can use System Manager to manage the cluster time.

### Managing the cluster time (cluster administrators only)

Problems can occur when the cluster time is inaccurate. Although Data ONTAP enables you to manually set the time zone, date, and time on the cluster, you should configure the Network Time Protocol (NTP) servers to synchronize the cluster time.

NTP is always enabled. However, configuration is still required for the cluster to synchronize with an external time source. Data ONTAP enables you to manage the cluster's NTP configuration in the following ways:

- You can associate a maximum of 10 external NTP servers with the cluster (`cluster time-service ntp server create`).
  - For redundancy and quality of time service, you should associate at least three external NTP servers with the cluster.
  - You can specify an NTP server by using its IPv4 or IPv6 address or fully qualified host name.
  - You can manually specify the NTP version (v3 or v4) to use.  
By default, Data ONTAP automatically selects the NTP version that is supported for a given external NTP server.  
If the NTP version you specify is not supported for the NTP server, time exchange cannot take place.
  - At the advanced privilege level, you can specify an external NTP server that is associated with the cluster to be the primary time source for correcting and adjusting the cluster time.

- You can display the NTP servers that are associated with the cluster (`cluster time-service ntp server show`).
- You can modify the cluster's NTP configuration (`cluster time-service ntp server modify`).
- You can disassociate the cluster from an external NTP server (`cluster time-service ntp server delete`).
- At the advanced privilege level, you can reset the configuration by clearing all external NTP servers' association with the cluster (`cluster time-service ntp server reset`).

A node that joins a cluster automatically adopts the NTP configuration of the cluster.

In addition to using NTP, Data ONTAP also enables you to manually manage the cluster time. This capability is helpful when you need to correct erroneous time (for example, a node's time has become significantly incorrect after a reboot). In that case, you can specify an approximate time for the cluster until NTP can synchronize with an external time server. The time you manually set takes effect across all nodes in the cluster.

You can manually manage the cluster time in the following ways:

- You can set or modify the time zone, date, and time on the cluster (`cluster date modify`).
- You can display the current time zone, date, and time settings of the cluster (`cluster date show`).

**Note:** Job schedules do not adjust to manual cluster date and time changes. These jobs are scheduled to run based on the current cluster time when the job was created or when the job most recently ran. Therefore, if you manually change the cluster date or time, you must use the `job show` and `job history show` commands to verify that all scheduled jobs are queued and completed according to your requirements.

#### Related information

[Network Time Protocol \(NTP\) Support](#)

## Date and Time window

The Date and Time window enables you to view the current date and time settings for your storage system and modify the settings when required.

### Command buttons

#### Edit

Opens the Edit Date and Time dialog box, which enables you to manually set the date, time, and time zone for your storage system.

#### Refresh

Updates the information in the window.

### Details area

The details area displays information about the date, time, time zone, NTP service, and time servers for your storage system.

### Related tasks

[Setting the time for a cluster](#) on page 35

[Setting up a network when an IP address range is disabled](#) on page 26



## SNMP

You can use System Manager to configure SNMP to monitor SVMs in your cluster.

### Enabling or disabling SNMP

You can enable or disable SNMP on your storage system by using System Manager. SNMP enables you to monitor Storage Virtual Machines (SVMs) in a cluster to avoid issues before they can occur and respond to issues when they occur.

#### Steps

1. Click the **Configurations** tab.
2. In the **Services** pane, click **SNMP**.
3. In the **SNMP** window, click either **Enable** or **Disable**.

### Setting SNMP information

You can use the Edit SNMP Settings dialog box in System Manager to update information about the storage system location, contact personnel, and to specify SNMP communities of your system.

#### About this task

System Manager uses SNMP protocols SNMPv1 and SNMPv2c, and an SNMP community to discover storage systems.

#### Steps

1. Click the **Configurations** tab.
2. In the **Services** pane, click **SNMP**.
3. Click **Edit**.
4. In the **General** tab, specify the storage system contact personnel and location, and SNMP communities.

The community name can be of 32 characters and must not contain the following special characters: , / : " ' |.

5. Click **OK**.
6. Verify the changes you made to the SNMP settings in the **SNMP** window.

#### Related references

[SNMP window](#) on page 83

### Enabling or disabling SNMP traps

SNMP traps enable you to monitor the health and state of various components of the storage system. You can use the Edit SNMP Settings dialog box in System Manager to enable or disable SNMP traps on your storage system.

#### About this task

Although SNMP is enabled by default, traps are disabled by default.

**Steps**

1. Click the **Configurations** tab.
2. In the **Services** pane, click **SNMP**.
3. In the **SNMP** window, click **Edit**.
4. In the **Edit SNMP Settings** dialog box, select the **Trap hosts** tab, and either select or clear the **Enable traps** check box.
5. If you enable SNMP traps, add the host name or IP address of the hosts to which the traps are sent.
6. Click **OK**.

**Related references**

[SNMP window](#) on page 83

**Testing the trap host configuration**

You can use System Manager to test that you have configured the trap host settings correctly.

**Steps**

1. Click the **Configurations** tab.
2. In the **Services** pane, click **SNMP**.
3. In the **SNMP** window, click **Test Trap Host**.
4. Click **OK**.

**Options to use when configuring SNMP**

You should be aware of the necessary options that you can set when configuring SNMP.

Location	Enter the location of the SNMP agent.
Contact	Enter the contact person for the SNMP agent.
Community name	Enter a single read-only community string for SNMPv1 and SNMPv2.
Username, engine ID and authentication protocol	Enter a user name, engine ID of the SNMP agent, and authentication type to use with SNMPv3.  <b>Note:</b> The default and recommended value for engine ID is local EngineID.
Trap	Enable or disable SNMP traps.
Host	Enter the destination host IP address.

**Managing SNMP on the cluster (cluster administrators only)**

You can configure SNMP to monitor SVMs in your cluster to avoid issues before they occur, and to respond to issues if they do occur. Managing SNMP involves configuring SNMP users and configuring SNMP trap host destinations (management workstations) for all SNMP events. SNMP is disabled by default on data LIFs.

You can create and manage read-only SNMP users in the data SVM. Data LIFs must be configured to receive SNMP requests on the SVM.

SNMP network management workstations, or managers, can query the SVM SNMP agent for information. The SNMP agent gathers information and forwards it to the SNMP managers. The SNMP agent also generates trap notifications whenever specific events occur. The SNMP agent on the SVM has read-only privileges; it cannot be used for any set operations or for taking a corrective action in response to a trap. Data ONTAP provides an SNMP agent compatible with SNMP versions v1, v2c, and v3. SNMPv3 offers advanced security by using passphrases and encryption.

For more information about SNMP support in clustered Data ONTAP systems, see TR-4220 on the NetApp Support site.

[mysupport.netapp.com](https://mysupport.netapp.com)

## SNMP window

The SNMP window enables you to view the current SNMP settings for your system. You can also change your system's SNMP settings, enable SNMP protocols, and add trap hosts.

### Command buttons

#### Enable/Disable

Enables or disables SNMP.

#### Edit

Opens the Edit SNMP Settings dialog box, which enables you to specify the SNMP communities for your storage system and enable or disable traps.

#### Test Trap Host

Sends a test trap to all the configured hosts to check whether the test trap reaches all the hosts and whether the configurations for SNMP are set correctly.

#### Refresh

Updates the information in the window.

### Details

The details area displays the following information about the SNMP server and host traps for your storage system:

#### SNMP

Displays whether SNMP is enabled or not.

#### Traps

Displays if SNMP traps are enabled or not.

#### Location

Displays the address of the SNMP server.

#### Contact

Displays the contact details for the SNMP server.

#### Trap host IP Address

Displays the IP addresses of the trap host.

#### Community Names

Displays the community name of the SNMP server.

#### Security Names

Displays the security style for the SNMP server.

### Related tasks

[Setting SNMP information](#) on page 81

*Enabling or disabling SNMP traps* on page 81

## LDAP

You can use System Manager to configure an LDAP server that centrally maintains user information.

### Viewing the LDAP client configuration

You can use System Manager to view the LDAP clients that are configured for a Storage Virtual Machine (SVM) in the cluster.

#### Steps

1. Click the **Configurations** tab.
2. In the **Services** pane, click **LDAP**.

The list of LDAP clients are displayed in the LDAP window.

### Using LDAP services

An LDAP server enables you to centrally maintain user information. If you store your user database on an LDAP server in your environment, you can configure your Storage Virtual Machine (SVM) to look up user information in your existing LDAP database.

#### About this task

Data ONTAP supports LDAP for user authentication, file access authorization, and user lookup and mapping services between NFS and CIFS.

### LDAP window

You can use the LDAP window to view LDAP clients for user authentication, file access authorization, user search, and mapping services between NFS and CIFS.

The LDAP window is displayed as view-only at the cluster level. However, you can create, edit, and delete LDAP clients from the Storage Virtual Machine (SVM) level.

#### Command button

##### Refresh

Updates the information in the window.

#### LDAP client list

Displays, in tabular format, details about LDAP clients.

##### LDAP Client Configuration

Displays the name of the LDAP client configuration that you specified.

##### Storage Virtual Machine

Displays the name of the SVM for each LDAP client configuration.

##### Active Directory Domain

Displays the Active Directory domain for each LDAP client configuration.

##### Active Directory Servers

Displays the Active Directory server for each LDAP client configuration.

### Preferred Active Directory Servers

Displays the preferred Active Directory server for each LDAP client configuration.

## Users

You can use System Manager to add, edit, and manage a cluster user account, and specify a login user method to access the storage system.

### Adding a cluster user account

You can use System Manager to add a cluster user account and specify a login user method to access the storage system.

#### Steps

1. Click the **Configurations** tab.
2. In the **Cluster User Details** pane, click **Users**.
3. Click **Add**.
4. Type the user name for the new user.
5. Type the password that the user uses to connect to the storage system, and then confirm the password.
6. Add one or more user login methods, and then click **Add**.

### Editing a cluster user account

You can use System Manager to edit a cluster user account by modifying the user login methods to access the storage system.

#### Steps

1. Click the **Configurations** tab.
2. In the **Cluster User Details** pane, click **Users**.
3. In the **Users** window, select the user account that you want to modify, and then click **Edit**.
4. In the **Modify User** dialog box, modify the user login methods, and then click **Modify**.

### Changing passwords for cluster user accounts

You can use System Manager to reset the password for a cluster user account.

#### Steps

1. Click the **Configurations** tab.
2. In the **Cluster User Details** pane, click **Users**.
3. Select the user account for which you want to modify the password, and then click **Change Password**.
4. In the **Change Password** dialog box, type the new password, confirm the new password, and then click **Change**.

## Locking or unlocking cluster user accounts

You can use System Manager to either lock or unlock cluster user accounts.

### Steps

1. Click the **Configurations** tab.
2. In the **Cluster User Details** pane, click **Users**.
3. Select the user account whose account status you want to modify and click either **Lock** or **Unlock**.

## User accounts (cluster administrators only)

You can create, modify, lock, unlock, or delete a cluster user account, reset a user's password, or display information about all user accounts.

You can manage cluster user accounts in the following ways:

- Creating a login method for a user by specifying the user's account name, the access method, the authentication method, and, optionally, the access-control role that the user is assigned
- Displaying users' login information, such as the account name, allowed access method, authentication method, access-control role, and account status
- Modifying the access-control role that is associated with a user's login method
 

**Note:** It is best to use a single role for all the access and authentication methods of a user account.
- Deleting a user's login method, such as the access method or the authentication method
- Changing the password for a user account
- Locking a user account to prevent the user from accessing the system
- Unlocking a previously locked user account to enable the user to access the system again

## Roles

You can use an access-control role to control the level of access a user has to the system. In addition to using the predefined roles, you can create new access-control roles, modify them, delete them, or specify account restrictions for the users of a role.

### Related concepts

[Predefined roles for cluster administrators](#) on page 88

[Predefined roles for SVM administrators](#) on page 307

## Users window

You can use the Users window to manage user accounts, reset a user's password, or display information about all user accounts.

### Command buttons

#### Add

Opens the Add User dialog box, which enables you to add user accounts.

**Edit**

Opens the Modify User dialog box, which enables you to modify user login methods.

**Note:** It is best to use a single role for all access and authentication methods of a user account.

**Delete**

Enables you to delete a selected user account.

**Change Password**

Opens the Change Password dialog box, which enables you to reset the user password.

**Lock**

Locks the user account.

**Refresh**

Updates the information in the window.

**Users list**

The area below the users list displays detailed information about the selected user.

**User**

Displays the name of the user account.

**Account Locked**

Displays whether the user account is locked.

**User Login Methods area****Application**

Displays the access method that a user can use to access the storage system. The supported access methods include the following:

- System console (console)
- HTTP(S) (http)
- Data ONTAP API (ontapi)
- Service Processor (service-processor)
- SSH (ssh)

**Authentication**

Displays the default supported authentication method, which is “password”.

**Role**

Displays the role of a selected user.

## Roles

You can use System Manager to create access-controlled user roles.

### Adding roles

You can use System Manager to add an access-control role and specify the command or command directory that the role's users can access. You can also control the level of access the role has to the

command or command directory and specify a query that applies to the command or command directory.

#### Steps

1. Click the **Configurations** tab.
2. In the **Cluster User Details** pane, click **Roles**.
3. In the **Roles** window, click **Add**.
4. In the **Add Role** dialog box, type the role name and add the role attributes.
5. Click **Add**.

## Editing roles

You can use System Manager to modify an access-control role's access to a command or command directory and restrict a user's access to only a specified set of commands. You can also remove a role's access to the default command directory.

#### Steps

1. Click the **Configurations** tab.
2. In the **Cluster User Details** pane, click **Roles**.
3. In the **Roles** window, select the role that you want to modify, and then click **Edit**.
4. In the **Edit Role** dialog box, modify the role attributes, and then click **Modify**.
5. Verify the changes that you made in the **Roles** window.

## Roles and permissions

The cluster administrator can restrict a user's access to only a specified set of commands by creating a restricted access-control role and assigning it to a user.

You can manage access-control roles in the following ways:

- Creating an access-control role and specifying the command or command directory that the role's users can access.
- Controlling the level of access the role has for the command or command directory and specifying a query that applies to the command or command directory.
- Modifying an access-control role's access to a command or command directory.
- Displaying information about access-control roles, such as the role name, the command, or command directory that a role can access, the access level, and the query.
- Deleting an access-control role.
- Restricting a user's access to only a specified set of commands.
- Displaying Data ONTAP APIs and their corresponding CLI commands.

## Predefined roles for cluster administrators

Data ONTAP offers predefined roles for cluster administrators that should meet most of your needs. You can create custom roles as necessary.

The following table lists the predefined roles for cluster administrators:



This role...	Has this level of access...	To the following commands or command directories
admin	all	All command directories ( <b>DEFAULT</b> )
autosupport	all	<ul style="list-style-type: none"> <li>• set</li> <li>• system node autosupport</li> </ul>
	none	All other command directories ( <b>DEFAULT</b> )
backup	all	vserver services ndmp
	readonly	volume
	none	All other command directories ( <b>DEFAULT</b> )
readonly	all	<ul style="list-style-type: none"> <li>• security login password</li> <li>• set</li> </ul>
	none	security
	readonly	All other command directories ( <b>DEFAULT</b> )
none	none	All command directories ( <b>DEFAULT</b> )

**Note:** The **autosupport** role is assigned to the predefined **autosupport** account, used by AutoSupport OnDemand. Data ONTAP prevents you from modifying or deleting the **autosupport** account. It also prevents you from assigning the **autosupport** role to other user accounts.

#### Related concepts

[Roles](#) on page 86

## Roles window

You can use the Roles window to manage roles for user accounts.

### Command buttons

#### Add

Opens the Add Role dialog box, which enables you to create an access-control role and specify the command or command directory that the role's users can access.

#### Edit

Opens the Edit Role dialog box, which enables you to add or modify role attributes.

#### Refresh

Updates the information in the window.

### Roles list

The roles list provides a list of roles that are available to be assigned to users.

### Role Attributes area

The details area displays the role attributes, such as the command or command directory that the selected role can access, the access level, and the query that applies to the command or command directory.

## Managing the network

---

You can use System Manager to manage the network of your storage system by creating and managing IPspaces, broadcast domains, subnets, network interfaces, Ethernet ports, and FC/FCoE adapters.

### IPspaces

You can use System Manager to create and manage IPspaces.

#### Editing IPspaces

You can use System Manager to rename an existing IPspace.

##### About this task

- All IPspace names must be unique within a cluster and must not consist of names reserved by the system, such as local or localhost.
- The system-defined “Default” and “Cluster” IPspaces cannot be modified.

##### Steps

1. Click the **Network** tab.
2. In the **IPspaces** tab, select the IPspace that you want to modify, and then click **Edit**.
3. In the **Edit IPspace** dialog box, rename the IPspace.
4. Click **Rename**.

#### Deleting IPspaces

You can use the System Manager to delete an IPspace when you no longer require it.

##### Before you begin

There must be no broadcast domains, network interfaces, peer relationships, or SVMs associated with the IPspace that you want to delete.

##### About this task

The system-defined “Default” and “Cluster” IPspaces cannot be deleted.

##### Steps

1. Click the **Network** tab.
2. In the **IPspaces** tab, select the IPspace that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Yes**.

## Configuring IPspaces (cluster administrators only)

IPspaces enable you to configure a single Data ONTAP cluster so that it can be accessed by clients from more than one administratively separate network domain, even if those clients are using the same IP address subnet range. This allows for separation of client traffic for privacy and security.

An IPspace defines a distinct IP address space in which Storage Virtual Machines (SVMs) reside. Ports and IP addresses defined for an IPspace are applicable only within that IPspace. A distinct routing table is maintained for each SVM within an IPspace; therefore, no cross-SVM or cross-IPspace traffic routing occurs.

**Note:** IPspaces support both IPv4 and IPv6 addresses on their routing domains.

If you are managing storage for a single organization, then you do not need to configure IPspaces. If you are managing storage for multiple companies on a single Data ONTAP cluster, and you are certain that none of your customers have conflicting networking configurations, then you also do not need to use IPspaces. In many cases, the use of Storage Virtual Machines (SVMs), with their own distinct IP routing tables, can be used to segregate unique networking configurations instead of using IPspaces.

## Standard properties of IPspaces

Special IPspaces are created by default when the cluster is first created. Additionally, special Storage Virtual Machines (SVMs) are created for each IPspace.

Two IPspaces are created automatically when the cluster is initialized:

- “Default” IPspace  
This IPspace is a container for ports, subnets, and SVMs that serve data. If your configuration does not need separate IPspaces for clients, all SVMs can be created in this IPspace. This IPspace also contains the cluster management and node management ports.
- “Cluster” IPspace  
This IPspace contains all cluster ports from all nodes in the cluster. It is created automatically when the cluster is created. It provides connectivity to the internal private cluster network. As additional nodes join the cluster, cluster ports from those nodes are added to the “Cluster” IPspace.

A “system” SVM exists for each IPspace. When you create an IPspace, a default system SVM of the same name is created:

- The system SVM for the “Cluster” IPspace carries cluster traffic between nodes of a cluster on the internal private cluster network.  
It is managed by the cluster administrator, and it has the name “Cluster”.
- The system SVM for the “Default” IPspace carries management traffic for the cluster and nodes, including the intercluster traffic between clusters.  
It is managed by the cluster administrator, and it uses the same name as the cluster.
- The system SVM for a custom IPspace that you create carries management traffic for that SVM.  
It is managed by the cluster administrator, and it uses the same name as the IPspace

One or more SVMs for clients can exist in an IPspace. Each client SVM has its own data volumes and configurations, and it is administered independently of other SVMs.

## Broadcast domains

You can use System Manager to create and manage broadcast domains.

### Editing broadcast domains

You can use System Manager to modify the attributes of a broadcast domain, such as the name, the MTU size, and the ports associated with the broadcast domain.

#### About this task

- You must not modify the MTU size of the broadcast domain to which the management port e0M is assigned.
- You cannot use System Manager to edit the broadcast domains in the Cluster IPspace. You must use the command-line interface instead.

#### Steps

1. Click the **Network** tab.
2. In the **Broadcast Domains** tab, select the broadcast domain that you want to modify, and then click **Edit**.
3. In the **Edit Broadcast Domain** dialog box, make the necessary changes.
4. Click **Save and Close**.

#### Related references

[Network window](#) on page 104

## Deleting broadcast domains

You can delete a broadcast domain by using System Manager when you no longer require the broadcast domain.

#### Before you begin

There must be no subnets associated with the broadcast domain that you want to delete.

#### About this task

- When you delete a broadcast domain, the ports associated with it are assigned to the Default IPspace, and the MTU settings of the ports are not changed.
- You cannot use System Manager to delete broadcast domains in the Cluster IPspace. You must use the command-line interface instead.

#### Steps

1. Click the **Network** tab.
2. In the **Broadcast Domains** tab, select the broadcast domain that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

### Related references

[Network window](#) on page 104

## Configuring broadcast domains (cluster administrators only)

Broadcast domains enable you to group network ports that belong to the same layer 2 network. The ports in the group can then be used by a Storage Virtual Machine (SVM) for data or management traffic.

A broadcast domain resides in an IPspace. During cluster initialization, the system creates two default broadcast domains:

- The “Default” broadcast domain contains ports that are in the “Default” IPspace. These ports are used primarily to serve data. Cluster management and node management ports are also in this broadcast domain.
- The “Cluster” broadcast domain contains ports that are in the “Cluster” IPspace. These ports are used for cluster communication and include all cluster ports from all nodes in the cluster.

If you have created unique IPspaces to separate client traffic, then you need to create a broadcast domain in each of those IPspaces.

## Subnets

You can use System Manager to manage subnets.

### Editing subnets

You can use System Manager to modify subnet attributes, such as the name, subnet address, range of IP addresses, and gateway address of the subnet.

#### About this task

- You cannot use System Manager to edit subnets in the Cluster IPspace. You must use the command-line interface (CLI) instead.
- Modifying the gateway address does not update the route. You must use the CLI to update the route.

#### Steps

1. Click the **Network** tab.
2. In the **Subnets** tab, select the subnet that you want to modify, and then click **Edit**.  
You can modify the subnet even when the LIF in that subnet is still in use.
3. In the **Edit Subnet** dialog box, make the necessary changes.
4. Click **Save and Close**.

### Related references

[Network window](#) on page 104

## Deleting subnets

You can use System Manager to delete a subnet when you no longer require the subnet and you want to reallocate the IP addresses that were assigned to the subnet.

### Before you begin

The subnet you want to delete must not have any LIFs using IP addresses from the subnet.

### About this task

You cannot use System Manager to delete subnets in the Cluster IPspace. You must use the command-line interface instead.

### Steps

1. Click the **Network** tab.
2. In the **Subnets** tab, select the subnet that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

### Related references

[Network window](#) on page 104

## Network interfaces

You can use System Manager to create and manage network interfaces.

### Creating network interfaces

You can use System Manager to create a network interface or LIF to access data from Storage Virtual Machines (SVMs), manage SVMs, and to provide an interface for intercluster connectivity.

### Before you begin

The broadcast domain that is associated with the subnet must have allocated ports.

### About this task

- Dynamic DNS (DDNS) is enabled by default when a LIF is created.  
However, if you configure the LIF for intercluster communication, for iSCSI and FC/FCoE protocols, or for management access only, DDNS is disabled.
- You can specify an IP address with or without using a subnet.
- You cannot use System Manager to create a network interface if the ports are degraded.  
You must use the command-line interface to create a network interface.

### Steps

1. Click the **Network** tab.
2. In the **Network Interfaces** tab, click **Create**.
3. In the **Create Network Interface** dialog box, specify an interface name.
4. Specify an interface role:

If you want to...	Then...
Associate the network interface with a data LIF	<ol style="list-style-type: none"> <li>Select <b>Serves Data</b>.</li> <li>Select the SVM for the network interface.</li> </ol>
Associate the network interface with an intercluster LIF	<ol style="list-style-type: none"> <li>Select <b>Intercluster Connectivity</b>.</li> <li>Select the IPspace for the network interface.</li> </ol>

5. Select the appropriate protocols.

The interface uses the selected protocols to access data from the SVM.

6. If you want to enable management access on the data LIF, select the **Enable Management Access** check box.

You cannot enable management access for intercluster LIFs or LIFs with FC/FCoE or iSCSI protocols.

7. Assign the IP address by choosing one of the following options:

If you want to...	Then...
Specify the IP address using a subnet	<ol style="list-style-type: none"> <li>Select <b>Using a subnet</b>.</li> <li>In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIF, only the subnets that are associated with the selected IPspace are displayed.</li> <li>If you want to assign a specific IP address to the interface, select <b>Use a specific IP address</b>, and then type the IP address. The IP address you specify is added to the subnet if it is not already present in the subnet range.</li> <li>Click <b>OK</b>.</li> </ol>
Specify the IP address manually without using a subnet	<ol style="list-style-type: none"> <li>Select <b>Without a subnet</b>.</li> <li>In the Add Details dialog box, perform the following steps: <ol style="list-style-type: none"> <li>Specify the IP address and network mask or prefix.</li> <li>Optional: Specify the gateway. The destination field is populated with the default value based on the family of the IP address.</li> <li>If you do not want the default value, specify the new destination value.  If a route does not exist, a new route is automatically created based on the gateway and destination.</li> </ol> </li> <li>Click <b>OK</b>.</li> </ol>

8. Select the required ports from the ports details area.

- For data LIFs, the details area displays all the ports from the broadcast domain associated with the IPspace of the SVM.
- For intercluster LIFs, the details area displays all the ports from the broadcast domain associated with the required IPspace.

9. Optional: Select the **Dynamic DNS (DDNS)** check box to enable DDNS.
10. Click **Create**.

**Related tasks**

[Configuring iSCSI protocol on SVMs](#) on page 46

**Related references**

[Network window](#) on page 104

## Editing network interfaces

You can use System Manager to modify the network interface to enable management access for a data LIF.

**About this task**

- You cannot modify the network settings of cluster LIFs, cluster management LIFs, or node management LIFs through System Manager.
- You cannot enable management access for an intercluster LIF.

**Steps**

1. Click the **Network** tab.
2. In the **Network Interfaces** tab, select the interface that you want to modify, and then click **Edit**.
3. In the **Edit Network Interface** dialog box, make the necessary changes.
4. Click **Save and Close**.

**Related references**

[Network window](#) on page 104

## Deleting network interfaces

You can use System Manager to delete a network interface to free the IP address of the interface and use the IP address for a different purpose.

**Before you begin**

The status of the network interface must be disabled.

**Steps**

1. Click the **Network** tab.
2. In the **Network Interfaces** tab, select the interface that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

**Related references**

[Network window](#) on page 104



## Migrating a LIF

You can use System Manager to migrate a data LIF or a cluster-management LIF to a different port on the same node or a different node within the cluster, if the port is either faulty or requires maintenance.

### Before you begin

The destination node and ports must be operational and must be able to access the same network as the source port.

### About this task

- If you are removing the NIC from the node, you must migrate LIFs hosted on the ports belonging to the NIC to other ports in the cluster.
- You cannot migrate iSCSI or FC LIFs.

### Steps

1. Click the **Network** tab.
2. In the **Network Interfaces** tab, select the interface that you want to migrate, and then click **Migrate**.
3. In the **Migrate Interface** dialog box, select the destination port to which you want to migrate the LIF.
4. Optional: Select the **Migrate Permanently** check box to set the destination port as the new home port for the LIF.
5. Click **Migrate**.

## What LIFs are

A LIF (logical interface) is an IP address or WWPN with associated characteristics, such as a role, a home port, a home node, a list of ports to fail over to, and a firewall policy. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

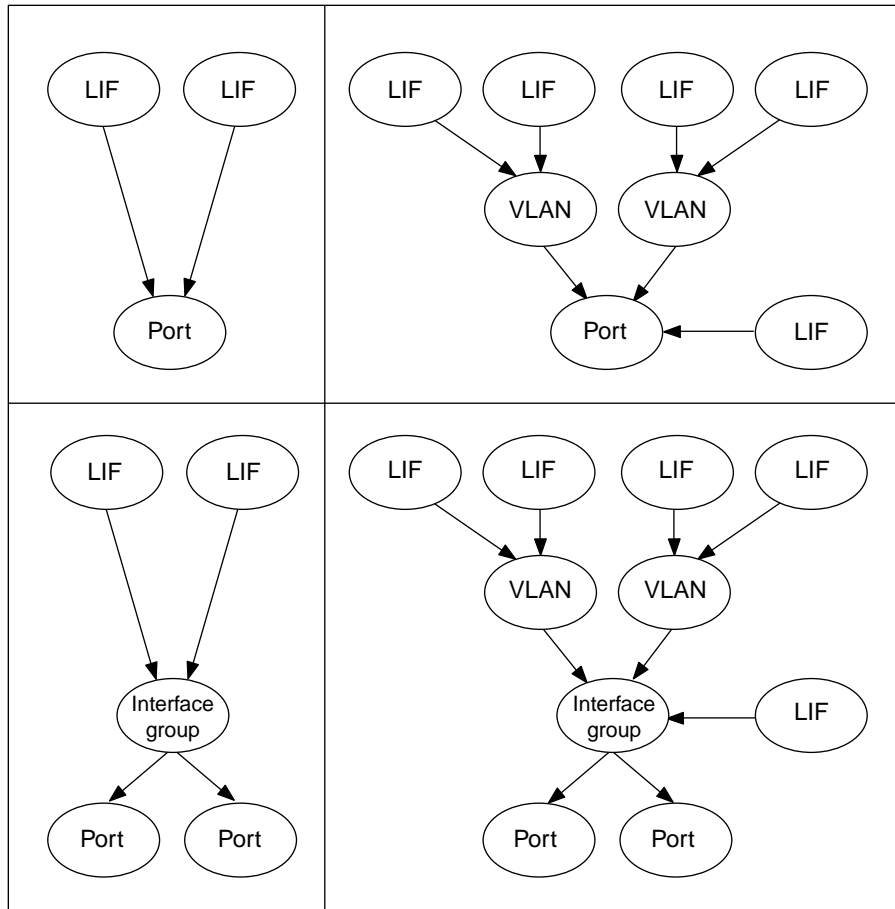
LIFs can be hosted on the following ports:

- Physical ports that are not part of interface groups
- Interface groups
- VLANs
- Physical ports or interface groups that host VLANs

While configuring SAN protocols such as FC on a LIF, it will be associated with a WWPN.

For more information about configuring WWPNs for LIFs using the FC protocol, see the *Clustered Data ONTAP SAN Administration Guide*.

The following figure illustrates the port hierarchy in a clustered Data ONTAP system:



## Roles for LIFs

A LIF role determines the kind of traffic that is supported over the LIF, along with the failover rules that apply and the firewall restrictions that are in place. A LIF can have any one of the five roles: node management, cluster management, cluster, intercluster, and data.

### node management LIF

A LIF that provides a dedicated IP address for managing a particular node in a cluster. Node management LIFs are created at the time of creating or joining the cluster. These LIFs are used for system maintenance, for example, when a node becomes inaccessible from the cluster.

### cluster management LIF

A LIF that provides a single management interface for the entire cluster.

A cluster management LIF can fail over to any node management or data port in the cluster. It cannot fail over to cluster or intercluster ports.

### cluster LIF

A LIF that is used to carry intracluster traffic between nodes in a cluster. Cluster LIFs must always be created on 10-GbE network ports.

Cluster LIFs can fail over between cluster ports on the same node, but they cannot be migrated or failed over to a remote node. When a new node joins a cluster, IP addresses are generated automatically. However, if you want to assign IP addresses manually to the cluster LIFs, you must ensure that the new IP addresses are in the same subnet range as the existing cluster LIFs.

**data LIF**

A LIF that is associated with a Storage Virtual Machine (SVM) and is used for communicating with clients.

You can have multiple data LIFs on a port. These interfaces can migrate or fail over throughout the cluster. You can modify a data LIF to serve as an SVM management LIF by modifying its firewall policy to **mgmt**.

Sessions established to NIS, LDAP, Active Directory, WINS, and DNS servers use data LIFs.

**intercluster LIF**

A LIF that is used for cross-cluster communication, backup, and replication. You must create an intercluster LIF on each node in the cluster before a cluster peering relationship can be established.

These LIFs can only fail over to ports in the same node. They cannot be migrated or failed over to another node in the cluster.

**Guidelines for creating LIFs**

There are certain guidelines that you should consider before creating a LIF.

- Each Storage Virtual Machine (SVM) must have at least one SVM management LIF that is configured to reach external services such as DNS, LDAP, Active Directory, NIS, and so on. SVM management LIF can be configured to either serve data and to reach external services (data-protocol=nfs,cifs,fcache) or only to reach external services (data-protocol=none).
- The maximum number of LIFs that can be created per node is dependent on the platform models that are part of the cluster. All nodes of a cluster that consists of different platform types must use the lowest LIF limit of any node in the cluster. You can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command, and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).  
[ONTAP 9 man page: network interface capacity show](#)  
[ONTAP 9 man page: network interface capacity details show](#)  
[ONTAP 9 man page: network interface capacity show](#)
- FC LIFs can be configured only on FC ports; iSCSI LIFs cannot coexist with any other protocols.  
[ONTAP 9 SAN Administration Guide](#)
- NAS and SAN protocols cannot coexist on the same LIF.
- You must use valid characters that are supported in ONTAP for naming LIFs.
- You should avoid using characters that are not in Unicode basic plane.

## Ethernet ports

You can use System Manager to create and manage Ethernet ports.

### Creating interface groups

You can use System Manager to create an interface group—single-mode, static multimode, or dynamic multimode (LACP)—to present a single interface to clients by combining the capabilities of the aggregated network ports.

#### Before you begin

Free ports must be available that do not belong to any broadcast domain or an interface group, or that host a VLAN.

#### Steps

1. Click the **Network** tab.
2. In the **Ethernet Ports** tab, click **Create Interface Group**.
3. In the **Create Interface Group** dialog box, specify the following settings:
  - Name of the interface group
  - Node
  - Ports that you want to include in the interface group
  - Usage mode of the ports: single, multiple, or LACP
  - Network load distribution: IP based, MAC address based, sequential, or port
  - Broadcast domain for the interface group, if required
4. Click **Create**.

#### Related references

[Network window](#) on page 104

### Creating VLAN interfaces

You can create a VLAN for maintaining separate broadcast domains within the same network domain by using System Manager.

#### Steps

1. Click the **Network** tab.
2. In the **Ethernet Ports** tab, click **Create VLAN**.
3. In the **Create VLAN** dialog box, select the node, the physical interface, and the broadcast domain (if required).

The physical interface list includes only Ethernet ports and interface groups. The list does not display interfaces that are in another interface group or an existing VLAN.

4. Type a VLAN tag, and then click **Add**.

You must add unique VLAN tags.

5. Click **Create**.

#### Related references

[Network window](#) on page 104

## Editing Ethernet port settings

You can edit Ethernet port settings, such as the duplex mode and speed settings, by using System Manager.

#### Steps

1. Click the **Network** tab.
2. Click **Ethernet Ports**.
3. Select the physical port, and then click **Edit**.
4. In the **Edit Ethernet Port** dialog box, modify the duplex mode and speed settings to either **manual** or **automatic**.
5. Click **Edit**.

## Editing interface group settings

You can use System Manager to add ports to an interface group or remove ports from an interface group, and modify the usage mode and load distribution pattern of the ports in the interface group.

#### About this task

You cannot modify the MTU settings of an interface group that is assigned to a broadcast domain.

#### Steps

1. Click the **Network** tab.
2. Click **Ethernet Ports**.
3. Select an interface group, and then click **Edit**.
4. Make the necessary changes, and then click **Save and Close**.

#### Related references

[Network window](#) on page 104

## Editing the MTU size of a VLAN

If you want to modify the MTU size of a VLAN interface that is not part of a broadcast domain, you can use System Manager to change the size.

#### About this task

You must not modify the MTU size of the management port e0M.

#### Steps

1. Click the **Network** tab.
2. Click **Ethernet Ports**.

3. Select the VLAN that you want to modify, and then click **Edit**.
4. In the **Edit VLAN** dialog box, make the necessary changes, and then click **Save**.

## Deleting VLANs

You can delete VLANs that are configured on network ports by using System Manager. You might have to delete a VLAN before removing a NIC from its slot. When you delete a VLAN, it is automatically removed from all the failover rules and groups that use the VLAN.

### Before you begin

There must be no LIFs associated with the VLAN.

### Steps

1. Click the **Network** tab.
2. Click **Ethernet Ports**.
3. Select the VLAN that you want to delete, and then click **Delete**.
4. Select the confirmation check box, and then click **Delete**.

### Related references

[Network window](#) on page 104

## Ports and adapters

Ports are grouped under nodes and the nodes are displayed based on the selected protocol category. For example, if the data is served using the FC protocol, then only the nodes with FCP adapters are displayed. The hosted interface count helps you in choosing a port which is less loaded.

## Types of network ports

The network ports are either physical ports or virtualized ports. VLANs and interface groups constitute the virtual ports. Interface groups treat several physical ports as a single port, while VLANs subdivide a physical port into multiple separate logical ports.

### physical ports

LIFs can be configured directly on physical ports.

### interface group

A port aggregate containing two or more physical ports that act as a single trunk port. An interface group can be single-mode, multimode, or dynamic multimode.

### VLAN

A logical port that receives and sends VLAN-tagged (IEEE 802.1Q standard) traffic. VLAN port characteristics include the VLAN ID for the port. The underlying physical port or interface group ports are considered VLAN trunk ports, and the connected switch ports must be configured to trunk the VLAN IDs.

The underlying physical port or interface group ports for a VLAN port can continue to host LIFs, which transmit and receive untagged traffic.

The port naming convention is *enumberlettere<number>letter*:

- The first character describes the port type.  
“e” represents Ethernet.
- The second character indicates the slot in which the port adapter is located.

- The third character indicates the port's position on a multiport adapter.  
“a” indicates the first port, “b” indicates the second port, and so on.

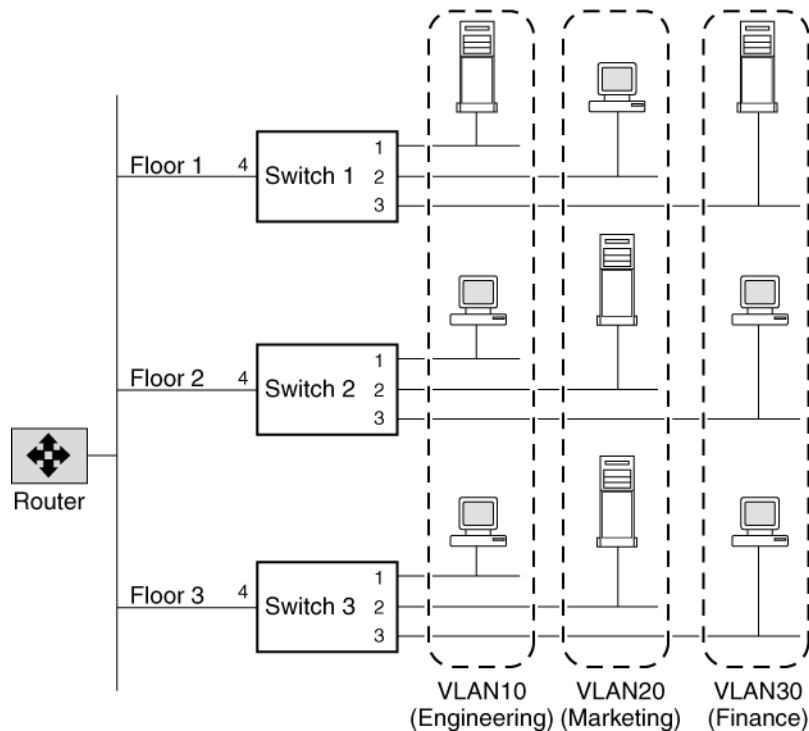
For example, e0b indicates that an Ethernet port is the second port on the node's motherboard.

VLANs must be named by using the syntax `port_name-vlan-id`. “port\_name” specifies the physical port or interface group and “vlan-id” specifies the VLAN identification on the network. For example, e1c-80 is a valid VLAN name.

## How VLANs work

Traffic from multiple VLANs can traverse a link that interconnects two switches by using VLAN tagging. A VLAN tag is a unique identifier that indicates the VLAN to which a frame belongs. A VLAN tag is included in the header of every frame sent by an end-station on a VLAN.

On receiving a tagged frame, the switch inspects the frame header and, based on the VLAN tag, identifies the VLAN. The switch then forwards the frame to the destination in the identified VLAN. If the destination MAC address is unknown, the switch limits the flooding of the frame to ports that belong to the identified VLAN.



For example, in this figure, if a member of VLAN 10 on Floor 1 sends a frame for a member of VLAN 10 on Floor 2, Switch 1 inspects the frame header for the VLAN tag (to determine the VLAN) and the destination MAC address. The destination MAC address is not known to Switch 1. Therefore, the switch forwards the frame to all other ports that belong to VLAN 10, that is, port 4 of Switch 2 and Switch 3. Similarly, Switch 2 and Switch 3 inspect the frame header. If the destination MAC address on VLAN 10 is known to either switch, that switch forwards the frame to the destination. The end-station on Floor 2 then receives the frame.

## FC/FCoE adapters

You can use System Manager to create and manage FC/FCoE adapters.

### Editing the FC/FCoE adapter speed

You can modify the FC/FCoE adapter speed setting by using the Edit FC/FCoE Adapter Settings dialog box in System Manager.

#### Steps

1. Click the **Network** tab.
2. In the **FC/FCoE Adapters** tab, select the adapter that you want to edit, and then click **Edit**.
3. In the **Edit FC/FCoE Adapter Settings** dialog box, set the adapter speed to “manual” or “automatic”, and then click **Edit**.

#### Related references

[Network window](#) on page 104

### Configuring subnets (cluster administrators only)

Subnets enable you to allocate specific blocks, or pools, of IP addresses for your Data ONTAP network configuration. This enables you to create LIFs more easily when using the `network interface create` command, by specifying a subnet name instead of having to specify IP address and network mask values.

A subnet is created within a broadcast domain, and it contains a pool of IP addresses that belong to the same layer 3 subnet. IP addresses in a subnet are allocated to ports in the broadcast domain when LIFs are created. When LIFs are removed, the IP addresses are returned to the subnet pool and are available for future LIFs.

It is recommended that you use subnets because they make the management of IP addresses much easier, and they make the creation of LIFs a simpler process. Additionally, if you specify a gateway when defining a subnet, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.

## Network window

You can use the Network window to view the list of network components, such as subnets, network interfaces, Ethernet ports, broadcast domains, FC/FCoE adapters, and IPspaces, and to create, edit, or delete these components in your storage system.

- [Tabs](#) on page 105
- [Subnet tab](#) on page 105
- [Network Interfaces tab](#) on page 106
- [Ethernet Ports tab](#) on page 107
- [Broadcast Domain tab](#) on page 109
- [FC/FCoE Adapters tab](#) on page 109
- [IPspaces tab](#) on page 110



**Tabs****Subnet**

Enables you to view a list of subnets, and create, edit, or delete subnets from your storage system.

**Network Interfaces**

Enables you to view a list of network interfaces, create, edit, or delete interfaces from your storage system, migrate the LIFs, change the status of the interface, and send the interface back to the home port.

**Ethernet Ports**

Enables you to view and edit the ports of a cluster, and create, edit, or delete interface groups and VLAN ports.

**Broadcast Domains**

Enables you to view a list of broadcast domains, and create, edit, or delete domains from your storage system.

**FC/FCoE Adapters**

Enables you to view the ports in a cluster, and edit the FC/FCoE adapter settings.

**IPspaces**

Enables you to view a list of IPspaces and broadcast domains, and create, edit, or delete an IPspace from your storage system.

**Subnet tab****Command buttons****Create**

Opens the Create Subnet dialog box, which enables you to create new subnets that contain configuration information for creating a network interface.

**Edit**

Opens the Edit Subnet dialog box, which enables you to modify certain attributes of a subnet such as the name, subnet address, range of IP addresses, and gateway details.

**Delete**

Deletes the selected subnet.

**Refresh**

Updates the information in the window.

**Subnet list****Name**

Specifies the name of the subnet.

**Subnet IP/Subnet mask**

Specifies the subnet address details.

**Gateway**

Specifies the IP address of the gateway.

**Available**

Specifies the number of IP addresses available in the subnet.

**Used**

Specifies the number of IP addresses used in the subnet.

**Total Count**

Specifies the total number of IP addresses (available and used) in the subnet.

**Broadcast domain**

Specifies the broadcast domain to which the subnet belongs.

**IPspace**

Specifies the IPspace to which the subnet belongs.

**Details area**

The area below the subnet list displays detailed information about the selected subnet, including the subnet range and a graph showing the available, used, and total number of IP addresses.

**Network Interfaces tab**

- For cluster LIFs and node management LIFs, you cannot use System Manager to perform the following actions:
  - Create, edit, delete, enable, or disable the LIFs
  - Migrate the LIFs or send the LIFs back to the home port
- For cluster management LIFs, you can use System Manager to migrate the LIFs, or send the LIFs back to the home port.  
However, you cannot create, edit, delete, enable, or disable the LIFs.
- For intercluster LIFs, you can use System Manager to create, edit, delete, enable, or disable the LIFs.  
However, you cannot migrate the LIFs, or send the LIFs back to the home port.
- You cannot create, edit, or delete network interfaces in the following configurations:
  - A MetroCluster configuration
  - SVMs configured for disaster recovery (DR).

**Command buttons****Create**

Opens the Create Network Interface dialog box, which enables you to create network interfaces and intercluster LIFs to serve data and manage SVMs.

**Edit**

Opens the Edit Network Interface dialog box, which you can use to enable management access for a data LIF.

**Delete**

Deletes the selected network interface.

This button is enabled only if the data LIF is disabled.

**Status**

Open the drop-down menu, which provides the option to enable or disable the selected network interface.

**Migrate**

Enables you to migrate a data LIF or a cluster management LIF to a different port on the same node or a different node within the cluster.

**Send to Home**

Enables you to host the LIF back on its home port.

This command button is enabled only when the selected interface is hosted on a non-home port and when the home port is available.

This command button is disabled when any node in the cluster is down.

### **Refresh**

Updates the information in the window.

### **Interface list**

You can move the pointer over the color-coded icon to view the operational status of the interface:

- Green specifies that the interface is enabled.
- Red specifies that the interface is disabled.

### **Interface Name**

Specifies the name of the network interface.

### **Storage Virtual Machine**

Specifies the SVM to which the interface belongs.

### **IP Address/WWPN**

Specifies the IP address or WWPN of the interface.

### **Current Port**

Specifies the name of the node and port on which the interface is hosted.

### **Data Protocol Access**

Specifies the protocol used to access data.

### **Management Access**

Specifies whether management access is enabled on the interface.

### **Subnet**

Specifies the subnet to which the interface belongs.

### **Role**

Specifies the operational role of the interface, which can be data, intercluster, cluster, cluster management, or node management.

### **Details area**

The area below the interface list displays detailed information about the selected interface: failover properties such as the home port, current port, speed of the ports, failover policy, failover group, and failover state, and general properties such as the administrative status, role, IPspace, broadcast domain, network mask, gateway, and DDNS status.

### **Ethernet Ports tab**

#### **Command buttons**

##### **Create Interface Group**

Opens the Create Interface Group dialog box, which enables you create interface groups by choosing the ports, and determining the use of ports and network traffic distribution.

##### **Create VLAN**

Opens the Create VLAN dialog box, which enables you to create a VLAN by choosing an Ethernet port or an interface group, and adding VLAN tags.

**Edit**

Opens one of the following dialog boxes:

- Edit Ethernet Port dialog box: Enables you to modify Ethernet port settings.
- Edit VLAN dialog box: Enables you to modify VLAN settings.
- Edit Interface Group dialog box: Enables you to modify interface groups.

You can only edit VLANs that are not associated with a broadcast domain.

**Delete**

Opens one of the following dialog boxes:

- Delete VLAN dialog box: Enables you to delete a VLAN.
- Delete Interface Group dialog box: Enables you to delete an interface group.

**Refresh**

Updates the information in the window.

**Ports list**

You can move the pointer over the color-coded icon to view the operational status of the port:

- Green specifies that the port is enabled.
- Red specifies that the port is disabled.

**Port**

Displays the port name of the physical port, VLAN port, or the interface group.

**Node**

Displays the node on which the physical interface is located.

**Broadcast Domain**

Displays the broadcast domain of the port.

**IPspace**

Displays the IPspace to which the port belongs.

**Type**

Displays the type of the interface such as interface group, physical interface, or VLAN.

**Details area**

The area below the ports list displays detailed information about the port properties.

**Details tab**

Displays administrative details and operational details.

As part of the operational details, the tab displays the health status of the ports. The ports can be healthy or degraded. A degraded port is a port on which continuous network fluctuations occur, or a port that has no connectivity to any other ports in the same broadcast domain.

In addition, the tab also displays the interface name, SVM details, and IP address details of the network interfaces that are hosted on the selected port. It also indicates whether the interface is at the home port or not.

**Performance tab**

Displays performance metrics graphs of the ethernet ports, including error rate and throughput.

Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You should refresh your browser to view the updated graphs.

## **Broadcast Domain tab**

### **Command buttons**

#### **Create**

Opens the Create Broadcast Domain dialog box, which enables you to create new broadcast domains to contain ports.

#### **Edit**

Opens the Edit Broadcast Domain dialog box, which enables you to modify the attributes of a broadcast domain, such as the name, MTU size, and associated ports.

#### **Delete**

Deletes the selected broadcast domain.

#### **Refresh**

Updates the information in the window.

## **Broadcast domain list**

### **Broadcast Domain**

Specifies the name of the broadcast domain.

### **MTU**

Specifies the MTU size.

### **IPspace**

Specifies the IPspace.

### **Combined Port Update Status**

Specifies the status of the port updates when you create or edit a broadcast domain. Any errors in the port updates are displayed in a separate window, which you can open by clicking the associated link.

## **Details area**

The area below the broadcast domain list displays all the ports in a broadcast domain. In a non-default IPspace, if a broadcast domain has ports with update errors, such ports are not displayed in the details area. You can move the pointer over the color-coded icon to view the operational status of the ports:

- Green specifies that the port is enabled.
- Red specifies that the port is disabled.

## **FC/FCoE Adapters tab**

### **Command buttons**

#### **Edit**

Opens the Edit FC/FCoE Settings dialog box, which enables you to modify the speed of the adapter.

#### **Status**

Enables you to bring the adapter online or take it offline.

**Refresh**

Updates the information in the window.

**FC/FCoE adapters list****WWNN**

Specifies the unique identifier of the FC/FCoE adapter.

**Node Name**

Specifies the name of the node that is using the adapter.

**Slot**

Specifies the slot that is using the adapter.

**WWPN**

Specifies the FC worldwide port name (WWPN) of the adapter.

**Status**

Specifies whether the status of the adapter is online or offline.

**Speed**

Specifies whether the speed settings are automatic or manual.

**Details area**

The area below the FC/FCoE adapters list displays detailed information about the selected adapters.

**Details tab**

Displays adapter details such as the media type, port address, data link rate, connection status, operation status, fabric status, and the speed of the adapter.

**Performance tab**

Displays performance metrics graphs of the FC/FCoE adapter, including IOPS and response time.

Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You should refresh your browser to see the updated graphs.

**IPspaces tab****Command buttons****Create**

Opens the Create IPspace dialog box, which enables you to create a new IPspace.

**Edit**

Opens the Edit IPspace dialog box, which enables you to rename an existing IPspace.

**Delete**

Deletes the selected IPspace.

**Refresh**

Updates the information in the window.

**IPspaces list****Name**

Specifies the name of the IPspace.

**Broadcast Domains**

Specifies the broadcast domain.

## Details area

The area below the IPspaces list displays the list of Storage Virtual Machines (SVMs) in the selected IPspace.

## Related tasks

- [\*Creating network interfaces\*](#) on page 94
- [\*Editing network interfaces\*](#) on page 96
- [\*Deleting network interfaces\*](#) on page 96
- [\*Creating subnets\*](#) on page 37
- [\*Editing subnets\*](#) on page 93
- [\*Deleting subnets\*](#) on page 94
- [\*Creating VLAN interfaces\*](#) on page 100
- [\*Creating interface groups\*](#) on page 100
- [\*Editing the FC/FCoE adapter speed\*](#) on page 104
- [\*Editing interface group settings\*](#) on page 101
- [\*Deleting VLANs\*](#) on page 102
- [\*Creating broadcast domains\*](#) on page 36
- [\*Editing broadcast domains\*](#) on page 92
- [\*Deleting broadcast domains\*](#) on page 92
- [\*Setting up a network when an IP address range is disabled\*](#) on page 26

## Managing physical storage

---

You can use System Manager to manage physical storage such as aggregates, storage pools, disks, array LUNs, nodes, Flash Cache, events, system alerts, AutoSupport notifications, jobs, and Flash Pool statistics.

### Aggregates

You can use System Manager to create aggregates to support the differing security, backup, performance, and data sharing requirements of your users.

### Editing aggregates

You can use System Manager to change the aggregate name, RAID type, and RAID group size of an existing aggregate when required.

#### Before you begin

For modifying the RAID type of an aggregate from RAID4 to RAID-DP, the aggregate must contain enough compatible spare disks, excluding the hot spares.

#### About this task

- You cannot change the RAID group of ONTAP systems that support array LUNs. RAID0 is the only available option.
- You cannot change the RAID type of partitioned disks. RAID-DP is the only option that is available for partitioned disks.
- You cannot rename a SnapLock Compliance aggregate.
- If the aggregate consists of SSDs with storage pool, you can modify only the name of the aggregate.
- If the triple parity disk size is 10 TB, and the other disks are smaller than 10 TB in size, then you can select RAID-DP or RAID-TEC as the RAID type.
- If the triple parity disk size is 10 TB, and if even one of the other disks is larger than 10 TB in size, then RAID-TEC is the only available option for RAID type.

#### Steps

1. Click **Hardware and Diagnostics > Aggregates**.
2. In the **Aggregates** window, select the aggregate that you want to edit, and then click **Edit**.
3. In the **Edit Aggregate** dialog box, modify the aggregate name, the RAID type, and the RAID group size, as required.
4. Click **Save**.

#### Related concepts

[What compatible spare disks are](#) on page 121



### Related references

[Aggregates window](#) on page 124

## Deleting aggregates

You can use System Manager to delete aggregates when you no longer require the data in the aggregates. However, you cannot delete the root aggregate because it contains the root volume, which contains the system configuration information.

### Before you begin

- All the FlexVol volumes or the Infinite Volume and the associated Storage Virtual Machines (SVMs) contained by the aggregate must be deleted.
- The aggregate must be offline.

### Steps

1. Click **Hardware and Diagnostics > Aggregates**.
2. Select one or more aggregates that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.
4. Verify that the deleted aggregates are no longer displayed in the **Aggregates** window.

### Related references

[Aggregates window](#) on page 124

## Changing the RAID configuration when creating an aggregate

While creating a new aggregate, you can modify the default values of the RAID type and RAID group size options of the aggregate by using System Manager.

### About this task

If the disk type of the aggregate disks is FSAS or MSATA, and the disk size is equal to or larger than 10 TB, then RAID-TEC is the only option available for RAID type.

### Steps

1. Click **Hardware and Diagnostics > Aggregates**.
2. In the **Aggregates** window, click **Create**.
3. In the **Create Aggregate** dialog box, perform the following steps:
  - a. Click **Change**.
  - b. In the **Change RAID Configuration** dialog box, specify the RAID type and RAID group size.

RAID-DP is the only supported RAID type for shared disks.

The recommended RAID group size is 12 disks through 20 disks for HDDs, and 20 disks through 28 disks for SSDs.
  - c. Click **Save**.

## Provisioning cache by adding SSDs

You can use System Manager to add SSDs as either storage pools or dedicated SSDs to provision cache. By adding SSDs, you can convert a non-root aggregate or a root aggregate that does not contain partitioned disks to a Flash Pool aggregate, or increase the cache size of an existing Flash Pool aggregate.

### About this task

- The added SSD cache does not add to the size of the aggregate, and you can add an SSD RAID group to an aggregate even when it is at the maximum size.
- You cannot use partitioned SSDs when you add cache by using System Manager.

### Related concepts

[How storage pool works](#) on page 132

## Provisioning cache to aggregates by adding SSDs

You can use System Manager to add storage pools or dedicated SSDs to provision cache by converting an existing non-root HDD aggregate or a root aggregate that does not contain partitioned disks to a Flash Pool aggregate.

### Before you begin

- The aggregate must be online.
- There must be sufficient spare SSDs or allocation units in the storage pool that can be assigned as cache disks.
- All nodes in the cluster must be running ONTAP 8.3 or later.  
If the cluster is in a mixed-version state, you can use the command-line interface to create a Flash Pool aggregate and provide SSD cache.
- You must have identified a valid 64-bit non-root aggregate composed of HDDs that can be converted to a Flash Pool aggregate.
- The aggregate must not contain any array LUNs.
- The aggregate must not provision storage to an Infinite Volume.
- You must be aware of platform-specific and workload-specific best practices for Flash Pool aggregate SSD tier size and configuration.

### Steps

1. Click **Hardware and Diagnostics > Aggregates**.
2. In the **Aggregates** window, select the aggregate, and then click **Add Cache**.
3. In the **Add Cache** dialog box, perform the appropriate action:

If you select the cache source as...	Do this...
Storage pools	<ol style="list-style-type: none"> <li>a. Select the storage pool from which cache can be obtained.</li> <li>b. Specify the cache size.</li> <li>c. Modify the RAID type, if required.</li> </ol>

If you select the cache source as...	Do this...
Dedicated SSDs	<p>Select the SSD size and the number of SSDs to include, and optionally modify the RAID configuration:</p> <ol style="list-style-type: none"> <li>Click <b>Change</b>.</li> <li>In the Change RAID Configuration dialog box, specify the RAID type and RAID group size, and then click <b>Save</b>.</li> </ol>

4. Click **Add**.

For mirrored aggregates, an Add Cache dialog box is displayed with the information that twice the number of selected disks will be added.

5. In the **Add Cache** dialog box, click **Yes**.

### Result

The cache disks are added to the selected aggregate. The updated information is displayed in the **Details** tab of the Aggregates window.

### Related information

[NetApp Technical Report 4070: Flash Pool Design and Implementation Guide](#)

## Increasing the cache for Flash Pool aggregates by adding SSDs

You can add SSDs as either storage pools or dedicated SSDs to increase the size of a Flash Pool aggregate by using System Manager.

### Before you begin

- The Flash Pool aggregate must be online.
- There must be sufficient spare SSDs or allocation units in the storage pool that can be assigned as cache disks.

### Steps

- Click **Hardware and Diagnostics > Aggregates**.
- In the **Aggregates** window, select the Flash Pool aggregate, and then click **Add Cache**.
- In the **Add Cache** dialog box, perform the appropriate action:

If you selected the cache source as...	Do this...
Storage pools	Select the storage pool from which cache can be obtained, and specify the cache size.
Dedicated SSDs	Select the SSD size and the number of SSDs to include.

4. Click **Add**.

For mirrored aggregates, an Add Cache dialog box is displayed with the information that twice the number of selected disks will be added.

5. In the **Add Cache** dialog box, click **Yes**.

**Result**

The cache disks are added to the selected Flash Pool aggregate. The updated information is displayed in the **Details** tab of the Aggregates window.

**Adding capacity disks**

You can increase the size of an existing non-root aggregate or a root aggregate containing disks by adding capacity disks. You can use System Manager to add HDDs or SSDs of the selected ONTAP disk type and to modify the RAID group options.

**Before you begin**

- The aggregate must be online.
- There must be sufficient compatible spare disks.

**About this task**

- It is a best practice to add disks that are of the same size as the other disks in the aggregate. If you add disks that are smaller in size than the other disks in the aggregate, the aggregate becomes suboptimal in configuration, which in turn can cause performance issues. If you add disks that are larger in size than the disks available in a pre-existing RAID group within the aggregate, then the disks are downsized, and their space is reduced to that of the other disks in that RAID group. If a new RAID group is created in the aggregate and similar size disks remain in the new RAID group, the disks will not be downsized. If you add disks that are not of the same size as the other disks in the aggregate, the selected disks might not be added; instead, other disks with a usable size between 90 percent and 105 percent of the specified size are automatically added. For example, for a 744 GB disk, all disks in the range of 669 GB through 781 GB are eligible for selection. For all the spare disks in this range, ONTAP first selects only partitioned disks, then selects only unpartitioned disks, and finally selects both partitioned disks and unpartitioned disks.
- You cannot use System Manager to add HDDs to the following configurations:
  - Aggregates containing only SSDs
  - Root aggregates containing partitioned disks

You must use the command-line interface to add HDDs to these configurations.

- For shared disks, RAID-DP is the only supported RAID type.
- You cannot use SSDs with storage pool.
- If the RAID type is RAID-DP, and if you are adding FSAS or MSATA type of disks that are equal to or larger than 10 TB in size, then you can add them only to **Specific RAID group**, and not to **New RAID group** or **All RAID groups**.  
The disks are added after downsizing the disk size to the size of the disks in the pre-existing RAID group of the existing aggregate.
- If the RAID group is RAID-TEC, and if you are adding FSAS or MSATA type of disks that are equal to or larger than 10 TB in size, then you can add them to **All RAID groups**, **New RAID group**, and **Specific RAID group**.  
The disks are added after downsizing the disk size to the size of the disks in the pre-existing RAID group of the existing aggregate.

**Steps**

1. Click **Hardware and Diagnostics > Aggregates**.

2. In the **Aggregates** window, select the aggregate to which you want to add capacity disks, and then click **Add Capacity**.
3. In the **Add Capacity** dialog box, perform the following steps:
  - a. Specify the disk type for the capacity disks by using the **Disk Type to Add** option.
  - b. Specify the number of capacity disks by using the **Number of Disks or Partitions** option.
4. Specify the RAID group to which the capacity disks are to be added by using the **Add Disks To** option.

By default, System Manager adds the capacity disks to **All RAID groups**.

- a. Click **Change**.
- b. In the **RAID Group Selection** dialog box, specify the RAID group as **New RAID group** or **Specific RAID group** by using the **Add Disks To** option.  
 Shared disks can be added only to the **New RAID group** option.
- c. Click **Save**.

5. Click **Add**.

For mirrored aggregates, an Add Capacity dialog box is displayed with the information that twice the number of selected disks will be added.

6. In the **Add Capacity** dialog box, click **Yes** to add the capacity disks.

### Result

The capacity disks are added to the selected aggregate, and the aggregate size is increased. The updated information is displayed in the **Details** tab of the Aggregates window.

### Related concepts

*What compatible spare disks are* on page 121

## Changing the RAID group when adding capacity disks

While adding capacity disks (HDDs) to an aggregate, you can change the RAID group to which you want to add the disks by using System Manager.

### About this task

- If the RAID type is RAID-DP, and if you are adding FSAS or MSATA type of disks that are equal to or larger than 10 TB in size, then you can add them only to **Specific RAID group**, and not to **New RAID group** or **All RAID groups**.

The disks are added after downsizing the disk size to the size of the existing aggregates.

- If the RAID group is RAID-TEC, and if you are adding FSAS or MSATA type of disks that are equal to or larger than 10 TB in size, then you can add them to **All RAID groups**, **New RAID group**, and **Specific RAID group**.

The disks are added after downsizing the disk size to the size of the existing aggregates.

### Steps

1. Click **Hardware and Diagnostics > Aggregates**.
2. In the **Aggregates** window, select the aggregate to which you want to add capacity disks, and then click **Add Capacity**.

3. In the **Add Capacity** dialog box, perform the following steps:
  - a. Click **Change**.
  - b. In the **Change RAID Configuration** dialog box, specify the RAID group to which you want to add the capacity disks.  
 You can change the default value **All RAID groups** to either **Specific RAID group** or **New RAID group**.
  - c. Click **Save**.

## Moving FlexVol volumes

You can nondisruptively move a FlexVol volume to a different aggregate or a node for capacity utilization and improved performance by using System Manager.

### Before you begin

If you are moving a data protection volume, data protection mirror relationships must be initialized before you move the volume.

### About this task

- When you move a volume that is hosted on a Flash Pool aggregate, only the data stored in the HDD tier is moved to the destination aggregate.  
 The cache data associated with the volume is not moved to the destination aggregate. Therefore, some performance degradation might occur after the volume move.  
 If the aggregate contains Infinite Volume constituents, the wizard does not display the constituents because you cannot use System Manager to move constituents of an Infinite Volume.
- You cannot move volumes from a SnapLock aggregate.

### Steps

1. Click **Hardware and Diagnostics > Aggregates**.
2. Select the aggregate that contains the volume, and then click **Volume Move**.
3. Type or select information as prompted by the wizard.
4. Confirm the details, and then click **Finish** to complete the wizard.

## Mirroring aggregates

You can use System Manager to protect data and provide increased resiliency by mirroring data in real-time, within a single aggregate. Mirroring aggregates removes single points of failure in connecting to disks and array LUNs.

### Before you begin

There must be sufficient free disks in the other pool to mirror the aggregate.

### About this task

You cannot mirror Flash Pool aggregate when the cache source is storage pools.

### Steps

1. Click **Hardware and Diagnostics > Aggregates**.

2. Select the aggregate that you want to mirror, and then click **Mirror**.
3. In the **Mirror this aggregate** dialog box, click **Mirror** to initiate the mirroring.

## Viewing aggregate information

You can use the Aggregates window in System Manager to view the name, status, and space information about an aggregate.

### Steps

1. Click **Hardware and Diagnostics > Aggregates**.
2. Select the aggregate that you want to view information about from the displayed list of aggregates.
3. Review the aggregate details in the **Aggregates** window.

## What aggregates are

To support the differing security, backup, performance, and data sharing needs of your users, you can group the physical data storage resources on your storage system into one or more aggregates. You can then design and configure these aggregates to provide the appropriate level of performance and redundancy.

Each aggregate has its own RAID configuration, plex structure, and set of assigned drives or array LUNs. The aggregate provides storage, based on its configuration, to its associated FlexVol volumes or Infinite Volume.

Aggregates have the following characteristics:

- They can be composed of drives or array LUNs.
- If they are composed of drives, they can be single-tier (composed of only HDDs or only SSDs) or they can be Flash Pool aggregates, which include both HDD RAID groups and an SSD cache.

The cluster administrator can assign one or more aggregates to a Storage Virtual Machine (SVM), in which case you can use only those aggregates to contain volumes for that SVM.

### Related information

[\*NetApp Technical Report 3437: Storage Subsystem Resiliency Guide\*](#)

## How RAID groups are named

Within each aggregate, RAID groups are named rg0, rg1, rg2, and so on in order of their creation. You cannot specify the names of RAID groups.

## How moving a FlexVol volume works

Knowing how moving a FlexVol volume works helps you to determine whether the volume move satisfies service-level agreements and to understand where a volume move is in the volume move process.

FlexVol volumes are moved from one aggregate or node to another within the same Storage Virtual Machine (SVM). A volume move does not disrupt client access during the move.

Moving a volume occurs in multiple phases:

- A new volume is made on the destination aggregate.
- The data from the original volume is copied to the new volume.  
During this time, the original volume is intact and available for clients to access.

- At the end of the move process, client access is temporarily blocked.  
During this time the system performs a final replication from the source volume to the destination volume, swaps the identities of the source and destination volumes, and changes the destination volume to the source volume.
- After completing the move, the system routes client traffic to the new source volume and resumes client access.

The move is not disruptive to client access because the time in which client access is blocked ends before clients notice a disruption and time out. Client access is blocked for 35 seconds by default. If the volume move operation cannot finish in the time that access is denied, the system aborts this final phase of the volume move operation and allows client access. The system attempts the final phase three times by default. After the third attempt, the system waits an hour before attempting the final phase sequence again. The system runs the final phase of the volume move operation until the volume move is complete.

## How Flash Pool aggregates work

In general, Flash Pool aggregates are used and managed in a similar manner as standard aggregates. However, you need to understand how both the SSD and HDD RAID groups interact and affect the rest of the system.

The SSD RAID groups, also called the *SSD cache*, can be composed of physical SSDs or allocation units from SSD storage pools (but not both).

The SSD cache does not contribute to the size of the aggregate as calculated against the maximum aggregate size. For example, even if an aggregate is at the maximum aggregate size, you can add an SSD RAID group to it. The SSDs *do* count toward the overall (node or HA pair) drive limit.

The HDD RAID groups in a Flash Pool aggregate behave the same as HDD RAID groups in a standard aggregate, following the same rules for mixing disk types, sizes, speeds, and checksums. For example, you cannot combine performance and capacity disks in the HDD RAID groups of a Flash Pool aggregate.

The checksum type, RAID type, and RAID group size values can be configured for the SSD cache RAID groups and HDD RAID groups independently. If the Flash Pool aggregate uses an SSD storage pool for its SSD cache, the cache RAID type can be changed only when the first SSD RAID groups are added, and the size of the SSD RAID groups are determined by the number of SSDs in the storage pool.

When you enable data compression manually for a volume in a Flash Pool aggregate, adaptive compression is enabled by default.

There is a platform-dependent maximum size for the SSD cache.

### Related information

[NetApp Hardware Universe](#)

## How you can use effective ONTAP disk type for mixing HDDs

Starting with Data ONTAP 8.1, certain ONTAP disk types are considered equivalent for the purposes of creating and adding to aggregates, and managing spares. ONTAP assigns an effective disk type for each disk type. You can mix HDDs that have the same effective disk type.

When the `raid.disktype.enable` option is set to **off**, you can mix certain types of HDDs within the same aggregate. When the `raid.disktype.enable` option is set to **on**, the effective disk type is the same as the ONTAP disk type. Aggregates can be created using only one disk type. The default value for the `raid.disktype.enable` option is **off**.



Starting with Data ONTAP 8.2, the option `raid.mix.hdd.disktype.capacity` must be set to **on** to mix disks of type BSAS, FSAS, and ATA. The option `raid.mix.hdd.disktype.performance` must be set to **on** to mix disks of type FCAL and SAS.

The following table shows how the disk types map to the effective disk type:

ONTAP disk type	Effective disk type
FCAL	SAS
SAS	SAS
ATA	FSAS
BSAS	FSAS
FCAL and SAS	SAS
MSATA	MSATA
FSAS	FSAS

## What compatible spare disks are

In System Manager, compatible spare disks are disks that match the properties of other disks in the aggregate. When you want to increase the size of an existing aggregate by adding HDDs (capacity disks) or change the RAID type of an aggregate from RAID4 to RAID-DP, the aggregate must contain sufficient compatible spare disks.

Disk properties that must match are the disk type, disk size (can be a higher size disk in case the same disk size is not available), disk RPM, checksum, node owner, pool, and shared disk properties. If you use higher sized disks, you must be aware that disk downsizing occurs and the size of all disks are reduced to the lowest disk size. Existing shared disks are matched with higher size non-shared disks, and the non-shared disks are converted to shared disks and added as spares.

If RAID mixing options, such as disk type mixing and disk RPM mixing, are enabled for the RAID group, the disk type and disk RPM of the existing disks of the aggregate are matched with the effective disk type and effective disk RPM of the spare disks to obtain compatible spares.

### Related tasks

[Adding capacity disks](#) on page 116

[Editing aggregates](#) on page 112

## How System Manager works with hot spares

A hot spare is a disk that is assigned to a storage system but not used by any RAID group. Hot spares do not contain any data and are assigned to a RAID group when a disk failure occurs in the RAID group. System Manager uses the largest disk as the hot spare.

When there are different disk types in the RAID group, the largest-sized disk of each disk type is left as the hot spare. For example, if there are 10 SATA disks and 10 SAS disks in the RAID group, the largest-sized SATA disk and the largest-sized SAS disk are serve as hot spares.

If the largest-sized disk is partitioned, then the hot spares are provided separately for partitioned and non-partitioned RAID groups. If the largest-sized disk is unpartitioned, then a single spare disk is provided.

The largest-sized non-partitioned disk is left as a hot spare if there are root partitions in the disk group. When a non-partitioned disk of the same size is not available, then spare root partitions are left as hot spares for the root partitioned group.

A single spare disk can serve as a hot spare for multiple RAID groups. System Manager calculates the hot spares based on the value set in the option `raid.min_spare_count` at the node level. For

example, if there are 10 SSDs in an SSD RAID group and the option `raid.min_spare_count` is set to **1** at the node level, System Manager leaves 1 SSD as the hot spare and uses the other 9 SSDs for SSD-related operations. Similarly, if there are 10 HDDs in an HDD RAID group and the option `raid.min_spare_count` is set to **2** at the node level, System Manager leaves 2 HDDs as hot spares and uses the other 8 HDDs for HDD-related operations.

System Manager enforces the hot spare rule for RAID groups when you create an aggregate, edit an aggregate, and when you add HDDs or SSDs to an aggregate. The hot spare rule is also used when you create a storage pool or add disks to an existing storage pool.

There are exceptions to the hot spare rule in System Manager:

- For MSATA or disks in a multi-disk carrier, the number of hot spares is twice the value set at the node level and the number must not be less than 2 at any time.
- Hot spares are not used if the disks are part of array LUNs or virtual storage appliances.

## Rules for displaying disk types and disk RPM

When you are creating an aggregate and adding capacity disks to an aggregate, you should understand the rules that apply when disk types and disk RPM are displayed.

When the disk type mixing and the disk RPM mixing options are not enabled, the actual disk type and actual disk RPM are displayed.

When these mixing options are enabled, the effective disk type and effective disk RPM are displayed instead of the actual disk type and actual disk RPM. For example, when the disk mixing option is enabled, System Manager displays BSAS disks as FSAS. Similarly, when the disk RPM mixing option is enabled, if the RPM of the disks is 10K and 15K, System Manager displays the effective RPM as 10K.

## Aggregate requirements for Infinite Volumes

The aggregates that are used by an Infinite Volume should be larger than 100 TB with a minimum of 1.1 TB of available space. If the Infinite Volume uses storage classes, the aggregates must also meet the requirements of the storage class.

If an aggregate has less than 1.1 TB of available space, it is not used by the Storage Virtual Machine (SVM) with Infinite Volume.

If the Infinite Volume uses storage classes, aggregates must meet the requirements of the storage class to be used. For example, if the storage class is designated to use aggregates of type **SAS**, aggregates created for that storage class must consist entirely of **SAS** disks.

### Related tasks

[Creating an Infinite Volume](#) on page 52

## What a namespace constituent is

Each Infinite Volume has a single namespace constituent that maps directory information and file names to the file's physical data location within the Infinite Volume.

Clients are not aware of the namespace constituent and do not interact directly with it. The namespace constituent is an internal component of the Infinite Volume.

## Aggregate requirements for destination Infinite Volumes

Before you create a destination Infinite Volume for a data protection mirror relationship with an Infinite Volume, you must create enough aggregate space in the destination cluster for the destination Infinite Volume to use.

An Infinite Volume spans several aggregates, and aggregates are automatically selected for a destination Infinite Volume when you initialize a data protection mirror relationship. If the data protection mirror relationship cannot be initialized because of insufficient aggregate space, you receive an error message that informs you how to adjust aggregate space before trying the operation again.

You should use the following guidelines to create aggregates for destination Infinite Volumes:

- The destination Infinite Volume and source Infinite Volume should have the same number of aggregates.  
For example, if the source Infinite Volume uses four aggregates, you should create four aggregates for the destination Infinite Volume. The same number of aggregates for the source and destination Infinite Volumes is recommended, but not required.
- The aggregates for the destination Infinite Volume must have enough space to contain a mirror copy of the source Infinite Volume.
- The aggregates must meet the requirements of the storage classes used by the source Infinite Volume, if the source Infinite Volume uses storage classes.

**Note:** The size of the destination Infinite Volume must be equal to or larger than the size of the source Infinite Volume to successfully create a data protection mirror relationship.

## How mirrored aggregates work

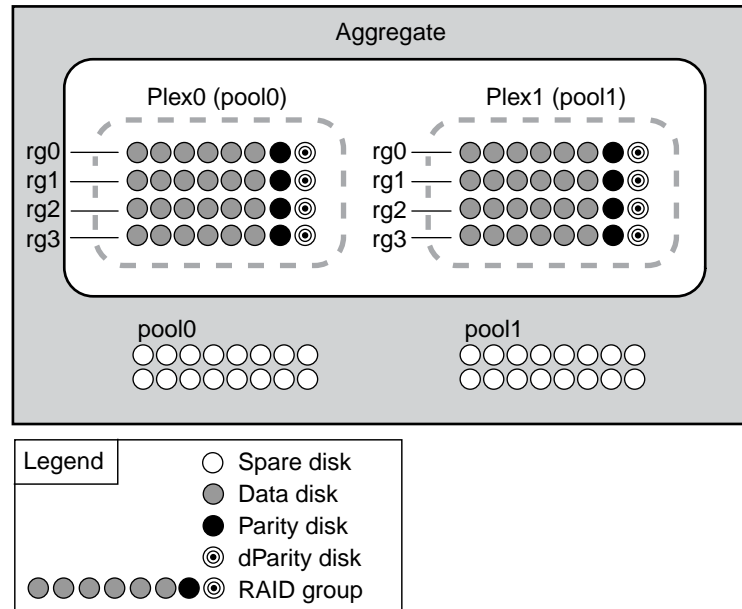
Mirrored aggregates have two *plexes* (copies of their data), which use the SyncMirror functionality to duplicate the data to provide redundancy.

When a mirrored aggregate is created (or when a second plex is added to an existing unmirrored aggregate), Data ONTAP copies the data in the original plex (plex0) to the new plex (plex1). The plexes are physically separated (each plex has its own RAID groups and its own pool), and the plexes are updated simultaneously. This provides added protection against data loss if more disks fail than the RAID level of the aggregate protects against or there is a loss of connectivity, because the unaffected plex continues to serve data while you fix the cause of the failure. After the plex that had a problem is fixed, the two plexes resynchronize and reestablish the mirror relationship.

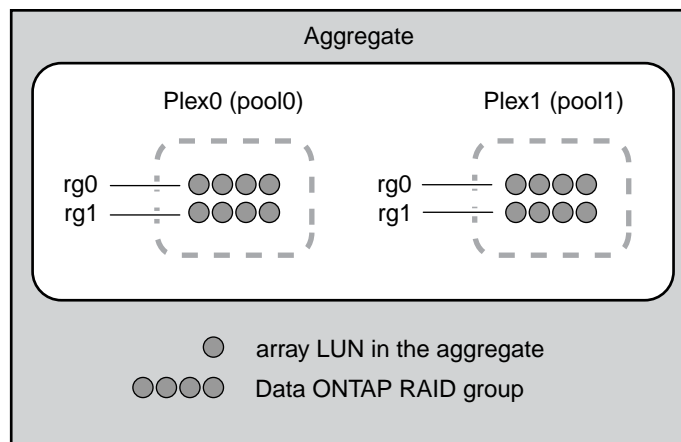
**Note:** The time for the two plexes to resynchronize can vary and depends on many variables such as aggregate size, system load, how much data has changed, and so on.

The disks and array LUNs on the system are divided into two pools: pool0 and pool1. Plex0 gets its storage from pool0 and plex1 gets its storage from pool1.

The following diagram shows an aggregate composed of disks with SyncMirror enabled and implemented. A second plex has been created for the aggregate, plex1. The data in plex1 is a copy of the data in plex0, and the RAID groups are also identical. The 32 spare disks are allocated to pool0 or pool1, 16 disks for each pool.



The following diagram shows an aggregate composed of array LUNs with SyncMirror enabled and implemented. A second plex has been created for the aggregate, plex1. Plex1 is a copy of plex0, and the RAID groups are also identical.



## Aggregates window

You can use the Aggregates window to create, display, and manage information about aggregates.

- [Aggregates window](#) on page 124
- [Aggregate list](#) on page 125
- [Details area](#) on page 126
- [Command buttons](#) on page 125

You cannot use System Manager to create or edit aggregates in a MetroCluster configuration. However, you can manage aggregates (view the aggregate information, delete the aggregate, change the status of the aggregate, and move a FlexVol volume) in a MetroCluster configuration.

## Command buttons

### Create

Opens the Create Aggregate dialog box, which enables you to create an aggregate.

### Edit

Opens the Edit Aggregate dialog box, which enables you to change the name of an aggregate or the level of RAID protection that you want to provide for this aggregate.

### Add Capacity

Opens the Add Capacity dialog box, which enables you to add capacity (HDDs or SSDs) to existing aggregates.

### Add Cache

Opens the Add Cache dialog box, which enables you to add cache disks (SSDs) to existing HDD aggregates or Flash Pool aggregates.

This button is not available for a cluster containing nodes with All Flash Optimized personality.

### Delete

Deletes the selected aggregate.

**Note:** This button is disabled for the root aggregate.

### Status

Displays the status of the selected aggregate. The status can be one of the following:

- Online  
Read and write access to volumes contained in this aggregate is allowed.
- Offline  
Some operations—such as parity reconstruction—are allowed, but data access is not allowed.
- Restrict  
No read or write access is allowed.

### Volume Move

Starts the Volume Move wizard, which enables you to move a FlexVol volume.

### Mirror

Opens the Mirror dialog box, requesting confirmation to mirror the aggregates.

### Refresh

Updates the information in the window.

## Aggregate list

Displays the name and the space usage information for each aggregate.

### Name

Displays the name of the aggregate.

### Node

Displays the name of the node to which the disks of the aggregate are assigned.

This field is available only at the cluster level.

### Type

Displays the type of aggregate.

This field is not displayed for a cluster containing nodes with All Flash Optimized personality.

**Used (%)**

Displays the percentage of space used in the aggregate.

**Available Space**

Displays the available space in the aggregate.

**Used Space**

Displays the amount of space that is used for data in the aggregate.

**Physical Space Used**

Displays the sum of the used physical capacity represented by all files and LUNs attached to the aggregate.

**Total Space**

Displays the total space of the aggregate.

**Volume Count**

Displays the number of volumes that are associated with the aggregate.

**Disk Count**

Displays the number of disks that are used to create the aggregate.

**Flash Pool**

Displays the total cache size of the Flash Pool aggregate. A value of NA indicates that the aggregate is not a Flash Pool aggregate.

This field is not displayed for a cluster containing nodes with All Flash Optimized personality.

**Mirrored**

Displays whether the aggregate is mirrored.

**SnapLock Type**

Displays the SnapLock type of the aggregate.

**Details area**

The area below the Aggregate list displays detailed information about the selected aggregate.

**Details tab**

Displays detailed information about the selected aggregate, such as the name of the aggregate, status, RAID type, whether the aggregate is a root aggregate, number of files in the aggregate, maximum number of files in the aggregate, checksum, total cache size, whether the aggregate is a 64-bit aggregate, and whether the aggregate is a Flash Pool aggregate.

**Volumes tab**

Displays details about the total number of volumes on the aggregate, total aggregate space, and the space committed to the aggregate. The total committed space is the sum of the total size of all the volumes (online and offline) and the Snapshot reserve space of the online volumes.

Details about the names of the volumes on the aggregate, Storage Virtual Machines (SVMs), available space, total space, and the percentage of space utilization of each volume on the selected aggregate are also displayed.

**Disk Layout tab**

Displays disk layout information, such as the name of the disk, disk type, physical size, usable size, disk position, disk status, plex name, plex status, RAID group, RAID type,

and storage pool (if any) for the selected aggregate. The disk port that is associated with the disk primary path and the disk name with the disk secondary path for a multipath configuration are also displayed.

#### Performance tab

Displays graphs that show the performance metrics of the aggregates, including total transfers, IOPS, and write workload impact. Performance metrics data for read, write, and total transfers is displayed, and the data for SSDs and HDDs is recorded separately. Performance metrics data for the impact of write workload to “nvlog” and dirty buffer is also displayed.

Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You must refresh your browser to see the updated graphs.

#### Efficiency tab

Displays the storage efficiency savings for the aggregate. You can view the total logical space used, total physical space used, overall savings from storage efficiency, volume data reduction ratio, aggregate data reduction ratio, and ratio of FlexClone volumes and Snapshot copies.

#### Related tasks

[Provisioning storage through aggregates](#) on page 38

[Deleting aggregates](#) on page 113

[Editing aggregates](#) on page 112

## Storage pools

You can use System Manager to create storage pools to enable SSDs to be shared by multiple Flash Pool aggregates.

### Creating a storage pool

A storage pool is a collection of SSDs (cache disks). You can use System Manager to combine SSDs to create a storage pool, which enables you to share the SSDs and SSD spares between an HA pair for allocation to two or more Flash Pool aggregates at the same time.

#### Before you begin

- Both nodes of the HA pair must be up and running in order to allocate SSDs and SSD spares through a storage pool.
- Storage pools must have a minimum of 3 SSDs.
- All SSDs in a storage pool must be owned by the same HA pair.

#### About this task

System Manager enforces the hot spare rule for SSD RAID groups when you use SSDs for adding disks to a storage pool. For example, if there are 10 SSDs in the SSD RAID group and the option `raid.min_spare_count` is set to 1 at the node level, System Manager leaves 1 SSD as the hot spare and uses the other 9 SSDs for SSD-related operations.

You cannot use partitioned SSDs when creating a storage pool by using System Manager.

#### Steps

1. Click **Hardware and Diagnostics > Storage Pools**.

2. In the **Storage Pools** window, click **Create**.
3. In the **Create Storage Pool** dialog box, specify the name for the storage pool, disk size, and the number of disks.
4. Click **Create**.

#### Related references

[Storage Pools window](#) on page 132

## Adding disks to a storage pool

You can add SSDs to an existing storage pool and increase its cache size by using System Manager.

#### Before you begin

Both nodes of the HA pair must be up and running in order to allocate SSDs and SSD spares through a storage pool.

#### About this task

- The SSDs that you add to a storage pool are distributed proportionally among the aggregates using the storage pool cache and to the free space of the storage pool.
- System Manager enforces the hot spare rule for SSD RAID groups when you use SSDs for adding disks to a storage pool.  
For example, if there are 10 SSDs in the SSD RAID group and the option `raid.min_spare_count` is set to 1 at the node level, System Manager leaves 1 SSD as the hot spare and uses the other 9 SSDs for SSD-related operations.
- You cannot use partitioned SSDs when adding disks to a storage pool by using System Manager.

#### Steps

1. Click **Hardware and Diagnostics > Storage Pools**.
2. In the **Storage Pools** window, select the storage pool, and then click **Add Disks**.
3. In the **Add Disks** dialog box, specify the number of disks that you want to add.
4. Click **Next**.
5. In the **Summary** dialog box, review how the cache is distributed among various aggregates and the free space of the storage pool.
6. Click **Add**.

#### Related references

[Storage Pools window](#) on page 132

## Deleting storage pools

You might want to delete a storage pool when the cache of the storage pool is not optimal or when it is no longer used by any aggregate or Flash Pool aggregate. You can delete a storage pool by using the Delete Storage Pool dialog box in System Manager.

#### Before you begin

The storage pool must not be used by any aggregate.



### Steps

1. Click **Hardware and Diagnostics > Storage Pools**.
2. In the **Storage Pools** window, select the storage pool that you want to delete, and then click **Delete**.
3. In the **Delete Storage Pool** dialog box, click **Delete**.

### Related references

[Storage Pools window](#) on page 132

## How you use SSD storage pools

To enable SSDs to be shared by multiple Flash Pool aggregates, you place them in a *storage pool*. After you add an SSD to a storage pool, you can no longer manage it as a stand-alone entity—you must use the storage pool to assign or allocate the storage provided by the SSD.

You create storage pools for a specific HA pair. Then, you add allocation units from that storage pool to one or more Flash Pool aggregates owned by the same HA pair. Just as disks must be owned by the same node that owns an aggregate before they can be allocated to it, storage pools can provide storage only to Flash Pool aggregates owned by one of the nodes that owns the storage pool.

If you need to increase the amount of Flash Pool cache on your system, you can add more SSDs to a storage pool, up to the maximum RAID group size for the RAID type of the Flash Pool caches using the storage pool. When you add an SSD to an existing storage pool, you increase the size of the storage pool's allocation units, including any allocation units that are already allocated to a Flash Pool aggregate.

You can use only one spare SSD for a storage pool, so that if an SSD in that storage pool becomes unavailable, Data ONTAP can use the spare SSD to reconstruct the partitions of the malfunctioning SSD. You do not need to reserve any allocation units as spare capacity; Data ONTAP can use only a full, unpartitioned SSD as a spare for SSDs in a storage pool.

After you add an SSD to a storage pool, you cannot remove it, just as you cannot remove disks from an aggregate. If you want to use the SSDs in a storage pool as discrete drives again, you must destroy all Flash Pool aggregates to which the storage pool's allocation units have been allocated, and then destroy the storage pool.

## How Flash Pool SSD partitioning increases cache allocation flexibility for Flash Pool aggregates

Flash Pool SSD partitioning, also known as *Advanced Drive Partitioning*, enables you to group SSDs together into an *SSD storage pool* that can be allocated to multiple Flash Pool aggregates. This amortizes the cost of the parity SSDs over more aggregates, increases SSD allocation flexibility, and maximizes SSD performance .

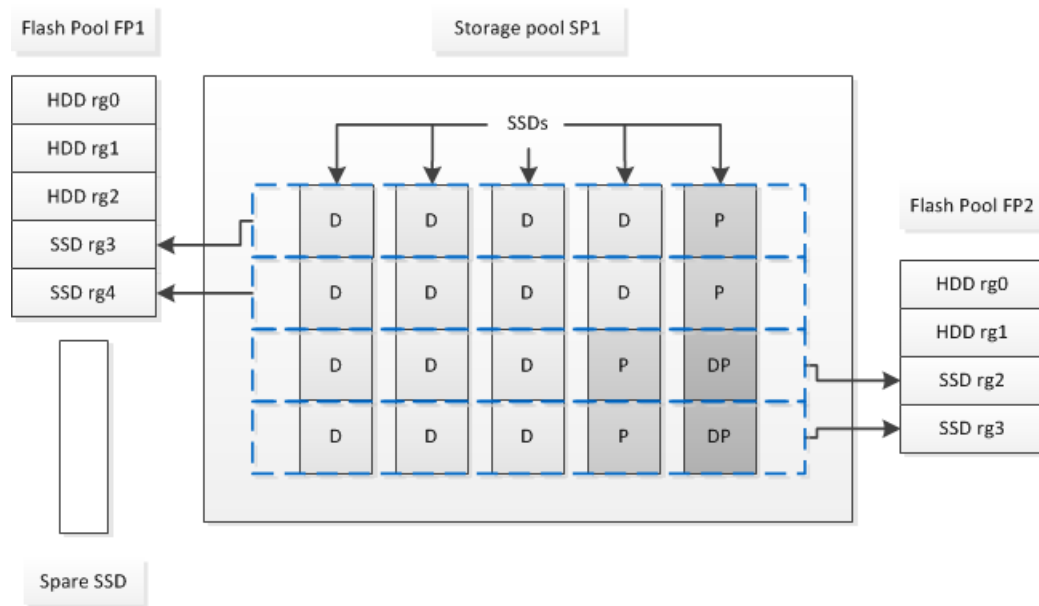
The storage pool is associated with an HA pair, and can be composed of SSDs owned by either node in the HA pair.

When you add an SSD to a storage pool, it becomes a *shared SSD*, and it is divided into 4 partitions.

Storage from an SSD storage pool is divided into *allocation units*, each of which represents 25% of the total storage capacity of the storage pool. Allocation units contain one partition from each SSD in the storage pool, and are added to a Flash Pool cache as a single RAID group. By default, for storage pools associated with an HA pair, two allocation units are assigned to each of the HA partners, but you can reassign the allocation units to the other HA partner if needed (allocation units must be owned by the node that owns the aggregate).

SSD storage pools do not have a RAID type. When an allocation unit is added to a Flash Pool aggregate, the appropriate number of partitions are designated to provide parity to that RAID group.

The following diagram shows one example of Flash Pool SSD partitioning. The SSD storage pool pictured is providing cache to two Flash Pool aggregates:



Storage pool SP1 is composed of 5 SSDs; in addition, there is one hot spare SSD available to replace any SSD that experiences a failure. Two of the storage pool's allocation units are allocated to Flash Pool FP1, and two are allocated to Flash Pool FP2. FP1 has a cache RAID type of RAID4, so the allocation units provided to FP1 contain only one partition designated for parity. FP2 has a cache RAID type of RAID-DP, so the allocation units provided to FP2 include a parity partition and a double-parity partition.

In this example, two allocation units are allocated to each Flash Pool aggregate; however, if one Flash Pool aggregate needed a larger cache, you could allocate three of the allocation units to that Flash Pool aggregate, and only one to the other.

## Requirements and best practices for using SSD storage pools

There are some technologies that cannot be combined with Flash Pool aggregates that use SSD storage pools.

You cannot use the following technologies with Flash Pool aggregates that use SSD storage pools for their cache storage:

- MetroCluster
- SyncMirror
- Mirrored aggregates can coexist with Flash Pool aggregates that use storage pools; however, Flash Pool aggregates cannot be mirrored.
- Physical SSDs
- Flash Pool aggregates can use SSD storage pools or physical SSDs, but not both.

SSD storage pools must conform to the following rules:

- SSD storage pools can contain only SSDs; HDDs cannot be added to an SSD storage pool.
- SSD storage pools can contain between 3 and 28 SSDs.
- If an SSD storage pool contains more SSDs than the maximum RAID4 RAID group size for SSDs, then it cannot be used for a Flash Pool aggregate whose cache has a RAID type of RAID4.

- All SSDs in an SSD storage pool must be owned by the same HA pair.
- You cannot use SSDs that have been partitioned for root-data partitioning in a storage pool.

If you provide storage from a single storage pool to two caches with different RAID types, and you expand the size of the storage pool beyond the maximum RAID group size for RAID4, the extra partitions in the RAID4 allocation units go unused. For this reason, it is a best practice to keep your cache RAID types homogenous for a storage pool.

You cannot change the RAID type of cache RAID groups allocated from a storage pool. You set the RAID type for the cache before adding the first allocation units, and you cannot change it later.

When you create a storage pool or add SSDs to an existing storage pool, you must use the same size SSDs. If a failure occurs and no spare of the correct size exists, Data ONTAP can use a larger SSD to replace the failed SSD. However, the larger SSD is right-sized to match the size of the other SSDs in the storage pool, resulting in lost SSD capacity.

You can use only one spare SSD for a storage pool. If the storage pool provides allocation units to Flash Pool aggregates owned by both nodes in the HA pair, then the spare SSD can be owned by either node. However, if the storage pool provides allocation units only to Flash Pool aggregates owned by one of the nodes in the HA pair, then the SSD spare must be owned by that same node.

## Considerations for when to use SSD storage pools

SSD storage pools provide many benefits, but they also introduce some restrictions that you should be aware of when deciding whether to use SSD storage pools or dedicated SSDs.

SSD storage pools make sense only when they are providing cache to two or more Flash Pool aggregates. SSD storage pools provide the following benefits:

- Increased storage utilization for SSDs used in Flash Pool aggregates  
SSD storage pools reduce the overall percentage of SSDs needed for parity by enabling you to share parity SSDs between two or more Flash Pool aggregates.
- Ability to share spares between HA partners  
Because the storage pool is effectively owned by the HA pair, one spare, owned by one of the HA partners, can function as a spare for the entire SSD storage pool if needed.
- Better utilization of SSD performance  
The high performance provided by SSDs can support access by both controllers in an HA pair.

These advantages must be weighed against the costs of using SSD storage pools, which include the following items:

- Reduced fault isolation  
The loss of a single SSD affects all RAID groups that include one of its partitions. In this situation, every Flash Pool aggregate that has cache allocated from the SSD storage pool that contains the affected SSD has one or more RAID groups in reconstruction.
- Reduced performance isolation  
If the Flash Pool cache is not properly sized, there can be contention for the cache between the Flash Pool aggregates that are sharing it. This risk can be mitigated with proper cache sizing and QoS controls.
- Decreased management flexibility  
When you add storage to a storage pool, you increase the size of all Flash Pool caches that include one or more allocation units from that storage pool; you cannot determine how the extra capacity is distributed.

## Considerations for adding SSDs to an existing storage pool versus creating a new one

You can increase the size of your SSD cache in two ways—by adding SSDs to an existing SSD storage pool or by creating a new SSD storage pool. The best method for you depends on your configuration and plans for the storage.

The choice between creating a new storage pool or adding storage capacity to an existing one is similar to deciding whether to create a new RAID group or add storage to an existing one:

- If you are adding a large number of SSDs, creating a new storage pool provides more flexibility because you can allocate the new storage pool differently from the existing one.
- If you are adding only a few SSDs, and increasing the RAID group size of your existing Flash Pool caches is not an issue, then adding SSDs to the existing storage pool keeps your spare and parity costs lower, and automatically allocates the new storage.

If your storage pool is providing allocation units to Flash Pool aggregates whose caches have different RAID types, and you expand the size of the storage pool beyond the maximum RAID4 RAID group size, the newly added partitions in the RAID4 allocation units are unused.

## Why you add disks to storage pools

You can add SSDs to an existing storage pool and increase its cache size. When you add SSDs to a storage pool that has allocation units already allocated to Flash Pool aggregates, you increase the cache size of each of those aggregates and the total cache of the storage pool.

If the allocation units of the storage pool are not yet allocated, adding SSDs to that storage pool does not affect the SSD cache size.

When you add SSDs to an existing storage pool, the SSDs must be owned by one node or the other of the same HA pair that already owned the existing SSDs in the storage pool. You can add SSDs that are owned by either node of the HA pair.

## How storage pool works

A *storage pool* is a collection of SSDs. You can combine SSDs to create a storage pool, which enables you to share the SSDs and SSD spares across multiple Flash Pool aggregates, at the same time.

Storage pools consist of allocation units, which you can use to provide SSDs and SSD spares to aggregates or to increase the existing SSD size.

After you add an SSD to a storage pool, you can no longer use the SSD as an individual disk. You must use the storage pool to assign or allocate the storage provided by the SSD.

### Related tasks

[Provisioning storage by creating a Flash Pool aggregate](#) on page 39

[Provisioning cache by adding SSDs](#) on page 114

## Storage Pools window

You can use the Storage Pools window to create, display, and manage a dedicated cache of SSDs, also known as *storage pools*. These storage pools can be associated with a non-root aggregate to provide SSD cache and with a Flash Pool aggregate to increase its size.

This page is not available for a cluster containing nodes with All Flash Optimized personality.

- [Command buttons](#) on page 133

- [Storage pools list](#) on page 133
- [Details tab](#) on page 133

## Command buttons

### Create

Opens the Create Storage Pool dialog box, which enables you to create a storage pool.

### Add Disks

Opens the Add Disks dialog box, which enables you to add cache disks to a storage pool.

### Delete

Deletes the selected storage pool.

### Refresh

Updates the information in the window.

## Storage pools list

### Name

Displays the name of the storage pool.

### Total Cache

Displays the total cache size of the storage pool.

### Spare Cache

Displays the available spare cache size of the storage pool.

### Used Cache (%)

Displays the percentage of used cache size of the storage pool.

### Allocation Unit

Displays the minimum allocation unit of the total cache size that you can use to increase the size of your storage pool.

### Owner

Displays the name of the HA pair or the node with which the storage pool is associated.

### State

Displays the state of the storage pool, which can be Normal, Degraded, Creating, Deleting, Reassigning, or Growing.

### Is Healthy

Displays whether storage pool is healthy or not.

## Details tab

Displays detailed information about the selected storage pool, such as the name, health, storage type, disk count, total cache, spare cache, used cache size (in percent), and allocation unit. The tab also displays the names of the aggregates that are provisioned by the storage pool.

## Disks tab

Displays detailed information about the disks in the selected storage pool, such as the names, disk types, useable size, and total size.

## Related tasks

[Adding disks to a storage pool](#) on page 128

[Creating a storage pool](#) on page 127

[Deleting storage pools](#) on page 128

## Disks

You can use System Manager to manage disks.

### Reassigning disks to nodes

You can use System Manager to reassign the ownership of spare disks from one node to another node to increase the capacity of an aggregate or storage pool.

#### About this task

- You can reassign disks if the following conditions are true:
  - The container type of the selected disks must be “spare” or “shared”.
  - The disks must be connected to nodes in an HA configuration.
  - The disks must be visible to the node.
- You *cannot* reassign a disk if the following conditions are true:
  - The container type of the selected disk is “shared”, and the data partition is not spare.
  - The disk is associated with a storage pool.
- You cannot reassign the data partition of shared disks if storage failover is not enabled on the nodes that are associated with the shared disks.
- For partition disks, you can reassign only the data partition of the disks.
- For MetroCluster configurations, you cannot use System Manager to reassign disks.  
You must use the command-line interface to reassign disks for MetroCluster configurations.

#### Steps

1. Click **Hardware and Diagnostics > Disks**.
2. In the **Disks** window, select the **Inventory** tab.
3. Select the disks that you want to reassign, and then click **Assign**.
4. In the **Warning** dialog box, click **Continue**.
5. In the **Assign Disks** dialog box, select the node to which you want to reassign the disks.
6. Click **Assign**.

### Viewing disk information

You can use the Disks window in System Manager to view the name, size, and container details of disks along with graphical information about capacity disks and cache disks.

#### Steps

1. Click **Hardware and Diagnostics > Disks**.
2. Select the disk that you want to view information about from the displayed list of disks.
3. Review the disk details.

**Related references**

[Disks window](#) on page 140

**Understanding RAID drive types**

Data ONTAP classifies drives (or, for partitioned drives, *partitions*) as one of four types for RAID: data, hot spare, parity, or dParity. You manage disks differently depending on whether they are spare or being used in an aggregate.

The RAID type is determined by how RAID is using a drive or partition; it is different from the Data ONTAP disk type.

You cannot affect the RAID type for a drive. The RAID type is displayed in the `Position` column for many storage commands.

For drives using root-data partitioning and SSDs in storage pools, a single drive might be used in multiple ways for RAID. For example, the root partition of a partitioned drive might be a spare partition, whereas the data partition might be being used for parity. For this reason, the RAID drive type for partitioned drives and SSDs in storage pools is displayed simply as *shared*.

**Data disk**

Holds data stored on behalf of clients within RAID groups (and any data generated about the state of the storage system as a result of a malfunction).

**Spare disk**

Does not hold usable data, but is available to be added to a RAID group in an aggregate. Any functioning disk that is not assigned to an aggregate but is assigned to a system functions as a hot spare disk.

**Parity disk**

Stores row parity information that is used for data reconstruction when a single disk drive fails within the RAID group.

**dParity disk**

Stores diagonal parity information that is used for data reconstruction when two disk drives fail within the RAID group, if RAID-DP is enabled.

**How ONTAP reports disk types**

ONTAP associates a type with every disk. ONTAP reports some disk types differently than the industry standards; you should understand how ONTAP disk types map to industry standards to avoid confusion.

When ONTAP documentation refers to a disk type, it is the type used by ONTAP unless otherwise specified. *RAID disk types* denote the role that a specific disk plays for RAID. RAID disk types are not related to ONTAP disk types.

For a specific configuration, the disk types that are supported depend on the storage system model, the shelf type, and the I/O modules that are installed in the system.

The following tables show how ONTAP disk types map to industry standard disk types for the SAS and FC storage connection types, and for storage arrays.

**SAS-connected storage**

ONTAP disk type	Disk class	Industry standard disk type	Description
BSAS	Capacity	SATA	Bridged SAS-SATA disks with added hardware to enable them to be plugged into a SAS-connected storage shelf
FSAS	Capacity	NL-SAS	Near Line SAS
MSATA	Capacity	SATA	SATA disk in multi-disk carrier storage shelf
SAS	Performance	SAS	Serial-Attached SCSI
SSD	Ultra-performance	SSD	Solid-state drives

**FC-connected storage**

ONTAP disk type	Disk class	Industry standard disk type
ATA	Capacity	SATA
FCAL	Performance	FC

**Storage arrays**

ONTAP disk type	Disk class	Industry standard disk type	Description
LUN	N/A	LUN	Logical storage device that is backed by storage arrays and used by ONTAP as a disk  These LUNs are referred to as <i>array LUNs</i> to distinguish them from the LUNs that ONTAP serves to clients.

**Related information**

[NetApp Hardware Universe](#)

[NetApp Technical Report 3437: Storage Subsystem Resiliency Guide](#)

**How hot spare disks work**

A hot spare disk is a disk that is assigned to a storage system and is ready for use, but is not in use by a RAID group and does not hold any data.

If a disk failure occurs within a RAID group, the hot spare disk is automatically assigned to the RAID group to replace the failed disks. The data of the failed disk is reconstructed on the hot spare replacement disk in the background from the RAID parity disk. The reconstruction activity is logged in the `/etc/message` file and an AutoSupport message is sent.



If the available hot spare disk is not the same size as the failed disk, a disk of the next larger size is chosen and then downsized to match the size of the disk that it is replacing.

## RAID protection for array LUNs

Storage arrays provide RAID protection for the array LUNs that they make available to Data ONTAP. Data ONTAP does not provide RAID protection.

Data ONTAP uses RAID0 (striping) for array LUNs. Data ONTAP supports a variety of RAID types on the storage arrays, except RAID0 because RAID0 does not provide storage protection.

When creating *RAID groups* on storage arrays, you need to follow the best practices of the storage array vendor to ensure that there is an adequate level of protection on the storage array so that disk failure does not result in loss of data or loss of access to data.

### Note:

- A *RAID group* on a storage array is the arrangement of disks that together form the defined RAID level.  
Each RAID group supports only one RAID type. The number of disks that you select for a RAID group determines the RAID type that a particular RAID group supports. Different storage array vendors use different terms to describe this entity—RAID groups, parity groups, disk groups, Parity RAID groups, and other terms.
- Data ONTAP supports RAID4 and RAID-DP on native disk shelves, but supports only RAID0 on array LUNs.

## Minimum number of hot spares you should have

Having insufficient spares increases the risk of a disk failure with no available spare, resulting in a degraded RAID group. A spare disk is also required to provide important information (a *core file*) to technical support in case of a controller disruption.

MSATA disks, or disks in a multi-disk carrier, should have four hot spares during steady state operation, and you should never allow the number of MSATA hot spares to dip below two.

For RAID groups composed of SSDs, you should have at least one spare disk.

For all other Data ONTAP disk types, you should have at least one matching or appropriate hot spare available for each kind of disk installed in your storage system. However, having two available hot spares for all disks provides the best protection against disk failure. Having at least two available hot spares provides the following benefits:

- When you have two or more hot spares for a data disk, Data ONTAP can put that disk into the maintenance center if needed.  
Data ONTAP uses the maintenance center to test suspect disks and take offline any disk that shows problems.
- Having two hot spares means that when a disk fails, you still have a spare available if another disk fails before you replace the first failed disk.

A single spare disk can serve as a hot spare for multiple RAID groups. However, if any disk in those RAID groups fails, then no spare is available for any future disk failures, or for a core file, until the spare is replaced. For this reason, having more than one spare is recommended.

## Spare requirements for multi-disk carrier disks

Maintaining the proper number of spares for disks in multi-disk carriers is critical for optimizing storage redundancy and minimizing the amount of time Data ONTAP must spend copying disks to achieve an optimal disk layout.

You must maintain a minimum of two hot spares for multi-disk carrier disks at all times. To support the use of the Maintenance Center, and to avoid issues caused by multiple concurrent disk failures, you should maintain at least four hot spares for steady state operation, and replace failed disks promptly.

If two disks fail at the same time with only two available hot spares, Data ONTAP might not be able to swap the contents of both the failed disk and its carrier mate to the spare disks. This scenario is called a *stalemate*. If this happens, you are notified through EMS messages and AutoSupport messages. When the replacement carriers become available, you must follow the instructions provided by the EMS messages or contact technical support to recover from the stalemate.

## Shelf configuration requirements for multi-disk carrier storage shelves

You can combine multi-disk carrier disk shelves with single-disk carrier disk shelves (standard disk shelves) on the same storage system and within in the same stack.

## How to determine when it is safe to remove a multi-disk carrier

Removing a multi-disk carrier before it is safe to do so can result in one or more RAID groups becoming degraded, or possibly even a storage disruption. System Manager enables you to determine when it is safe to remove a multi-disk carrier.

When a multi-disk carrier has to be replaced, the following events must have occurred before you can remove the carrier safely:

- An AutoSupport message must have been logged indicating that the carrier is ready to be removed.
- An EMS message must have been logged indicating that the carrier is ready to be removed.
- The state of both disks in the carrier must be displayed as **broken** in the Disks window. You must remove the disks only after the carrier mate of a failed disk is evacuated. You can click Details to view the disk evacuation status in the Properties tab of the Disks window.
- The fault LED (amber) on the carrier must be lit continuously indicating that it is ready for removal.
- The activity LED (green) must be turned off indicating there is no disk activity.
- The shelf digital display only shows the shelf ID number.

**Attention:** You cannot reuse the carrier mate of a failed disk. When you remove a multi-disk carrier that contains a failed disk, you must replace it with a new carrier.

## Considerations for sizing RAID groups

Configuring an optimum RAID group size requires a trade-off of factors. You must decide which factors—speed of RAID rebuild, assurance against risk of data loss due to drive failure, optimizing I/O performance, and maximizing data storage space—are most important for the aggregate that you are configuring.

When you create larger RAID groups, you maximize the space available for data storage for the same amount of storage used for parity (also known as the “parity tax”). On the other hand, when a disk fails in a larger RAID group, reconstruction time is increased, impacting performance for a longer

period of time. In addition, having more disks in a RAID group increases the probability of a multiple disk failure within the same RAID group.

### HDD or array LUN RAID groups

You should follow these guidelines when sizing your RAID groups composed of HDDs or array LUNs:

- All RAID groups in an aggregate should have a similar number of disks.  
The RAID groups do not have to be exactly the same size, but you should avoid having any RAID group that is less than one half the size of other RAID groups in the same aggregate when possible.
- The recommended range of RAID group size is between 12 and 20.  
The reliability of performance disks can support a RAID group size of up to 28, if needed.
- If you can satisfy the first two guidelines with multiple RAID group sizes, you should choose the larger size.

### SSD RAID groups in Flash Pool aggregates

The SSD RAID group size can be different from the RAID group size for the HDD RAID groups in a Flash Pool aggregate. Usually, you should ensure that you have only one SSD RAID group for a Flash Pool aggregate, to minimize the number of SSDs required for parity.

### SSD RAID groups in SSD aggregates

You should follow these guidelines when sizing your RAID groups composed of SSDs:

- All RAID groups in an aggregate should have a similar number of drives.  
The RAID groups do not have to be exactly the same size, but you should avoid having any RAID group that is less than one half the size of other RAID groups in the same aggregate when possible.
- For RAID-DP, the recommended range of RAID group size is between 20 and 28.

## Considerations for ONTAP RAID groups for array LUNs

Setting up ONTAP RAID groups for array LUNs requires planning and coordination with the storage array administrator so that the administrator makes the number and size of array LUNs that you need available to ONTAP.

For array LUNs, ONTAP uses RAID0 RAID groups to determine where to allocate data to the LUNs on the storage array. The RAID0 RAID groups are not used for RAID data protection. The storage arrays provide RAID data protection.

**Note:** ONTAP RAID groups are similar in concept to what storage array vendors call RAID groups, parity groups, disk groups, Parity RAID groups, and other terms.

Follow these steps when planning your ONTAP RAID groups for array LUNs:

1. Plan the size of the aggregate that best meets your data needs.
2. Plan the number and size of RAID groups that you need for the size of the aggregate.  
**Note:** It is best to use the default RAID group size for array LUNs. The default RAID group size is adequate for most organizations. The default RAID group size is different for array LUNs and disks.
3. Plan the size of the LUNs that you need in your RAID groups.

- To avoid a performance penalty, all array LUNs in a particular RAID group should be of the same size.
  - The LUNs should be of the same size in all RAID groups in the aggregate.
4. Ask the storage array administrator to create the number of LUNs of the size that you need for the aggregate.  
The LUNs should be optimized for performance, according to the instructions in the storage array vendor documentation.
  5. Create all the RAID groups in the aggregate simultaneously.

**Note:**

- Do not mix array LUNs from storage arrays with different characteristics in the same ONTAP RAID group.
- If you create a new RAID group for an existing aggregate, ensure that the new RAID group is of the same size as the other RAID groups in the aggregate, and that the array LUNs are of the same size as the LUNs in the other RAID groups in the aggregate.

**Disks window**

You can use the Disks window to view all the disks in your storage system.

- [Command buttons](#) on page 140
- [Summary](#) on page 140
- [Inventory](#) on page 141
- [Inventory details area](#) on page 142

**Command buttons****Assign**

Assigns or reassigns the ownership of the disks to a node.

This button is enabled only if the container type of the selected disks is unassigned, spare, or shared.

**Zero Spares**

Erases all the data, and formats the spare disks and array LUNs.

**Refresh**

Updates the information in the window.

**Tabs****Summary**

Displays detailed information about the disks in the cluster, including the size of the spare disks and assigned disks. The tab also graphically displays information about spare disks, aggregates, and root aggregates for HDDs and information about spare disks, disks in a storage pool, aggregates, Flash Pool aggregates, and root aggregates for cache disks (SSDs).

The HDD panel is not displayed for systems with All Flash Optimized personality.

The details panel provides additional information about partitioned and unpartitioned spare disks (disk type, node, disk size, RPM, checksum, number of available disks, and spare capacity), in tabular format.

**Inventory****Name**

Displays the name of the disk.

**Container Type**

Displays the purpose for which the disk is used. The possible values are Aggregate, Broken, Foreign, Label Maintenance, Maintenance, Shared, Spare, Unassigned, Volume, Unknown, and Unsupported.

**Partition Type**

Displays the partition type of the disk.

**Node Name**

Displays the name of the node that contains the aggregate.

This field is available only at the cluster level.

**Home owner**

Displays the name of the home node to which this disk is assigned.

**Current owner**

Displays the name of the node that currently owns this disk.

**Root owner**

Displays the name of the node that currently owns the root partition of this disk.

**Data Owner**

Displays the name of the node that currently owns the data partition of this disk.

**Data1 Owner**

Displays the name of the node that currently owns the data1 partition of the disk.

**Data2 Owner**

Displays the name of the node that currently owns the data2 partition of the disk.

**Storage Pool**

Displays the name of the storage pool with which the disk is associated.

**Type**

Displays the type of the disk.

**Firmware Version**

Displays the firmware version of the disk.

**Model**

Displays the model of the disk.

**RPM**

Displays the effective speed of the disk drive when the option `raid.mix.hdd.rpm.capacity` is enabled, and displays the actual speed of the disk drive when the option `raid.mix.hdd.rpm.capacity` is disabled.

This field is not applicable to SSDs.

**Effective Size**

Displays the usable space available on the disk.

**Physical Space**

Displays the total physical space of the disk.

**Shelf**

Displays the shelf on which the physical disks are located.

This field is hidden by default.

#### **Bay**

Displays the bay within the shelf for the physical disk.

This field is hidden by default.

#### **Pool**

Displays the name of the pool to which the selected disk is assigned.

This field is hidden by default.

#### **Checksum**

Displays the type of the checksum.

This field is hidden by default.

#### **Carrier ID**

Specifies information about disks that are located within the specified multi-disk carrier.  
The ID is a 64-bit value.

This field is hidden by default.

### **Inventory details area**

The area below the inventory tab displays detailed information about the selected disk, including information about the aggregate or volume (if applicable), vendor ID, zeroing state (in percent), serial number of the disk, and error details in case of a broken disk. For shared disks, the Inventory details area displays the names of all the aggregates, including the root and the non-root aggregates.

#### **Related tasks**

[Viewing disk information](#) on page 134

## **Array LUNs**

You can use System Manager to assign array LUNs to an existing aggregate and manage array LUNs.

### **Assigning array LUNs**

You can use System Manager to assign unassigned array LUNs to an existing aggregate to increase the size of the aggregate.

#### **About this task**

- You can assign array LUNs if the following conditions are true:
  - The container type of the selected array LUNs must be “unassigned”.
  - The disks must be connected to nodes in an HA pair.
  - The disks must be visible to the node.
- For MetroCluster configurations, you cannot use System Manager to assign array LUNs as spares.  
You must use the command-line interface instead.

#### **Steps**

1. Click **Hardware and Diagnostics > Array LUNs**.

2. Select the array LUNs, and then click **Assign**.
3. In the **Assign Array LUNs** dialog box, select the node to which you want to assign the array LUNs.
4. Click **Assign**.

## Reassigning spare array LUNs to nodes

You can use System Manager to reassign the ownership of spare array LUNs from one node to another to increase the capacity of an aggregate.

### About this task

- You can reassign array LUNs if the following conditions are true:
  - The container type of the selected array LUNs must be “spare”.
  - The disks must be connected to nodes in an HA pair.
  - The disks must be visible to the node.
- For MetroCluster configurations, you cannot use System Manager to reassign array LUNs as spares.  
You must use the command-line interface instead.

### Steps

1. Click **Hardware and Diagnostics > Array LUNs**.
2. Select the spare array LUNs that you want to reassign, and then click **Assign**.
3. In the **Warning** dialog box, click **Continue**.
4. In the **Assign Array LUNs** dialog box, select the node to which you want to reassign the spare array LUNs.
5. Click **Assign**.

## Zeroing spare array LUNs

You can use System Manager to erase all the data and to format the spare array LUNs by writing zeros to the array LUNs. These array LUNs can then be used in new aggregates.

### About this task

When you zero the spare array LUNs, all the spares in the cluster, including disks, are zeroed. You can zero the spare array LUNs for a specific node or for the entire cluster.

### Steps

1. Click **Hardware and Diagnostics > Array LUNs**.
2. Click **Zero Spares**.
3. In the **Zero Spares** dialog box, select a node or “All nodes” from which you want to zero the array LUNs.
4. Select the **Zero all non-zeroed spares** check box to confirm the zeroing operation.
5. Click **Zero Spares**.

## About disks and array LUNs

A disk is the basic unit of storage for storage systems that use Data ONTAP to access native disk shelves. An array LUN is the basic unit of storage that third-party storage arrays provide to storage systems that run Data ONTAP.

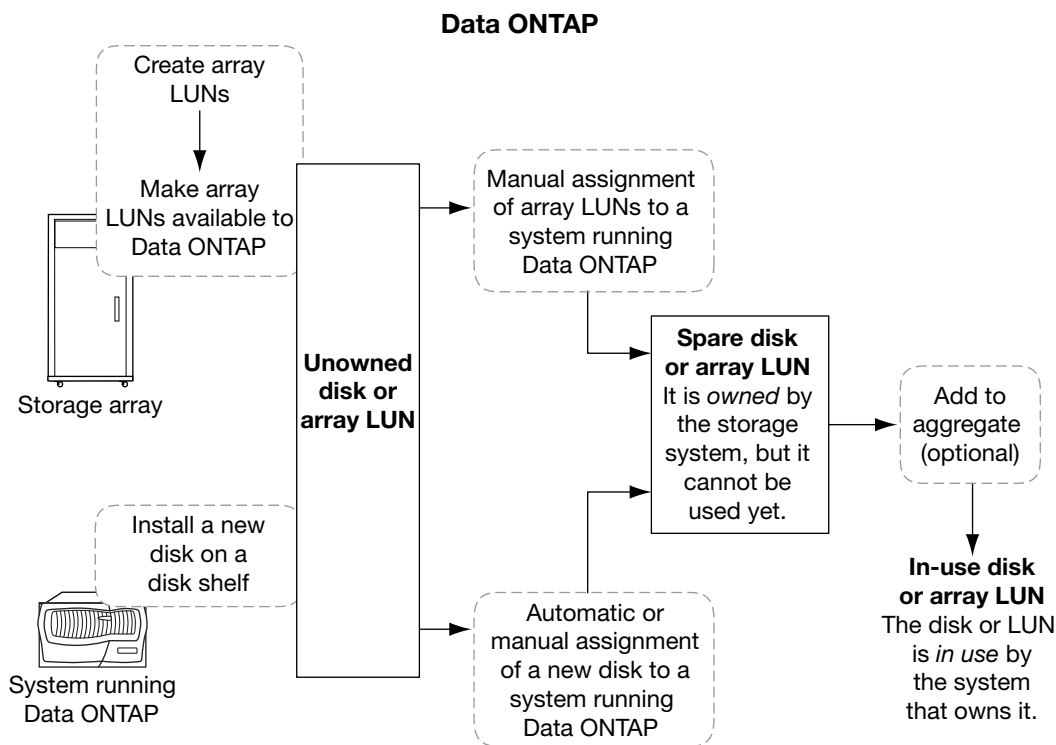
Data ONTAP enables you to assign ownership to your disks and array LUNs, and to add them to an aggregate. Data ONTAP also provides a number of ways to manage your disks, including removing them, replacing them, and sanitizing them. Because array LUNs are provided by the third-party storage array, you use the third-party storage array for all other management tasks for array LUNs.

You can create an aggregate using either disks or array LUNs. After you have created the aggregate, you manage it using Data ONTAP in exactly the same way, whether it was created from disks or array LUNs.

## How disks and array LUNs become available for use

When you add a disk or array LUN to a system running Data ONTAP, the disk or array LUN goes through several stages before it can be used by Data ONTAP to store data or parity information.

The process for making a disk available for use differs slightly from the process for making an array LUN available for use. Both processes are shown in the following diagram:



The process for disks includes the following actions:

1. The administrator physically installs the disk into a disk shelf. Data ONTAP can see the disk, but the disk is still unowned.
2. If the system is configured to support disk autoassignment, Data ONTAP assigns ownership for the disk; otherwise, the administrator must assign ownership of the disk manually. The disk is now a spare disk.
3. The administrator or Data ONTAP adds the disk to an aggregate. The disk is now in use by that aggregate. It could contain data or parity information.

The process for array LUNs includes the following actions:



1. The storage array administrator creates the array LUN and makes it available to Data ONTAP. Data ONTAP can see the array LUN, but the array LUN is still unowned.
2. The Data ONTAP administrator assigns ownership of the array LUN to a Data ONTAP system. The array LUN is now a spare array LUN.
3. The Data ONTAP administrator adds the array LUN to an aggregate. The array LUN is now in use by that aggregate and is storing data.

## Rules for mixing array LUNs in an aggregate

Data ONTAP does not support the mixing of different types of storage in the same aggregate because it causes performance degradation.

There are restrictions on the types of array LUNs that you can mix in the same aggregate, which you must follow when you add array LUNs to an aggregate. Data ONTAP does not prevent you from mixing different types of array LUNs, but it does prevent you from mixing native disks and array LUNs in the same aggregate.

You cannot mix the following types of array LUNs in the same aggregate:

- Array LUNs from storage arrays from different vendors
- Array LUNs from storage arrays from the same vendor but from different storage array families
 

**Note:** Storage arrays in the same family share the same characteristics—for example, the same performance characteristics. For more information about how Data ONTAP defines family members for a vendor, see the *FlexArray Virtualization Implementation Guide for Third-Party Storage* guide.
- Array LUNs from different drive types (for example, FC and SATA)
 

You cannot mix array LUNs from different drive types in the same aggregate even if array LUNs are from the same series and the same vendor. Before setting up this type of configuration, you should consult your authorized reseller to plan the best implementation for your environment.

## Array LUNs window

The Array LUNs window enables you to assign ownership to your array LUNs and to add them to an aggregate.

The Array LUNs link in the left navigation pane is displayed only if there are any spare array LUNs, or if the V\_StorageAttach license is installed.

- [Command buttons](#) on page 145
- [Array LUN list](#) on page 146
- [Details area](#) on page 146

### Command buttons

#### Assign

Enables you to assign or reassign the ownership of array LUNs to a node.

#### Zero Spares

Erases all the data, and formats the spare array LUNs and disks.

#### Refresh

Updates the information in the window.

**Array LUN list**

Displays information such as the name, state, and vendor for each array LUN.

**Name**

Specifies the name of the array LUN.

**State**

Specifies the state of the array LUN.

**Vendor**

Specifies the name of the vendor.

**Used Space**

Specifies the space used by the array LUN.

**Total Size**

Specifies the size of the array LUN.

**Container**

Specifies the aggregate to which the array LUN belongs.

**Node name**

Specifies the name of the node to which the array LUN belongs.

**Home owner**

Displays the name of the home node to which the array LUN is assigned.

**Current owner**

Displays the name of the node that currently owns the array LUN.

**Array name**

Specifies the name of the array.

**Pool**

Displays the name of the pool to which the selected array LUN is assigned.

**Details area**

The area below the Array LUNs list displays detailed information about the selected array LUN.

## Nodes

You can use System Manager to view the details of the nodes in the cluster.

## Initializing the ComplianceClock time

You can use System Manager to initialize the ComplianceClock time to the current cluster time. You must initialize the ComplianceClock time in order to create SnapLock aggregates.

**Before you begin**

The SnapLock license must be installed.

**About this task**

You cannot modify or stop the ComplianceClock time after it is initialized.

**Steps**

1. Click **Hardware and Diagnostics > Nodes**.

2. Select the node, and then click **Initialize ComplianceClock**.
3. In the **Initialize ComplianceClock** dialog box, click **Yes** to initialize the ComplianceClock time to the current cluster time.

## Nodes window

You can use the Nodes to view the details of the nodes in the cluster.

- [Command buttons](#) on page 147
- [Nodes list](#) on page 147

### Command buttons

#### Initialize ComplianceClock

Initializes the ComplianceClock of the selected node to the current value of the system clock.

#### Refresh

Updates the information in the window.

### Nodes list

#### Name

Displays the name of the node.

#### State

Displays the state of the node, whether it is up or down.

#### Up Time

Displays the duration for which the node is up.

#### Data ONTAP Version

Displays the Data ONTAP version that is installed on the node.

#### Model

Displays the platform model number of the node.

#### System ID

Displays the ID of the node.

#### Serial No

Displays the serial number of the node.

#### All Flash Optimized

Displays if the node has an All Flash Optimized personality or not.

### Details area

Displays detailed information about the selected node.

#### Details tab

Displays information related to the selected node such as name of the node, state of the node, and the duration for which the node is up.

#### Performance tab

Displays throughput, IOPS, and latency of the selected node.

Changing the client time zone or the cluster time zone impacts the performance metrics graphs. Refresh your browser to see the updated graphs.

## Flash Cache

You can use System Manager to manage Flash Cache.

### Enabling or disabling Flash Cache

You can enable or disable the WAFL external cache functionality for a storage system that has a PAM II card or Flash Cache module installed by using System Manager. You can enable Flash Cache based on the workload requirements of your storage system.

#### Steps

1. Click **Hardware and Diagnostics > Flash Cache**.
2. Select the node.
3. Click **Enable** or **Disable**, as required.

### How Flash Cache works

Using Flash Caches improves the performance of a storage system.

You can configure Flash Cache and disks based on the workload requirements of a storage system. By determining the read workload (number of read operations) served by Flash Cache and disks, you can analyze the performance of the storage system.

Flash Cache does not contain any data during storage system boot or when control is returned to the storage system after a takeover event. Therefore, disks serve all the data read requests of the storage system.

The Flash Cache module is slowly populated with data when data read requests are served. Because the data read requests served by Flash Cache are faster than those served by the disks, the performance of the storage system improves.

Data read requests served by the Flash Cache module replace the data read requests served by the disks and, therefore, the performance improvement in the storage system is directly related to the disk reads that are replaced. To understand the impact of Flash Cache on storage system performance, you must view the read workload graph when the Flash Cache contains data.

### Flash Cache window

You can use the Flash Cache window to enable or disable Flash Cache for a storage system that has a Flash Cache module installed. You can also view the read workload statistics.

This page is not available for a cluster containing nodes with All Flash Optimized personality.

#### Command buttons

##### Enable/Disable

Enables or disables Flash Cache.

##### Flash Cache Read Workload

Displays a graph specifying the rate of read workload served by the disks and the Flash Cache module, thereby indicating the performance of the storage system.

**Details area**

Displays information about the system read latency (in seconds), the caching mode that specifies the caching configuration, the state of Flash Cache (enabled or disabled), and the size of the Flash Cache (in GB). If there are multiple Flash Cache cards, the total cache size from all the cards is displayed.

## Events

You can use System Manager to view the event log and event notifications.

### Events window

You can use the Events window to view the event log and event notifications.

**Command buttons****Refresh**

Updates the information in the window.

**Events list****Time**

Displays the time when the event occurred.

**Node**

Displays the node and the cluster on which the event occurred.

**Severity**

Displays the severity of the event. The possible severity levels are:

- **Emergency**  
Specifies that the event source unexpectedly stopped, and the system experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.
- **Alert**  
Specifies that the event source has an alert, and action must be taken to avoid downtime.
- **Critical**  
Specifies that the event source is critical, and might lead to service disruption if corrective action is not taken immediately.
- **Error**  
Specifies that the event source is still performing, and a corrective action is required to avoid service disruption.
- **Warning**  
Specifies that the event source experienced an occurrence that you must be aware of. Events of this severity might not cause service disruption; however, corrective action might be required.
- **Notice**  
Specifies that the event source is normal, but the severity is a significant condition that you must be aware of.
- **Informational**  
Specifies that the event source has an occurrence that you must be aware of. No corrective action might be required.

- **Debug**  
Specifies that the event source includes a debugging message.

By default, the alert severity type, emergency severity type, and the error severity type are displayed.

#### **Source**

Displays the source of the event.

#### **Event**

Displays the description of the event.

#### **Details area**

Displays the event details, including the event description, message name, sequence number, message description, and corrective action for the selected event.

## **System alerts**

You can use System Manager to monitor different parts of a cluster.

### **Monitoring the health of your system**

Health monitors proactively monitor certain critical conditions in your cluster and raise alerts if they detect a fault or risk. If there are active alerts, the system health status reports a degraded status for the cluster. The alerts include the information that you need to respond to degraded system health.

If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions. After you resolve the problem, the system health status automatically returns to OK.

The system health status reflects multiple separate health monitors. A degraded status in an individual health monitor causes a degraded status for the overall system health.

Data ONTAP supports the following cluster switches for system health monitoring in your cluster:

- NetApp CN1601
- NetApp CN1610
- Cisco Nexus 5010
- Cisco Nexus 5020
- Cisco Nexus 5596
- Cisco Catalyst 2960-24TT-L

### **Acknowledging system health alerts**

You can use System Manager to acknowledge and respond to system health alerts for subsystems. You can use the information displayed to take the recommended action and correct the problem reported by the alert.

#### **Steps**

1. Click **Hardware and Diagnostics > System Alerts**.
2. In the **System Alerts** window, click the arrow icon next to the name of subsystem.
3. Select the alert that you want to acknowledge, and then click **Acknowledge**.

4. Type your name, and then click **Acknowledge**.

#### Related references

[System Alerts window](#) on page 153

## Suppressing system health alerts

You can use System Manager to suppress system health alerts that do not require any intervention from you.

#### Steps

1. Click **Hardware and Diagnostics > System Alerts**.
2. In the **System Alerts** window, click the arrow icon next to the name of subsystem.
3. Select the alert that you want to suppress, and then click **Suppress**.
4. Type your name, and then click **Suppress**.

#### Related references

[System Alerts window](#) on page 153

## Deleting system health alerts

You can use System Manager to delete system health alerts to which you have already responded.

#### Steps

1. Click **Hardware and Diagnostics > System Alerts**.
2. In the **System Alerts** window, click the arrow icon next to the name of subsystem.
3. Select the alert that you want to delete, and then click **Delete**.
4. Click **OK**.

#### Related references

[System Alerts window](#) on page 153

## Available cluster health monitors

There are several health monitors that monitor different parts of a cluster. Health monitors help you to recover from errors within Data ONTAP subsystems by detecting events, sending alerts to you, and deleting events as they clear.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
Cluster switch (cluster-switch)	Switch (Switch-Health)	Monitors cluster network switches and management network switches for temperature, utilization, interface configuration, redundancy (cluster network switches only), and fan and power supply operation. The cluster switch health monitor communicates with switches through SNMP. SNMPv2c is the default setting.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
MetroCluster Fabric	Switch	Monitors the MetroCluster configuration back-end fabric topology and detects misconfigurations such as incorrect cabling and zoning, and ISL failures.
MetroCluster Health	Interconnect, RAID, and storage	Monitors FC-VI adapters, FC initiator adapters, left-behind aggregates and disks, and inter-cluster ports
Node connectivity (node-connect)	CIFS nondisruptive operations (CIFS-NDO)	Monitors SMB connections for nondisruptive operations to Hyper-V applications.
	Storage (SAS-connect)	Monitors shelves, disks, and adapters at the node level for appropriate paths and connections.
System	not applicable	Aggregates information from other health monitors.
System connectivity (system-connect)	Storage (SAS-connect)	Monitors shelves at the cluster level for appropriate paths to two HA clustered nodes.

## Ways to respond to system health alerts

When a system health alert occurs, you can acknowledge it, learn more about it, repair the underlying condition, and prevent it from occurring again.

When a health monitor raises an alert, you can respond in any of the following ways:

- Get information about the alert, which includes the affected resource, alert severity, probable cause, possible effect, and corrective actions.
- Get detailed information about the alert, such as the time when the alert was raised and whether anyone else has acknowledged the alert already.
- Get health-related information about the state of the affected resource or subsystem, such as a specific shelf or disk.
- Acknowledge the alert to indicate that someone is working on the problem, and identify yourself as the “Acknowledger.”
- Resolve the problem by taking the corrective actions provided in the alert, such as fixing cabling to resolve a connectivity problem.
- Delete the alert, if the system did not automatically clear it.
- Suppress an alert to prevent it from affecting the health status of a subsystem.  
Suppressing is useful when you understand a problem. After you suppress an alert, it can still occur, but the subsystem health displays as “ok-with-suppressed.” when the suppressed alert occurs.



## System Alerts window

You can use the System Alerts window to learn more about system health alerts. You can also acknowledge, delete, and suppress alerts from the window.

### Command buttons

#### Acknowledge

Enables you to acknowledge the selected alert to indicate that the problem is being addressed and identifies the person who clicks the button as the “Acknowledger.”

#### Suppress

Enables you to suppress the selected alert to prevent the system from notifying you about the same alert again and identifies you as the “Suppressor.”

#### Delete

Deletes the selected alert.

#### Refresh

Updates the information in the window.

### Alerts list

#### SubSystem (No. of Alerts)

Displays the name of the subsystem, such as the SAS connection, switch health, CIFS NDO, or MetroCluster, for which the alert is generated.

#### Alert ID

Displays the alert ID.

#### Node

Displays the name of the node for which the alert is generated.

#### Severity

Displays the severity of the alert as Unknown, Other, Information, Degraded, Minor, Major, Critical, or Fatal.

#### Resource

Displays the resource that generated the alert, such as a specific shelf or disk.

#### Time

Displays the time when the alert was generated.

### Details area

The details area displays detailed information about the alert, such as the time when the alert was generated and whether the alert has been acknowledged. The area also includes information about the probable cause and possible effect of the condition generated by the alert, and the recommended actions to correct the problem reported by the alert.

### Related tasks

[Acknowledging system health alerts](#) on page 150

[Suppressing system health alerts](#) on page 151

[Deleting system health alerts](#) on page 151

## AutoSupport notifications

You can use System Manager to configure AutoSupport notifications that help you to monitor your storage system health.

### Setting up AutoSupport notifications

You can use the Edit AutoSupport Settings dialog box in System Manager to set up AutoSupport notifications by specifying an email address from which email notifications are sent and adding multiple email host names.

#### Steps

1. Click **Hardware and Diagnostics > AutoSupport**.
2. Select the node, and then click **Edit**.
3. In the **Email Recipient** tab, type the email address from which email notifications are sent, specify the email recipients and the message content for each email recipient, and add the mail hosts.

You can add up to five email addresses of the host names.

4. In the **Others** tab, select a transport protocol for delivering the email messages from the drop-down list and specify the HTTP or HTTPS proxy server details.
5. Click **OK**.
6. Verify that configuration you have set for AutoSupport notification is set up correctly in the **AutoSupport** window.

### Enabling or disabling AutoSupport settings

You can enable or disable AutoSupport settings on your storage system by using System Manager. AutoSupport messages enable you to monitor your storage system health or send notifications to technical support and your internal support organization.

#### About this task

The AutoSupport option is enabled by default.

#### Steps

1. Click **Hardware and Diagnostics > AutoSupport**.
2. Select the node, and then click **Enable** or **Disable**.
3. Click **OK**.
4. Verify that the AutoSupport status correctly displays the change you made.

### Adding AutoSupport email recipients

You can use the **Email Recipient** tab of the Edit AutoSupport Settings dialog box in System Manager to add email addresses of the recipients of AutoSupport notifications.

#### Steps

1. Click **Hardware and Diagnostics > AutoSupport**.

2. Select the node, and then click **Edit**.
3. In the **Email Recipient** tab, type the address of the email recipient, specify whether the recipient receives a full message or a short message, and then click **Add**.
4. Click **OK**.
5. Verify that the details you specified are displayed in the **AutoSupport** window.

## Testing AutoSupport settings

You can use the AutoSupport Test dialog box in System Manager to test that you have configured the AutoSupport settings correctly.

### Steps

1. Click **Hardware and Diagnostics > AutoSupport**.
2. Select the node, and then click **Test**.
3. In the **AutoSupport Test** dialog box, enter the AutoSupport subject text “Test AutoSupport” or any text that notifies the recipients that you are testing the AutoSupport settings.
4. Click **Test**.

An email message with the subject “Test AutoSupport” or the text that you typed in the **AutoSupport subject** field is sent to the specified recipients.

## Generating AutoSupport data

You can use System Manager to generate AutoSupport data for a single node or multiple nodes to monitor their health and to send notifications to technical support.

### Steps

1. Click **Hardware and Diagnostics > AutoSupport**.
2. Select the node, and then click **AutoSupport Request > Generate AutoSupport**.  
By default, the AutoSupport data is generated for all nodes.
3. In the **Generate AutoSupport** dialog box, perform the following steps:
  - a. If you want to generate AutoSupport data for a specific node, clear the **Generate Autosupport data for all nodes** check box, and then select the node.
  - b. Type the case number.
4. Click **Generate**.
5. In the **Confirmation** dialog box, click **OK**.

## Viewing AutoSupport summary

System Manager enables you to view the status and details of all the previous AutoSupport data in order to review the data that has been sent to technical support. You can also view the information to understand the health and performance of your storage system.

### Steps

1. Click **Hardware and Diagnostics > AutoSupport**.
2. Select the node, and then click **AutoSupport Request > View Previous Summary**.

The AutoSupport data for all the nodes is displayed.

3. Click **OK**.

## AutoSupport severity types

AutoSupport messages have severity types that help you understand the purpose of each message—for example, to draw immediate attention to an emergency problem, or only to provide information.

Messages have one of the following severities:

- **Alert:** Alert messages indicate that a next-higher level event might occur if you do not take some action.  
You must take an action against alert messages within 24 hours.
- **Emergency:** Emergency messages are displayed when a disruption has occurred.  
You must take an action against emergency messages immediately.
- **Error:** Error conditions indicate what might happen if you ignore.
- **Notice:** Normal but significant condition.
- **Info:** Informational message provides details about the issue, which you can ignore.
- **Debug:** Debug-level messages provide instructions you should perform.

If your internal support organization receives AutoSupport messages through email, the severity appears in the subject line of the email message.

## AutoSupport window

The AutoSupport window enables you to view the current AutoSupport settings for your system. You can also change your system's AutoSupport settings.

### Command buttons

#### Enable

Enables AutoSupport notification.

#### Disable

Disables AutoSupport notification.

#### Edit

Opens the Edit AutoSupport Settings dialog box, which enables you to specify an email address from which email notifications are sent and to add multiple email addresses of the host names.

#### Test

Opens the AutoSupport Test dialog box, which enables you to generate an AutoSupport test message.

### AutoSupport Request

Provides the following AutoSupport requests:

#### Generate AutoSupport

Generates AutoSupport data for a selected node or all nodes.

#### View Previous Summary

Displays the status and details of all the previous AutoSupport data.

#### Refresh

Updates the information in the window.

### Details area

The details area displays AutoSupport setting information such as the node name, AutoSupport status, transport protocol used, and name of the proxy server.

### Related tasks

[Setting up a support page](#) on page 27

## Jobs

You can use System Manager to manage job tasks such as displaying job information and monitoring the progress of a job.

### Jobs

*Jobs* are asynchronous task and typically long-running volume operations, such as copying, moving, or mirroring data. Jobs are placed in a job queue and are run when resources are available. The cluster administrator can perform all the tasks related to job management.

A job can be one of the following categories:

- A *server-affiliated* job is placed in queue by the management framework to be run in a specific node.
- A *cluster-affiliated* job is placed in queue by the management framework to be run in any node in the cluster.
- A *private* job is specific to a node and does not use the replicated database (RDB) or any other cluster mechanism.

You require the advanced privilege level or higher to run the commands to manage private jobs.

You can manage jobs in the following ways:

- Displaying job information, including the following:
  - Jobs on a per-node basis
  - Cluster-affiliated jobs
  - Completed jobs
  - Job history
- Monitoring a job's progress
- Displaying information about the initialization state for job managers.

You can determine the outcome of a completed job by checking the event log.

### Job window

You can use the Job window to manage job tasks such as displaying job information and monitoring the progress of a job.

#### Command button

##### Refresh

Updates the information in the window.

**Tabs****Current Jobs**

This tab displays information about the job tasks that are in progress.

**Job History**

This tab displays information about all the jobs.

**Job list****Job ID**

Displays the ID of the job.

**Start Time**

Displays the start time of the job.

**Job Name**

Displays the name of the job.

**Node**

Displays the name of the node.

**State**

Displays the state of the job.

**Job Description**

Displays the description of the job.

**Progress**

Displays the state of the job.

**Schedule Name**

Displays the name of the schedule.

## Flash Pool statistics

You can use System Manager to view the real-time SSD tier read and write workloads for a selected Flash Pool aggregate.

### Flash Pool aggregate Statistics window

You can view the real-time SSD tier read and write workloads for a selected Flash Pool aggregate.

This page is not available for a cluster containing nodes with All Flash Optimized personality.

**Displaying Statistics for Flash Pool aggregate**

From the list of Flash Pool aggregates, you can select the Flash Pool aggregate whose statistics you want to view.

**SSD Cache Read Workload**

Displays a graphical view of the total read requests that are sent to the Flash Pool aggregate in comparison with the read operations that are performed by the SSD tier.

**SSD Cache Write Workload**

Displays a graphical view of the total write requests that are sent to the Flash Pool aggregate in comparison with the write operations that are performed by the SSD tier.

## Managing logical storage

---

You can use System Manager to manage the logical storage such as Storage Virtual Machines (SVMs), volumes, Qtrees, protocols, policies and so on.

### Storage Virtual Machines

You can use System Manager to manage the SVMs in your cluster.

#### SVM Dashboard window

The dashboard provides a cumulative at-a-glance information about your SVM and its performance. You can use the Dashboard window to view important information related to your SVM such as the protocols configured, the volumes that are nearing capacity, and the performance.

##### SVM Details

This window displays details about the SVM through various panels such as the protocol status, volumes nearing capacity, and SVM performance.

##### Protocol Status

Provides an overview of the protocols that are configured for the SVM. You can click the protocol name to view the configuration.

If a protocol is not configured or if a protocol license is not available for the SVM, you can click the protocol name to configure the protocol or add the protocol license.

##### Volumes Nearing Capacity

Displays information about the volumes that are nearing a capacity utilization of 80 percent or more, and therefore require immediate attention or corrective action.

##### SVM Performance

Displays the performance metrics of the protocols in the SVM, including latency and IOPS.

If the information about the SVM performance cannot be retrieved from Data ONTAP, you cannot view the respective graph. In such cases, System Manager displays the specific error message.

The refresh interval for this panel is 15 seconds.

### Monitoring SVMs

The dashboard in System Manager enables you to monitor the health and performance of a Storage Virtual Machine (SVM).

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. View the details in the dashboard panels.

## Editing SVM settings

You can use System Manager to edit the properties of Storage Virtual Machines (SVMs), such as the name service switch, name mapping switch, and aggregate list.

### About this task

- You can edit the values of the following SVMs properties:
  - Name service switch
  - Protocols that are allowed to serve data
 

**Note:** The CIFS protocol that is configured on the SVM continues to serve data even when you disallow it on that SVM.
  - The list of aggregates that are available to create volumes
 

If you do not specify the aggregates for SVMs with Infinite Volume, the Infinite Volume spans across all the aggregates in the cluster.

**Note:** For FlexVol volumes, you can assign aggregates only if you have delegated administration to an SVM administrator.
- System Manager does not display the values of the name service switch and the name mapping switch for an SVM that is created through the command-line interface, or whose services are not configured and not set to the default values by Data ONTAP.
 

You can use the command-line interface to view the services because the Services tab is disabled. System Manager only displays the name service switch and the name mapping switch of an SVM when it is created by using System Manager or when services of the SVM are set to their default values by Data ONTAP.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. In the **Details** tab, modify the required data protocols.
4. In the **Resource Allocation** tab, choose one of the following methods to delegate volume creation:

If you want to provision volume creation...	Then...
For all aggregates	Select the <b>Do not delegate volume creation</b> option.
For specific aggregates	<ol style="list-style-type: none"> <li>a. Select the <b>Delegate volume creation</b> option.</li> <li>b. Select the required aggregates for delegating volume creation.</li> </ol>

5. In the **Service** tab, specify the name service switch sources for the required database types and the order in which they should be consulted to retrieve name service information.

The default values for each of the database types are as follows:

- hosts: files, dns
- namemap: files
- group: files



- netgroup: files
- passwd: files

6. Click **Save and Close**.

#### Related concepts

*How ONTAP name service switch configuration works* on page 165

## Deleting SVMs

You can use System Manager to delete Storage Virtual Machines (SVMs) that you no longer require from the storage system configuration.

#### Before you begin

You must have completed the following tasks:

1. Disabled the Snapshot copies, data protection (DP) mirrors, and load-sharing (LS) mirrors for all the volumes
  - Note:** You must use the CLI to disable LS mirrors.
2. Deleted all the igroups that belong to the SVM manually if you are deleting SVMs with FlexVol volume
3. Deleted all the portsets
4. Deleted all the volumes in the SVM, including the root volume
5. Unmapped the LUNs, taken them offline, and deleted them
6. Deleted the CIFS server if you are deleting SVMs with FlexVol volume
7. Deleted any customized user accounts and roles that are associated with the SVM
8. Stopped the SVM

#### About this task

When you delete SVMs, the following objects associated with the SVM are also deleted:

- LIFs, LIF failover groups, and LIF routing groups
- Export policies
- Efficiency policies

If you delete SVMs that are configured to use Kerberos, or modify SVMs to use a different Service Principal Name (SPN), the original service principal of the SVM is not automatically deleted or disabled from the Kerberos realm. You must manually delete or disable the principal. You must have the Kerberos realm administrator's user name and password to delete or disable the principal.

If you want to move data from an SVM to another SVM before you delete the first SVM, you can use the SnapMirror technology.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

## Starting SVMs

You can use System Manager to provide data access from a Storage Virtual Machine (SVM) by starting the SVM.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM that you want to start, and then click **Start**.

### Result

The SVM starts serving data to clients.

## Stopping SVMs

You can use System Manager to stop a Storage Virtual Machine (SVM) if you want to troubleshoot any issue with the SVM, delete the SVM, or stop data access from the SVM.

### Before you begin

All the clients connected to the SVM must be disconnected.

**Attention:** If any clients are connected to the SVM when you stop it, data loss might occur.

### About this task

- You cannot stop SVMs during storage failover (SFO).
- When you stop the SVM, an SVM administrator cannot log in to the SVM.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM that you want to stop, and then click **Stop**.

### Result

The SVM stops serving data to clients.

## What SVMs are

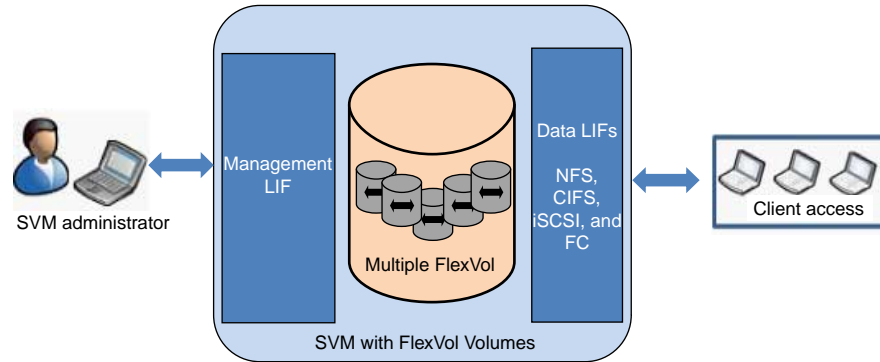
Storage Virtual Machines (SVMs, formerly known as Vservers) contain data volumes and one or more LIFs through which they serve data to the clients. Starting with clustered Data ONTAP 8.1.1, SVMs can either contain one or more FlexVol volumes, or a single Infinite Volume.

SVMs securely isolate the shared virtualized data storage and network, and each SVM appears as a single dedicated server to the clients. Each SVM has a separate administrator authentication domain and can be managed independently by its SVM administrator.

In a cluster, SVMs facilitate data access. A cluster must have at least one SVM to serve data. SVMs use the storage and network resources of the cluster. However, the volumes and LIFs are exclusive to the SVM. Multiple SVMs can coexist in a single cluster without being bound to any node in a cluster. However, they are bound to the physical cluster on which they exist.

A cluster can have one or more SVMs with FlexVol volumes and SVMs with Infinite Volume.

## SVM with FlexVol volumes

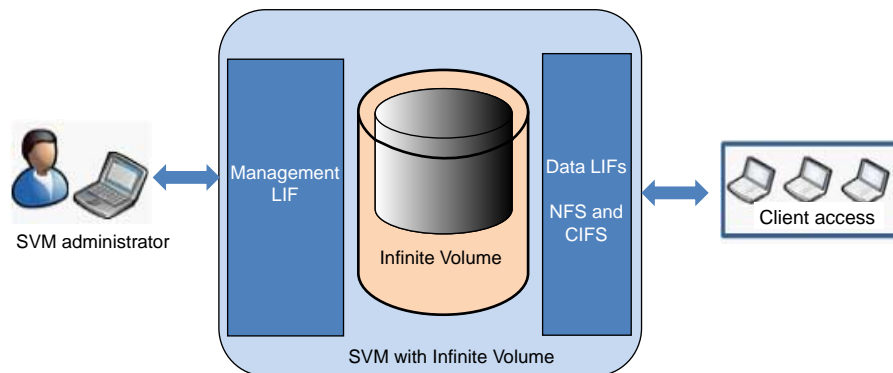


Each SVM with FlexVol volumes in a NAS environment presents a single directory hierarchical view and has a unique namespace. The namespace enables NAS clients to access data without specifying the physical location of the data. The namespace also enables the cluster and SVM administrators to manage distributed data storage as a single directory with multiple levels of hierarchy.

The volumes within each NAS SVM are related to each other through junctions and are mounted on junction paths. These junctions present the file system in each volume. The root volume of the SVM is a FlexVol volume that resides at the top level of the namespace hierarchy; additional volumes are mounted to the SVM root volume to extend the namespace. As volumes are created for the SVM, the root volume of the SVM contains junction paths.

SVMs with FlexVol volumes can contain files and LUNs. They provide file-level data access by using NFS and CIFS protocols for the NAS clients, and block-level data access by using iSCSI and Fibre Channel (FC) (FCoE included) for SAN hosts.

## SVM with Infinite Volume



SVMs with Infinite Volume can contain only one Infinite Volume to serve data. Each SVM with Infinite Volume includes only one junction path, which has a default value of `/NS`. The junction provides a single mount point for the large namespace provided by the SVM with Infinite Volume. You cannot add more junctions to an SVM with Infinite Volume. However, you can increase the size of the Infinite Volume.

SVMs with Infinite Volume can contain only files. They provide file-level data access by using NFS and CIFS protocols. SVMs with Infinite Volume cannot contain LUNs and do not provide block-level data access.

**Note:** The Data ONTAP command-line interface (CLI) continues to use the term *Vserver* in the output, and `vserver` as a command or parameter name has not changed.

## Managing SVMs

Storage Virtual Machine (SVM) administrators can administer SVMs and its resources, such as volumes, protocols, and services, depending on the capabilities assigned by the cluster administrator. SVM administrators cannot create, modify, or delete SVMs.

**Note:** SVM administrators cannot log in to System Manager.

SVM administrators might have all or some of the following administration capabilities:

- Data access protocol configuration  
SVM administrators can configure data access protocols, such as NFS, CIFS, iSCSI, and Fibre Channel (FC) protocol (Fibre Channel over Ethernet or FCoE included).
- Services configuration  
SVM administrators can configure services such as LDAP, NIS, and DNS.
- Storage management  
SVM administrators can manage volumes, quotas, qtrees, and files.
- LUN management in a SAN environment
- Management of Snapshot copies of the volume
- Monitoring SVM  
SVM administrators can monitor jobs, network connection, network interface, and the SVM health.

### Related information

*NetApp Documentation: ONTAP 9*

## Types of SVMs

A cluster consists of three types of SVMs, which help in managing the cluster and its resources and data access to the clients and applications.

A cluster contains the following types of SVMs:

- Admin SVM  
The cluster setup process automatically creates the admin SVM for the cluster. The admin SVM represents the cluster.
- Node SVM  
A node SVM is created when the node joins the cluster, and the node SVM represents the individual nodes of the cluster.
- System SVM (advanced)  
A system SVM is automatically created for cluster-level communications in an IPspace.
- Data SVM  
A data SVM represents the data serving SVMs. After the cluster setup, a cluster administrator must create data SVMs and add volumes to these SVMs to facilitate data access from the cluster. A cluster must have at least one data SVM to serve data to its clients.

**Note:** Unless otherwise specified, the term SVM refers to data (data-serving) SVM, which applies to both SVMs with FlexVol volumes and SVMs with Infinite Volume.

In the CLI, SVMs are displayed as Vservers.

## Why you use SVMs

Storage Virtual Machines (SVMs, formerly known as Vservers) provide data access to clients regardless of the physical storage or controller, similar to any storage system. SVMs provide benefits such as nondisruptive operations, scalability, security, and unified storage.

SVMs provide the following benefits:

- **Multi-tenancy**  
SVM is the fundamental unit of secure multi-tenancy, which enables partitioning of the storage infrastructure so that it appears as multiple independent storage systems. These partitions isolate the data and management.
- **Nondisruptive operations**  
SVMs can operate continuously and nondisruptively for as long as they are needed. SVMs help clusters to operate continuously during software and hardware upgrades, addition and removal of nodes, and all administrative operations.
- **Scalability**  
SVMs meet on-demand data throughput and the other storage requirements.
- **Security**  
Each SVM appears as a single independent server, which enables multiple SVMs to coexist in a cluster while ensuring no data flows among them.
- **Unified storage**  
SVMs can serve data concurrently through multiple data access protocols. SVMs provide file-level data access through NAS protocols, such as CIFS and NFS, and block-level data access through SAN protocols, such as iSCSI and FC (FCoE included). SVMs can serve data to SAN and NAS clients independently at the same time.  
  
**Note:** SVMs with Infinite Volume can serve data only through NFS and CIFS protocols.
- **Delegation of management**  
Each SVM can have its own user and administration authentication. SVM administrators can manage the SVMs that they are authorized to access. However, SVM administrators have privileges assigned by the cluster administrators.
- **Easy management of large datasets**  
With SVMs with Infinite Volume, management of large and unstructured data is easier because the SVM administrator can manage one data container instead of many.

## How ONTAP name service switch configuration works

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each Storage Virtual Machine (SVM).

### Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for...	Valid sources are...
hosts	Converting host names to IP addresses	files, dns
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

### Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type...	To look up information in...	Managed by the command families...
files	Local source files	vserver services name-service unix-user vserver services name-service unix-group vserver services name-service netgroup vserver services name-service dns hosts
nis	External NIS servers as specified in the NIS domain configuration of the SVM	vserver services name-service nis-domain
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	vserver services name-service ldap
dns	External DNS servers as specified in the DNS configuration of the SVM	vserver services name-service dns

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include **files** and configure local users as a fallback in case NIS or LDAP authentication fails.

### Related tasks

[Editing SVM settings](#) on page 160

## Storage Virtual Machines window

You can use the Storage Virtual Machines window to manage your Storage Virtual Machines (SVMs) and display information about them.

You cannot manage (create, edit, delete, start, or stop) an SVM configured for disaster recovery (DR) by using System Manager. Also, you cannot view the storage objects associated with the SVM configured for disaster recovery in the application interface.

## Command buttons

### Create

Opens the Storage Virtual Machine (SVM) Setup wizard, which enables you to create a new SVM.

### Edit

Opens the Edit Storage Virtual Machine dialog box, which enables you to modify the properties, such as the name service switch, name mapping switch, and aggregate list, of a selected SVM.

### Delete

Deletes the selected SVMs.

### Start

Starts the selected SVM.

### Stop

Stops the selected SVM.

### Manage

Manages the storage, policies, and configuration for the selected SVM.

### Refresh

Updates the information in the window.

## SVM list

The SVM list displays the name of each SVM and the allowed protocols on it.

You can view only data SVMs by using System Manager.

### Name

Displays the name of the SVM.

### State

Displays the SVM state, such as Running, Starting, Stopped, or Stopping.

### Subtype

Displays the subtype of the SVM, which can be one of the following:

- default  
Specifies that the SVM is a data-serving SVM.
- dp-destination  
Specifies that the SVM is configured for disaster recovery.
- sync-source  
Specifies that the SVM is in the primary site of a MetroCluster configuration.
- sync-destination  
Specifies that the SVM is in the surviving site of a MetroCluster configuration.

### Allowed Protocols

Displays the allowed protocols, such as CIFS and NFS, on each SVM.

### IPspace

Displays the IPspace of the associated SVM.

### Volume Type

Displays the allowed volume type, such as FlexVol volume and Infinite Volume, on each SVM.

### Configuration State

Displays whether the configuration state of the SVM is locked or unlocked.

### Details area

The area below the SVM list displays detailed information, such as the type of volumes allowed, language, and Snapshot policy, about the selected SVM.

You can also configure the protocols that are allowed on this SVM. If you have not configured the protocols while creating the SVM, you can click the protocol link to configure the protocol.

You cannot configure protocols for an SVM configured for disaster recovery by using System Manager.

**Note:** If the FCP service is already started for the SVM, clicking the FC/FCoE link opens the Network Interfaces window.

The color indicates the status of the protocol configuration:

Status	Description
Green	<p>LIFs exist and the protocol is configured. You can click the link to view the configuration details.</p> <p><b>Note:</b> Configuration might be partially completed. However, service is running. You can create the LIFs and complete the configuration from the Network Interfaces window.</p>
Yellow	<p>Indicates one of the following:</p> <ul style="list-style-type: none"> <li>LIFs exist. Service is created but is not running.</li> <li>LIFs exist. Service is not created.</li> <li>Service is created. LIFs do not exist.</li> </ul>
Grey	The protocol is not configured. You can click the protocol link to configure the protocol.
Grey border	The protocol license has expired or is missing. You can click the protocol link to add the licenses in the Licenses page.

### Peer Storage Virtual Machines area

Displays a list of the SVMs that are peered with the selected SVM along with details of the applications that are using the peer relationship.

## Volumes

You can use System Manager to create, edit, and delete volumes.

You can access all the volumes in the cluster by using the Volumes tab or you can access the volumes specific to an SVM by using **SVMs > Volumes**.

**Note:** The Volumes tab is displayed only if you have enabled the CIFS and NFS licenses.



## Editing the volume properties

You can modify volume properties such as the volume name, security style, fractional reserve, and space guarantee by using System Manager. You can modify storage efficiency settings (deduplication schedule and policy, and compression) and space reclamation settings. You can also edit the export policy and incremental tape backup settings of Infinite Volumes.

### About this task

- You can set the fractional reserve to either zero percent or 100 percent.
- Data compression is not supported on 32-bit volumes.
- You cannot modify the security style of an Infinite Volume.
- For Data ONTAP 8.3.1 clusters, you can enable both inline and background compression for ONTAP Cloud for Amazon Web Services (AWS).  
However, compression is not supported for Data ONTAP Edge.
- You cannot use System Manager to modify the following properties of Infinite Volumes with storage classes:
  - SnapDiff settings
  - Storage efficiency settings
  - Space guarantee settings
- You cannot rename a SnapLock Compliance volume.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume that you want to modify, and then click **Edit**.  
The Edit Volume dialog box is displayed.
5. In the **General** tab, modify the following properties as required:
  - Volume name
  - Security style for the volume
  - Thin provisioning
6. Click the **Storage Efficiency** tab, and enable storage efficiency by configuring the following properties:
  - Deduplication
  - Data compression

You cannot enable background compression for a volume that is contained by an aggregate with All Flash Optimized personality. You can enable only inline compression for these volumes.

You can enable inline deduplication only on a volume that is contained by an aggregate with All Flash Optimized personality, or on a volume in a Flash Pool aggregate.

7. For SnapLock volumes, click the **SnapLock** tab, and perform the following steps:

- a. Specify the autocommit period.

The autocommit period determines how long a file in that volume must remain unchanged before it is committed to WORM state.

- b. Specify the minimum retention period and maximum retention period.

The values must be in the range of 1 day through 70 years or Infinite.

- c. Select the default retention period.

The default retention period must be within the specified minimum retention period and maximum retention period.

**8. Click the **Advanced** tab, and enable the following properties:**

- If you want the volume to automatically grow when the used space in the volume is above the grow threshold, select **Grow**.
- If you want the volume to grow or shrink in size in response to the amount of used space, select **Grow or Shrink**.
  - a. Specify the maximum size to which the volume can grow.
  - b. Specify the incremental size by which the volume can grow.
- Enable automatic deletion of older Snapshot copies by choosing one of the following options:
  - Try  
Deletes the Snapshot copies that are not locked by any other subsystems.
  - Destroy  
Deletes the Snapshot copies that are locked by the data-backing functionality.
  - Disrupt  
Deletes the Snapshot copies that can disrupt the data transfer.
- Select the caching policy that you want to assign to the volume.  
This option is available only for FlexVol volumes in a Flash Pool aggregate.
- Select the retention priority for cached data in the volume.  
This option is available only for FlexVol volumes in a Flash Pool aggregate.
- Specify the fractional reserve that you want to set for the volume.
- Update the access time for reading the file.  
This option is disabled for SnapLock volumes.

**9. Click **Save and Close**.**

**Related tasks**

[Setting up CIFS](#) on page 258

**Related references**

[Volumes window](#) on page 206

## Editing data protection volumes

You can use System Manager to modify the volume name for a data protection (DP) volume. If the source volume does not have storage efficiency enabled, you might want to enable storage efficiency only on the destination volume.

### About this task

You cannot modify storage efficiency on a mirror DP volume.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the data protection volume for which you want to edit the properties, and then click **Edit**.
5. In the **Edit Data Protection Volume** dialog box, modify the volume name.
6. Select **Enable Storage Efficiency**.

If storage efficiency is already enabled on the volume, then the check box is selected by default.

7. Optional: Click the **Advanced** tab, and perform the following steps:
  - a. Select the caching policy that you want to assign to the volume.
  - b. Select the retention priority for the cached data in the volume.

These options are only available for data protection FlexVol volumes in a Flash Pool aggregate.

8. Click **Save**.

## Deleting volumes

You can use System Manager to delete a FlexVol volume or an Infinite Volume when you no longer require the data that it contains, or if you have copied the data that it contains to another location. When you delete a volume, all the data in the volume is destroyed, and you cannot recover this data.

### Before you begin

- If the FlexVol volume is cloned, the FlexClone volumes must be either split from the parent volume or destroyed.
- The volume must be unmounted and in the offline state.
- If the volume is in one or more SnapMirror relationships, the SnapMirror relationships must be deleted.
- You can delete a complete SnapLock Enterprise volume or a file in a SnapLock Enterprise volume; however, you cannot delete only the data within a file in a SnapLock Enterprise volume.
- You cannot delete a SnapLock Compliance volume if data is committed to the volume.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.

3. Click the **Volumes** tab.
4. Select the volumes that you want to delete, and then click **Delete**.
5. Select the confirmation check box, and then click **Delete**.

#### Related references

[Volumes window](#) on page 206

## Creating FlexClone volumes

You can use System Manager to create a FlexClone volume when you require a writable, point-in-time copy of an existing FlexVol volume. You might want to create a copy of a volume for testing or to provide access to the volume for additional users, without giving them access to the production data.

#### Before you begin

- The FlexClone license must be installed on the storage system.
- The volume that you want to clone must be online and a non-root volume.

#### About this task

The base Snapshot copy that is used to create a FlexClone volume of a SnapMirror destination is marked as busy and cannot be deleted. If a FlexClone volume is created from a Snapshot copy that is not the most recent Snapshot copy, and that Snapshot copy no longer exists on the source volume, all SnapMirror updates to the destination volume fail.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume from the volume list.
5. Click **Clone > Create > Volume**.
6. In the **Create FlexClone Volume** dialog box, type the name of the FlexClone volume that you want to create.
7. Optional: If you want to enable thin provisioning for the new FlexClone volume, select **Thin Provisioning**.  
By default, this setting is the same as that of the parent volume.
8. Create a new Snapshot copy or select an existing Snapshot copy that you want to use as the base Snapshot copy for creating the new FlexClone volume.
9. Click **Clone**.

#### Related references

[Volumes window](#) on page 206

## Creating FlexClone files

You can use System Manager to create a FlexClone file, which is a writable copy of a parent file. You can use these copies to test applications.

### Before you begin

- The file that is cloned must be part of the active file system.
- The FlexClone license must be installed on the storage system.

### About this task

- FlexClone files are supported only for FlexVol volumes, not for Infinite Volumes.  
You can create a FlexClone file of a parent file that is within a volume by accessing the parent file from the volume it resides in and not the parent volume.
- You cannot create a FlexClone file on a SnapLock volume.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume from the volume list.
5. Click **Clone > Create > File**.
6. In the **Create FlexClone File** dialog box, select the file that you want to clone, and then specify a name for the FlexClone file.
7. Click **Clone**.

### Result

The FlexClone file is created in the same volume as the parent file.

### Related references

[Volumes window](#) on page 206

## Splitting a FlexClone volume from its parent volume

If you want a FlexClone volume to have its own disk space rather than using that of its parent volume, you can split the volume from its parent by using System Manager. After the split, the FlexClone volume becomes a normal FlexVol volume.

### Before you begin

The FlexClone volume must be online.

### About this task

The clone-splitting operation deletes all the existing Snapshot copies of the clone. The Snapshot copies that are required for SnapMirror updates are also deleted. Therefore, any further SnapMirror updates might fail.

You can pause the clone-splitting operation if you have to perform any other operation on the volume. You can resume the process after the operation is complete.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the FlexClone volume that you want to split from its parent volume.
5. Click **Clone > Split**.
6. Confirm the clone-split operation, and then click **Start Split** in the confirmation dialog box.

#### Related references

[Volumes window](#) on page 206

## Viewing the FlexClone volume hierarchy

You can use System Manager to view the hierarchy of FlexClone volumes and their parent volumes.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume from the volume list.
5. Click **Clone > View Hierarchy**.

Volumes that have at least one child FlexClone volume are displayed. The FlexClone volumes are displayed as children of their respective parent volumes.

#### Related references

[Volumes window](#) on page 206

## Changing the status of a volume

You can use System Manager to change the status of a FlexVol volume or an Infinite Volume when you want to take the volume offline, bring it back online, or restrict access to the volume. However, you cannot take a root volume offline.

#### Before you begin

- If you want a volume to be the target of a volume copy or a SnapMirror replication operation, the volume must be in the restricted state.
- For NAS volumes, the volume must be unmounted before you can take it offline.

#### About this task

You can take a volume offline to perform maintenance on the volume, move it, or destroy it. When a volume is offline, it is unavailable for read or write access by clients.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume for which you want to modify the status.
5. From the **Status** menu, click the volume status that you want.
6. In the confirmation dialog box, click the button for the volume status that you want.

**Related references**

[Volumes window](#) on page 206

**Viewing the Snapshot copies**

You can use System Manager to view a list of all the saved Snapshot copies for a selected volume from the Snapshot Copies tab in the lower pane of the Volumes window or the Infinite Volume window. You can use the list of saved Snapshot copies to rename, restore, or delete the selected Snapshot copy.

**Before you begin**

The volume must be online.

**About this task**

You can view Snapshot copies for only one volume at a time.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. In the upper pane of the **Infinite Volume** window, select the volume for which you want to view the Snapshot copies.
5. In the lower pane, click **Snapshot Copies**.

The list of available Snapshot copies for the selected volume is displayed.

**Creating Snapshot copies**

You can use System Manager to create a Snapshot copy of a volume outside a specified schedule to capture the state of the file system at a specific point in time.

**About this task**

It takes longer to create a Snapshot copy of an Infinite Volume than it does to create a Snapshot copy of a FlexVol volume because an Infinite Volume is larger than a FlexVol volume.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.

3. Click the **Volumes** tab.
4. Select the volume for which you want to create the Snapshot copy.
5. Click **Snapshot Copies > Create**.
6. In the **Create Snapshot Copy** dialog box, if you want to change the default name, specify a new name for the Snapshot copy.  
  
Valid characters are ASCII characters, numerals, the hyphen (-), underscore (\_), period (.), and the plus (+) symbols.  
  
The default name of a Snapshot copy consists of the volume name and the timestamp.
7. Click **Create**.
8. Verify that the Snapshot copy you created is included in the list of Snapshot copies in the **Snapshot Copies** tab.

#### Related references

[Volumes window](#) on page 206

## Setting the Snapshot copy reserve

You can use System Manager to reserve space (in percentage) for Snapshot copies in a volume. Setting the Snapshot copy reserve ensures that enough disk space is allocated for the Snapshot copies so that they do not consume the active file system space.

#### About this task

- The default space reserved for Snapshot copies is five percent for SAN and VMware volumes.
- You cannot use System Manager to modify the Snapshot copy reserve settings of Infinite Volumes with storage classes.  
Instead, you must use OnCommand Workflow Automation.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume for which you want to set the Snapshot copy reserve.
5. Click **Snapshot Copies > Configure**.
6. Type or select the percentage of the volume space that you want to reserve for the Snapshot copies, and then click **OK**.

#### Related references

[Volumes window](#) on page 206



## Hiding the Snapshot copy directory

You can use System Manager to hide the Snapshot copy directory (.snapshot) so that it is not visible when you view your volume directories. By default, the .snapshot directory is visible.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume for which you want hide the Snapshot copy directory.
5. Click **Snapshot Copies > Configure**.
6. Ensure that **Make snapshot directory (.snapshot) visible** is not selected, and then click **Ok**.

### Related references

[Volumes window](#) on page 206

## Scheduling automatic Snapshot copies

You can use System Manager to set up a schedule for creating automatic Snapshot copies of a volume. You can specify the time and frequency of creating the copies and specify the number of Snapshot copies that are saved.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Click **Snapshot Copies > Configure**.
5. In the **Configure Volume Snapshot Copies** dialog box, select **Enable scheduled Snapshot Copies**.
6. Select a Snapshot policy.  
Only policy-based Snapshot policies are available.
7. Click **OK** to save your changes and start your Snapshot copy schedule.

### Related references

[Volumes window](#) on page 206

## Restoring a volume from a Snapshot copy

You can use System Manager to restore a volume to a state recorded in a previously created Snapshot copy to retrieve lost information. When you restore a Snapshot copy, the restore operation overwrites the existing volume configuration. Any changes made to the data in the volume after the Snapshot copy was created are lost.

### Before you begin

- The SnapRestore license must be installed on your system.

- If the FlexVol volume you want to restore contains a LUN, the LUN must be unmounted or unmapped.
- There must be enough available space for the restored volume.
- Users accessing the volume must be notified that you are going to revert a volume, and that the data from the selected Snapshot copy replaces the current data in the volume.
- If you are restoring an Infinite Volume, the Snapshot copy must be valid, and the Infinite Volume must be online.

#### About this task

- If the volume contains junction points to other volumes, the volumes mounted on these junction points will not be restored.
- For Infinite Volume, you must restore the entire volume. You cannot restore single files or parts of files.
- You cannot restore Snapshot copies for SnapLock Compliance volumes.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume that you want to restore from a Snapshot copy.
5. Click **Snapshot Copies > Restore**.
6. Select the appropriate Snapshot copy, and then click **Restore**.
7. Select the confirmation check box, and then click **Restore**.

#### Related references

[Volumes window](#) on page 206

## Extending the expiry date of Snapshot copies

You can use System Manager to extend the expiry date of Snapshot copies in a volume.

#### Before you begin

The SnapLock license must be installed.

#### About this task

You can extend the expiry date only for Snapshot copies in a data protection (DP) volume that is the destination in a SnapLock for SnapVault relationship.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume.

5. Click the **Snapshot Copies** tab.
6. Select the Snapshot copy, and then click **Extend Expiry Date**.
7. In the **Extend Expiry Date** dialog box, specify the expiry date.  
The values must be in the range of 1 day through 70 years or Infinite.
8. Click **OK**.

## Renaming Snapshot copies

You can use System Manager to rename a Snapshot copy to help you organize and manage your Snapshot copies.

### About this task

- You cannot rename the Snapshot copies of an Infinite Volume.
- You cannot rename the Snapshot copies of a SnapLock DP volume, which are committed to WORM, that is in a SnapVault relationship.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume that contains the Snapshot copy that you want to rename.
5. In the lower pane of the **Volumes** window, click **Snapshot Copies**.
6. In the lower window pane, select the Snapshot copy that you want to rename, and then click **Rename**.
7. Specify the new name, and then click **Rename**.  
Valid characters are ASCII characters, numerals, hyphen (-), underscore (\_), period (.), and the plus (+) symbol.
8. Verify the Snapshot copy name in the **Snapshot Copies** tab of the **Volumes** window.

### Related references

[Volumes window](#) on page 206

## Deleting Snapshot copies

You can delete a Snapshot copy to conserve disk space or to free disk space by using System Manager. You can also delete a Snapshot copy if it is no longer required.

### Before you begin

If you want to delete a Snapshot copy that is busy or locked, you must have released the Snapshot copy from the application that was using it.

### About this task

- You cannot delete the base Snapshot copy in a parent volume if a FlexClone volume is using that Snapshot copy.

The base Snapshot copy is the Snapshot copy that is used to create the FlexClone volume. The base Snapshot copy always displays the status **busy** and Application Dependency as **busy, vclone** in the parent volume.

- You cannot delete a locked Snapshot copy that is used in a SnapMirror relationship. The Snapshot copy is locked and is required for the next update.
- You cannot delete a Snapshot copy from a SnapLock DP volume that is used in a SnapVault relationship before the Snapshot copy's expiry time.
- You cannot delete the unexpired Snapshot copies of a SnapLock DP volume, which are committed to WORM, that is in a SnapVault relationship.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume that contains the Snapshot copy that you want to delete.
5. Click **Storage > Volumes or Infinite Volumes**, and then click **Snapshot Copies** in the lower pane.
6. Select the Snapshot copy that you want to delete.
7. Click **Delete**.
8. Select the confirmation check box, and then click **Delete**.

### Related references

[Volumes window](#) on page 206

### Related information

[NetApp Documentation: ONTAP 9](#)

## Resizing volumes

When your volume reaches nearly full capacity, you can increase the size of the volume, delete some Snapshot copies, or adjust the Snapshot reserve. You can use the Volume Resize wizard in System Manager to provide more free space.

### About this task

- For a volume that is configured to grow automatically, you can modify the limit to which the volume can grow automatically, based on the increased size of the volume.
- You cannot reduce the size of an Infinite Volume.
- You cannot use System Manager to resize Infinite Volumes with storage classes. Instead, you must use OnCommand Workflow Automation.
- You cannot resize a data protection volume if its mirror relationship is broken or if a reverse resynchronization operation has been performed on the volume. Instead, you must use the command-line interface (CLI).

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume that you want to resize.
5. Click **Resize**.
6. Type or select information as prompted by the wizard.
7. Confirm the details, and then click **Finish** to complete the wizard.
8. Verify the changes you made to the available space and total space of the volume in the **Volumes** window.

**Related references**

[Volumes window](#) on page 206

**Enabling storage efficiency on a volume**

You can use System Manager to enable storage efficiency and configure deduplication and data compression or only deduplication on a volume to save storage space. If you have not enabled storage efficiency when you created the volume, you can do so later by editing the volume.

**Before you begin**

- The volume must be online.
- If you want to use a policy-based deduplication schedule, you must have created an efficiency policy.

**About this task**

- You can enable background compression only if you have enabled background deduplication.
- You can enable inline compression and inline deduplication with or without enabling background compression and background deduplication respectively.
- You can enable inline deduplication only on volumes contained by an aggregate with All Flash Optimized personality and on volumes contained by a Flash Pool aggregate.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume for which you want to enable storage efficiency, and then click **Edit**.
5. In the **Edit Volume** dialog box, click **Storage Efficiency**.
6. Select the **Background Deduplication** check box.
7. Select one of the following methods to run deduplication:

If you want to run deduplication...	Then...
Based on a storage efficiency policy	<ol style="list-style-type: none"> <li>Ensure that the <b>Policy based</b> option is selected.</li> <li>Click <b>Choose</b> to select a storage efficiency policy.</li> <li>Click <b>OK</b>.</li> </ol>
When required	Select the <b>On-demand</b> option.

- Optional: Select the **Background Compression** check box to enable background compression.  
You cannot enable background compression for a volume contained by an aggregate with All Flash Optimized personality.
- Optional: Select the **Inline Compression** check box to compress data while it is being written to the volume.  
  
By default, inline compression is enabled on volumes contained by an aggregate with All Flash Optimized personality.
- Optional: Select the **Inline Deduplication** check box to run deduplication before data is written to the disk.  
  
By default, inline deduplication is enabled on volumes contained by an aggregate with All Flash Optimized personality.
- Click **Save and Close**.

#### Related references

[Volumes window](#) on page 206

## Changing the deduplication schedule

You can use System Manager to change the deduplication schedule by choosing to run deduplication manually, automatically, or on a schedule that you specify.

#### Steps

- Click the **SVMs** tab.
- Select the SVM, and then click **Manage**.
- Click the **Volumes** tab.
- Select the read/write volume for which you want to modify the deduplication schedule.
- Click **Edit**, and then click the **Storage Efficiency** tab.
- Change the deduplication schedule as required.
- Click **Save and Close**.

#### Related references

[Volumes window](#) on page 206

## Running deduplication operations

You can use System Manager to run deduplication immediately after creating a FlexVol volume or an Infinite Volume, or schedule deduplication to run at a specified time.

### Before you begin

- Deduplication must be enabled on the volume.
- The volume must be online and mounted.

### About this task

Deduplication is a background process that consumes system resources during the operation; therefore, it might impact other operations that are in progress. You must cancel deduplication before you can perform any other operation.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume for which you want to run deduplication.
5. Click **Storage Efficiency**.
6. If you are running deduplication on the volume for the first time, run deduplication on the entire volume data by selecting **Scan Entire Volume** in the **Storage Efficiency** dialog box.
7. Click **Start**.
8. View the last-run details of the deduplication operation in the **Storage Efficiency** tab of the **Volumes** window.

### Related references

[Volumes window](#) on page 206

## Moving FlexVol volumes between aggregates or nodes

You can nondisruptively move a FlexVol volume to a different aggregate or a different node for capacity utilization and improved performance by using System Manager.

### Before you begin

If you are moving a data protection volume, the data protection mirror relationships must be initialized before you move the volume.

### About this task

You cannot move SnapLock volumes between aggregates and nodes.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.

3. Click the **Volumes** tab.
4. Select the volume that you want to move, and then click **Move**.
5. In the **Move Volume dialog box**, select the destination aggregate or node for the volume.
6. Click **Move**.

### Manually triggering the cutover for volume move

For a volume move operation, you can use System Manager to manually trigger the cutover when the volume enters the cutover deferred phase. You can set the duration of the cutover and the cutover action to be performed by the system if the operation fails within that duration.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume for which the volume move operation has been initiated.
5. In the **Volume Move Details** tab, click **Cutover**.
6. In the **Cutover** dialog box, click **Advanced Options**.
7. Optional: Specify the cutover action and the cutover window period.
8. Click **OK**.

### Assigning volumes to Storage QoS

You can limit the throughput of FlexVol volumes by assigning them to Storage Quality of Service (QoS) policy groups. You can assign Storage QoS for new volumes or modify Storage QoS details for volumes that are already assigned to a policy group by using System Manager.

#### About this task

- You can assign Storage QoS only to read/write (rw) volumes that are online.
- You cannot assign Storage QoS to a volume if the following storage objects are assigned to a policy group:
  - Parent Storage Virtual Machine (SVM) of the volume
  - Child LUNs of the volume
  - Child files of the volume
- You can assign Storage QoS or modify QoS details for a maximum of 10 volumes at the same time.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select one or more volumes for which you want to assign Storage QoS.



5. Click **Storage QoS**.

6. In the **Quality of Service Details** dialog box, select the **Manage Storage Quality of Service** check box if you want to manage the workload performance of the FlexVol volume.

If some of the volumes you selected are already assigned to a policy group, the changes that you make might affect the performance of these volumes.

7. Create a new storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the FlexVol volume:

If you want to...	Then do the following...
Create a new policy group	<p><b>a.</b> Specify the policy group name.</p> <p><b>b.</b> Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. If you do not specify the maximum throughput limit, the value is set to Unlimited and the unit that you specify does not affect the maximum throughput.</p>
Select an existing policy group	<p>Select <b>Existing Policy Group</b> and click <b>Choose</b> to select an existing policy group from the Select Policy Group dialog box.</p> <p>You can also choose to modify the maximum throughput for the selected policy group.</p> <p>If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.</p>

8. Optional: Click the link that specifies the number of volumes to review the list of selected volumes, and then click **Discard** if you want to remove any volumes from the list.

The link is displayed only when multiple volumes are selected.

9. Click **OK**.

## Creating a mirror relationship from a source SVM

You can use System Manager to create a mirror relationship from the source Storage Virtual Machine (SVM), and to assign a mirror policy and schedule to the mirror relationship. The mirror copy enables quick availability of data if the data on the source volume is corrupted or lost.

### Before you begin

- The SnapMirror license must be enabled on the source cluster and the destination cluster.
- While mirroring a volume, if you create a SnapLock volume, then the SnapMirror and SnapLock licenses must be installed on both the source cluster and destination cluster.
- The source cluster and destination cluster must be in a healthy peer relationship.
- For Infinite Volumes, the destination Storage Virtual Machine (SVM) must not contain a read/write Infinite Volume or an Infinite Volume with storage classes.
- The destination aggregate must have free space available.
- If the source Infinite Volume and destination Infinite Volume share aggregates with other Infinite Volumes or FlexVol volumes in the same cluster, sufficient shared aggregate space must be available for the destination Infinite Volume.  
If the source Infinite Volume and destination Infinite Volume do not share aggregates with other Infinite Volumes or FlexVol volumes in the same cluster, you can create the same number and size of aggregates for the destination volume as those used by the source volume.

- If the destination volume exists, the volume must not be the destination for any other mirror relationship.
- The capacity of the destination volume must be greater than or equal to the capacity of the source volume.
- If autogrow is disabled, the free space on the destination volume must be at least five percent more than the used space on the source volume.

#### About this task

- You cannot use System Manager to create a mirror relationship if the source volume is an Infinite Volume with storage classes.  
Instead, you should use OnCommand Workflow Automation.
- System Manager does not support a cascade relationship.  
For example, a destination volume in a relationship cannot be the source volume in another relationship.
- You can create a mirror relationship between SnapLock volumes of the same type only.  
For example, if the source volume is a SnapLock Enterprise volume, then the destination volume must also be a SnapLock Enterprise volume.
- You can use System Manager to only view the FlexGroup volume relationships.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume for which you want to create a mirror relationship, and then click **Protect**.  
The **Protect** option is available only for a read/write volume.
5. In the **Create Protection Relationship** dialog box, select **Mirror** from the **Relationship Type** drop-down list.
6. Optional: Select the **Create version-flexible mirror relationship** check box to create a mirror relationship that is independent of the ONTAP version running on the source cluster and destination cluster, and to back up the Snapshot copies from the source volume.  
If you select this option, the SnapLock volumes will not be displayed.
7. Specify the cluster, the SVM, and the destination volume.
8. If the selected SVM is not peered, use the **Authenticate** link to enter the credentials of the remote cluster and create the SVM peer relationship.
9. Optional: Enter an alias name for the remote SVM in the **Enter Alias Name for SVM** dialog box.
10. For FlexVol volumes, create a new destination volume or select an existing volume:

If you want to...	Do the following...
Create a new volume	If you want to change the default name, which is displayed in the format <i>source_SVM_name_source_volume_name_mirror</i> , specify a new name, and select the containing aggregate for the destination volume.

If you want to...	Do the following...
Select an existing volume	Select the <b>Select Volume</b> option.  <b>Note:</b> Only those volumes with the same language attribute as that of the source volume are listed.

For Infinite Volumes, you can create a destination volume only if the destination SVM does not contain a volume.

**11.** Select an existing policy or create a new policy:

If you want to...	Do the following...
Select an existing policy	Select a mirror policy from the list.
Create a new policy	<ol style="list-style-type: none"> <li>Click <b>Create Policy</b>.</li> <li>Specify a policy name, and set the schedule transfer priority. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to normal.</li> <li>Select the <b>Transfer All Source Snapshot Copies</b> check box to include the “all_source_snapshots” rule to the mirror policy, which will enable you to back up all the Snapshot copies from the source volume.</li> <li>Select the <b>Enable Network Compression</b> check box to compress the data that is being transferred.</li> <li>Click <b>Create</b>.</li> </ol>

**12.** Specify a schedule for the relationship:

If...	Do the following...
You want to assign an existing schedule	From the list of schedules, select an existing schedule.
You want to create a new schedule	<ol style="list-style-type: none"> <li>Click <b>Create Schedule</b>.</li> <li>Specify a name for the schedule.</li> <li>Select either <b>Basic</b> or <b>Advanced</b>. <ul style="list-style-type: none"> <li>Basic: You can select this option to specify only the day of the week, time, and the transfer interval.</li> <li>Advanced: You can select this option to specify a cron-style schedule.</li> </ul> </li> <li>Click <b>Create</b>.</li> </ol>
You do not want to assign a schedule	Select <b>None</b> .

**13.** Select **Initialize Relationship**.

**14.** Click **Create**.

**Result**

A new destination volume of type *dp* is created with the following default settings:

- Autogrow is enabled.
- Compression is disabled.
- The language attribute is set to match the language attribute of the source volume.

If the destination FlexVol volume is on a different SVM than the source, then a peer relationship is created between the two SVMs if the relationship does not already exist.

A mirror relationship is created between the source volume and the destination volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.

#### Related references

[Protection window](#) on page 364

## Creating a vault relationship from a source SVM

You can use System Manager to create a vault relationship from the source Storage Virtual Machine (SVM), and to assign a vault policy to the vault relationship to create a backup vault. In the event of data loss or corruption on a system, backed-up data can be restored from the backup vault destination.

#### Before you begin

- The SnapVault license or SnapMirror license must be enabled on both the source cluster and the destination cluster.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination aggregate must have available space.
- The source aggregate and the destination aggregate must be 64-bit aggregates.
- A vault (XDP) policy must exist.  
If a vault policy does not exist, you must create one or accept the default vault policy (named XDPDefault) that is automatically assigned.
- The capacity of the destination volume must be greater than or equal to the capacity of the source volume.
- If autogrow is disabled, the free space on the destination volume must be at least five percent more than the used space on the source volume.

#### About this task

- System Manager does not support a cascade relationship.  
For example, a destination volume in a relationship cannot be the source volume in another relationship.
- You can create a vault relationship only between a non-SnapLock (primary) volume and a Snaplock destination (secondary) volume.
- You can use System Manager to only view the FlexGroup volume relationships.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.

4. Select the volume for which you want to create a vault relationship, and then click **Protect**.  
The **Protect** option is available only for a read/write volume.
5. In the **Create Protection Relationship** dialog box, select **Vault** from the **Relationship Type** drop-down list.
6. Specify the cluster, the SVM, and the destination volume.
7. If the selected SVM is not peered, use the **Authenticate** link to enter the credentials of the remote cluster, and create an SVM peer relationship.
8. Optional: Enter an alias name for the remote SVM in the **Enter Alias Name for SVM** dialog box.
9. Create a new destination volume or select an existing volume:

If you want to...	Do the following...
Create a new volume	<ol style="list-style-type: none"> <li>a. If you want to change the default name, which is displayed in the format <i>source_SVM_name_source_volume_name_vault</i>, specify a new name, and select the containing aggregate for the destination volume.</li> <li>b. Select <b>Enable dedupe</b> to enable deduplication on the new destination volume. If deduplication is disabled on the source volume, then the check box for the new volume is selected by default.</li> </ol>
Select an existing volume	Select the <b>Select Volume</b> option.  <b>Note:</b> Only those volumes with the same language attribute as that of the source volume are listed.

10. If you are creating a SnapLock volume, specify the default retention period.  
The default retention period can be set to any value between 1 day through 70 years or Infinite.
11. Select an existing policy or create a new policy:

If you want to...	Do the following...
Select an existing policy	Select a vault policy from the list.  You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.
Create a new policy	<ol style="list-style-type: none"> <li>a. Click <b>Create Policy</b>.</li> <li>b. Specify a policy name, and set the schedule transfer priority. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to normal.</li> <li>c. Select the <b>Enable Network Compression</b> check box to compress the data that is being transferred.</li> <li>d. Click <b>Create</b>.</li> </ol> <p>You can also specify the SnapMirror label and destination retention count for the vault policy. For the new SnapMirror label to be effective, you must ensure that a Snapshot copy with the same label is created on the source volume.</p>

12. Specify a schedule for the relationship:

If...	Do the following...
You want to assign an existing schedule	From the list of schedules, select an existing schedule.
You want to create a new schedule	<ol style="list-style-type: none"> <li>Click <b>Create Schedule</b>.</li> <li>Specify a name for the schedule.</li> <li>Select <b>Basic</b> or <b>Advanced</b>. <ul style="list-style-type: none"> <li>Basic: You can select this option to specify only the day of the week, time, and the transfer interval.</li> <li>Advanced: You can select this option to specify a cron-style schedule.</li> </ul> </li> <li>Click <b>Create</b>.</li> </ol>
You do not want to assign a schedule	Select <b>None</b> .

**13.** Optional: Select **Initialize Relationship**.

**14.** Click **Create**.

### Result

If you chose to create a new destination volume, a volume of type *dp* is created with the following default settings:

- Autogrow is enabled.
- Deduplication is enabled or disabled as per the user preference or the source volume deduplication setting.
- Compression is disabled.
- The language attribute is set to match the language attribute of the source volume.

If the destination volume is on a different SVM than the source volume, then a peer relationship is created between the two SVMs if a peer relationship did not exist.

A vault relationship is created between the source volume and the destination volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.

### Related references

[Protection window](#) on page 364

## Creating a mirror and vault relationship from a source SVM

You can use System Manager to create a mirror and vault relationship from the source Storage Virtual Machine (SVM). Creating this relationship enables you to better protect your data by periodically transferring data from the source volume to the destination volume. It also enables you to retain data for long periods by creating backups of the source volume.

### Before you begin

- The source cluster must be running ONTAP 8.3.2 or later.
- The SnapMirror license must be enabled on both the source cluster and destination cluster that contain the source volume and destination volume.

- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination aggregate must have available space.
- The source aggregate and the destination aggregate must be 64-bit aggregates.
- If the destination volume exists, the volume must not be the destination for any other protection relationship.
- The capacity of the destination volume must be greater than or equal to the capacity of the source volume.
- If autogrow is disabled, the free space on the destination volume must be at least five percent more than the used space on the source volume.

#### About this task

- System Manager does not support a cascade relationship.  
For example, a destination volume in a relationship cannot be the source volume in another relationship.
- The destination volume that is created for a mirror and vault relationship is not thin-provisioned.
- You can use System Manager to only view the FlexGroup volume relationships.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume for which you want to create a mirror and vault relationship, and then click **Protect**.  
The **Protect** option is available only for a read/write volume.
5. In the **Create Protection Relationship** dialog box, select **Mirror and Vault** from the **Relationship Type** drop-down list.
6. Specify the cluster, the SVM, and the destination volume.
7. If the selected SVM is not peered, use the **Authenticate** link to enter the credentials of the remote cluster and create the SVM peer relationship.
8. Optional: Enter an alias name for the remote SVM in the **Enter Alias Name for SVM** dialog box.
9. Create a new destination volume or select an existing volume:

If you want to...	Do the following...
Create a new volume	<ol style="list-style-type: none"> <li>a. If you want to change the default name, which is displayed in the format <code>source_SVM_name_source_volume_name_mirror_vault</code>, specify a new name, and then select the containing aggregate for the destination volume.</li> <li>b. Select <b>Enable dedupe</b> to enable deduplication on the new destination volume. If deduplication is disabled on the source volume, then the check box for the new volume is selected by default.</li> </ol>

If you want to...	Do the following...
Select an existing volume	Select the <b>Select Volume</b> option.  <b>Note:</b> Only those volumes with the same language attribute as the source volume are listed.

10. Select an existing policy or create a new policy:

If you want to...	Do the following...
Select an existing policy	Click <b>Browse</b> , and then select a mirror and vault policy.  You can select the policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.
Create a new policy	<ol style="list-style-type: none"> <li>Click <b>Create Policy</b>.</li> <li>Specify the policy name, and set the schedule transfer priority. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to normal.</li> <li>Select the <b>Enable Network Compression</b> check box to compress the data that is being transferred.</li> <li>Click <b>Create</b>.</li> </ol> <p>You can also specify the SnapMirror label and destination retention count for the policy. For the new SnapMirror label to be effective, you must ensure that a Snapshot copy with the same label is created on the source volume.</p>

11. Specify a schedule for the relationship:

If...	Do the following...
You want to assign an existing schedule	From the list of schedules, select an existing schedule.
You want to create a new schedule	<ol style="list-style-type: none"> <li>Click <b>Create Schedule</b>.</li> <li>Specify a name for the schedule.</li> <li>Select <b>Basic</b> or <b>Advanced</b>. <ul style="list-style-type: none"> <li>Basic: You can select this option to specify only the day of the week, time, and the transfer interval.</li> <li>Advanced: You can select this option to specify a cron-style schedule.</li> </ul> </li> <li>Click <b>Create</b>.</li> </ol>
You do not want to assign a schedule	Select <b>None</b> .

12. Optional: Select **Initialize Relationship** to initialize the relationship.

13. Click **Create**.



## Creating an NFS datastore for VMware

You can use the Create NFS Datastore for VMware wizard in System Manager to create an NFS datastore for VMware. You can create a volume for the NFS datastore and specify the ESX servers that can access the NFS datastore.

### Before you begin

The NFS service must be licensed.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume and click **Provision Storage for VMware**.
5. In the **Create NFS Datastore for VMware** wizard, type or select information as requested by the wizard.
6. Confirm the details, and then click **Finish** to complete the wizard.

## Creating FlexGroup volumes

You can use System Manager to create a FlexGroup volume by selecting specific aggregates or by selecting system recommended aggregates.

### About this task

You can create only read/write (rw) FlexGroup volumes.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Click the **FlexGroups** tab.
5. Click **Create**.
6. In the **Create FlexGroup** window, specify a name for the FlexGroup volume.
7. Optional: Select the space reserve.
8. Select the required aggregates or select **Recommended per best practices**.
9. Specify a size for the FlexGroup volume.
10. Click **Save** to create the FlexGroup volume.

## Editing FlexGroup volumes

You can use System Manager to edit the properties of an existing FlexGroup volume.

### Before you begin

The FlexGroup volume must be online.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Click the **FlexGroups** tab.
5. Select the FlexGroup volume that you want to modify, and click **Edit**.
6. Select the security style for the FlexGroup volume.
7. Enable **Fractional Reserve (100%)** to enable fractional reserve for the FlexGroup volume.
8. Enable **Update Access Time on Read** to specify the access time when a file is read.
9. Click **Save Changes** to save the changes.

## Resizing FlexGroup volumes

You can use System Manager to resize a FlexGroup volume by resizing existing resources or adding new resources.

### Before you begin

- To resize a FlexGroup volume, there must be enough free space on the existing aggregates.
- To expand a FlexGroup volume, there must be enough free space on the cluster.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Click the **FlexGroups** tab.
5. Select the FlexGroup volume that you want to resize, and click **Actions > Resize**.
6. Select a resize option:

If you want to...	Then...
Resize using existing resources	<ol style="list-style-type: none"> <li>a. Click <b>Resizing using the existing resources</b>.</li> <li>b. Specify the size to which you want to resize the FlexGroup volume.</li> <li>c. Specify the percentage of Snapshot reserve.</li> </ol>

If you want to...	Then...
Expand by adding new resources	<ol style="list-style-type: none"> <li>a. Click <b>Expanding by adding new resources</b>.</li> <li>b. Select the aggregates that you want to use for adding resources.</li> <li>c. Specify the size to which you want to expand the FlexGroup volume.</li> </ol>

7. Click **Resize** to resize the FlexGroup volume.

## Changing the status of a FlexGroup volume

You can use System Manager to change the status of a FlexGroup volume when you want to take the FlexGroup volume offline, bring it back online, or restrict access to the FlexGroup volume.

### About this task

System Manager does not support constituent level of management for FlexGroup volumes.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Click the **FlexGroups** tab.
5. Select the FlexGroup volume for which you want to modify the status.
6. Click **Action > Change status to**, and then update the FlexGroup volume status by selecting the status of your choice.

## Deleting FlexGroup volumes

You can use System Manager to delete a FlexGroup volume when you no longer require the FlexGroup volume.

### Before you begin

- The junction path of the FlexGroup volume must be unmounted.
- The FlexGroup volume must be offline.

### About this task

System Manager does not support constituent level of management for FlexGroup volumes.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Click the **FlexGroups** tab.
5. Select the FlexGroup volume that you want to delete, and then click **Delete**.
6. Select the confirmation check box, and then click **OK**.

## Viewing FlexGroup volume information

You can use System Manager to view information about a FlexGroup volume. You can view a graphical representation of the space allocated, the protection status, and the performance of the FlexGroup volume.

### About this task

You can also view the Snapshot copies that are available for the FlexGroup volume, the data protection relationships for the FlexGroup volume, and the average performance metrics, read performance metrics, and write performance metrics of the FlexGroup volume based on latency, IOPS, and throughput.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Click the **FlexGroups** tab.
5. From the displayed list of FlexGroup volumes, expand the FlexGroup volume about which you want to view information.  
  
The information about the FlexGroup volume, the space allocated to the FlexGroup volume, the protection status of the FlexGroup volume, and the performance information about the FlexGroup volume are displayed.
6. Click the **Show More Details** link to view more information about the FlexGroup volume.
7. Click the **Snapshot Copies** tab to view the Snapshot copies for the FlexGroup volume.
8. Click the **Data Protection** tab to view the data protection relationships for the FlexGroup volume.
9. Click the **Performance** tab to view the the average performance metrics, read performance metrics, and write performance metrics of the FlexGroup volume based on latency, IOPS, and throughput.

## What volume granular encryption is

Volume granular encryption (VGE) is the process of protecting the user data, including the metadata, by encrypting the data before storing it on the disk. The data is decrypted and provided to the user only after proper authentication is provided. To encrypt data, an encryption key is required. Each volume is assigned an encryption key to encrypt/decrypt operations of its data.

## How FlexVol volumes work

FlexVol volumes allow you to manage the logical layer of the file system independently of the physical layer of storage. Multiple FlexVol volumes can exist within a single separate, physically defined aggregate structure of disks and RAID groups. FlexVol volumes contained by the same aggregate share the physical storage resources, RAID configuration, and plex structure of that aggregate.

Using multiple FlexVol volumes enables you to do the following:

- Perform administrative and maintenance tasks (for example, backup and restore) on individual FlexVol volumes rather than on a single, large file system.
- Set services (for example, Snapshot copy schedules) differently for individual FlexVol volumes.

- Minimize interruptions in data availability by taking individual FlexVol volumes offline to perform administrative tasks on them while the other FlexVol volumes remain online.
- Save time by backing up and restoring individual FlexVol volumes instead of all the file systems an aggregate contains.

## What an Infinite Volume is

An Infinite Volume is a single, scalable volume that can store up to 2 billion files and tens of petabytes of data.

With an Infinite Volume, you can manage multiple petabytes of data in one large logical entity and clients can retrieve multiple petabytes of data from a single junction path for the entire volume.

An Infinite Volume uses storage from multiple aggregates on multiple nodes. You can start with a small Infinite Volume and expand it nondisruptively by adding more disks to its aggregates or by providing it with more aggregates to use.

## Considerations for creating a FlexClone volume from a SnapMirror source or destination volume

You can create a FlexClone volume from the source or destination volume in an existing volume SnapMirror relationship. However, doing so could prevent future SnapMirror replication operations from completing successfully.

Replication might not work because when you create the FlexClone volume, you might lock a Snapshot copy that is used by SnapMirror. If this happens, SnapMirror stops replicating to the destination volume until the FlexClone volume is destroyed or is split from its parent. You have two options for addressing this issue:

- If you require the FlexClone volume on a temporary basis and can accommodate a temporary stoppage of the SnapMirror replication, you can create the FlexClone volume and either delete it or split it from its parent when possible.  
The SnapMirror replication continues normally when the FlexClone volume is deleted or is split from its parent.
- If a temporary stoppage of the SnapMirror replication is not acceptable, you can create a Snapshot copy in the SnapMirror source volume, and then use that Snapshot copy to create the FlexClone volume. (If you are creating the FlexClone volume from the destination volume, you must wait until that Snapshot copy replicates to the SnapMirror destination volume.)  
This method of creating a Snapshot copy in the SnapMirror source volume allows you to create the clone without locking a Snapshot copy that is in use by SnapMirror.

## Snapshot configuration

You can configure Snapshot copies by setting a schedule to an existing Snapshot policy. You can have a maximum of 255 Snapshot copies of a FlexVol volume. You can change the maximum number of Snapshot copies for a Snapshot policy's schedule.

## Guidelines for working with Snapshot copies of Infinite Volumes

You can create, manage, and restore Snapshot copies of Infinite Volumes. However, you should be aware of the factors affecting the Snapshot creation process and the requirements for managing and restoring the copies.

### Guidelines for creating Snapshot copies of Infinite Volumes

- The volume must be online.
- The Snapshot copy schedule should not be less than hourly.

It takes longer to create a Snapshot copy of an Infinite Volume than of a FlexVol volume. If you schedule Snapshot copies of Infinite Volumes for less than hourly, Data ONTAP tries but might not meet the schedule. Scheduled Snapshot copies are missed when the previous Snapshot copy is still being created.

- Time should be synchronized across all the nodes that the Infinite Volume spans. Synchronized time helps schedules for Snapshot copies run smoothly and restoration of Snapshot copies function properly.
- The Snapshot copy creation job can run in the background. Creating a Snapshot copy of an Infinite Volume is a volume-level job (unlike the same operation on a FlexVol volume), and the operation spans multiple nodes in the cluster.
- After you create Snapshot copies of an Infinite Volume, you cannot rename the copy or modify the comment or SnapMirror label for the copy.

### **Guidelines for managing Snapshot copy disk consumption**

- You cannot calculate the amount of disk space that can be reclaimed if Snapshot copies of an Infinite Volume are deleted.
- The size of a Snapshot copy for an Infinite Volume excludes the size of namespace mirror constituents.
- To reclaim disk space used by Snapshot copies of Infinite Volumes, you must manually delete the copies. You cannot use the automatic Snapshot copy deletion feature to automatically delete Snapshot copies of Infinite Volumes. However, you can manually delete Snapshot copies of Infinite Volumes, and you can run the delete operation in the background.

### **Guidelines for restoring Snapshot copies of Infinite Volumes**

- You must restore the entire Snapshot copy of the Infinite Volume. You cannot restore single files or parts of files. You also cannot restore a Snapshot copy of a single constituent.
- The Snapshot copy must be in a valid state. You cannot use admin privilege to restore a Snapshot copy of an Infinite Volume if the copy is in a partial or invalid state because the commands require diagnostic privilege. However, you can contact technical support to run the commands for you.
- Restored Snapshot copies inherit the current efficiency settings of the Infinite Volume.

## **When Snapshot copies of Infinite Volumes are accessible**

Snapshot copies of an Infinite Volume are restorable and fully accessible to clients only when the Snapshot copies are in a valid state.

A Snapshot copy of an Infinite Volume consists of information spanning multiple constituents across multiple aggregates. Although a Snapshot copy cannot be created if a constituent is offline, a constituent might be deleted or taken offline after the Snapshot copy is created. If a Snapshot copy of an Infinite Volume references a constituent that is offline or deleted, the Snapshot copy might not be fully accessible to clients or restorable.

The availability of a Snapshot copy of an Infinite Volume is indicated by its state, as explained in the following table:

State	Description	Client access to the Snapshot copy	Impact on restore
Valid	The copy is complete.	Fully accessible to clients	Can be restored
Partial	Data is missing or incomplete.	Partially accessible to clients	Cannot be restored without assistance from technical support
Invalid	Namespace information is missing or incomplete.	Inaccessible to clients	Cannot be restored

The validity of a Snapshot copy is not tied directly to the state of the Infinite Volume. A valid Snapshot copy can exist for an Infinite Volume with an offline state, depending on when the Snapshot copy was created compared to when the Infinite Volume went offline. For example, a valid Snapshot copy exists before a new constituent is created. The new constituent is offline, which puts the Infinite Volume in an offline state. However, the Snapshot copy remains valid because it references its required preexisting constituents. The Snapshot copy does not reference the new, offline constituent.

## How volume guarantees work for FlexVol volumes

Volume guarantees (sometimes called *space guarantees*) determine how space for a volume is allocated from its containing aggregate—whether or not the space is preallocated for the volume.

The guarantee is an attribute of the volume.

You set the guarantee when you create a new volume; you can also change the guarantee for an existing volume, provided that sufficient free space exists to honor the new guarantee.

Volume guarantee types can be **volume** (the default type) or **none**.

- A guarantee type of **volume** allocates space in the aggregate for the entire volume when you create the volume, regardless of whether that space is used for data yet.  
The allocated space cannot be provided to or allocated for any other volume in that aggregate.
- A guarantee of **none** allocates space from the aggregate only as it is needed by the volume.  
The amount of space consumed by volumes with this guarantee type grows as data is added instead of being determined by the initial volume size, which might leave space unused if the volume data does not grow to that size. The maximum size of a volume with a guarantee of **none** is not limited by the amount of free space in its aggregate. It is possible for the total size of all volumes associated with an aggregate to exceed the amount of free space for the aggregate, although the amount of space that can actually be used is limited by the size of aggregate.  
Writes to LUNs or files (including space-reserved LUNs and files) contained by that volume could fail if the containing aggregate does not have enough available space to accommodate the write.

When space in the aggregate is allocated for a **volume** guarantee for an existing volume, that space is no longer considered free in the aggregate, even if the volume is not yet using the space. Operations that consume free space in the aggregate, such as creation of aggregate Snapshot copies or creation of new volumes in the containing aggregate, can occur only if there is enough available free space in that aggregate; these operations are prevented from using space already allocated to another volume.

When the free space in an aggregate is exhausted, only writes to volumes or files in that aggregate with preallocated space are guaranteed to succeed.

Guarantees are honored only for online volumes. If you take a volume offline, any allocated but unused space for that volume becomes available for other volumes in that aggregate. When you try to bring that volume back online, if there is insufficient available space in the aggregate to fulfill its guarantee, it will remain offline. You must force the volume online, at which point the volume's guarantee will be disabled.

**Related information**

*[NetApp Technical Report 3965: NetApp Thin Provisioning Deployment and Implementation Guide Data ONTAP 8.1 \(7-Mode\)](#)*

**How incremental tape backup uses SnapDiff and Snapshot copies**

The storage capacity potential of an Infinite Volume is larger than what a traditional file-scanning backup application can back up in a reasonable time. An incremental backup of Infinite Volumes to tape by using SnapDiff and Snapshot copies is the only viable solution for large Infinite Volumes.

**What SnapDiff is**

SnapDiff is an internal Data ONTAP engine that quickly identifies the file and directory differences between two Snapshot copies.

By finding the differences between two Snapshot copies, SnapDiff eliminates the file scanning requirements of a traditional backup application during an incremental backup, which reduces the backup processing to only the time it takes to write the changed or added data.

When incrementally backing up an Infinite Volume to tape using SnapDiff, the backup application uses the SnapDiff application programming interfaces (APIs) to communicate with the SnapDiff engine to identify new, changed, and deleted files between two Snapshot copies of the active file system in an Infinite Volume. The differencing process uses the namespace constituent and namespace mirror constituents in an Infinite Volume to determine names for the list of new, changed, and deleted files. When these changes are identified, the backup application backs up the identified data from the list produced during the differencing process.

**FlexClone volumes and space guarantees**

A FlexClone volume inherits its initial space guarantee from its parent volume. For example, if you create a FlexClone volume from a parent volume with a space guarantee of **volume**, then the FlexClone volume's initial space guarantee will be **volume** also. You can change the FlexClone volume's space guarantee.

For example, suppose that you have a 100-MB FlexVol volume with a space guarantee of **volume**, with 70 MB used and 30 MB free, and you use that FlexVol volume as a parent volume for a new FlexClone volume. The new FlexClone volume has an initial space guarantee of **volume**, but it does not require a full 100 MB of space from the aggregate, as it would if you had copied the volume. Instead, the aggregate needs to allocate only 30 MB (100 MB minus 70 MB) of free space to the clone.

If you have multiple clones with the same parent volume and a space guarantee of **volume**, they all share the same shared parent space with each other, so the space savings are even greater.

**Note:** The shared space depends on the existence of the shared Snapshot copy (the base Snapshot copy that was used to create the FlexClone volume). If you delete this shared Snapshot copy, you lose the space savings provided by the FlexClone volume.

**Thin provisioning for greater efficiencies using FlexVol volumes**

With thin provisioning, when you create volumes and LUNs in a given aggregate, you do not actually allocate any space for those in advance. The space is allocated as data is written to the volumes or LUNs.

The unused aggregate space is available to other volumes and LUNs. By allowing as-needed provisioning and space reclamation, thin provisioning can improve storage utilization and decrease storage costs.

A FlexVol volume can share its containing aggregate with other FlexVol volumes. Therefore, a single aggregate is the shared source of all the storage used by the FlexVol volumes it contains. Flexible



volumes are no longer bound by the limitations of the disks on which they reside. A FlexVol volume can be sized based on how much data you want to store in it, rather than on the size of your disk. This flexibility enables you to maximize the performance and capacity utilization of the storage systems. Because FlexVol volumes can access all available physical storage in the system, improvements in storage utilization are possible.

#### Example

A 500-GB volume is allocated with only 100 GB of actual data; the remaining 400 GB allocated has no data stored in it. This unused capacity is assigned to a business application, even though the application might not need all 400 GB until later. The allocated but unused 400 GB of excess capacity is temporarily wasted.

With thin provisioning, the storage administrator provisions 500 GB to the business application but uses only 100 GB for the data. The difference is that with thin provisioning, the unused 400 GB is still available to other applications. This approach allows the application to grow transparently, and the physical storage is fully allocated only when the application needs it. The rest of the storage remains in the free pool to be used as needed.

## Using space reservations with FlexVol volumes

Using space reservation, you can provision FlexVol volumes. Thin provisioning appears to provide more storage than is actually available from a given aggregate, as long as not all of that storage is currently being used.

Thick provisioning sets aside enough storage from the aggregate to ensure that any block in the volume can be written to at any time.

Aggregates can provide storage to volumes contained by more than one Storage Virtual Machine (SVM). If you are using thin provisioning, and you need to maintain strict separation between your SVMs (for example, if you are providing storage in a multi-tenancy environment), you should either use fully allocated volumes (thick provisioning) or ensure that your aggregates are not shared between tenants.

When the space reserve is set to “Default”, the ONTAP space reservation settings apply to the volumes.

#### Related information

[NetApp Technical Report 3563: NetApp Thin Provisioning Increases Storage Utilization With On Demand Allocation](#)

[NetApp Technical Report 3483: Thin Provisioning in a NetApp SAN or IP SAN Enterprise Environment](#)

## Considerations when using thin provisioning with Infinite Volumes

You can use thin provisioning with an Infinite Volume, enabling you to allocate more storage to users than is physically available. Before using thin provisioning, you should understand what it is, where and when it is configured, and what its advantages and disadvantages are.

#### What thin provisioning is

With thin provisioning, the size of an Infinite Volume is not limited by the size of its associated aggregates. You can create a large volume on a small amount of storage, adding disks only as they are required. For example, you can create a 500 TB volume using aggregates that only have 250 TB of available space. The storage provided by the aggregates is used only as data is written. Thin provisioning is also called *aggregate overcommitment*.

The alternative of thin provisioning is thick provisioning, which allocates physical space immediately, regardless of whether that space is used for data yet. The allocated space cannot be used

by any other volumes. When you use thick provisioning, all of the space required for the volume is allocated from the aggregate at the time of creating the volume.

Thin provisioning affects only the data constituents of an Infinite Volume. The namespace constituent and namespace mirror constituents of an Infinite Volume always use thick provisioning. For example, if you create a new Infinite Volume with a 10 TB namespace constituent and use thin provisioning, the namespace constituent will consume 10 TB of space even if the Infinite Volume does not contain any data.

### When and where thin provisioning is configured

The way that you configure thin provisioning on an Infinite Volume depends on whether the Infinite Volume uses storage classes.

For an Infinite Volume without storage classes, thick and thin provisioning are configured at the volume level in the following way:

- When you create an Infinite Volume, thin provisioning is used.
- You can switch between thick and thin provisioning after the Infinite Volume is created.  
Before changing a volume from thin provisioning to thick provisioning, you must ensure that the physical storage can support the provisioned size.

For an Infinite Volume with storage classes, thick and thin provisioning are configured at the storage-class level in the following way:

- You can choose to use thick or thin provisioning for each storage class independent of other storage classes.  
For example, one storage class of an Infinite Volume can use thin provisioning while another storage class of the same Infinite Volume uses thick provisioning.
- All configuration of thick and thin provisioning is performed by using workflows OnCommand Workflow Automation.
- If an Infinite Volume uses storage classes, it is not possible to configure thick or thin provisioning at the Infinite Volume level.

### Advantages of thin provisioning

Using thin provisioning with Infinite Volumes provides the following advantages:

- Defers physical storage costs until the storage is actually required  
Users receive the space allocation that they expect, and valuable resources do not remain unused.
- Facilitates monitoring of aggregate usage  
When you use thin provisioning, information about aggregate usage—for example, the `Used Size`, `Used Percentage`, and `Available Size`—reflects the actual space used to store data. When you use thick provisioning, aggregate usage information reflects the allocated space, which typically differs from the space that is actually used to store data.
- In some cases, eliminates the need to change the volume size after adding disks  
If you add more disks to existing aggregates, you do not have to resize the Infinite Volume to make use of the added capacity as long as the total size of the Infinite Volume's associated aggregates is less than the Infinite Volume's size.

### Disadvantages of thin provisioning

Thin provisioning includes the following disadvantages:

- If you have overcommitted your aggregate, you must monitor your available space and add storage to the aggregate as needed to avoid write errors due to insufficient space.

- In a multi-tenancy environment, if you share aggregates among volumes that use thin provisioning, be aware that one tenant's aggregate space availability can be adversely affected by the growth of another tenant's volumes.
- The process of balancing incoming files across data constituents is less effective when an Infinite Volume uses thin provisioning because the reported percentage of used space does not always represent the physical used space.

### More information about thin provisioning

For more information about thin provisioning, see *Thin Provisioning Deployment and Implementation Guide (TR-3965)*.

### Related information

[NetApp Technical Report 3965: NetApp Thin Provisioning Deployment and Implementation Guide Data ONTAP 8.1 \(7-Mode\)](#)

## Benefits of storage efficiency

Storage efficiency enables you to store the maximum amount of data for the lowest cost and accommodate rapid data growth while consuming less space. You can use technologies such as RAID-DP, FlexVol, Snapshot copies, deduplication, data compression, SnapMirror, and FlexClone to increase storage utilization and decrease storage costs. When used together, these technologies help to achieve increased performance.

- High-density disk drives, such as serial advanced technology attachment (SATA) drives mitigated with RAID-DP technology, provide increased efficiency and read performance.
- RAID-DP is a double-parity RAID6 implementation that protects against dual disk drive failures.
- Thin provisioning enables you to maintain a common unallocated storage space that is readily available to other applications as required.  
It is based on FlexVol technology.
- Snapshot copies are a point-in-time, read-only view of a data volume, which consume minimal storage space.  
Two Snapshot copies created in sequence differ only by the blocks added or changed in the time interval between the two. This block incremental behavior limits the associated consumption of storage capacity.
- Deduplication saves storage space by eliminating redundant data blocks within a FlexVol volume.
- Data compression stores more data in less space and reduces the time and bandwidth required to replicate data during volume SnapMirror transfers.  
You have to choose the type of compression (inline or background) based on your requirement and the configurations of your storage system. Inline compression checks if data can be compressed, compresses data, and then writes data to the volume. Background compression runs on all the files, irrespective of whether the file is compressible or not, after all the data is written to the volume.
- SnapMirror technology is a flexible solution for replicating data over local area, wide area, and Fibre Channel networks.  
It can serve as a critical component in implementing enterprise data protection strategies. You can replicate your data to one or more storage systems to minimize downtime costs in case of a production site failure. You can also use SnapMirror technology to centralize the backup of data to disks from multiple data centers.
- FlexClone technology copies data volumes, files, and LUNs as instant virtual copies.

A FlexClone volume, file, or LUN is a writable point-in-time image of the FlexVol volume or another FlexClone volume, file, or LUN. This technology enables you to use space efficiently, storing only data that changes between the parent and the clone.

- The unified architecture integrates multiprotocol support to enable both file-based and block-based storage on a single platform.

With FlexArray Virtualization, you can virtualize your entire storage infrastructure under one interface, and you can apply all the preceding efficiencies to your non-NetApp systems.

## Data compression and deduplication

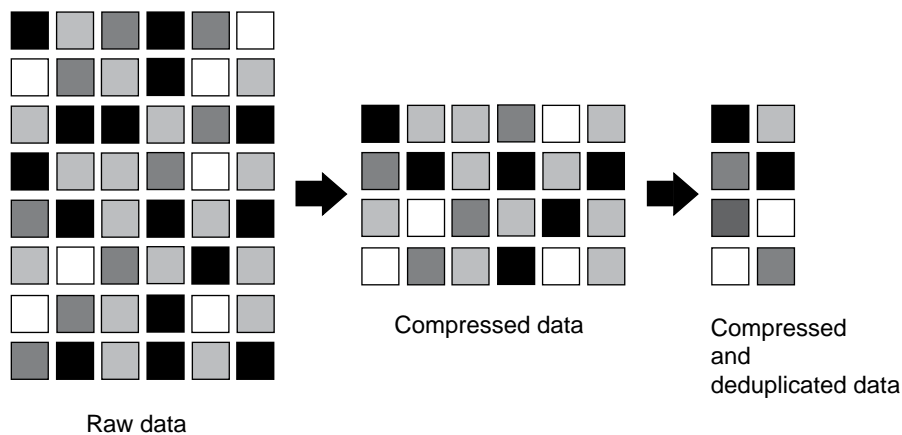
Beginning with Data ONTAP 8.0.1, data compression is supported with deduplication.

When both data compression and deduplication are enabled on a FlexVol volume, the data is first compressed and then deduplicated. Therefore, deduplication can further increase the space savings by removing duplicate blocks in the FlexVol volume.

Though data compression and deduplication can be enabled on a FlexVol volume, the savings might not be the sum of the savings when each is run individually on a data set. The combined savings can yield higher savings than running deduplication or data compression individually.

You can achieve better savings when you run the data compression scanner before deduplication. This is because data compression scanner cannot run on data that is locked by deduplication, but deduplication can run on compressed data.

The following illustration shows how data is first compressed and then deduplicated:



When you run deduplication on a FlexVol volume that contains uncompressed data, it scans all the uncompressed blocks in the FlexVol volume and creates a digital fingerprint for each of the blocks.

**Note:** If a FlexVol volume has compressed data, but the compression option is disabled on that volume, then you might lose the space savings when you run the `sis undo` command.

## Guidelines for using deduplication

You must remember certain guidelines about system resources and free space when using deduplication.

The guidelines are as follows:

- If you have a performance-sensitive solution, you must carefully consider the performance impact of deduplication and measure the impact in a test setup before using deduplication.
- Deduplication is a background process that consumes system resources while it is running.

If the data does not change very often in a FlexVol volume, it is best to run deduplication less frequently. Multiple concurrent deduplication operations running on a storage system lead to a higher consumption of system resources.

- You must ensure that sufficient free space exists for deduplication metadata in the volumes and aggregates.
- If deduplication is used on the source volume, you must use deduplication on the destination volume.
- You must use automatic mode when possible so that deduplication runs only when significant additional data has been written to each FlexVol volume.
- You must run deduplication before creating a Snapshot copy to obtain maximum savings.
- You must set the Snapshot reserve to greater than 0 if Snapshot copies are used.

## Options for resizing volumes

You can use the Volume Resize wizard to change your volume size, adjust the Snapshot reserve, delete Snapshot copies, and dynamically view the results of your changes.

The Volume Resize wizard displays a bar graph that displays the current space allocations within the volume, including the amount of used and free space. When you make changes to the size or Snapshot reserve of the volume, this graph is updated dynamically to reflect the changes.

You can also use the **Calculate space** button to determine the amount of space that is freed by deleting selected Snapshot copies. This operation is not supported on an Infinite Volume.

You cannot use System Manager to resize Infinite Volumes with storage classes. Instead, you can use OnCommand Workflow Automation.

You can use the Volume Resize wizard to make the following changes to your volume:

### Change the volume size

You can change the total volume size to increase or decrease storage space. You cannot reduce the size of an Infinite Volume.

### Adjust Snapshot reserve

You can adjust the amount of space reserved for Snapshot copies to increase or decrease storage space.

### Delete Snapshot copies

You can delete Snapshot copies to reclaim volume space.

**Note:** Snapshot copies that are in use cannot be deleted.

### Assign aggregates to Storage Virtual Machines (SVMs) with Infinite Volume

You can assign specific aggregates to the SVM so that the Infinite Volume will use those specific aggregates and not use any aggregate in the cluster.

### Autogrow

You can specify the limit to which the volume can be grown automatically, if required.

## Considerations when moving volumes

Moving a volume has many considerations and recommendations that are influenced by the volume you are moving or by the system configuration. You should understand the considerations associated with moving volumes.

- If you move a volume that has inline deduplication enabled from an aggregate with All Flash Optimized personality or a Flash Pool aggregate to an HDD aggregate, inline deduplication is disabled on the volume.

- If you move a volume that has background deduplication and inline compression enabled from an aggregate with All Flash Optimized personality to an HDD aggregate, then background compression, background deduplication, and inline compression are automatically enabled on the volume.
- If you move a volume that has background compression enabled from an HDD aggregate to an aggregate with All Flash Optimized personality, background compression is disabled on the volume.
- If you move a volume from a Flash Pool aggregate to a non-Flash Pool aggregate, the caching policies and retention priority are disabled.
- If you move a volume from a non-Flash Pool aggregate to a Flash Pool aggregate, the **default** caching policy and the **default** retention priority are automatically assigned to the volume.

## How moving a FlexVol volume works

Knowing how moving a FlexVol volume works helps you to determine whether the volume move satisfies service-level agreements and to understand where a volume move is in the volume move process.

FlexVol volumes are moved from one aggregate or node to another within the same Storage Virtual Machine (SVM). A volume move does not disrupt client access during the move.

Moving a volume occurs in multiple phases:

- A new volume is made on the destination aggregate.
- The data from the original volume is copied to the new volume.  
During this time, the original volume is intact and available for clients to access.
- At the end of the move process, client access is temporarily blocked.  
During this time the system performs a final replication from the source volume to the destination volume, swaps the identities of the source and destination volumes, and changes the destination volume to the source volume.
- After completing the move, the system routes client traffic to the new source volume and resumes client access.

The move is not disruptive to client access because the time in which client access is blocked ends before clients notice a disruption and time out. Client access is blocked for 35 seconds by default. If the volume move operation cannot finish in the time that access is denied, the system aborts this final phase of the volume move operation and allows client access. The system attempts the final phase three times by default. After the third attempt, the system waits an hour before attempting the final phase sequence again. The system runs the final phase of the volume move operation until the volume move is complete.

## Volumes window

You can use the Volumes window to manage your FlexVol volumes and Infinite Volumes and to display information about these volumes. You can also use the FlexGroup tab to manage your FlexGroup volumes and to view information about them.

You cannot view or manage volumes that are in Storage Virtual Machines (SVMs) that are configured for disaster recovery (DR) by using System Manager. You must use the command-line interface instead.

- [Volumes tab](#) on page 207
- [FlexGroup tab](#) on page 212

## Volumes tab

### Command buttons

#### Create

Opens the Create Volume dialog box, which enables you to add FlexVol volumes and Infinite Volumes.

This button is disabled if an Infinite Volume already exists.

#### Edit

Opens the Edit Volume dialog box, which enables you to modify a selected volume.

#### Delete

Deletes the selected volume or volumes.

#### Clone

Provides a list of clone options, including the following:

- Create  
Creates a clone of the selected volume or a clone of a file from the selected volume.
- Split  
Splits the clone from the parent volume.
- View Hierarchy  
Displays information about the clone hierarchy.

The Clone option is not available for Infinite Volumes.

#### Status

Changes the status of the selected volume or volumes to one of the following statuses:

- Online
- Offline
- Restrict

An Infinite Volume can go into a mixed state, which means its constituents are not all in the same state. However, you cannot set the status of an Infinite Volume to a mixed state, which is a read-only state. A mixed state typically occurs when most constituents are online, but one constituent is offline. For example, if you take an aggregate offline that contains constituents, you also cause the constituents to go offline.

When you change the status of an Infinite Volume, the status of the constituents is changed one after the other. The Infinite Volume is in mixed state until the operation is complete.

#### Snapshot Copies

Provides a list of Snapshot options, including the following:

- Create  
Displays the Create Snapshot dialog box, which you can use to create a Snapshot copy of the selected volume.
- Configure  
Configures the Snapshot settings.
- Restore  
Restores a Snapshot copy of the selected volume.

**Resize**

Opens the Volume Resize wizard, which enables you to change the volume size.

This option is not available for Infinite Volumes with storage classes.

**Storage Efficiency**

Opens the Storage Efficiency dialog box, which you can use to manually start deduplication or to abort a running deduplication operation. This button is displayed only if deduplication is enabled on the storage system.

This option is not available for Infinite Volumes with storage classes.

**SnapLock Type**

Displays the SnapLock type of the volume.

**Mount**

Enables you to mount an Infinite Volume on the namespace of the Storage Virtual Machine (SVM) with Infinite Volume.

**Unmount**

Enables you to unmount an Infinite Volume before you change the junction path or delete the Infinite Volume.

**Storage QoS**

Opens the Quality of Service details dialog box, which you can use to assign one or more volumes to a new or existing policy group.

This option is not available for Infinite Volumes.

**Move**

Opens the Move Volume dialog box, which you can use to move volumes from one aggregate or node to another aggregate or node within the same SVM.

**Protect**

Opens the Create Protection Relationship dialog box, which enables you to create data protection relationships between a source volume and a destination volume.

**Refresh**

Updates the information in the window.

**Volume list**

Displays the volume name and storage information about each volume.

**Name**

Displays the name of the volume.

**Aggregate**

Displays the name of the aggregate.

**Status**

Displays the status of the volume.

**Thin Provisioned**

Displays whether space guarantee is set for the selected volume. Valid values for online volumes are Yes and No.

**Type**

Displays the type of volume: **rw** for read/write, **ls** for load sharing, or **dp** for data protection.



**Root volume**

Displays whether the volume is a root volume.

**% Used**

Displays the amount of space (in percentage) that is used in the volume.

**Available Space**

Displays the available space in the volume.

**Total Space**

Displays the total space in the volume, which includes the space that is reserved for Snapshot copies.

**Storage Efficiency**

Displays whether deduplication is enabled or disabled for the selected volume.

**Policy Group**

Displays the name of the Storage QoS policy group to which the volume is assigned. By default, this column is hidden.

**Is Volume Moving**

Displays whether a volume is being moved from one aggregate to another aggregate, or from one node to another node.

**Is Encrypted**

Displays whether the volume is encrypted or not.

**Clone**

Displays whether the volume is a FlexClone volume.

**Details area**

The area below the Volume list displays detailed information about the selected volume.

**Details tab**

Displays general information about the selected volume, such as the maximum file count and current file count on the volume, cache policy of the volume that is hosted on a Flash Pool aggregate, policy group to which the volume is assigned, maximum throughput of the policy group, and export policy. The tab also displays whether an Infinite Volume is associated with storage classes.

For SnapLock volumes, the Details tab displays the SnapLock details such as the expiry date, ComplianceClock time, maximum retention period, minimum retention period, default retention period, and autocommit period.

**Space Allocation tab**

Displays the allocation of space in the volume.

- Bar graph  
Displays (in graphical format) details about the volume space.
- Volume  
Displays the total data space of the volume and the space reserved for Snapshot copies.
- Available  
Displays the amount of space that is available in the volume for data and for Snapshot copies, and the total space available in the volume.
- Used  
Displays the amount of space in the volume that is used for data and for Snapshot copies, and the total volume space that is used.

The **Space Allocation** tab displays different information depending on whether the volume is configured for NAS or SAN. For a NAS volume, the tab displays the following information:

- Used data space
- Available data space
- Used Snapshot reserve space
- Available Snapshot reserve space (this is applicable only if the Snapshot reserve is greater than zero)

For a SAN volume, the tab displays the following information:

- Space used by data in LUNs
- Available space
- Space used by Snapshot copies

### Snapshot Copies tab

Displays (in tabular format) the Snapshot copies of the selected volume. This tab contains the following command buttons:

- Create  
Opens the Create Snapshot Copy dialog box, which enables you to create a Snapshot copy of the selected volume.
- Rename  
Opens the Rename Snapshot Copy dialog box, which enables you to rename a selected Snapshot copy.
- Delete  
Deletes the selected Snapshot copy.
- Restore  
Restores a Snapshot copy.
- Extend Expiry Date  
Extends the expiry date of a Snapshot copy.
- Refresh  
Updates the information in the window.

### Storage Efficiency tab

Displays information in the following panes:

- Bar graph  
Displays (in graphical format) the volume space that is used by data and Snapshot copies. You can view details about the space used before and after applying storage efficiency savings.
- Details  
Displays information about deduplication properties, including whether deduplication is enabled on the volume, the deduplication mode, the deduplication status, type, and whether inline or background compression is enabled on the volume.
- Last run details  
Provides details about the last-run deduplication operation on the volume. Space savings resulting from compression and deduplication operations that are applied on the data on the volume are also displayed.

**Data Protection tab**

Displays data protection information about the volume.

If the source volume (read/write volume) is selected, the tab displays all the mirror, vault, and mirror and vault relationships that are related to the destination volume (DP volume). If the destination volume is selected, the tab displays the relationship with the source details:

- **Destination Storage Virtual Machine**  
Displays the SVM that contains the volume to which data is mirrored or vaulted in a relationship.
- **Destination Volume**  
Displays the volume to which data is mirrored or vaulted in a relationship.
- **Is Healthy**  
Displays the health of a relationship as Good or Bad.
- **Relationship State**  
Displays the state of the relationship as Snapmirrored, Uninitialized, or Broken Off.
- **Transfer Status**  
Displays the relationship status such as Idle, Transferring, or Aborting.
- **Type**  
Displays the type of relationship as Mirror, Vault, Version-Flexible Mirror, or Mirror and Vault.
- **Lag Time**  
Displays the difference between the current time and the timestamp of the Snapshot copy that was last transferred successfully to the destination storage system. It indicates the time difference between the data that is currently on the source system and the latest data that is stored on the destination system. The value that is displayed can be positive or negative. The value is negative if the time zone of the destination system is behind the time zone of the source storage system.
- **Policy**  
Displays the protection policy that is assigned to the relationship.

If some or all of the cluster peer relationships of the local cluster are in an unhealthy state, the Data Protection tab might take some time to display the protection relationships relating to a healthy cluster peer relationship. Relationships relating to unhealthy cluster peer relationships are not displayed.

**Volume Move Details tab**

Displays information about a volume that is being moved, such as the state and phase of the volume move, the destination node and aggregate to which the volume is being moved, the percentage of volume move that is complete, the estimated time to complete the volume move operation, and details of the volume move operation.

This tab contains the following command button:

**Cutover**

Opens the Cutover dialog box, which enables you to manually trigger the cutover.

The **Cutover** command button is displayed only if the volume move operation is in the “replication” or “hard deferred” state.

**Performance tab**

Displays information about the performance metrics of the selected volume, including throughput, IOPS, and latency.

Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You must refresh your browser to view the updated graphs.

## FlexGroup tab

### Command buttons

#### Create

Opens the Create FlexGroup window, which enables you to create FlexGroup volumes.

#### Edit

Opens the Edit FlexGroup window, which enables you to edit the properties of the selected FlexGroup volume.

#### Delete

Deletes the selected FlexGroup volume.

### Actions

Provides the following AutoSupport requests:

#### Change status to

Changes the status of the selected FlexGroup volume to one of the following status:

- Online
- Offline
- Restrict

#### Resize

Opens the Resize FlexGroup window, which enables you to resize the FlexGroup volume by resizing existing resources or expand the FlexGroup volume by adding new resources.

#### Refresh

Updates the information in the window.

## FlexGroup List

### Status

Displays the status of the FlexGroup volume.

### Name

Displays the name of the FlexGroup volume.

### SVM

Displays the name of the Storage Virtual Machine (SVM) to which the FlexGroup volume belongs.

This is displayed only when you access the FlexGroup volume by navigation through **Volumes > FlexGroups**.

### Aggregates

Displays the name of the aggregates that belong to the FlexGroup volume.

### Thin Provisioned

Displays whether space guarantee is set for the selected FlexGroup volume. Valid values for online FlexGroup volumes are Yes and No.

### Type

Displays the type of the FlexGroup volume: **rw** for read/write or **dp** for data protection.

**Available Space**

Displays the available space in the FlexGroup volume.

**Total Space**

Displays the total space in the FlexGroup volume, which includes the space that is reserved for Snapshot copies.

**% Used**

Displays the amount of space (in percentage) that is used in the FlexGroup volume.

**Details area**

You can expand the FlexGroup volume to view information about the selected FlexGroup volume. You can click Show More Details to view detailed information about the selected FlexGroup volume.

**Overview tab**

Displays general information about the selected FlexGroup volume, and displays a pictorial representation of the space allocation of the FlexGroup volume, the protection status of the FlexGroup volume, and the performance of the FlexGroup volume.

The refresh interval for the performance data is 15 seconds.

**Snapshot Copies tab**

Displays the Snapshot copies of the selected FlexGroup volume.

**Data Protection tab**

Displays data protection information about the FlexGroup volume.

If a volume is selected, the tab displays all the mirror relationships that are related to the volume.

**Performance tab**

Displays information about the average performance metrics, read performance metrics, and write performance metrics of the selected FlexGroup volume, including throughput, IOPS, and latency.

Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You must refresh your browser to view the updated graphs.

**Related tasks**

- [Creating FlexVol volumes](#) on page 51
- [Creating FlexClone volumes](#) on page 172
- [Creating FlexClone files](#) on page 173
- [Deleting volumes](#) on page 171
- [Setting the Snapshot copy reserve](#) on page 176
- [Deleting Snapshot copies](#) on page 179
- [Creating Snapshot copies](#) on page 175
- [Editing the volume properties](#) on page 169
- [Changing the status of a volume](#) on page 174
- [Enabling storage efficiency on a volume](#) on page 181
- [Changing the deduplication schedule](#) on page 182
- [Running deduplication operations](#) on page 183
- [Splitting a FlexClone volume from its parent volume](#) on page 173
- [Resizing volumes](#) on page 180
- [Restoring a volume from a Snapshot copy](#) on page 177
- [Scheduling automatic Snapshot copies](#) on page 177

[Renaming Snapshot copies](#) on page 179

[Hiding the Snapshot copy directory](#) on page 177

[Viewing the FlexClone volume hierarchy](#) on page 174

## Application Provisioning

You can use System Manager to provision storage for Oracle application types over NFS.

### Provisioning storage for Oracle application type over NFS

You can use System Manager to provision storage by creating and exporting one or more volumes for single or multiple instances (Oracle RAC) of Oracle databases over the NFS protocol for a NAS-optimized cluster on an All Flash FAS platform.

#### Before you begin

- All the nodes in the cluster must be running Data ONTAP 8.3.2.
- The NFS service must be licensed and started on the Storage Virtual Machine (SVM).
- You must have created data LIFs for NFS in the SVMs in which you want to provision storage.
- You must have the following database information: Oracle database name, database instance ID, server name, capacity required for datafiles, capacity required for redo logs, number of redo log copies, and capacity required for archive logs.

#### About this task

- Volumes are thin provisioned.
- In the event of a failure, a rollback operation is not supported.  
You must manually delete the volumes that were created partially before performing this task again.
- Most of the cluster configurations are already completed at the factory and are optimized for optimum storage efficiency and performance.  
You must *not* modify these configurations.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Application Provisioning** tab.
4. In the **Application Provisioning** window, select the appropriate application type, and then choose one of the following actions:

If the application type is...	Then...
NFS Oracle Single	Specify the necessary information, including the database name, database server, datafile size, redo logs capacity, redo copies, archive logs size, Oracle binaries volume size, span HA controller nodes, export policy name, and volume export policy rule.

If the application type is...	Then...
NFS Oracle RAC (multiple instances)	Specify the necessary information, including the database name, datafile size, redo logs capacity, redo copies, archive logs size, span HA controller nodes, database instance ID and server name for the required database instances, export policy name, volume export policy rule, unique Oracle cluster name, Oracle binaries volume size, grid binaries volume size, CRS voting volume size, and CRS volume count.

**5. Click **Provision Storage**.**

A summary table is displayed with the volume name, volume size, aggregate on which the volumes is created, junction path, the local node's IP address, and export policy.

**6. Review the summary, and then click **Done**.**

**Related references**

[Examples of application-specific volume settings](#) on page 215

### Examples of application-specific volume settings

Volumes are automatically created and exported based on your database requirements and volume settings are determined by rules specific to the application type. You should review examples of how space is provisioned for Oracle and Oracle RAC application types.

Data aggregates are created in each of the nodes and the volumes that are created on these aggregates are thin provisioned.

Storage efficiency policy is enabled by default with the schedule set to “daily”, quality of service (QoS) is set to “best\_effort”, inline compression and inline deduplication are enabled by default, and volume autogrow is enabled. Access time (atime) update is enabled on the cluster. However, access time updates are disabled by System Manager while creating volumes. Therefore, every time a file is read or written, the access time field in the directory is not updated.

**Attention:** Enabling the access time update causes performance degradation to the data-serving capability of the cluster.

### Example volume settings for Oracle (single instance)

The following table provides an example of how space is provisioned based on the following values for Oracle:

- Number of nodes: 2
- Database name: dbname
- Database instance ID (SID): db
- Database server name: dbserver
- Datafile size: 10 TB
- Redo log size: 5 GB
- Redo log copies: 2
- Provision space for archive logs: Yes
- Archive log size: 5 TB
- Provision space for Oracle binaries: Yes
- Oracle binaries size: 16 GB

- HA node spanning: Yes

If HA node spanning is set to No, all the volumes are created on one node.

Node	Data type	Volume name	Volume size
node1	Oracle binaries	oracle_binary_dbserver	16 GB
	Datafiles	oracledata1_dbname	5 TB
	Redo logs	redo_mirror1_dbname	5 GB
	Archive logs	oracle_archive1_dbname	5 TB
node2	Datafiles	oracledata2_dbname	5 TB
	Redo logs	redo_mirror2_dbname	5 GB

Archive logs can be created on either node1 or node2.

### Example volume settings for Oracle RAC (two instances)

The following table provides an example about how space is provisioned based on the following values for Oracle RAC with two database instances:

- Number of nodes: 2
  - Database name: dbname
  - Database SID for instance 1: db01
  - Database server name for instance 1: dbserver01
  - Database SID for instance 2: db02
  - Database server name for instance 2: dbserver02
  - Datafile size: 30 TB
  - Redo log size: 10 GB
  - Redo log copies: 2
  - Provision space for archive logs: Yes
  - Archive log size: 10 TB
  - Provision space for Oracle binaries: Yes
  - Oracle binaries size: 32 GB
  - Provision space for grid binaries: Yes
  - Grid binaries size: 32 GB
  - Provision space for CRS/Voting: Yes
  - CRS/Voting size: 6 GB
  - Unique Oracle cluster name: oracluster
  - HA node spanning: Yes
- If HA node spanning is set to No, all the volumes are created on one node.



Node	Data type	Volume name	Volume size
node1	Oracle binaries	oracle_binary_dbserver01	16 GB
	Grid binaries	oracle_grid_dbserve r01	16 GB
	CRS/Voting	voting0_oraccluster	2 GB
	CRS/Voting	voting2_oraccluster	2 GB
	Datafiles	oracledata1_dbname	15 TB
	Redo logs	redo_mirror1_dbna me_db01	10 GB
	Redo logs	redo_mirror1_dbna me_db02	10 GB
	Archive logs	oracle_archive_dbna me	10 TB
node2	Oracle binaries	oracle_binary_dbser ver02	16 GB
	Grid binaries	oracle_grid_dbserve r02	16 GB
	CRS/Voting	voting1_oraccluster	2 GB
	Datafiles	oracledata2_dbname	15 TB
	Redo logs	redo_mirror2_dbna me_db01	10 GB
	Redo logs	redo_mirror2_dbna me_db02	10 GB

**Related tasks**

[Provisioning storage for Oracle application type over NFS](#) on page 214

## Namespace

You can use the Namespace window in System Manager to mount or unmount FlexVol volumes to a junction in the SVM namespace.

## Mounting volumes

You can use System Manager to mount volumes to a junction in the Storage Virtual Machine (SVM) namespace.

**About this task**

- If you mount the volume to a junction path with a language setting that is different from that of the immediate parent volume in the path, NFSv3 clients cannot access some of the files because some characters might not be decoded correctly.  
This issue does not occur if the immediate parent directory is the root volume.
- You can mount a SnapLock volume only under the root of the SVM.

- You cannot mount a regular volume under a SnapLock volume.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Namespace** tab.
4. Click **Mount**, and then select the volume that is to be mounted.
5. Optional: If you want to change the default junction name, specify a new name.
6. Click **Browse**, and then select a junction path to mount the volume.
7. Click **OK**, and then click **Mount**.
8. Verify the new junction path in the **Details** tab.

**Unmounting FlexVol volumes**

You can use the Namespace window in System Manager to unmount FlexVol volumes from a junction in the Storage Virtual Machine (SVM) namespace.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Namespace** tab.
4. Select the volume that has to be unmounted, and then click **Unmount**.
5. Select the confirmation check box, and then click **Unmount**.

**Changing export policies**

When a volume is created, it automatically inherits the default export policy of the root volume of the Storage Virtual Machine (SVM). You can use System Manager to change the default export policy associated with the volume to redefine the client access to data.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Namespace** tab.
4. Select the volume, and then click **Change Export Policy**.
5. Select the export policy, and then click **Change**.
6. Verify that the Export Policy column in the **Namespace** window displays the export policy that you applied to the volume.

**Result**

The default export policy is replaced with your new custom policy.

## Namespace window

You can use the Namespace window to manage the NAS namespace of Storage Virtual Machines (SVMs).

### Command buttons

#### Mount

Opens the Mount Volume dialog box, which enables you to mount a volume to the junction in an SVM namespace.

#### Unmount

Opens the Unmount Volume dialog box, which enables you to unmount a volume from its parent volume.

#### Change Export Policy

Opens the Change Export Policy dialog box, which enables you to change the existing export policy associated with the volume.

#### Refresh

Updates the information in the window.

### Namespace list

#### Path

Specifies the junction path of the mounted volume. You can expand the junction path to view the related volumes and qtrees.

#### Storage Object

Specifies the name of the volume mounted on the junction path. You can also view the qtrees that the volume contains.

#### Export Policy

Specifies the export policy of the mounted volume.

#### Security Style

Specifies the security style for the volume. Possible values include UNIX (for UNIX mode bits), NTFS (for CIFS ACLs), and Mixed (for mixed NFS and CIFS permissions).

### Details tab

Displays general information about the selected volume or qtree, such as the name, type of storage object, junction path of the mounted object, and export policy. If the selected object is a qtree, details about the space hard limit, space soft limit, and space usage are displayed.

## Shares

You can use System Manager to create, edit, and manage shares.

### Creating a CIFS share

You can use System Manager to create a share that enables you to specify a folder, qtree, or volume that CIFS users can access.

#### Before you begin

You must have installed the CIFS license before you set up and start CIFS.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Shares** tab.
4. Click **Create Share**.
5. In the **Create Share** window, click **Browse** and select the folder, qtree, or volume that should be shared.
6. Specify a name for the new CIFS share.
7. Optional: Select the **Enable continuous availability for Hyper-V and SQL** check box to permit SMB 3.0 and later clients that support it to open files persistently during nondisruptive operations.  
  
Files opened using this option are protected from disruptive events, such as failover, giveback, and LIF migration.
8. Select the **Encrypt data while accessing this share** check box to enable SMB 3.0 encryption.
9. Provide a description or comment for the share and click **Create**.

**Result**

The share is created with the access permissions set to “Full Control for Everyone” in the group.

**Related tasks**

[Setting up CIFS](#) on page 258

**Related references**

[Shares window](#) on page 223

## Stopping share access

You can use System Manager to stop a share when you want to remove the shared network access to a folder, qtree, or volume.

**Before you begin**

You must have installed the CIFS license.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Shares** tab.
4. From the list of shares, select the share that you want to stop sharing and click **Stop Sharing**.
5. Select the confirmation check box and click **Stop**.
6. Verify that the share is no longer listed in the **Shares** window.

**Related references**

[Shares window](#) on page 223

## Creating home directory shares

You can use System Manager to create a home directory share and manage home directory search paths.

### Before you begin

CIFS must be set up and started.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Shares** tab.
4. Click **Create Home Directory** and provide the pattern information that determines how a user is mapped to a directory.
5. Click **Create**.
6. Verify that the home directory you created is listed in the **Shares** window.

## Editing share settings

You can use System Manager to modify the settings of a share, such as the symbolic link settings, share access permissions of users or groups, and the type of access to the share. You can also enable or disable continuous availability of a share over Hyper-V, and enable or disable access-based enumeration (ABE).

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Shares** tab.
4. Select the share that you want to modify from the share list and click **Edit**.
5. In the **Edit Share Settings** dialog box, modify the share settings as required:
  - a. In the **General** tab, enable continuous availability of a share over Hyper-V.  
 Enabling continuous availability permits SMB 3.0 and later clients that support SMB 3.0 to open files persistently during nondisruptive operations. Files that are opened persistently are protected from disruptive events, such as failover, giveback, and LIF migration.
  - b. In the **Permissions** tab, add users or groups and assign permissions to specify the type of access.
  - c. In the **Options** tab, perform the following actions on the share:
    - Select the settings for the symbolic links.
    - Enable opportunistic locks (oplocks).
    - Enable clients to browse through the share.
    - View Snapshot copies.
    - Notify changes.

- Enable ABE.
  - Enable BranchCache.
  - Enable data to be encrypted using SMB 3.0 while accessing this share.
6. Click **Save and Close**.
  7. Verify the changes that you made to the selected share in the **Shares** window.

#### Related references

[Shares window](#) on page 223

## How ONTAP enables dynamic home directories

ONTAP home directories enable you to configure an SMB share that maps to different directories based on the user that connects to it and a set of variables. Instead of creating separate shares for each user, you can configure one share with a few home directory parameters to define a user's relationship between an entry point (the share) and the home directory (a directory on the Storage Virtual Machine (SVM)).

A user that is logged in as a guest user does not have a home directory and cannot access other users' home directories. There are four variables that determine how a user is mapped to a directory:

#### Share name

This is the name of the share that you create to which the user connects. You must set the home directory property for this share.

The share name can use the following dynamic names:

- `%w` (the user's Windows user name)
- `%d` (the user's Windows domain name)
- `%u` (the user's mapped UNIX user name)

To make the share name unique across all home directories, the share name must contain either the `%w` or the `%u` variable. The share name can contain both the `%d` and the `%w` variable (for example, `%d/%w`), or the share name can contain a static portion and a variable portion (for example, `home_%w`).

#### Share path

This is the relative path, which is defined by the share and is therefore associated with one of the share names, that is appended to each search path to generate the user's entire home directory path from the root of the SVM. It can be static (for example, `home`), dynamic (for example, `%w`), or a combination of the two (for example, `eng/%w`).

#### Search paths

This is the set of absolute paths from the root of the SVM that you specify that directs the ONTAP search for home directories. You can specify one or more search paths by using the `vserver cifs home-directory search-path add` command. If you specify multiple search paths, ONTAP tries them in the order specified until it finds a valid path.

#### Directory

This is the user's home directory that you create for the user. The directory name is usually the user's name. You must create the home directory in one of the directories that are defined by the search paths.

As an example, consider the following setup:

- User: John Smith

- User domain: acme
- User name: jsmith
- SVM name: vs1
- Home directory share name #1: home\_%w - share path: %w
- Home directory share name #2: %w - share path: %d/%w
- Search path #1: /aggr0home/home
- Search path #2: /aggr1home/home
- Search path #3: /aggr2home/home
- Home directory: /aggr1home/home/jsmith

Scenario 1: The user connects to \\vs1\home\_jsmith. This matches the first home directory share name and generates the relative path jsmith. ONTAP now searches for a directory named jsmith by checking each search path in order:

- /aggr0home/home/jsmith does not exist; moving on to search path #2.
- /aggr1home/home/jsmith does exist; therefore, search path #3 is not checked; the user is now connected to his home directory.

Scenario 2: The user connects to \\vs1\jsmith. This matches the second home directory share name and generates the relative path acme/jsmith. ONTAP now searches for a directory named acme/jsmith by checking each search path in order:

- /aggr0home/home/acme/jsmith does not exist; moving on to search path #2.
- /aggr1home/home/acme/jsmith does not exist; moving on to search path #3.
- /aggr2home/home/acme/jsmith does not exist; the home directory does not exist; therefore, the connection fails.

## Shares window

You can use the Shares window to manage your shares and display information about them.

- [Command buttons](#) on page 223
- [Shares list](#) on page 224
- [Details area](#) on page 224

### Command buttons

#### Create Share

Opens the Create Share dialog box, which enables you to create a share.

#### Create Home Directory

Opens the Create Home Directory Share dialog box, which enables you to create a new home directory share.

#### Edit

Opens the Edit Settings dialog box, which enables you to modify the properties of a selected share.

#### Stop Sharing

Stops the selected object from being shared.

**Refresh**

Updates the information in the window.

**Shares list**

The shares list displays the name and path of each share.

**Share Name**

Displays the name of the share.

**Path**

Displays the complete path name of an existing folder, qtree, or volume that is shared. Path separators can be backward or forward slashes, although Data ONTAP displays them as forward slashes.

**Home Directory**

Displays the name of the home directory share.

**Comment**

Displays any description for the share.

**Continuously Available Share**

Displays whether the share is enabled for continuous availability.

**Details area**

The area below the shares list displays the share properties and the access rights for each share.

**Properties**

- **Name**  
Displays the name of the share.
- **Oplocks status**  
Specifies if the share uses opportunistic locks (oplocks).
- **Browsable**  
Specifies whether the share can be browsed by Windows clients.
- **Show Snapshot**  
Specifies whether Snapshot copies can be viewed by clients.
- **Continuously Available Share**  
Specifies whether the share is enabled or disabled for continuous availability.
- **Access-Based Enumeration**  
Specifies whether access-based enumeration (ABE) is enabled or disabled on the share.
- **BranchCache**  
Specifies whether BranchCache is enabled or disabled on the share.
- **SMB Encryption**  
Specifies whether data encryption using SMB 3.0 is enabled at the SVM level or at the share level. If SMB encryption is enabled at SVM level, it applies for all the shares and the value is shown as Enabled (at the SVM level).

**Share access control**

Displays the access rights of the domain users and groups and local users and groups for the share.



**Related tasks**

[Creating a CIFS share](#) on page 219

[Stopping share access](#) on page 220

[Editing share settings](#) on page 221

## LUNs

You can use System Manager to manage LUNs.

You can access all the LUNs in the cluster by using the LUNs tab or you can access the LUNs specific to the SVM by using **SVMs > LUNs**.

**Note:** The LUNs tab is displayed only if you have enabled the FC/FCoE and iSCSI licenses.

## Creating FC SAN optimized LUNs

You can use System Manager to create one or more FC SAN optimized LUNs during the initial setup of a cluster on an All Flash FAS platform.

**Before you begin**

- You must ensure that only one Storage Virtual Machine (SVM) has been created with the name `AFF_SAN_DEFAULT_SVM`, and that this SVM does not contain any LUNs.
- You must have verified that the hardware setup has been completed successfully.

[NetApp Documentation: ONTAP 9](#)

**About this task**

- This method is available only during the initial setup of a cluster with two or more nodes. System Manager uses only the first two nodes to create LUNs.
- Each LUN is created on a separate volume.
- Volumes are thin provisioned.
- Space reservation is disabled on the created LUNs.
- Most of the cluster configurations are already completed at the factory and are optimized for optimum storage efficiency and performance. You must not modify these configurations.

**Steps**

1. Log in to System Manager by using your cluster administrator credentials.  
After you create LUNs using this method, you cannot use this method again.  
If you close the dialog box without creating LUNs, you must navigate to the LUNs tab and click **Create** to access the dialog box again.
2. In the **LUN details** area of the **Create LUNs** dialog box, specify the application type:

If the application type is...	Then...
Oracle	<ol style="list-style-type: none"> <li>Specify the database name and size.</li> <li>If you have deployed Oracle Real Application Clusters (RAC), then select the <b>Oracle RAC</b> check box. Only two RAC nodes are supported. You must ensure that Oracle RAC has a minimum of two initiators added to the initiator group.</li> </ol>
SQL	Specify the number of databases and the size of each database.
Other	<ol style="list-style-type: none"> <li>Specify the name and size of each LUN.</li> <li>If you want to create more LUNs, click <b>Add more LUNs</b>, and then specify the name and size for each LUN.</li> </ol>

Data, log, binary, and temporary LUNs are created based on the selected application type.

- In the **Map to these Initiators** area, perform these steps:
  - Specify the initiator group name and the type of operating system.
  - Add the host initiator WWPN by selecting it from the drop-down list or by typing the initiator in the text box.

Only one initiator group is created.

- Click **Create**.

A summary table is displayed with the LUNs that are created.

- Click **Close**.

#### Related information

*[NetApp Documentation: ONTAP 9](#)*

## Application-specific LUN settings

System Manager supports Oracle, SQL, and other application types while creating FC SAN optimized LUNs on an All Flash FAS cluster. LUN settings such as the LUN size are determined by rules specific to the application type. For SQL and Oracle, LUN settings are automatically created.

If your cluster contains two or more nodes, System Manager uses only the first two nodes selected by the API to create LUNs. Data aggregates are already created in each of the two nodes. The size of each volume created is equal to the available capacity of the aggregate. The volumes are thin-provisioned and space reservation is disabled on the LUNs.

Storage efficiency policy is enabled by default with the schedule set to “daily” and quality of service (QoS) set to “best\_effort”. By default, access time (atime) update is enabled on the cluster. However, access time updates are disabled by System Manager while creating volumes and therefore every time a file is read or written, the access time field in the directory is not updated.

**Note:** Enabling the access time update causes performance degradation to the data-serving capability of the cluster.

### LUN settings for SQL

By default, LUNs and volumes are provisioned for a single instance of the SQL server with 2 databases of 1 TB each and 24 physical cores. Space is provisioned for LUNs and volumes according to specific rules for the SQL server. Load balancing is performed for LUNs across the HA pair. You

can modify the number of databases. For each database, eight data LUNs and one log LUN is created. One temporary LUN is created for each SQL instance.

The following table provides information about how space is provisioned for the default values of SQL:

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
node1	node1_aggr1	data	db01_data01	db01_data01	Database size ÷ 8	125
		data	db01_data02	db01_data02	Database size ÷ 8	125
		data	db01_data03	db01_data03	Database size ÷ 8	125
		data	db01_data04	db01_data04	Database size ÷ 8	125
		data	db02_data01	db02_data01	Database size ÷ 8	125
		data	db02_data02	db02_data02	Database size ÷ 8	125
		data	db02_data03	db02_data03	Database size ÷ 8	125
		data	db02_data04	db02_data04	Database size ÷ 8	125
		log	db01_log	db01_log	Database size ÷ 20	50
		temp	sql_temp	sql_temp	Database size ÷ 3	330
node2	node2_aggr1	data	db01_data05	db01_data05	Database size ÷ 8	125
		data	db01_data06	db01_data06	Database size ÷ 8	125
		data	db01_data07	db01_data07	Database size ÷ 8	125
		data	db01_data08	db01_data08	Database size ÷ 8	125
		data	db02_data05	db02_data05	Database size ÷ 8	125
		data	db02_data06	db02_data06	Database size ÷ 8	125
		data	db02_data07	db02_data07	Database size ÷ 8	125
		data	db02_data08	db02_data08	Database size ÷ 8	125
		log	db02_log	db02_log	Database size ÷ 20	50

### LUN settings for Oracle

By default, LUNs and volumes are provisioned for one database of 2 TB. Space is provisioned for LUNs and volumes according to specific rules for Oracle. By default, Oracle Real Application Clusters (RAC) is not selected.

The following table provides information about how space is provisioned for the default values of Oracle:

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
node1	node1_aggr1	data	ora_vol01	ora_lundata01	Database size ÷ 8	250
		data	ora_vol02	ora_lundata02	Database size ÷ 8	250
		data	ora_vol03	ora_lundata03	Database size ÷ 8	250
		data	ora_vol04	ora_lundata04	Database size ÷ 8	250
		log	ora_vol05	ora_lunlog1	Database size ÷ 40	50
		binaries	ora_vol06	ora_orabin1	Database size ÷ 40	50
node2	node2_aggr1	data	ora_vol07	ora_lundata05	Database size ÷ 8	250
		data	ora_vol08	ora_lundata06	Database size ÷ 8	250
		data	ora_vol09	ora_lundata07	Database size ÷ 8	250
		data	ora_vol10	ora_lundata08	Database size ÷ 8	250
		log	ora_vol11	ora_lunlog2	Database size ÷ 40	50

For Oracle RAC, LUNs are provisioned for grid files. Only two RAC nodes are supported for Oracle RAC.

The following table provides information about how space is provisioned for the default values of Oracle RAC:

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
node1	node1_aggr1	data	ora_vol01	ora_lundata01	Database size ÷ 8	250
		data	ora_vol02	ora_lundata02	Database size ÷ 8	250
		data	ora_vol03	ora_lundata03	Database size ÷ 8	250

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
		data	ora_vol04	ora_lundata04	Database size ÷ 8	250
		log	ora_vol05	ora_lunlog1	Database size ÷ 40	50
		binaries	ora_vol06	ora_orabin1	Database size ÷ 40	50
		grid	ora_vol07	ora_lungrid1	10 GB	10
node2	node2_aggr1	data	ora_vol08	ora_lundata05	Database size ÷ 8	250
		data	ora_vol09	ora_lundata06	Database size ÷ 8	250
		data	ora_vol10	ora_lundata07	Database size ÷ 8	250
		data	ora_vol11	ora_lundata08	Database size ÷ 8	250
		log	ora_vol12	ora_lunlog2	Database size ÷ 40	50
		binaries	ora_vol13	ora_orabin2	Database size ÷ 40	50

### LUN settings for Other application type

Each LUN is provisioned in a volume. The space is provisioned in the LUNs based on the specified size. Load balancing is performed across the nodes for all the LUNs.

## Creating LUNs

You can use System Manager to create LUNs for an existing aggregate, volume, or qtree when there is available free space. You can create a LUN in an existing volume or create a new FlexVol volume for the LUN. You can also enable Storage Quality of Service (QoS) to manage the workload performance.

### About this task

If you specify the LUN ID, System Manager checks the validity of the LUN ID before adding it. If you do not specify a LUN ID, Data ONTAP automatically assigns one.

While selecting the LUN multiprotocol type, you should have considered the guidelines for using each type.

In a MetroCluster configuration, System Manager displays only the following aggregates for creating FlexVol volumes for the LUN:

- In normal mode, when you create volumes on sync-source SVMs or data-serving SVMs in the primary site, only those aggregates that belong to the cluster in the primary site are displayed.
- In switched-over mode, when you create volumes on sync-destination SVMs or data-serving SVMs in the surviving site, only switched-over aggregates are displayed.

**Steps**

1. Click the **LUNs** tab.
2. In the **LUN Management** tab, click **Create**.
3. Browse and select an SVM in which you want to create the LUNs.
4. In the **Create LUN Wizard**, specify the name, size, type, description for the LUN, and select the **Space Reserve**, and then click **Next**.
5. Create a new FlexVol volume for the LUN or select an existing volume or qtree, and then click **Next**.
6. Add initiator groups if you want to control host access to the LUN, and then click **Next**.
7. Select the **Manage Storage Quality of Service** check box if you want to manage the workload performance of the LUN.
8. Create a new storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the LUN:

If you want to...	Then do the following...
Create a new policy group	<ol style="list-style-type: none"> <li>a. Specify the policy group name.</li> <li>b. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group do not exceed the specified throughput limit. If you do not specify the maximum throughput limit, the value is set to unlimited and the unit that you specify does not affect the maximum throughput.</li> <li>c. Click <b>Next</b>.</li> </ol>
Select an existing policy group	<ol style="list-style-type: none"> <li>a. Select <b>Existing Policy Group</b>, and then click <b>Choose</b> to select an existing policy group from the Select Policy Group dialog box. You can also choose to modify the maximum throughput for the selected policy group.</li> <li>b. Click <b>Next</b>.  If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.</li> </ol>

9. Review the specified details in the **LUN summary** window, and then click **Next**.
10. Confirm the details, and then click **Finish** to complete the wizard.

**Related concepts**

[Guidelines for using LUN multiprotocol type](#) on page 239

**Related references**

[LUNs window](#) on page 243

## Deleting LUNs

You can use System Manager to delete LUNs and return the space used by the LUNs to their containing aggregates or volumes.

### Before you begin

- The LUN must be offline.
- The LUN must be unmapped from all initiator hosts.

### Steps

1. Click the **LUNs** tab.
2. In the **LUN Management** tab, select one or more LUNs that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

### Related references

[LUNs window](#) on page 243

## Creating initiator groups

You can use System Manager to create an initiator group. Initiator groups enable you to control host access to specific LUNs. You can use port sets to limit which LIFs an initiator can access.

### Steps

1. Click the **LUNs** tab.
2. In the **Initiator Groups** tab, click **Create**.
3. In the **General** tab of the **Create Initiator Group** dialog box, specify the initiator group name, operating system, port set, and supported protocol for the group.
4. Click **Create**.

### Related references

[LUNs window](#) on page 243

## Deleting initiator groups

You can use the Initiator Groups tab in System Manager to delete initiator groups.

### Before you begin

All the LUNs mapped to the initiator group must be manually unmapped.

### Steps

1. Click the **LUNs** tab.
2. In the **Initiator Groups** tab, select one or more initiator groups that you want to delete, and then click **Delete**.
3. Click **Delete**.

4. Verify that the initiator groups you deleted are no longer displayed in the **Initiator Groups** tab.

**Related references**

[LUNs window](#) on page 243

## Adding initiators

You can use System Manager to add initiators to an initiator group. An initiator provides access to a LUN when the initiator group that it belongs to is mapped to that LUN.

**Steps**

1. Click the **LUNs** tab.
2. In the **LUN Management** tab, select the initiator group to which you want to add initiators and click **Edit**.
3. In the **Edit Initiator Group** dialog box, click **Initiators**.
4. Click **Add**.
5. Specify the initiator name and click **OK**.
6. Click **Save and Close**.

**Related references**

[LUNs window](#) on page 243

## Deleting initiators from an initiator group

You can use the Initiator Groups tab in System Manager to delete an initiator.

**Before you begin**

All the LUNs mapped to the initiator group that contains the initiators must be manually unmapped.

**Steps**

1. Click the **LUNs** tab.
2. In the **Initiator Groups** tab, select one or more initiators that you want to delete, and then click **Delete**.

**Related references**

[LUNs window](#) on page 243

## Creating port sets

You can use System Manager to create port sets to limit access to your LUNs.

**Steps**

1. Click the **LUNs** tab.
2. In the **Portsets** tab, click **Create**.
3. In the **Create Portset** dialog box, select the type of protocol.
4. Choose the network interface that you want to associate with the port set.



5. Click **Create**.

## Deleting port sets

You can use System Manager to delete a port set when it is no longer required.

### Steps

1. Click the **LUNs** tab.
2. In the **Portsets** tab, select one or more port sets and click **Delete**.
3. Confirm the deletion by clicking **Delete**.

## Cloning LUNs

LUN clones enable you to create multiple readable and writable copies of a LUN. You can use System Manager to create a temporary copy of a LUN for testing or to create a copy of your data available to additional users without providing them access to the production data.

### Before you begin

- You must have installed the FlexClone license on the storage system.
- When space reservation is disabled on a LUN, the volume that contains the LUN must have enough space to accommodate changes to the clone.

### About this task

- When you create a LUN clone, automatic deletion of the LUN clone is enabled by default in System Manager. As a result, the LUN clone is deleted when Data ONTAP triggers automatic deletion to conserve space.
- You cannot clone LUNs on SnapLock volumes.

### Steps

1. Click the **LUNs** tab.
2. In the **LUN Management** tab, select the LUN that you want to clone, and then click **Clone**.
3. Optional: If you want to change the default name, specify a new name.
4. Click **Clone**.
5. Verify that the LUN clone you created is listed in the **LUNs** window.

### Related references

[LUNs window](#) on page 243

## Editing LUNs

You can use the LUN properties dialog box in System Manager to change the name, description, size, space reservation setting, or the mapped initiator hosts of a LUN.

### Steps

1. Click the **LUNs** tab.

2. In the **LUN Management** tab, select the LUN that you want to edit from the list of LUNs, and click **Edit**.
3. Make the required changes.
4. Click **Save and Close**.

**Related references**

[LUNs window](#) on page 243

## Bringing LUNs online

You can use the **LUN Management** tab in System Manager to bring selected LUNs online and make them available to the host.

**Before you begin**

Any host application accessing the LUN must be quiesced or synchronized.

**Steps**

1. Click the **LUNs** tab.
2. In the **LUN Management** tab, select one or more LUNs that you want to bring online.
3. Click **Status > Online**.

**Related references**

[LUNs window](#) on page 243

## Taking LUNs offline

You can use the **LUN Management** tab in System Manager to take selected LUNs offline and make them unavailable for block protocol access.

**Before you begin**

Any host application accessing the LUN must be quiesced or synchronized.

**Steps**

1. Click the **LUNs** tab.
2. In the **LUN Management** tab, select one or more LUNs that you want to take offline.
3. Click **Status > Offline**.

**Related references**

[LUNs window](#) on page 243

## Moving LUNs

You can use System Manager to move a LUN from its containing volume to another volume or qtree within a Storage Virtual Machine (SVM). You can move the LUN to a volume that is hosted on an

aggregate containing high-performance disks, thereby improving the performance when accessing the LUN.

#### About this task

- You cannot move a LUN to a qtree within the same volume.
- If you have created a LUN from a file using the command-line interface (CLI), you cannot move the LUN using System Manager.
- The LUN move operation is nondisruptive; it can be performed when the LUN is online and serving data.
- You cannot use System Manager to move the LUN if the allocated space in the destination volume is not sufficient to contain the LUN, and even if autogrow is enabled on the volume. You should use the CLI instead.
- You cannot move LUNs on SnapLock volumes.

#### Steps

1. Click the **LUNs** tab.
2. In the **LUN Management** tab, select the LUN that you want to move from the list of LUNs, and then click **Move**.
3. Optional: In the **Move Options** area of the **Move LUN** dialog box, specify a new name for the LUN if you want to change the default name.
4. Select the storage object to which you want to move the LUN and perform one of the following actions:

If you want to move the LUN to...	Then...
A new volume	<ol style="list-style-type: none"> <li>a. Select an aggregate in which you want to create the new volume.</li> <li>b. Specify a name for the volume.</li> </ol>
An existing volume or qtree	<ol style="list-style-type: none"> <li>a. Select a volume to which you want to move the LUN.</li> <li>b. If the selected volume contains any qtrees, select the qtree to which you want to move the LUN.</li> </ol>

5. Click **Move**.
6. Confirm the LUN move operation, and click **Continue**.

For a brief period of time, the LUN is displayed on both the origin and destination volume. After the move operation is complete, the LUN is displayed on the destination volume.

The destination volume or qtree is displayed as the new container path for the LUN.

## Assigning LUNs to Storage QoS

You can use System Manager to limit the throughput of LUNs by assigning them to Storage Quality of Service (QoS) policy groups. You can assign Storage QoS for new LUNs or modify Storage QoS details for LUNs that are already assigned to a policy group.

### About this task

- You cannot assign Storage QoS to a LUN if the following storage objects are assigned to a policy group:
  - Parent volume of the LUN
  - Parent Storage Virtual Machine (SVM) of the LUN
- You can assign Storage QoS or modify QoS details for a maximum of 10 LUNs at the same time.

### Steps

1. Click the **LUNs** tab.
2. In the **LUN Management** tab, select one or more LUNs for which you want to assign Storage QoS.
3. Click **Storage QoS**.
4. In the **Quality of Service Details** dialog box, select the **Manage Storage Quality of Service** check box if you want to manage the workload performance of the LUN.

If some of the LUNs you selected are already assigned to a policy group, the changes that you make might affect the performance of these LUNs.

5. Create a new storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the LUN:

If you want to...	Then do the following...
Create a new policy group	<ol style="list-style-type: none"> <li>a. Specify the policy group name.</li> <li>b. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group do not exceed the specified throughput limit. If you do not specify the maximum throughput limit, the value is set to Unlimited and the unit that you specify does not affect the maximum throughput.</li> </ol>
Select an existing policy group	<p>Select <b>Existing Policy Group</b> and click <b>Choose</b> to select an existing policy group from the Select Policy Group dialog box.</p> <p>You can also choose to modify the maximum throughput for the selected policy group.</p> <p>If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.</p>

6. Optional: Click the link that specifies the number of LUNs to review the list of selected LUNs, and click **Discard** if you want to remove any LUNs from the list.

The link is displayed only when multiple LUNs are selected.

7. Click **OK**.

## Editing initiator groups

You can use the Edit Initiator Group dialog box in System Manager to change the name of an existing initiator group and its operating system. You can add initiators to or remove initiators from the initiator group. You can also change the port set associated with the initiator group.

### Steps

1. Click the **LUNs** tab.
2. In the **Initiator Groups** tab, select the initiator group that you want to modify, and then click **Edit**.
3. Make the necessary changes.
4. Click **Save and Close**.
5. Verify the changes you made to the initiator group in the **Initiator Groups** tab.

### Related references

[LUNs window](#) on page 243

## Editing initiators

You can use the Edit Initiator Group dialog box in System Manager to change the name of an existing initiator in an initiator group.

### Steps

1. Click the **LUNs** tab.
2. In the **Initiator Groups** tab, select the initiator group to which the initiator belongs, and then click **Edit**.
3. In the **Edit Initiator Group** dialog box, click **Initiators**.
4. Select the initiator that you want to edit and click **Edit**.
5. Change the name and click **OK**.
6. Click **Save and Close**.

### Related references

[LUNs window](#) on page 243

## Editing port sets

You can use the Portsets tab in System Manager to edit settings related to port sets.

### Steps

1. Click the **LUNs** tab.
2. In the **Portsets** tab, select the port set you want to edit and click **Edit**.
3. In the **Edit Portset** dialog box, make the necessary changes.
4. Click **Save and Close**.

**Related tasks**

[Configuring iSCSI protocol on SVMs](#) on page 46

**Viewing LUN information**

You can use the LUN Management tab in System Manager to view details about a LUN, such as its name, status, size, and type.

**Steps**

1. Click the **LUNs** tab.
2. In the **LUN Management** tab, select the LUN that you want to view information about from the displayed list of LUNs.
3. Review the LUN details in the **LUNs** window.

**Viewing initiator groups**

You can use the Initiator Groups tab in System Manager to view all the initiator groups and the initiators mapped to these initiator groups, and the LUNs and LUN ID mapped to the initiator groups.

**Steps**

1. Click the **LUNs** tab.
2. Click **Initiator Groups** and review the initiator groups that are listed in the upper pane.
3. Select an initiator group to view the initiators that belong to it, which are listed in the **Initiators** tab in the lower pane.
4. Select an initiator group to view the LUNs mapped to it, which are listed in the **Mapped LUNs** in the lower pane.

**Guidelines for working with FlexVol volumes that contain LUNs**

When you work with FlexVol volumes that contain LUNs, you must change the default settings for Snapshot copies. You can also optimize the LUN layout to simplify administration.

Snapshot copies are required for many optional features, such as SnapMirror, SyncMirror, dump and restore, and ndmcopy.

When you create a volume, Data ONTAP automatically performs the following:

- Reserves 5 percent of the space for Snapshot copies
- Schedules Snapshot copies

Because the internal scheduling mechanism for creating Snapshot copies within Data ONTAP does not ensure that the data within a LUN is in a consistent state, you should change these Snapshot copy settings by performing the following tasks:

- Turn off the automatic Snapshot copy schedule.
- Delete all existing Snapshot copies.
- Set the percentage of space reserved for Snapshot copies to zero.

You should use the following guidelines to create volumes that contain LUNs:

- Do not create any LUNs in the system's root volume.  
Data ONTAP uses this volume to administer the storage system. The default root volume is /vol/vol0.

- You should use a SAN volume to contain the LUN.
- You should ensure that no other files or directories exist in the volume that contains the LUN. If this is not possible and you are storing LUNs and files in the same volume, you should use a separate qtree to contain the LUNs.
- If multiple hosts share the same volume, you should create a qtree on the volume to store all the LUNs for the same host.  
This is a best practice that simplifies LUN administration and tracking.
- To simplify management, you should use naming conventions for LUNs and volumes that reflect their ownership or the way that they are used.

#### Related information

*[NetApp Documentation: ONTAP 9](#)*

## LUN size and type

When you create a LUN, you must specify the LUN size and the type for your host operating system.

The LUN Multiprotocol Type, or operating system type, determines the layout of data on the LUN, and the minimum and maximum sizes of the LUN. After the LUN is created, you cannot modify the LUN host operating system type.

## Understanding space reservations for LUNs

Understanding how the space reservation setting (combined with the volume guarantee) affects how space is set aside for LUNs helps you to understand the ramifications of disabling space reservations, and why certain combinations of LUN and volume settings are not useful.

When a LUN has space reservations enabled (a space-reserved LUN), and its containing volume has a volume guarantee, free space from the volume is set aside for the LUN at creation time; the size of this reserved space is governed by the size of the LUN. Other storage objects in the volume (other LUNs, files, Snapshot copies, and so on) are prevented from using this space.

When a LUN has space reservations disabled (a non-space-reserved LUN), no space is set aside for that LUN at creation time. The storage required by any write operation to the LUN is allocated from the volume when it is needed, provided sufficient free space is available.

If a space-reserved LUN is created in a none-guaranteed volume, the LUN behaves the same as a non-space-reserved LUN. This is because a none-guaranteed volume has no space to allocate to the LUN; the volume itself can only allocate space as it is written to, due to its none guarantee. Therefore, creating a space-reserved LUN in a none-guaranteed volume is not recommended; employing this configuration combination might provide write guarantees that are in fact impossible.

When the space reserve is set to “Default”, the ONTAP space reservation settings apply to the LUNs. ONTAP space reservation settings also apply to the container volumes if new volumes are created.

## Guidelines for using LUN multiprotocol type

The LUN multiprotocol type, or operating system type, specifies the operating system of the host accessing the LUN. It also determines the layout of data on the LUN, and the minimum and maximum size of the LUN.

**Note:** Not all Data ONTAP versions support all LUN multiprotocol types. For the most up-to-date information, see the Interoperability Matrix.

The following table describes the LUN multiprotocol type values and the guidelines for using each type:

LUN multiprotocol type	When to use
AIX	If your host operating system is AIX.
HP-UX	If your host operating system is HP-UX.
Hyper-V	Use if you are using Windows Server 2008 or Windows Server 2012 Hyper-V and your LUNs contain virtual hard disks (VHDs). If you are using hyper_v for your LUN type, you should also use hyper_v for your igroup OS type.  <b>Note:</b> For raw LUNs, you can use the type of child operating system as the LUN multiprotocol type.
Linux	If your host operating system is Linux.
NetWare	If your host operating system is NetWare.
OpenVMS	If your host operating system is OpenVMS.
Solaris	If your host operating system is Solaris and you are not using Solaris EFI labels.
Solaris EFI	If you are using Solaris EFI labels.  <b>Note:</b> Using any other LUN multiprotocol type with Solaris EFI labels might result in LUN misalignment problems.
VMware	If you are using an ESX Server and your LUNs will be configured with VMFS.  <b>Note:</b> If you configure the LUNs with RDM, you can use the guest operating system as the LUN multiprotocol type.
Windows 2003 MBR	If your host operating system is Windows Server 2003 using the MBR partitioning method.
Windows 2003 GPT	If you want to use the GPT partitioning method and your host is capable of using it. Windows Server 2003, Service Pack 1 and later are capable of using the GPT partitioning method, and all 64-bit versions of Windows support it.
Windows 2008 or later	If your host operating system is Windows Server 2008 or later; both MBR and GPT partitioning methods are supported.
Xen	If you are using Xen and your LUNs will be configured with Linux LVM with Dom0.  <b>Note:</b> For raw LUNs, you can use the type of guest operating system as the LUN multiprotocol type.

**Related tasks**

[Creating LUNs](#) on page 229

**Related information**

[NetApp Interoperability](#)

[Solaris Host Utilities 6.1 Installation and Setup Guide](#)

[Solaris Host Utilities 6.1 Quick Command Reference](#)

[Solaris Host Utilities 6.1 Release Notes](#)



## Understanding LUN clones

LUN clones are writable, space-efficient clones of parent LUNs. Creating LUN clones is highly space-efficient and time-efficient because the cloning operation does not involve physically copying any data. Clones help in space storage utilization of the physical aggregate space.

You can clone a complete LUN without the need of a backing Snapshot copy in a SAN environment. The cloning operation is instantaneous and clients that are accessing the parent LUN do not experience any disruption or outage. Clients can perform all normal LUN operations on both parent entities and clone entities. Clients have immediate read/write access to both the parent and cloned LUN.

Clones share the data blocks of their parent LUNs and occupy negligible storage space until clients write new data either to the parent LUN, or to the clone. By default, the LUN clone inherits the space reserved attribute of the parent LUN. For example, if space reservation is disabled on the parent LUN, then space reservation is also disabled on the LUN clone.

**Note:** When you clone a LUN, you must ensure that the volume has enough space to contain the LUN clone.

## Resizing a LUN

You can resize a LUN to be bigger or smaller than its original size. When you resize a LUN, you have to perform the steps on the host side that are recommended for the host type and the application that is using the LUN.

## Initiator hosts

Initiator hosts can access the LUNs mapped to them. When you map a LUN on a storage system to the igroup, you grant all the initiators in that group access to that LUN. If a host is not a member of an igroup that is mapped to a LUN, that host does not have access to the LUN.

## VMware RDM

When you perform raw device mapping (RDM) on VMware, the operating system type of the LUN must be the operating system type of the guest operating system.

## What igroups are

Initiator groups (igroups) are tables of FC protocol host WWPNs or iSCSI host node names. You can define igroups and map them to LUNs to control which initiators have access to LUNs.

Typically, you want all of the host's initiator ports or software initiators to have access to a LUN. If you are using multipathing software or have clustered hosts, each initiator port or software initiator of each clustered host needs redundant paths to the same LUN.

You can create igroups that specify which initiators have access to the LUNs either before or after you create LUNs, but you must create igroups before you can map a LUN to an igroup.

Initiator groups can have multiple initiators, and multiple igroups can have the same initiator. However, you cannot map a LUN to multiple igroups that have the same initiator. An initiator cannot be a member of igroups of differing otypes.

## Required information for creating igroups

There are a number of attributes required when creating igroups, including the name of the igroup, type of igroup, ostype, iSCSI node name for iSCSI igroups, and WWPN for FCP igroups.

### igroup name

The igroup name is a case-sensitive name that must satisfy several requirements.

The igroup name:

- Contains 1 to 96 characters. Spaces are not allowed.
- Can contain the letters A through Z, a through z, numbers 0 through 9, hyphen (“-”), underscore (“\_”), colon (“:”), and period (“.”).
- Must start with a letter or number.

The name you assign to an igroup is independent of the name of the host that is used by the host operating system, host files, or Domain Name Service (DNS). If you name an igroup aix1, for example, it is not mapped to the actual IP host name (DNS name) of the host.

**Note:** You might find it useful to provide meaningful names for igroups, ones that describe the hosts that can access the LUNs mapped to them.

### igroup type

The igroup type can be mixed type, iSCSI, or FC/FCoE.

### igroup ostype

The ostype indicates the type of host operating system used by all of the initiators in the igroup. All initiators in an igroup must be of the same ostype. The ostyles of initiators are **solaris**, **windows**, **hpux**, **aix**, **netware**, **xen**, **hyper\_v**, **vmware**, and **linux**.

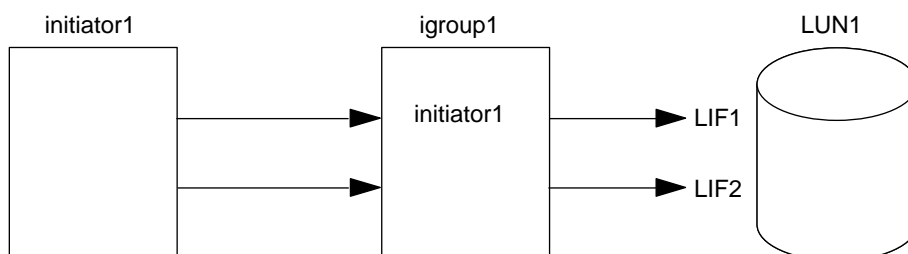
You must select an ostyle for the igroup.

## Ways to limit LUN access with port sets and igroups

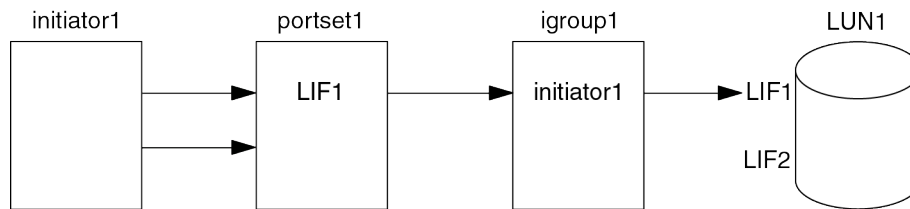
In addition to using Selective LUN Map (SLM), you can limit access to your LUNs through igroups and port sets.

Port sets can be used with SLM to further restrict access of certain targets to certain initiators. When using SLM with port sets, LUNs will be accessible on the set of LIFs in the port set on the node that owns the LUN and on that node's HA partner.

In the following example, initiator1 does not have a port set. Without a port set, initiator1 can access LUN1 through both LIF1 and LIF2.



You can limit access to LUN1 by using a port set. In the following example, initiator1 can access LUN1 only through LIF1. However, initiator1 cannot access LUN1 through LIF2 because LIF2 is not in port set1.



## LUNs window

You can use the LUNs window to create and manage LUNs and to display information about LUNs. You can also add, edit, or delete initiator groups and initiator IDs.

- [LUN Management tab](#) on page 243
- [Initiator Groups tab](#) on page 244
- [Portsets tab](#) on page 245

### LUN Management tab

This tab enables you to create, clone, delete, move, or edit the settings of LUNs. You can also assign LUNs to a Storage Quality of Service (QoS) policy group.

#### Command buttons

##### Create

Opens the Create LUN wizard, which enables you to create LUNs.

In a cluster on an All Flash FAS platform that does not contain any existing LUNs, the Create FC SAN optimized LUNs dialog box is opened, which enables you to set up one or more FC SAN optimized LUNs.

##### Clone

Opens the Clone LUN dialog box, which enables you to clone the selected LUNs.

##### Edit

Opens the Edit LUN dialog box, which enables you to edit the settings of the selected LUN.

##### Delete

Deletes the selected LUN.

##### Status

Enables you to change the status of the selected LUN to either Online or Offline.

##### Move

Opens the Move LUN dialog box, which enables you to move the selected LUN to a new volume or an existing volume or qtree within the same Storage Virtual Machine (SVM).

##### Storage QoS

Opens the Quality of Service details dialog box, which enables you to assign one or more LUNs to a new or existing policy group.

##### Refresh

Updates the information in the window.

**LUNs list****Name**

Displays the name of the LUN.

**Container Path**

Displays the name of the file system (volume or qtree) that contains the LUN.

**Space Reservation**

Specifies whether space reservation is enabled or disabled.

**Available Size**

Displays the space available in the LUN.

**Total Size**

Displays the total space in the LUN.

**%Used**

Displays the total space (in percentage) that is used.

**Type**

Specifies the LUN type.

**Status**

Specifies the status of the LUN.

**Policy Group**

Displays the name of the Storage QoS policy group to which the LUN is assigned. By default, this column is hidden.

**Details area**

The area below the LUNs list displays details related to the selected LUN.

**Details tab**

Displays details related to the LUN such as the LUN serial number, whether the LUN is a clone, LUN description, the policy group to which the LUN is assigned, maximum throughput of the policy group, and details about the LUN move operation. You can also view details about the initiator groups and initiators that are associated with the selected LUN.

**Performance tab**

Displays performance metrics graphs of the LUNs, including data rate, IOPS, and response time.

Changing the client time zone or the cluster time zone impacts the performance metrics graphs. Refresh your browser to see the updated graphs.

**Initiator Groups tab**

This tab enables you to create, delete, or edit the settings of initiator groups and initiator IDs.

**Command buttons****Create**

Opens the Create Initiator Group dialog box, which enables you to create initiator groups to control host access to specific LUNs.

**Edit**

Opens the Edit Initiator Group dialog box, which enables you to edit the settings of the selected initiator group.

**Delete**

Deletes the selected initiator group.

**Refresh**

Updates the information in the window.

**Initiator Groups list****Name**

Displays the name of the initiator group.

**Type**

Specifies the type of protocol supported by the initiator group. The supported protocols are iSCSI, FC/FCoE, or Mixed (iSCSI and FC/FCoE).

**Operating System**

Specifies the operating system for the initiator group.

**Portset**

Displays the port set that is associated with the initiator group.

**Initiator Count**

Displays the number of initiators added to the initiator group.

**Details area**

The area below the Initiator Groups list displays details about the initiators that are added to the selected initiator group and the LUNs that are mapped to the initiator group.

**Portsets tab**

This tab enables you to create, delete, or edit the settings of port sets.

**Command buttons****Create**

Opens the Create Portset dialog box, which enables you to create port sets to limit access to your LUNs.

**Edit**

Opens the Edit Portset dialog box, which enables you to select the network interfaces that you want to associate with the port set.

**Delete**

Deletes the selected port set.

**Refresh**

Updates the information in the window.

**Portsets list****Portset Name**

Displays the name of the port set.

**Type**

Specifies the type of protocol supported by the port set. The supported protocols are iSCSI, FC/FCoE, or Mixed (iSCSI and FC/FCoE).

**Interface Count**

Displays the number of network interfaces that are associated with the port set.

### Initiator Group Count

Displays the number of initiator groups that are associated with the port set.

### Details area

The area below the Portsets list displays details about the network interfaces and initiator groups associated with the selected port set.

### Related tasks

[Creating LUNs](#) on page 229  
[Deleting LUNs](#) on page 231  
[Creating initiator groups](#) on page 231  
[Deleting initiator groups](#) on page 231  
[Adding initiators](#) on page 232  
[Deleting initiators from an initiator group](#) on page 232  
[Editing LUNs](#) on page 233  
[Editing initiator groups](#) on page 237  
[Editing initiators](#) on page 237  
[Bringing LUNs online](#) on page 234  
[Taking LUNs offline](#) on page 234  
[Cloning LUNs](#) on page 233

## Qtrees

You can use System Manager create, edit, and delete Qtrees.

### Creating qtrees

Qtrees enable you to manage and partition your data within the volume. You can use the Create Qtree dialog box in System Manager to add a new qtree to a volume on your storage system.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Qtrees** tab.
4. Click **Create**.
5. In the **Details** tab of the **Create Qtree** dialog box, type a name for the qtree.
6. Select the volume to which you want to add this qtree.  
The Volume browse list includes only volumes that are online.
7. If you want to disable oplocks for the qtree, clear the **Enable Oplocks for files and directories in this Qtree** check box.  
By default, oplocks are enabled for each qtree.
8. If you want to change the default inherited security style, select a new one.  
The default security style of the qtree is the security style of the volume that contains the qtree.
9. If you want to change the default inherited export policy, select an existing export policy or create a new export policy.

The default export policy of the qtree is the export policy assigned to the volume that contains the qtree.

10. If you want to restrict the disk space usage, click the **Quotas** tab.
  - a. If you want to apply quotas on the qtree, click **Qtree quota**, and then specify the disk space limit.
  - b. If you want to apply quotas for all the users on the qtree, click **User quota**, and then specify the disk space limit.
11. Click **Create**.
12. Verify that the new qtree you created is included in the list of qtrees in the **Qtrees** window.

#### Related references

[Qtrees window](#) on page 250

## Deleting qtrees

You can delete a qtree and reclaim the disk space it uses within a volume by using System Manager. When you delete a qtree, all quotas applicable to that qtree are no longer applied by Data ONTAP.

#### Before you begin

- The qtree status must be normal.
- The qtree must not contain any LUN.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Qtrees** tab.
4. In the **Qtrees** window, select one or more qtrees that you want to delete, and then click **Delete**.
5. Select the confirmation check box, and then click **Delete**.
6. Verify that the qtree you deleted is no longer included in the list of qtrees in the **Qtrees** window.

#### Related references

[Qtrees window](#) on page 250

## Editing qtrees

You can use System Manager to modify the properties of a qtree, such as the security style, enable or disable opportunistic locks (oplocks), or assign a new or existing export policy.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Qtrees** tab.
4. Select the qtree that you want to edit and click **Edit**.

5. In the **Edit Qtree** dialog box, edit the following properties:
  - Oplocks
  - Security style
  - Export policy
6. Click **Save**.
7. Verify the changes you made to the selected qtree in the **Qtrees** window.

#### Related references

[Qtrees window](#) on page 250

## Assigning export policies to qtrees

Instead of exporting an entire volume, you can export a specific qtree on a volume to make it directly accessible to clients. You can use System Manager to export a qtree by assigning an export policy to it. You can assign an export policy to one or more qtrees from the Qtrees window.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Qtrees** tab.
4. Select one or more qtrees for which you want to assign an export policy and click **Change Export Policy**.
5. In the **Export Policy** dialog box, create a new export policy or select an existing export policy.
 

[Creating an export policy](#) on page 277
6. Click **Save**.
7. Verify that the export policy and its related export rules that you assigned to the qtrees is displayed in the **Details** tab of the appropriate qtree.

## Viewing qtree information

You can use the Qtrees window in System Manager to view the volume that contains the qtree; the name, security style, and status of the qtree; and the oplocks status.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Qtrees** tab.
4. Select the qtree that you want to view information about from the displayed list of qtrees.
5. Review the qtree details in the **Qtrees** window.

## What a qtree is

A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a FlexVol volume. You can create up to 4995 qtrees per volume. There is no maximum limit



for the storage system as a whole. You can create qtrees for managing and partitioning your data within the volume. Qtrees are available only for FlexVol volumes, not for Infinite Volumes.

In general, qtrees are similar to volumes. However, they have the following key differences:

- Snapshot copies can be enabled or disabled for individual volumes but not for individual qtrees.
- Qtrees do not support space reservations or space guarantees.

There are no restrictions on how much disk space can be used by the qtree or how many files can exist in the qtree.

## Qtree options

A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a FlexVol volume and are used to manage and partition data within the volume.

**Note:** Qtrees are not available for Infinite Volumes.

You can specify the following options when creating a qtree:

- Name of the qtree
- Volume in which you want the qtree to reside
- Oplocks  
By default, oplocks are enabled for the qtree. If you disable oplocks for the entire storage system, oplocks are not set even if you enable oplocks on a per-qtree basis
- Security style  
The security style can be UNIX, NTFS, or Mixed (UNIX and NTFS). By default, the security style of the qtree is the same as that of the selected volume.
- Export policy  
Create a new export policy or select an existing policy. By default, the export policy of the qtree is same as that of the selected volume.
- Space usage limits for qtree and user quotas

### Related concepts

[Security styles](#) on page 249

## Security styles

Storage systems running Data ONTAP operating system supports different types of security styles for a storage object. By default, the security style of a qtree is the same as that for the root directory of the volume.

### UNIX

The user's UID and GID, and the UNIX-style permission bits of the file or directory determine user access. The storage system uses the same method for determining access for both NFS and CIFS requests.

If you change the security style of a qtree or a volume from NTFS to UNIX, the storage system disregards the Windows NT permissions that were established when the qtree or volume used the NTFS security style.

### NTFS

For CIFS requests, Windows NT permissions determine user access. For NFS requests, the storage system generates and stores a set of UNIX-style permission bits that are at least as restrictive as the Windows NT permissions.

The storage system grants NFS access only if the UNIX-style permission bits allow the user access.

If you change the security style of a qtree or a volume from UNIX to NTFS, files created before the change do not have Windows NT permissions. For these files, the storage system uses only the UNIX-style permission bits to determine access.

### **Mixed**

Some files in the qtree or volume have the UNIX security style and some have the NTFS security style. A file's security style depends on whether the permission was last set from CIFS or NFS.

For example, if a file currently uses the UNIX security style and a CIFS user sends a set-ACL request to the file, the file's security style is changed to NTFS. If a file currently uses the NTFS security style and an NFS user sends a set-permission request to the file, the file's security style is changed to UNIX.

### **Related concepts**

[Qtree options](#) on page 249

## **Qtrees window**

You can use the Qtrees window to create, display, and manage information about qtrees.

- [Command buttons](#) on page 250
- [Qtree list](#) on page 250
- [Details area](#) on page 251

### **Command buttons**

#### **Create**

Opens the Create Qtree dialog box, which enables you to create a new qtree.

#### **Edit**

Opens the Edit Qtree dialog box, which enables you to change the security style and to enable or disable oplocks (opportunistic locks) on a qtree.

#### **Change Export Policy**

Opens the Export Policy dialog box, which enables you to assign one or more qtrees to new or existing export policies.

#### **Delete**

Deletes the selected qtree.

This button is disabled unless the status of the selected qtree is normal.

#### **Refresh**

Updates the information in the window.

### **Qtree list**

The qtree list displays the volume in which the qtree resides and the qtree name.

#### **Name**

Displays the name of the qtree.

#### **Volume**

Displays the name of the volume in which the qtree resides.

**Security Style**

Specifies the security style of the qtree.

**Status**

Specifies the current status of the qtree.

**Oplocks**

Specifies whether the oplocks setting is enabled or disabled for the qtree.

**Export Policy**

Displays the name of the export policy to which the qtree is assigned.

**Details area****Details tab**

Displays detailed information about the selected qtree, such as the mount path of the volume containing the qtree, details about the export policy, and the export policy rules.

**Related tasks**

[Creating qtrees](#) on page 246

[Deleting qtrees](#) on page 247

[Editing qtrees](#) on page 247

## Quotas

You can use System Manager to create, edit, and delete quotas.

### Creating quotas

Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree. You can use the Add Quota wizard in System Manager to create a quota and apply it to a specific volume or qtree.

**About this task**

Using System Manager, the minimum value that you can specify for hard and soft limits on the number of files that the quota can own is one thousand. If you want to specify a value lower than one thousand, you should use the command-line interface (CLI).

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Quotas** tab.
4. In the **User Defined Quotas** tab, click **Create**.  
The Create Quota Wizard is displayed.
5. Type or select information as prompted by the wizard.
6. Confirm the details, and then click **Finish** to complete the wizard.

**After you finish**

You can use the local user name or RID to create user quotas. If you create the user quota or group quota using the user name or group name, then the `/etc/passwd` file and `/etc/group` file must be updated, respectively.

**Related references**

[Quotas window](#) on page 256

**Deleting quotas**

You can use System Manager to delete one or more quotas as your users and their storage requirements and limitations change.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Quotas** tab.
4. Select one or more quotas that you want to delete and click **Delete**.
5. Select the confirmation check box, and then click **Delete**.

**Related references**

[Quotas window](#) on page 256

**Editing quota limits**

You can use System Manager to edit the disk space threshold, the hard and soft limits on the amount of disk space that the quota target can use, and the hard and soft limits on the number of files that the quota target can own.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Quotas** tab.
4. Select the quota that you want to edit, and click **Edit Limits**.
5. In the **Edit Limits** dialog box, edit the quota settings as required.

One hundred (100) is the minimum value that you can specify for hard and soft limits on the number of files that the quota can own. If you want to specify a value lower than 100, you should use the command-line interface (CLI).
6. Click **Save and Close**.
7. Verify the changes that you made to the selected quota in the **User Defined Quotas** tab.

**Related references**

[Quotas window](#) on page 256

## Activating or deactivating quotas

You can use System Manager to activate or deactivate quotas on one or more selected volumes on your storage system, as your users and their storage requirements and limitations change.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Quotas** tab.
4. In the **Quota Status on Volumes** tab, select one or more volumes for which you want to activate or deactivate quotas.
5. Click either **Activate** or **Deactivate**.
6. If you are deactivating a quota, select the confirmation check box and click **OK**.
7. Verify the quota status on the volumes in the Status column.

### Related references

[Quotas window](#) on page 256

## Resizing quotas

You can use the Resize Quota dialog box in System Manager to adjust the active quotas in the specified volume so that they reflect the changes that you have made to a quota.

### Before you begin

Quotas must be enabled for the volumes for which you want to resize quotas.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Quotas** tab.
4. In the **Quota Status on Volumes** tab of the **Quotas** window, select one or more volumes for which you want to resize the quotas.
5. Click **Resize**.

### Related references

[Quotas window](#) on page 256

## Viewing quota information

You can use the Quotas window in System Manager to view quota details such as the volume and the qtrees to which the quota is applied, the type of quota, the user or group to which the quota is applied, and the space and file usage.

### Steps

1. Click the **SVMs** tab.

2. Select the SVM, and then click **Manage**.
3. Click the **Quotas** tab.
4. Perform the appropriate action:

If...	Then...
You want to view details of all the quotas that you created	Click the <b>User Defined Quotas</b> tab.
You want to view the details of the quotas that are currently active	Click the <b>Quota Report</b> tab.

5. Select the quota that you want to view information about from the displayed list of quotas.
6. Review the quota details.

## Types of quotas

Quotas can be classified on the basis of the targets they are applied to.

The following are the types of quotas based on the targets they are applied to:

### User quota

The target is a user.

The user can be represented by a UNIX user name, UNIX UID, a Windows SID, a file or directory whose UID matches the user, Windows user name in pre-Windows 2000 format, and a file or directory with an ACL owned by the user's SID. You can apply it to a volume or a qtree.

### Group quota

The target is a group.

The group is represented by a UNIX group name, a GID, or a file or directory whose GID matches the group. Data ONTAP does not apply group quotas based on a Windows ID. You can apply it to a volume or a qtree.

### Qtree quota

The target is a qtree, specified by the path name to the qtree.

You can determine the size of the target qtree.

### Default quota

Automatically applies a quota limit to a large set of quota targets without creating separate quotas for each target.

Default quotas can be applied to all three types of quota target (users, groups, and qtrees). The quota type is determined by the value of the type field.

## Quota limits

You can apply a disk space limit or limit the number of files for each quota type. If you do not specify a limit for a quota, none is applied.

### Disk space soft limit

Disk space limit applied to soft quotas.

### Disk space hard limit

Disk space limit applied to hard quotas.

### Threshold limit

Disk space limit applied to threshold quotas.

**Files soft limit**

The maximum number of files on a soft quota.

**Files hard limit**

The maximum number of files on a hard quota.

**Quota management**

System Manager includes several features that help you to create, edit, or delete quotas. You can create a user, group, or tree quota and you can specify quota limits at the disk and file levels. All quotas are established on a per-volume basis.

After creating a quota, you can perform the following tasks:

- Enable and disable quotas
- Resize quotas

**How qtree changes affect quotas**

When you delete, rename, or change the security style of a qtree, the quotas applied by Data ONTAP might change, depending on the current quotas being applied.

**How changing the security style of a qtree affects user quotas**

You can apply Access Control Lists (ACLs) on qtrees by using NTFS or mixed security styles, but not by using the UNIX security style. Therefore, changing the security style of a qtree might affect how quotas are calculated. You should always reinitialize quotas after you change the security style of a qtree.

If you change the security style of a qtree from NTFS or mixed to UNIX, any ACLs on files in that qtree are ignored and the file usage is charged against the UNIX user IDs.

If you change the security style of a qtree from UNIX to either mixed or NTFS, the previously hidden ACLs become visible. In addition, any ACLs that were ignored become effective again, and the NFS user information is ignored. If no ACL existed before, the NFS information continues to be used in the quota calculation.

**Note:** To make sure that quota usages for both UNIX and Windows users are properly calculated after you change the security style of a qtree, you must reinitialize quotas for the volume containing that qtree.

**Example**

The following example shows how a change in the security style of a qtree results in a different user being charged for the usage of a file in the particular qtree.

Suppose NTFS security is in effect on qtree A, and an ACL gives Windows user corp\joe ownership of a 5 MB file. User corp\joe is charged with 5 MB of disk space usage for qtree A.

Now you change the security style of qtree A from NTFS to UNIX. After quotas are reinitialized, Windows user corp\joe is no longer charged for this file; instead, the UNIX user corresponding to the UID of the file is charged for the file. The UID could be a UNIX user mapped to corp\joe or the root user.

## How quotas work with users and groups

When you specify a user or group as the target of a quota, the limits imposed by that quota are applied to that user or group. However, some special groups and users are handled differently. There are different ways to specify IDs for users, depending on your environment.

## Quotas window

You can use the Quotas window to create, display, and manage information about quotas.

- [Tabs](#) on page 256
- [Command buttons](#) on page 256
- [User Defined Quotas list](#) on page 256
- [Details area](#) on page 257

### Tabs

#### User Defined Quotas

You can use the **User Defined Quotas** tab to view details of the quotas that you create and to create, edit, or delete quotas.

#### Quota Report

You can use the Quota Report tab to view the space and file usage and to edit the space and file limits of quotas that are active.

#### Quota Status on Volumes

You can use the Quota Status on Volumes tab to view the status of a quota and to turn quotas on or off and to resize quotas.

### Command buttons

#### Create

Opens the Create Quota wizard, which enables you to create quotas.

#### Edit Limits

Opens the Edit Limits dialog box, which enables you to edit settings of the selected quota.

#### Delete

Deletes the selected quota from the quotas list.

#### Refresh

Updates the information in the window.

### User Defined Quotas list

The quotas list displays the name and storage information for each quota.

#### Volume

Specifies the volume to which the quota is applied.

#### Qtree

Specifies the qtree associated with the quota. “All Qtrees” indicates that the quota is associated with all the qtrees.

#### Type

Specifies the quota type: user, or group, or tree.



**User/Group**

Specifies a user or a group associated with the quota. "All Users" indicates that the quota is associated with all the users. "All groups" indicates that the quota is associated with all the groups.

**Quota Target**

Specifies the type of target that the quota is assigned to. The target can be qtree, user, or group.

**Space Hard Limit**

Specifies the disk space limit applied to hard quotas.

This field is hidden by default.

**Space Soft Limit**

Specifies the disk space limit applied to soft quotas.

This field is hidden by default.

**Threshold**

Specifies the disk space limit applied to threshold quotas.

This field is hidden by default.

**File Hard Limit**

Specifies the maximum number of files in a hard quota.

This field is hidden by default.

**File Soft Limit**

Specifies the maximum number of files in a soft quota.

This field is hidden by default.

**Details area**

The area below the quotas list displays quota details such as the quota error, space usage and limits, and file usage and limits.

**Related tasks**

[Creating quotas](#) on page 251

[Deleting quotas](#) on page 252

[Editing quota limits](#) on page 252

[Activating or deactivating quotas](#) on page 253

[Resizing quotas](#) on page 253

## CIFS protocol

You can use System Manager to enable and configure CIFS servers to allow CIFS clients to access files on the cluster.

## Setting up CIFS

You can use System Manager to enable and configure CIFS servers to allow CIFS clients to access files on the cluster.

### Before you begin

- The CIFS license must be installed on your storage system.
- While configuring CIFS in the Active Directory domain, the following requirements must be met:
  - DNS must be enabled and configured correctly.
  - The storage system must be able to communicate with the domain controller using the fully qualified domain name (FQDN).
  - The time difference (clock skew) between the cluster and the domain controller must not be more than five minutes.
- If CIFS is the only protocol configured on the Storage Virtual Machine (SVM), the following requirements must be met:
  - The root volume security style must be NTFS.  
By default, System Manager sets the security style as UNIX.
  - Superuser access must be set to **Any** for CIFS protocol.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Configuration** tab, click **Setup**.
5. In the **General** tab of the **CIFS Server Setup** dialog box, specify the NetBIOS name and the Active Directory domain details.
6. Click the **Options** tab and perform the following actions:
  - In the SMB settings area, select or clear the SMB signing and SMB encryption check box as required.
  - Specify the default UNIX user.
  - In the WINS Servers area, add the required IP address.
7. Click **Setup**.

### Related tasks

[Creating a CIFS share](#) on page 219

[Editing the volume properties](#) on page 169

[Modifying export policy rules](#) on page 279

### Related references

[CIFS window](#) on page 266

## Editing the general properties for CIFS

You can modify the general properties for CIFS, such as the default UNIX and Windows user by using System Manager. You can also enable or disable SMB signing for the CIFS server.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Configuration** tab, click **Options**.
5. In the **CIFS Options** dialog box, modify the following CIFS server properties, as required:
  - UNIX user
  - Windows user
  - IP address
  - Enable or disable SMB signing  
 Enabling SMB signing helps to ensure that the data is not compromised. However, you might encounter performance degradation in the form of increased CPU usage on both the clients and the server, although the network traffic remains the same. You can disable SMB signing on any of your Windows clients that do not require protection against replay attacks. For information about disabling SMB signing on Windows clients, see the Microsoft Windows documentation.
  - Enable or disable SMB 3.0 encryption
6. Click either **Save** or **Save and Close**.

### Related references

[CIFS window](#) on page 266

## Adding home directory paths

You can use System Manager to specify one or more paths that can be used by the storage system to resolve the location of users' CIFS home directories.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Home Directories** area of the **Configuration** tab, click **Manage**.
5. In the **Manage Home Directories** dialog box, specify the paths used by the storage system to search for users' CIFS home directories.
6. Click **Add**, and then click **Save and Close**.

### Related references

[CIFS window](#) on page 266

## Deleting home directory paths

You can use System Manager to delete a home directory path when you do not want the storage system to use the path to resolve the location of users' CIFS home directories.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Home Directories** area of the **Configuration** tab, click **Manage**.
5. In the **Manage Home Directories** dialog box, select the home directory path that you want to delete and click **Delete**.
6. Click **Save and Close**.

### Related references

[CIFS window](#) on page 266

## Resetting CIFS domain controllers

You can use System Manager to reset the CIFS connection to domain controllers for the specified domain. Failure to reset the domain controller information can cause a connection failure.

### About this task

You have to update the discovery information of the storage system's available domain controller after you add or delete a domain from the list of preferred domain controllers. You can update the storage system's available domain controller discovery information in Data ONTAP through the command-line interface (CLI).

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Domain** tab, click **Reset**.

### Related references

[CIFS window](#) on page 266

## Updating the CIFS group policy configuration

You have to update the group policy after the policy configuration is changed through the CLI. You can use the CIFS window in System Manager to update the group policy.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.

3. Click the **SVM Settings** tab.
4. Click the **Domain** tab.
5. In the **Group Policy** area, select the group policy configuration that you want to update and click **Update**.

## Enabling or disabling a CIFS group policy configuration

You can enable or disable the CIFS group policy configuration from the CIFS window in System Manager.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. Click the **Domain** tab.
5. In the Group Policy area, select the group policy configuration that you want to enable or disable and click either **Enable** or **Disable**.

## Reloading CIFS group policy

You have to reload a CIFS group policy if the status of the policy is changed. You can use the CIFS window in System Manager to reload the group policy.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. Click the **Domain** tab.
5. In the Group Policy area, select the group policy configuration that you want to reload and click **Reload**.

## Setting up BranchCache

You can use System Manager to configure BranchCache on a CIFS-enabled Storage Virtual Machine (SVM) to enable caching of content on computers local to requesting clients.

### Before you begin

- CIFS must be licensed and a CIFS server must be configured.
- For BranchCache version 1, SMB 2.1 or later must be enabled.
- For BranchCache version 2, SMB 3.0 must be enabled and the remote Windows clients must support BranchCache 2.

### About this task

- You can configure BranchCache on SVMs with FlexVol volumes.

- You can create an all-shares BranchCache configuration if you want to offer caching services for all the content contained within all the SMB shares on the CIFS server.
- You can create a per-share BranchCache configuration if you want to offer caching services for the content contained within selected SMB shares on the CIFS server.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **BranchCache** tab, click **Set Up**.
5. In the **BranchCache Setup** dialog box, enter the following information:
  - a. Specify the path to the hash store.  
The path can be to an existing directory where you want the hash data to be stored. The destination path must be read-writable. Read-only paths, such as Snapshot directories, are not allowed.
  - b. Specify the maximum size (in KB, MB, GB, TB, or PB) for a hash data store.  
If the hash data exceeds this value, older hashes are deleted to provide space for newer hashes. The default size for the hash store is 1 GB.
  - c. Specify the operating mode for the BranchCache configuration.  
The default operating mode is set to all shares.
  - d. Specify a server key to prevent clients from impersonating the BranchCache server.  
You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key. If the server key contains any spaces, you must enclose the server key in quotation marks.
  - e. Select the required BranchCache version.  
By default, all the versions supported by the client are selected.
6. Click **Set Up**.

## Modifying the BranchCache settings

You can use the CIFS window in System Manager to modify BranchCache settings that are configured for a CIFS-enabled Storage Virtual Machine (SVM). You can change the hash store path, the hash store size, the operating mode, and the BranchCache versions that are supported.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **BranchCache** tab, click **Edit**.
5. In the **Modify BranchCache Settings** dialog box, modify the appropriate information:
  - Hash store path

If you modify the hash store path, you are provided with an option to retain the cached hash data from the previous hash store.

- Hash store size
- Operating mode
- BranchCache version

6. Click **Modify**.

## Deleting the BranchCache configuration

You can use System Manager to delete the BranchCache configuration if you no longer want to offer caching services on the Storage Virtual Machine (SVM) that is configured for BranchCache.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **BranchCache** tab, click **Delete**.
5. Select the confirmation check box, and then click **Delete**.

You can also remove existing hashes from the hash store.

### Related tasks

[What happens when you delete the BranchCache configuration](#) on page 266

## Adding preferred domain controllers

System Manager automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers for a specific domain.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Domain** tab, click **Add** in the Preferred Domain Controllers area.
5. Enter the fully qualified domain name (FQDN) and the IP addresses of the domain controllers that you want to add.  
  
You can add multiple domain controllers by entering the IP addresses, separated by commas.
6. Click **Save**.
7. Verify that the domain controller you added is displayed in the list of preferred domain controllers.

## Editing preferred domain controllers

You can use System Manager to modify the IP address of the preferred domain controllers that are configured for a specific domain.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the Preferred Domain Controllers area of the **Domain** tab, double-click the domain controller that you want to edit.
5. Modify the IP addresses of the domain controller and click **Save**.

## Deleting preferred domain controllers

You can use System Manager to delete a preferred domain controller to which the Storage Virtual Machine (SVM) computer account is associated. You can do this when you no longer want to use a particular domain controller.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Domain** tab, select the domain that you want to delete from the **Preferred Domain Controllers** area and click **Delete**.
5. Select the confirmation check box, and then click **Delete**.

## Viewing CIFS domain information

You can use System Manager to view information about the domain controllers and servers that are connected to the storage system.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. Click the **Domain** tab.
5. Review the information about the connected domain controllers and servers.

## SMB concepts

Clients can access files on Storage Virtual Machines (SVMs) using the SMB protocol, provided that Data ONTAP can properly authenticate the user.

When an SMB client connects to a CIFS server, Data ONTAP authenticates the user with a Windows domain controller. Data ONTAP uses two methods to obtain the domain controllers to use for authentication:



- It queries DNS servers in the domain that the CIFS server is configured to use for domain controller information.
- It queries a list of preferred domain controllers you can optionally specify.

Next, Data ONTAP must obtain UNIX credentials for the user. It does this by using mapping rules on the SVM or by using a default UNIX user instead. For SVMs, you can specify which mapping services to use, local files or LDAP, and the order in which mapping services are searched. Additionally, you can specify the default UNIX user.

Data ONTAP then checks different name services for UNIX credentials for the user, depending on the name services configuration of the SVM. The options are local UNIX accounts, NIS domains, and LDAP domains. You must configure at least one of them so that Data ONTAP can successfully authorize the user. You can specify multiple name services and the order in which they are searched.

## How ONTAP enables you to provide SMB client access to UNIX symbolic links

You must understand certain concepts about how ONTAP enables you to manage symbolic links. This is important to provide access to SMB users connecting to the Storage Virtual Machine (SVM).

A symbolic link is a file that is created in a UNIX environment that contains a reference to another file or directory. If a client accesses a symbolic link, the client is redirected to the target file or directory to which the symbolic link refers.

ONTAP provides SMB clients the ability to follow UNIX symbolic links that are configured on the SVM. This feature is optional, and you can configure it on a per-share basis with one of the following settings:

- Enabled with read/write access
- Enabled with read-only access
- Disabled by hiding symbolic links from SMB clients
- Disabled with no access to symbolic links from SMB clients

There are two types of symbolic links: relative symbolic links and absolute symbolic links.

### Relative

A relative symbolic link contains a reference to a file or directory relative to its parent directory. Therefore, the path of the file that it is referring to should not begin with a slash (/). If you enable symbolic links on a share, relative symbolic links work without further configuration.

### Absolute

An absolute symbolic link contains a reference to a file or directory in the form of an absolute path. Therefore, the path of the file that it is referring to should begin with a slash (/). It is treated as an absolute path location of the file from the root of the file system. An absolute symbolic link can refer to a file or directory within or outside of the file system of the symbolic link. If the target is not in the same local file system, the symbolic link is called a *widelink*. If you enable symbolic links on a share, absolute symbolic links do not work right away. You must first create a mapping between the UNIX path of the symbolic link to the destination CIFS path. When creating absolute symbolic link mappings, you can specify whether it is a local link or a widelink. If you create an absolute symbolic link to a file or directory outside of the local share but set the locality to local, ONTAP disallows access to the target.

Note that if a client attempts to delete a local symbolic link (absolute or relative), only the symbolic link is deleted, not the target file or directory. However, if a client attempts to delete a widelink, it might delete the actual target file or directory to which the widelink

refers. ONTAP does not have control over this because the client can explicitly open the target file or directory outside the SVM and delete it.

## Using BranchCache to cache SMB share content at a branch office

BranchCache was developed by Microsoft to enable caching of content on computers local to requesting clients. The Data ONTAP implementation of BranchCache can reduce wide-area network (WAN) utilization and provide improved access response time when users in a branch office access content stored on Storage Virtual Machines (SVMs) using SMB.

If you configure BranchCache, Windows BranchCache clients first retrieve content from the SVM and then cache the content on a computer within the branch office. If another BranchCache-enabled client in the branch office requests the same content, the SVM first authenticates and authorizes the requesting user. The SVM then determines whether the cached content is still up-to-date and, if it is, sends the client metadata about the cached content. The client then uses the metadata to retrieve content directly from the locally based cache.

## What happens when you delete the BranchCache configuration

If you previously configured BranchCache but do not want the Storage Virtual Machine (SVM) to continue providing cached content, you can delete the BranchCache configuration on the CIFS server. You must be aware of what happens when you delete the configuration.

When you delete the configuration, Data ONTAP removes the configuration information for that SVM from the cluster and stops the BranchCache service. You can choose whether Data ONTAP should delete the hash store on the SVM.

Deleting the BranchCache configuration does not disrupt access by BranchCache-enabled clients. Thereafter, when BranchCache-enabled clients request metadata information on existing SMB connections for content that is already cached, Data ONTAP responds with a Microsoft defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the SVM.

After the BranchCache configuration is deleted, SMB shares do not advertise BranchCache capabilities. To access content that has not previously been cached using new SMB connections, clients make normal read SMB requests.

### Related tasks

[Deleting the BranchCache configuration](#) on page 263

## CIFS window

You can use the CIFS window to configure the CIFS server, manage domain controllers, manage symbolic UNIX mappings, and configure BranchCache.

### Configuration tab

This tab enables you to create and manage the CIFS server.

#### Server

Specifies the status of the CIFS server, name of the server, authentication mode, and the name of the active directory domain.

#### Home Directories

Specifies home directory paths and the style to determine how PC user names are mapped to home directory entries.

### Command buttons

- Setup

Opens the CIFS Setup wizard, which enables you to set up CIFS on your Storage Virtual Machine (SVM).

- **Options**  
Displays the CIFS Options dialog box, which enables you to enable or disable SMB 3.0 signing, enable or disable SMB 3.0 encryption, and add Windows Internet Name Service (WINS) servers.  
SMB signing ensures that the network traffic between the CIFS server and the client is not compromised.
- **Delete**  
Enables you to delete the CIFS server.
- **Refresh**  
Updates the information in the window.

### **Domain tab**

This tab enables you to view and reset your CIFS domain controllers, and to add or delete preferred domain controllers. You can also use this tab to manage CIFS group policy configurations.

#### **Servers**

Displays information about discovered authentication servers and your preferred domain controllers on the CIFS-enabled SVM.

You can also reset the information about the discovered servers, add a preferred domain controller, delete a domain controller, or refresh the list of domain controllers.

#### **Group Policy**

Enables you to view, enable, or disable group policy configurations on the CIFS server. You can also reload a group policy if the status of the policy is changed.

### **Symlinks tab**

This tab enables you to manage mappings of UNIX symbolic links for CIFS users.

#### **Path Mappings**

Displays the list of symbolic link mappings for CIFS.

#### **Command buttons**

- **Create**  
Opens the Create New Symlink Path Mappings dialog box, which enables you to create a UNIX symbolic link mapping.
- **Edit**  
Opens the Edit Symlink Path Mappings dialog box, which enables you to modify the CIFS share and path.
- **Delete**  
Enables you to delete the symbolic link mapping.
- **Refresh**  
Updates the information in the window.

### **BranchCache tab**

This tab enables you to set up and manage BranchCache settings on CIFS-enabled SVMs with FlexVol volumes.

You can view the status of the BranchCache service, path to the hash store, size of the hash store, and the operating mode, server key, and version of BranchCache.

### Command buttons

- **Setup**  
Opens the BranchCache Setup dialog box, which enables you to configure BranchCache for the CIFS server.
- **Edit**  
Opens the Modify BranchCache Settings dialog box, which enables you to modify the properties of the BranchCache configuration.
- **Delete**  
Enables you to delete the BranchCache configuration.
- **Refresh**  
Updates the information in the window.

### Related tasks

[Setting up CIFS](#) on page 258

[Editing the general properties for CIFS](#) on page 259

[Adding home directory paths](#) on page 259

[Deleting home directory paths](#) on page 260

[Resetting CIFS domain controllers](#) on page 260

## NFS protocol

You can use System Manager to authenticate NFS clients to access data on the SVM.

### Editing NFS settings

You can use System Manager to edit the NFS settings, such as enabling or disabling NFSv3, NFSv4, and NFSv4.1; enabling or disabling read and write delegations for NFSv4 clients; and enabling NFSv4 ACLs. You can also edit the default Windows user.

#### About this task

NFSv4 is not supported on Infinite Volumes.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **NFS**.
5. In the **NFS** window, click **Edit**.
6. In the **Edit NFS Settings** dialog box, make the necessary changes.
7. Click **Save and Close**.

#### Related references

[NFS window](#) on page 269

## How ONTAP handles NFS client authentication

NFS clients must be properly authenticated before they can access data on the Storage Virtual Machine (SVM). ONTAP authenticates the clients by checking their UNIX credentials against the name services that you configure.

When an NFS client connects to the SVM, ONTAP obtains the UNIX credentials for the user by checking different name services, depending on the name services configuration of the SVM. ONTAP can check credentials for local UNIX accounts, NIS domains, and LDAP domains. At least one of them must be configured so that ONTAP can successfully authenticate the user. You can specify multiple name services and the order in which ONTAP searches them.

In a pure NFS environment with UNIX volume security styles, this configuration is sufficient to authenticate and provide the proper file access for a user connecting from an NFS client.

If you are using mixed, NTFS, or unified volume security styles, ONTAP must obtain a CIFS user name for the UNIX user for authentication with a Windows domain controller. This can happen either by mapping individual users using local UNIX accounts or LDAP domains, or by using a default CIFS user instead. You can specify which name services ONTAP searches in which order, or specify a default CIFS user.

## NFS window

You can use the NFS window to display and configure your NFS settings.

### Server Status

Displays the status of the NFS service. The service is enabled if the NFS protocol is configured on the Storage Virtual Machine (SVM).

**Note:** If you have upgraded to Data ONTAP 8.3 or later from an NFS-enabled storage system running Data ONTAP 8.1.x, the NFS service is enabled in Data ONTAP 8.3 or later. However, you must enable support for NFSv3 or NFSv4 because NFSv2 is no longer supported.

### Command buttons

#### Enable

Enables the NFS service.

#### Disable

Disables the NFS service.

#### Edit

Opens the Edit NFS Settings dialog box, which enables you to edit NFS settings.

#### Refresh

Updates the information in the window.

### Related tasks

[Editing NFS settings](#) on page 268

## iSCSI protocol

You can use System Manager to configure the iSCSI protocol that enables you to transfer block data to hosts using SCSI protocol over TCP/IP.

## Creating iSCSI aliases

An iSCSI alias is a user-friendly identifier that you assign to an iSCSI target device (in this case, the storage system) to make it easier to identify the target device in user interfaces. You can use System Manager to create an iSCSI alias.

### About this task

An iSCSI alias is a string of 1 to 128 printable characters, and must not include spaces.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. In the **Service** tab of the **iSCSI** window, click **Edit**.
6. In the **Edit iSCSI Service Configuration** dialog box, enter an iSCSI alias in the **Target Alias** field, and then click **OK**.

### Related references

[iSCSI window](#) on page 275

## Enabling or disabling the iSCSI service on storage system interfaces

You can use System Manager to control which network interfaces are used for iSCSI communication by enabling or disabling the interfaces. When the iSCSI service is enabled, iSCSI connections and requests are accepted over those network interfaces that are enabled for iSCSI, but not over disabled interfaces.

### Before you begin

You must have terminated any outstanding iSCSI connections and sessions currently using the interface. By default, the iSCSI service is enabled on all Ethernet interfaces after you enable the iSCSI license.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. In the **iSCSI Interfaces** area, select the interface on which you want to enable or disable the iSCSI service.
6. Click **Enable** or **Disable**, as required.

### Related tasks

[Configuring iSCSI protocol on SVMs](#) on page 46

**Related references**

[iSCSI window](#) on page 275

**Adding the security method for iSCSI initiators**

You can use System Manager to add an initiator and specify the security method that is used to authenticate the initiator.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. In the iSCSI window, click the **Initiator Security** tab.
6. Click **Add** in the **Initiator Security** area.
7. Specify the initiator name and the security method to authenticate the initiator.  
For CHAP authentication, you must provide the user name and password, and confirm your password for inbound settings. For outbound settings, this login information is optional.
8. Click **OK**.

**Related references**

[iSCSI window](#) on page 275

**Editing default security settings**

You can use the Edit Default Security dialog box in System Manager to edit the default security settings for iSCSI initiators that are connected to the storage system.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. In the **Default Security** area on the **Initiator Security** tab, click **Edit**.
6. In the **Edit Default Security** dialog box, change the security type.  
For CHAP authentication, you must provide the user name and password, and confirm your password for inbound settings. For outbound settings, this login information is optional.
7. Click **OK**.

**Related references**

[iSCSI window](#) on page 275

## Editing initiator security

The security style configured for an initiator specifies how the authentication is done for that initiator during the iSCSI connection login phase. You can use System Manager to change the security for selected iSCSI initiators by changing the authentication method.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. In the **Initiator Security** tab, select one or more initiators from the initiator list, and then click **Edit** in the **Initiator Security** area.
6. Change the security type.  
For CHAP authentication, you must provide the user name and password and confirm your password for inbound settings. For outbound settings, this is optional.
7. Click **OK**.
8. Verify the changes you made in the **Initiator Security** tab.

### Related references

[iSCSI window](#) on page 275

## Changing the default iSCSI initiator authentication method

You can use System Manager to change the default iSCSI authentication method, which is the authentication method that is used for any initiator that is not configured with a specific authentication method.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. In the **Initiator Security** tab, click **Edit** in the **Default Security** area.
6. Change the security type.  
For CHAP authentication, you must provide the user name and password and confirm your password for inbound settings. For outbound settings, this is optional.
7. Click **OK**.

### Related references

[iSCSI window](#) on page 275



## Setting the default security for iSCSI initiators

You can use System Manager to remove the authentication settings for an initiator and use the default security method to authenticate the initiator.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. In the **Initiator Security** tab, select the initiator whose security setting you want change.
6. Click **Set Default** in the **Initiator Security** area, and then click **Set Default** in the confirmation box.

### Related references

[iSCSI window](#) on page 275

## Starting or stopping the iSCSI service

You can use System Manager to start or stop the iSCSI service on your storage system.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. Click either **Start** or **Stop**, as required.

### Related references

[iSCSI window](#) on page 275

## Viewing initiator security information

You can use System Manager to view the default authentication information and all the initiator-specific authentication information.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **iSCSI**.
5. In the **Initiator Security** tab of the **iSCSI** window, review the details.

## What iSCSI is

The iSCSI protocol is a licensed service on the storage system that enables you to transfer block data to hosts using the SCSI protocol over TCP/IP. The iSCSI protocol standard is defined by RFC 3270.

In an iSCSI network, storage systems are targets that have storage target devices, which are referred to as LUNs (logical units). A host with an iSCSI host bus adapter (HBA), or running iSCSI initiator software, uses the iSCSI protocol to access LUNs on a storage system. The iSCSI protocol is implemented over the storage system's standard Ethernet interfaces using a software driver.

The connection between the initiator and target uses a standard TCP/IP network. No special network configuration is needed to support iSCSI traffic. The network can be a dedicated TCP/IP network, or it can be your regular public network. The storage system listens for iSCSI connections on TCP port 3260.

### Related information

*RFC 3270: [www.ietf.org/rfc/rfc3270.txt](http://www.ietf.org/rfc/rfc3270.txt)*

## What iSCSI nodes are

In an iSCSI network, there are two types of nodes: targets and initiators. Targets are storage systems, and initiators are hosts. Switches, routers, and ports are TCP/IP devices only, and are not iSCSI nodes.

## Initiator security

You can select from the following authentication methods:

- none  
There is no authentication for the initiator.
- deny  
The initiator is denied access when it attempts to authenticate to the storage system.
- CHAP  
The initiator logs in using a Challenge Handshake Authentication Protocol (CHAP) user name and password. You can specify a CHAP password or generate a random password.
- default  
The initiator uses the default security settings. The initial setting for default initiator security is none.

In CHAP authentication, the storage system sends the initiator a challenge value. The initiator responds with a value calculated using a one-way hash function. The storage system then checks the response against its own version of the value calculated using the same one-way hash function. If the values match, the authentication is successful.

## What CHAP authentication is

The Challenge Handshake Authentication Protocol (CHAP) enables authenticated communication between iSCSI initiators and targets. When you use CHAP authentication, you define CHAP user names and passwords on both the initiator and the storage system.

During the initial stage of an iSCSI session, the initiator sends a login request to the storage system to begin the session. The login request includes the initiator's CHAP user name and CHAP algorithm. The storage system responds with a CHAP challenge. The initiator provides a CHAP response. The storage system verifies the response and authenticates the initiator. The CHAP password is used to compute the response.

## iSCSI window

You can use the iSCSI window to start or stop the iSCSI service, change a storage system iSCSI node name, and create or change the iSCSI alias of a storage system. You can also add or change the initiator security setting for an iSCSI initiator that is connected to your storage system.

### Tabs

#### Service

You can use the **Service** tab to start or stop the iSCSI service, change a storage system iSCSI node name, and create or change the iSCSI alias of a storage system.

#### Initiator Security

You can use the **Initiator Security** tab to add or change the initiator security setting for an iSCSI initiator that is connected to your storage system.

### Command buttons

#### Edit

Opens Edit iSCSI Service Configurations dialog box, which enables you to change iSCSI node name and iSCSI alias of the storage system.

#### Start

Starts the iSCSI service.

#### Stop

Stops the iSCSI service.

#### Refresh

Updates the information in the window.

### Details area

The details area displays information about the status of the iSCSI service, iSCSI target node name, and iSCSI target alias. You can use this area to enable or disable the iSCSI service on a network interface.

### Related tasks

[Creating iSCSI aliases](#) on page 270

[Enabling or disabling the iSCSI service on storage system interfaces](#) on page 270

[Adding the security method for iSCSI initiators](#) on page 271

[Editing default security settings](#) on page 271

[Editing initiator security](#) on page 272

[Changing the default iSCSI initiator authentication method](#) on page 272

[Setting the default security for iSCSI initiators](#) on page 273

[Starting or stopping the iSCSI service](#) on page 273

## FC/FCoE protocol

You can use System Manager to configure FC/FCoE protocols.

### Starting or stopping the FC or FCoE service

The FC service enables you to manage FC target adapters for use with LUNs. You can use System Manager to start the FC service to bring the adapters online and allow access to the LUNs on the

storage system. You can stop the FC service to take the FC adapters offline and prevent access to the LUNs.

#### Before you begin

- The FC license must be installed.
- An FC adapter must be present in the target storage system.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **FC/FCoE**.
5. Click either **Start** or **Stop**, as required.
6. If you are stopping the FC or FCoE service, click **Stop**.

#### Related references

[FC/FCoE window](#) on page 277

## Changing an FC or FCoE node name

If you replace a storage system chassis and reuse it in the same Fibre Channel SAN, the node name of the replaced storage system in certain cases might be duplicated. You can change the node name of the storage system by using System Manager.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **FC/FCoE**.
5. Click **Edit**.
6. Type the new name, and then click **OK**.

#### Related references

[FC/FCoE window](#) on page 277

## What FC is

FC is a licensed service on the storage system that enables you to export LUNs and transfer block data to hosts using the SCSI protocol over a Fibre Channel fabric.

## What FC nodes are

In an FC network, nodes include targets, initiators, and switches.

Targets are storage systems, and initiators are hosts. Nodes register with the Fabric Name Server when they are connected to an FC switch. Each Storage Virtual Machine (SVM) that has a FCP service is a different FC target node.

## The FCoE protocol

Fibre Channel over Ethernet (FCoE) is a new model for connecting hosts to storage systems. Like the traditional FC protocol, FCoE maintains existing FC management and controls, but it uses a 10-gigabit Ethernet network as the hardware transport.

Setting up an FCoE connection requires one or more supported converged network adapters (CNAs) in the host, connected to a supported data center bridging (DCB) Ethernet switch. The CNA is a consolidation point and effectively serves as both an HBA and an Ethernet adapter.

In general, you can configure and use FCoE connections the same way you use traditional FC connections.

## FC/FCoE window

You can use the FC/FCoE window to start or stop the FC service.

### Command buttons

#### Edit

Opens the Edit Node Name dialog box, which enables you to change the FC or FCoE node name.

#### Start

Starts the FC/FCoE service.

#### Stop

Stops the FC/FCoE service.

#### Refresh

Updates the information in the window.

### FC/FCoE details

The details area displays information about the status of FC/FCoE service, the node name, and the FC/FCoE adapters.

### Related tasks

[Starting or stopping the FC or FCoE service](#) on page 275

[Changing an FC or FCoE node name](#) on page 276

[Configuring FC and FCoE protocols on SVMs](#) on page 48

## Export policies

You can use System Manager to create, edit, and manage export policies.

## Creating an export policy

You can use System Manager to create an export policy so that clients can access specific volumes.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.

4. In the **Policies** pane, click **Export Policies**.
5. Click **Create**.
6. In the **Create Export Policy** dialog box, specify a name for the export policy.
7. If you want to create a new export policy by copying the rules from an existing export policy, select the **Copy Rules from** check box, and then select the SVM and the export policy.  
  
You should not select the destination SVM for disaster recovery from the drop-down menu to create an export policy.
8. In the **Export Rules** area, click **Add** to add rules to the export policy.
9. Click **Create**.
10. Verify that the export policy you created is displayed in the **Export Policies** window.

## Renaming export policies

System Manager enables you to rename an existing export policy.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Export Policies**.
5. Select the export policy that you want to rename, and then click **Rename Policy**.
6. In the **Rename Policy** dialog box, specify a new policy name, and then click **Modify**.
7. Verify the changes that you made in the **Export Policies** window.

## Deleting export policies

You can use System Manager to delete export policies that are no longer required.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Export Policies**.
5. Select the export policy that you want to delete, and then click **Delete Policy**.
6. Select the confirmation check box, and then click **Delete**.

## Adding rules to an export policy

You can use System Manager to add rules to an export policy, which enables you to define client access to data.

### Before you begin

You must have created the export policy to which you want to add the export rules.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Export Policies**.
5. Select the export policy and from the **Export Rules** tab, and then click **Add**.
6. In the **Create Export Rule** dialog box, perform the following steps:
  - a. Specify the client that requires access to the data.  
 You can specify multiple clients as comma-separated values.  
 You can specify the client in any of the following formats:
    - As a host name; for instance, host1
    - As an IPv4 address; for instance, 10.1.12.24
    - As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
    - As an IPv6 address; for instance, FE80::0202:B3FF:FE1E:8329
    - As an IPv6 address with a network mask; for instance, 2001:db8::/32
    - As a netgroup, with the netgroup name preceded by an at sign (@); for instance, @netgroup
    - As a domain name preceded by a period (.); for instance, .example.com

**Note:** You must not enter an IP address range, such as 10.1.12.10 through 10.1.12.70. Entries in this format are interpreted as a text string and treated as a host name.

You can enter the IPv4 address 0.0.0.0/0 to provide access to all the hosts.
  - b. If you want to modify the rule index number, select the appropriate rule index number.
  - c. Select one or more access protocols.  
 If you do not select any access protocol, the default value “Any” is assigned to the export rule.
  - d. Select one or more security types and access rules.
7. Click **OK**.
8. Verify that the export rule you added is displayed in the **Export Rules** tab for the selected export policy.

**Modifying export policy rules**

You can use System Manager to modify the specified client, access protocols, and access permissions of an export policy rule.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.

4. In the **Policies** pane, click **Export Policies**.
5. In the **Export Policies** window, select the export policy whose export rule you want to edit, and in the **Export Rules** tab, select the rule and click **Edit**.
6. Modify the following parameters as required:
  - Client specification
  - Access protocols
  - Access details
7. Click **OK**.
8. Verify that the updated changes for the export rule are displayed in the **Export Rules** tab.

#### Related tasks

[Setting up CIFS](#) on page 258

## Deleting export policy rules

You can use System Manager to delete export policy rules that are no longer required.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Export Policies**.
5. Select the export policy whose export rule you want to delete.
6. In the **Export Rules** tab, select the export rule that you want to delete, and then click **Delete**.
7. In the confirmation box, click **Delete**.

## How export policies control client access to volumes or qtrees

Export policies contain one or more *export rules* that process each client access request. The result of the process determines whether the client is denied or granted access and what level of access. An export policy with export rules must exist on the SVM for clients to access data.

You associate exactly one export policy with each volume or qtree to configure client access to the volume or qtree. The SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes or qtrees:

- Assign different export policies to each volume or qtree of the SVM for individual client access control to each volume or qtree in the SVM.
- Assign the same export policy to multiple volumes or qtrees of the SVM for identical client access control without having to create a new export policy for each volume or qtree.

If a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied.

You can modify an export policy dynamically on a system running Data ONTAP.



## Export Policies window

You can use the Export Policies window to create, view, and manage information about export policies and its related export rules.

### Export Policies

The Export Policies window enables you to view and manage the export policies created for the Storage Virtual Machine (SVM).

#### Command buttons

- **Create**  
Opens the Create Export Policy dialog box, which enables you to create an export policy and add export rules. You can also copy export rules from an existing SVM.
- **Rename**  
Opens the Rename Policy dialog box, which enables you to rename the selected export policy.
- **Delete**  
Opens the Delete Export Policy dialog box, which enables you to delete the selected export policy.
- **Refresh**  
Updates the information in the window.

### Export Rules tab

The Export Rules tab enables you to view information about the export rules created for a particular export policy. You can also add, edit, and delete rules.

#### Command buttons

- **Add**  
Opens the Create Export Rule dialog box, which enables you to add an export rule to the selected export policy.
- **Edit**  
Opens the Modify Export Rule dialog box, which enables you to modify the attributes of the selected export rule.
- **Delete**  
Opens the Delete Export Rule dialog box, which enables you to delete the selected export rule.
- **Move Up**  
Moves up the rule index of the selected export rule.
- **Move Down**  
Moves down the rule index of the selected export rule.
- **Refresh**  
Updates the information in the window.

#### Export rules list

- **Rule Index**  
Specifies the priority based on which the export rules are processed. You can use the Move Up and Move Down buttons to choose the priority.

- **Client**  
Specifies the client to which the rule applies.
- **Access Protocols**  
Displays the access protocol that is specified for the export rule.  
If you have not specified any access protocol, the default value “Any” is considered.
- **Read-Only Rule**  
Specifies one or more security types for read-only access.
- **Read/Write Rule**  
Specifies one or more security types for read/write access.
- **Superuser Access**  
Specifies the security type or types for superuser access.

### Assigned Objects tab

The Assigned Objects tab enables you to view the volumes and qtrees that are assigned to the selected export policy. You can also view whether the volume is encrypted or not.

## Efficiency policies

You can use System Manager to create, edit, and delete efficiency policies.

### Adding efficiency policies

You can use System Manager to add efficiency policies to run the deduplication operation on a volume on a specified schedule or when the change in volume data reaches a specified threshold value.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Efficiency Policies**.
5. Click **Add**, and then specify the policy name.
6. Specify how the storage efficiency policy should be run:
  - Select **Schedule** and specify the schedule name and the schedule details.  
You can specify the maximum run-time duration of the efficiency policy, if required.
  - Select **ChangeLog Threshold** and specify the threshold value for the change in volume data (in percent).
7. Optional: Select the **Set QoS policy to background** check box to reduce performance impact on client operations.
8. Click **Add**.

## Editing efficiency policies

System Manager enables you to modify the attributes of an efficiency policy such as the policy name, schedule name, and maximum runtime.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Efficiency Policies**.
5. In the **Efficiency Policies** window, select the policy that you want to edit, and then click **Edit**.
6. In the **Edit Efficiency Policy** dialog box, make the necessary changes.
7. Click **Save**.

## Deleting efficiency policies

System Manager enables you to delete an efficiency policy that is no longer required.

### Before you begin

The efficiency policy must be disabled.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Efficiency Policies**.
5. Select the efficiency policy that you want to delete, and then click **Delete**.
6. Select the confirmation check box, and then click **Delete**.

## Enabling or disabling efficiency policies

You can use System Manager to enable or disable an efficiency policy.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Efficiency Policies**.
5. Select one or more efficiency policies that you want to enable or disable.
6. Click **Status > Enable** or **Status > Disable**, as required.
7. If you are disabling an efficiency policy, select the confirmation check box, and then click **OK**.

## What an efficiency policy is

An efficiency policy is a job schedule for a deduplication operation on a FlexVol volume or Infinite Volume.

You can run deduplication on a FlexVol volume or Infinite Volume either by scheduling the operations to start at a specific time or by specifying a threshold percentage after which the operations are triggered. You can schedule a deduplication operation by creating job schedules that are enclosed within the efficiency policies or you can specify a threshold percentage, which waits for the new data to exceed the specified percentage and then triggers the deduplication. The volume efficiency policies support only job schedules that are of type cron.

## Understanding predefined efficiency policies

Starting with Data ONTAP 8.3, you can configure a volume with efficiency policies to achieve additional space savings. You can configure a volume to run inline compression without a scheduled or manually started background efficiency operation configured on the volume.

When you create a Storage Virtual Machine (SVM), the following efficiency policies are created automatically and cannot be deleted:

- **Default**  
You can configure a volume with the efficiency policy to run the scheduled deduplication operations on the volume.
- **Inline-only**  
You can configure a volume with the inline-only efficiency policy and enable inline compression, to run inline compression on the volume without any scheduled or manually started background efficiency operations.

For more information about the inline-only and default efficiency policies, see the man pages.

## Efficiency Policies window

You can use the Efficiency Policies window to create, display, and manage information about efficiency policies.

### Command buttons

#### Add

Opens the Add Efficiency Policy dialog box, which enables you to run a deduplication operation on a volume for a specified duration (schedule-based) or when the change in volume data reaches a specified threshold value (threshold-based).

#### Edit

Opens the Edit Efficiency Policy dialog box, which enables you to modify the schedule, threshold value, QoS type, and maximum run time for a deduplication operation.

#### Delete

Opens the Delete Efficiency Policy dialog box, which enables you to delete the selected efficiency policy.

#### Status

Open a drop-down menu, which provides options to enable or disable the selected efficiency policy.

#### Refresh

Updates the information in the window.

## Efficiency policies list

### Policy

Specifies the name of an efficiency policy.

### Status

Specifies the status of an efficiency policy. The status can be one of the following:

- Enabled  
Specifies that the efficiency policy can be assigned to a deduplication operation.
- Disabled  
Specifies that the efficiency policy is disabled. You can enable the policy by using the status drop-down menu and assign it later to a deduplication operation.

### Run By

Specifies whether the storage efficiency policy is run based on a schedule or based on a threshold value (change log threshold).

### QoS Policy

Specifies the QoS type for the storage efficiency policy. The QoS type can be one of the following:

- Background  
Specifies that the QoS policy is running in the background, which reduces potential performance impact on the client operations.
- Best-effort  
Specifies that the QoS policy is running on a best-effort basis, which enables you to maximize the utilization of system resources.

### Maximum Runtime

Specifies the maximum run-time duration of an efficiency policy. If this value is not specified, the efficiency policy is run till the operation is complete.

### Details area

The area below the efficiency policy list displays additional information about the selected efficiency policy, including the schedule name and the schedule details for a schedule-based policy, and the threshold value for a threshold-based policy.

## Protection policies

You can use System Manager to create, edit, and delete protection policies.

### Creating protection policies

You can use System Manager to create asynchronous mirror, vault, or mirror and vault policies and then apply these policies to a data protection relationship.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Protection Policies**.

5. Click **Create**.
6. In the **Create Policy** dialog box, select the policy type that you want to create.
7. Specify the policy name and transfer priority.  
Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to Normal.
8. Optional: For a policy of type asynchronous mirror, select the **Transfer All Source Snapshot Copies** check box to include the “all\_source\_snapshots” rule to the mirror policy, which backs up all the Snapshot copies from the source volume.
9. Optional: Select the **Enable Network Compression** check box to compress the data that is being transferred during a data transfer.
10. Optional: Click **Add Comments** to add additional comments for the policy.
11. For a policy of type vault or mirror vault, specify a SnapMirror label and a destination retention count.
12. Click **Create**.

## Deleting protection policies

You can delete a protection policy if you no longer want to use the policy by using System Manager.

### About this task

The cluster-level mirror or vault policies are not displayed.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **Protection Policies**.
5. In the **Protection Policies** window, select the policy that you want to delete, and then click **Delete**.
6. In the **Delete Policy** dialog box, click **Delete**.

## Editing protection policies

You can use System Manager to modify a protection policy and apply the policy to a data protection relationship.

### About this task

The protection policies are not displayed at the cluster level.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.

4. In the **Policies** pane, click **Protection Policies**.
5. Select the protection policy that you want to modify, and then click **Edit**.
6. Modify the transfer priority and enable or disable network compression.
7. For an asynchronous mirror policy, back up all the source Snapshot copies.
8. For a vault or mirror vault policy, modify the SnapMirror label and retention count.  
You cannot remove the sm\_created label for a mirror vault policy.
9. Click **Save**.

## Managing data protection using SnapMirror policies

To manage a data protection mirror, vault, or mirror and vault relationship, you must assign a policy to the relationship. You use the policy to maximize the efficiency of the transfers to the backup secondaries and manage the update operations for SnapVault backups.

SVM disaster recovery relationships support only SnapMirror policies.

FlexVol volumes support data protection mirror, vault, and mirror and vault relationships and policies.

## Protection Policies window

You can use the Protection Policies window to create, manage, and display information about mirror, vault, and mirror vault policies.

- [Command buttons](#) on page 287
- [Protection policies list](#) on page 287
- [Details area](#) on page 288

### Command buttons

#### Create

Opens the Create Policy dialog box, which enables you to create a mirror, vault, or mirror vault policy.

#### Edit

Opens the Edit Policy dialog box, which enables you to edit a policy.

#### Delete

Opens the Delete Policy dialog box, which enables you to delete a policy.

#### Refresh

Updates the information in the window.

### Protection policies list

#### Name

Displays the name of the protection policy.

#### Type

Displays the policy type, which can be Vault, Mirror Vault, or Asynchronous Mirror.

#### Comment

Displays the description specified for the policy.

#### Transfer Priority

Displays the data transfer priority, such as Normal or Low.

**Details area****Policy Details tab**

Displays details of the protection policy, such as the user who created the policy, number of rules, retention count, and status of network compression.

**Policy Rules tab**

Displays details of the rules that are applied to the policy. The Policy Rules tab is displayed only if the selected policy contains rules.

## QoS policy groups

You can use System Manager to create, edit, and delete QoS policy groups.

### Creating QoS policy groups

You can use System Manager to create Storage Quality of Service (QoS) policy groups to limit the throughput of workloads and to monitor workload performance.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **QoS Policy Groups**.
5. In the **QoS Policy Groups** window, click **Create**.
6. In the **Create Policy Group** dialog box, specify a policy group name and the maximum throughput limit (in IOPS, B/s, KB/s, MB/s, and so on).  
  
If you do not specify the maximum throughput limit, the value is set to Unlimited and the unit that you specify does not affect the maximum throughput.
7. Click **OK**.

### Deleting QoS policy groups

System Manager enables you to delete a Storage QoS policy group that is no longer required.

**Before you begin**

You must have unassigned all the storage objects that are assigned to the policy group.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **QoS Policy Groups**.
5. In the **QoS Policy Groups** window, select the policy group that you want to delete, and then click **Delete**.
6. In the confirmation dialog box, click **Delete**.



## Editing QoS policy groups

You can use the Edit Policy Group dialog box in System Manager to modify the name and maximum throughput of an existing Storage Quality of Service (QoS) policy group.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Policies** pane, click **QoS Policy Groups**.
5. Select the QoS policy group that you want to edit, and then click **Edit**.

If you do not specify the maximum throughput limit, the value is set to Unlimited and the unit that you specify does not affect the maximum throughput.

6. In the **Edit Policy Group** dialog box, edit the QoS policy group details, and then click **Save**.

## Managing workload performance by using Storage QoS

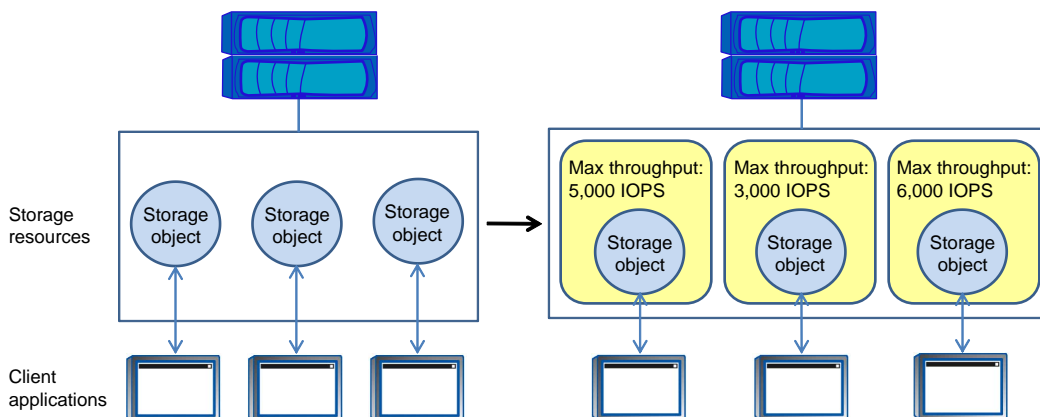
Storage QoS (Quality of Service) can help you manage risks around meeting your performance objectives. You use Storage QoS to limit the throughput to workloads and to monitor workload performance. You can reactively limit workloads to address performance problems and you can proactively limit workloads to prevent performance problems.

A workload represents the input/output (I/O) operations to one of the following kinds of storage objects:

- FlexVol volumes
- LUNs

You assign a storage object to a policy group to control and monitor a workload. You can monitor workloads without controlling them.

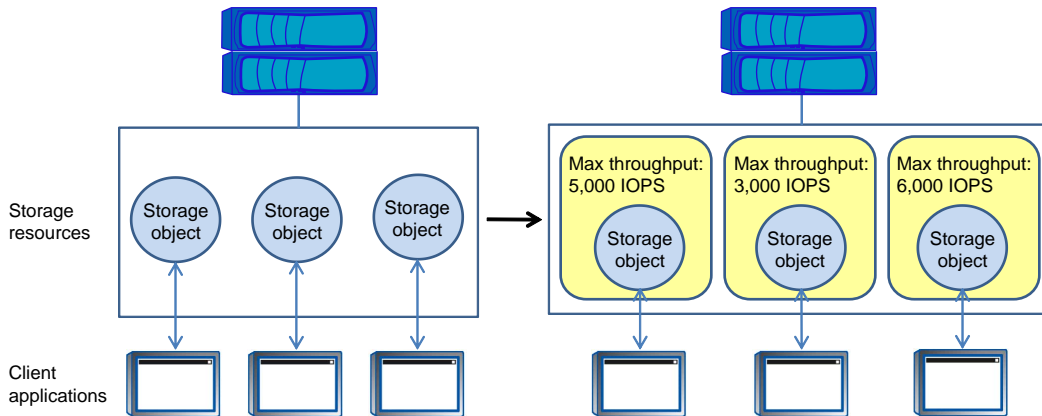
The following illustration shows an example environment before and after using Storage QoS. On the left, workloads compete for cluster resources to transmit I/O. These workloads get "best effort" performance, which means you have less performance predictability (for example, a workload might get such good performance that it negatively impacts other workloads). On the right are the same workloads assigned to policy groups. The policy groups enforce a maximum throughput limit.



## How Storage QoS works

Storage QoS controls workloads that are assigned to policy groups by throttling and prioritizing client operations (SAN and NAS data requests) and system operations.

The following illustration shows an example environment before and after using Storage QoS. On the left, workloads compete for cluster resources to transmit I/O. These workloads get "best effort" performance, which means you have less performance predictability (for example, a workload might get such good performance that it negatively impacts other workloads). On the right are the same workloads assigned to policy groups that enforce maximum throughput limits.



## How the maximum throughput limit works

You can specify one service-level objective for a Storage QoS policy group: a maximum throughput limit. A maximum throughput limit, which you define in terms of IOPS, MBps, or both, specifies the throughput that the workloads in the policy group cannot collectively exceed.

When you specify a maximum throughput for a policy group, Storage QoS controls client operations to ensure that the combined throughput for all workloads in the policy group does not exceed the specified maximum throughput.

For example, assume that you create the policy group "untested\_apps" and specify a maximum throughput of 300 MBps. You assign three volumes to the policy group. The combined throughput to those three volumes cannot exceed 300 MBps.

**Note:** The combined throughput to the workloads in a policy group might exceed the specified limit by up to 10 percent. A deviation might occur if you have a workload that experiences rapid changes in throughput (sometimes called a *bursty workload*).

Note the following about specifying a maximum throughput:

- You must not set the limit too low because you might underutilize the cluster.
- You must consider the minimum amount of throughput that you want to reserve for workloads that do not have limits.  
For example, you can ensure that your critical workloads get the throughput that they need by limiting noncritical workloads.
- You might want to provide room for growth.  
For example, if you see an average utilization of 500 IOPS, you might specify a limit of 1,000 IOPS.

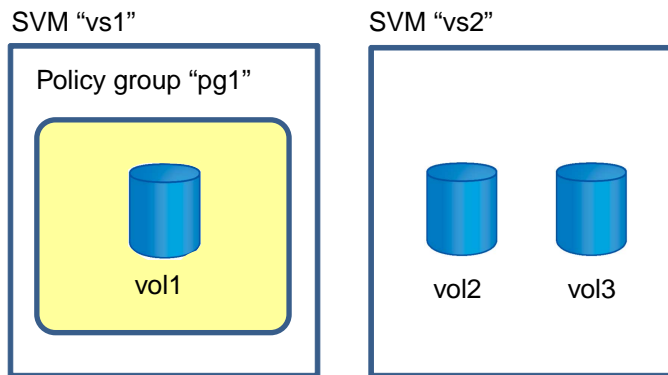
## Rules for assigning storage objects to policy groups

You should be aware of rules that dictate how you can assign storage objects to Storage QoS policy groups.

### Storage objects and policy groups must belong to the same SVM

A storage object must be contained by the Storage Virtual Machine (SVM) to which the policy group belongs. You specify the SVM to which the policy group belongs when you create the policy group. Multiple policy groups can belong to the same SVM.

In the following illustration, the policy group pg1 belongs to SVM vs1. You cannot assign volumes vol2 or vol3 to policy group pg1 because those volumes are contained by a different SVM.

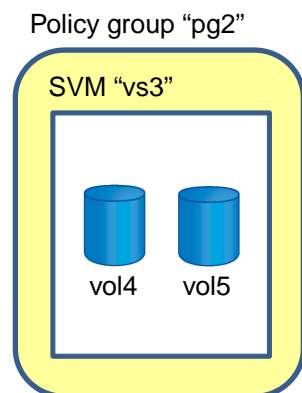


### Nested storage objects cannot belong to policy groups

You cannot assign a storage object to a policy group if its containing object or its child objects belong to a policy group. The following table lists the restrictions.

If you assign the...	Then you cannot assign...
Volume to a policy group	The volume's containing SVM or any child LUNs to a policy group
LUN to a policy group	The LUN's containing volume or SVM to a policy group

In the following illustration, the SVM vs3 is assigned to policy group pg2. You cannot assign volumes vol4 or vol5 to a policy group because an object in the storage hierarchy (SVM vs3) is assigned to a policy group.



### Some types of volumes not supported with Storage QoS

You can assign FlexVol volumes to policy groups. Infinite Volumes are not supported with Storage QoS.

The following FlexVol volume variations are not supported with Storage QoS:

- Data protection mirrors
- Load-sharing mirrors
- Node root volumes

## QoS Policy Groups window

Storage QoS (Quality of Service) can help you manage risks related to meeting your performance objectives. Storage QoS enables you to limit the throughput of workloads and to monitor workload performance. You can use the QoS Policy groups window to manage your policy groups and view information about them.

- [Command buttons](#) on page 292
- [QoS Policy Groups list](#) on page 292
- [Details area](#) on page 292

### Command buttons

#### Create

Opens the Create QoS Policy Group dialog box, which enables you to create new policy groups.

#### Edit

Opens the Edit QoS Policy Group dialog box, which enables you to modify the selected policy group.

#### Delete

Deletes the selected policy groups.

#### Refresh

Updates the information in the window.

### QoS Policy Groups list

The QoS Policy Groups list displays the policy group name and the maximum throughput for each policy group.

#### Name

Displays the name of the QoS policy group.

#### Maximum Throughput

Displays the maximum throughput limit specified for the policy group.

The value is displayed as Unlimited if you have not specified any maximum throughput limit.

#### Storage Objects Count

Displays the number of storage objects assigned to the policy group.

### Details area

The area below the QoS Policy Groups list displays detailed information about the selected policy group.

**Assigned Storage Objects tab**

Displays the name and type of the storage object that is assigned to the selected policy group.

## NIS services

You can use System Manager to add, edit, and manage Network Information Service (NIS) domains.

### Adding NIS domains

You can maintain host information centrally using NIS. You can use System Manager to add the NIS domain name of your storage system. Only one NIS domain can be active on a Storage Virtual Machine (SVM) at any given time.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **NIS**.
5. Click **Create**.
6. Type the NIS domain name and add one or more NIS servers.
7. Click **Create**.

### Editing NIS domains

You can use System Manager to modify NIS domains based on the requirement for Storage Virtual Machine (SVM) authentication and authorization.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **NIS**.
5. Select the NIS domain, and then click **Edit**.
6. Make the necessary changes, and then click **Edit**.

### Managing NIS domains

A Network Information Service (NIS) domain provides a directory of hostnames and IP addresses in a network. A Storage Virtual Machine (SVM) administrator can manage NIS domains by creating, modifying, deleting, or displaying information about them. NIS cannot be configured for the cluster management server.

You can configure multiple NIS domains for a given SVM, but only one NIS domain can be active on an SVM at any given time. You can also configure an NIS domain with more than one SVM.

## NIS window

The NIS window enables you to view the current NIS settings for your storage system.

### Command buttons

#### Create

Opens the Create NIS Domain dialog box, which enables you to create NIS domains.

#### Edit

Opens the Edit NIS Domain dialog box, which enables you to add, delete, or modify NIS servers.

#### Delete

Deletes the selected NIS domain.

#### Refresh

Updates the information in the window.

## LDAP client services

You can use System Manager to add, edit, and delete LDAP client configurations.

## Adding an LDAP client configuration

You can use System Manager to add an LDAP client configuration to use the LDAP services. An LDAP server enables you to centrally maintain user information. You must first set up an LDAP client to use LDAP services.

### About this task

The LDAP client configuration is view-only at the cluster level. You must add the LDAP client from the Storage Virtual Machine (SVM) level.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **LDAP Client**.
5. In the **LDAP Client** window, click **Add**.
6. Type the name of the LDAP client.
7. Add either the Active Directory domain or the Active Directory server.
8. Click **Binding**, and then specify the authentication details.
9. Click **Save and Close**.
10. Verify that the LDAP client you added is displayed in the **LDAP Client** window.

## Deleting an LDAP client configuration

You can delete an LDAP client configuration when you do not want any Storage Virtual Machine (SVM) to be associated with it by using System Manager.

### About this task

The LDAP client configuration is view-only at the cluster level. You must delete the LDAP client from the SVM level.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **LDAP Client**.
5. Select the LDAP client, and then click **Delete**.
6. Select the confirmation check box, and then click **Delete**.
7. Verify that the LDAP client you deleted is no longer displayed in the **LDAP Client** window.

## Editing an LDAP client configuration

You can edit an LDAP client configuration using the Edit LDAP Client window in System Manager.

### About this task

The LDAP client configuration is view-only at the cluster level. You must edit the LDAP client from the Storage Virtual Machine (SVM) level.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **LDAP Client**.
5. In the **LDAP Client** window, select the LDAP client, and then click **Edit**.
6. In the **Edit LDAP Client** dialog box, edit the LDAP client configuration as required.
7. Click **Save and Close**.
8. Verify that the changes you made to the LDAP client are displayed in the **LDAP Client** window.

## LDAP Client window

You can use the LDAP Client window to create LDAP clients for user authentication, file access authorization, user search, and mapping services between NFS and CIFS at the Storage Virtual Machine (SVM) level.

### Command buttons

#### Add

Opens the Create LDAP Client dialog box, which enables you to create and configure LDAP clients.

#### Edit

Opens the Edit LDAP Client dialog box, which enables you to edit the LDAP client configurations. You can also edit the active LDAP clients.

#### Delete

Opens the Delete LDAP Client(s) dialog box, which enables you to delete LDAP client configurations. You can also delete an active LDAP client.

#### Refresh

Updates the information in the window.

### LDAP client list

Displays, in tabular format, details about LDAP clients.

#### LDAP Client Configuration

Displays the name of the LDAP client configuration that you specified.

#### Active Directory Domain

Displays the Active Directory domain for each LDAP client configuration.

#### Active Directory Servers

Displays the Active Directory server for each LDAP client configuration.

#### Preferred Active Directory Servers

Displays the preferred Active Directory server for each LDAP client configuration.

## LDAP configuration services

You can use System Manager to manage LDAP configurations.

## Editing active LDAP clients

You can use System Manager to associate an active LDAP client with a Storage Virtual Machine (SVM), which enables you to use LDAP as a name service or for name mapping.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **LDAP Configuration**.
5. In the **LDAP Configuration** window, click **Edit**.



6. In the **Active LDAP Client** dialog box, select the LDAP client that you want to edit and perform the following actions:
  - Enable or disable the LDAP client.
  - Modify the active directory domain servers.
  - Modify the preferred active directory servers.
7. Click **OK**.
8. Verify that the changes you made are updated in the **LDAP Configuration** window.

## Deleting active LDAP clients

You can use System Manager to delete an active LDAP client when you do not want a Storage Virtual Machine (SVM) to be associated with it.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **LDAP Configuration**.
5. Click **Delete**.
6. Select the confirmation check box, and then click **Delete**.

## LDAP Configuration window

You can use the LDAP Configuration window to edit or delete active LDAP clients at the Storage Virtual Machine (SVM) level.

### Command buttons

#### Edit

Opens the Active LDAP Client dialog box, which enables you to edit the active LDAP client properties such as state, active directory domain servers, and preferred active directory servers.

#### Delete

Opens the Delete Active LDAP Client dialog box, which enables you to delete the active LDAP client.

#### Refresh

Updates the information in the window.

### LDAP Configuration area

Displays the details about the active LDAP client.

#### LDAP client name

Displays the name of the active LDAP client.

#### State

Displays if the active LDAP client is enabled or disabled.

**Active Directory Domain Servers**

Displays the Active Directory domain for the active LDAP client.

**Preferred Active Directory Servers**

Displays the preferred Active Directory server for the active LDAP client.

## Kerberos realm services

You can use System Manager to create and manage Kerberos realm services.

### Creating a Kerberos realm configuration

If you want to use Kerberos authentication for client access, you must configure the Storage Virtual Machine (SVM) to use an existing Kerberos realm. You can use System Manager to create a Kerberos realm configuration, which enables SVMs to use Kerberos security services for NFS.

**Before you begin**

- CIFS license must be installed if CIFS shares are used, and NFS license must be installed if an LDAP server is used.
- Active Directory (Windows 2003 or Windows 2008) with DES MD5 encryption capability must be available.
- You must have set the time zone and synchronized the time across the cluster by configuring NTP. This prevents authentication errors, and ensures that timestamps in log files are consistent across the cluster.

**About this task**

While creating a Kerberos realm, you have to set the following attributes in the Create Kerberos Realm wizard:

- Kerberos realm
- KDC IP address and port number.  
The default port number is 88.
- Kerberos Key Distribution Center (KDC) vendor
- Administrative server IP address if the KDC vendor is not Microsoft
- Password server IP address
- Active Directory server name and IP address if the KDC vendor is Microsoft

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **Kerberos Realm**.
5. In the **Kerberos Realm** window, click **Create**.
6. Type or select information as prompted by the wizard.

7. Confirm the details, and then click **Finish** to complete the wizard.

#### Related tasks

[Setting the time for a cluster](#) on page 35

#### Related information

[NetApp Technical Report 4073: Secure Unified Authentication with NetApp Storage Systems: Kerberos, NFSv4, and LDAP for User Authentication over NFS \(with a Focus on Clustered Data ONTAP\)](#)

## Editing a Kerberos realm configuration

You can use System Manager to edit a Kerberos realm configuration at the Storage Virtual Machine (SVM) level.

#### About this task

You can modify the following attributes by using the Kerberos Realm Edit wizard:

- KDC IP address and port number
- The IP address of the administrative server if the KDC vendor is not Microsoft
- The IP address of the password server
- Active Directory server name and IP address if the KDC vendor is Microsoft

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **Kerberos Realm**.
5. In the **Kerberos Realm** window, select the Kerberos realm configuration that you want to modify, and then click **Edit**.
6. Type or select information as prompted by the wizard.
7. Confirm the details, and then click **Finish** to complete the wizard.

## Deleting Kerberos realm configurations

You can use System Manager to delete a Kerberos realm configuration.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **Kerberos Realm**.
5. In the **Kerberos Realm** window, select one or more Kerberos realm configurations that you want to delete, and then click **Delete**.

6. Select the confirmation check box, and then click **Delete**.

## Using Kerberos with NFS for strong security

You can use Kerberos to provide strong authentication between SVMs and NFS clients to provide secure NFS communication. Configuring NFS with Kerberos increases the integrity and security of NFS client communications with the storage system.

## Kerberos authentication for CIFS

With Kerberos authentication, upon connection to your CIFS server, the client negotiates the highest possible security level. However, if the client cannot use Kerberos authentication, Microsoft NTLM or NTLM V2 is used to authenticate with the CIFS server.

## Kerberos Realm window

You can use the Kerberos Realm window to provide authentication between Storage Virtual Machines (SVMs) and NFS clients to ensure secure NFS communication.

### Command buttons

#### Create

Opens the Kerberos Realm Create wizard, which enables you to configure a Kerberos realm to retrieve user information.

#### Edit

Opens the Kerberos Realm Edit wizard, which enables you to edit a Kerberos realm configuration based on the requirement for SVM authentication and authorization.

#### Delete

Opens the Delete Kerberos Realm(s) dialog box, which enables you to delete Kerberos realm configuration.

#### Refresh

Updates the information in the window.

### Kerberos Realm list

Provides details about the Kerberos realms, in tabular format.

#### Realm

Specifies the name of the Kerberos realm.

#### KDC Vendor

Specifies the name of the Kerberos Distribution Center (KDC) vendor.

#### KDC IP Address

Specifies the KDC IP address used by the configuration.

### Details area

The details area displays information such as the KDC IP address and port number, KDC vendor, administrative server IP address and port number, Active Directory server and server IP address of the selected Kerberos realm configuration.

## Kerberos interface services

You can use System Manager to manage Kerberos interface services.

### Editing Kerberos configuration

You can use System Manager to enable Kerberos and edit a Kerberos configuration associated with a Storage Virtual Machine (SVM). This enables the SVM to use Kerberos security services for NFS.

#### Before you begin

- You must have at least one Kerberos realm configured at the SVM level.
- You must have a minimum of two data LIFs on the SVM.  
One data LIF is used by the Service Principal Name (SPN) for both the UNIX and CIFS-related Kerberos traffic. The other data LIF is used for accessing non-Kerberos traffic.

**Note:** The CIFS server is not required for basic NFS Kerberos access. It is required for multiprotocol access or when using Active Directory as an LDAP server for name mapping purposes.

#### About this task

If you are using Microsoft Active Directory Kerberos, the first 15 characters of any SPNs used in the domain must be unique. Microsoft Active Directory has a limitation for SPNs of 15 characters maximum and does not allow duplicate SPNs.

#### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **Kerberos Interface**.
5. In the **Kerberos Interface** window, select the interface, and then click **Edit**.
6. In the **Edit Kerberos Configuration** dialog box, make the necessary changes, and then click **OK**.

#### Related information

*[NetApp Technical Report 4073: Secure Unified Authentication with NetApp Storage Systems: Kerberos, NFSv4, and LDAP for User Authentication over NFS \(with a Focus on Clustered Data ONTAP\)](#)*

## Kerberos Interface window

You can use the Kerberos Interface window to enable Kerberos and to edit the Kerberos configuration for Storage Virtual Machines (SVMs).

### Command buttons

#### Edit

Opens the Edit Kerberos Configuration dialog box, which you can use to enable Kerberos and to edit the Kerberos configuration associated with the SVM.

**Refresh**

Updates the information in the window.

**Kerberos Interface list**

Provides details about the Kerberos configuration.

**Interface Name**

Specifies the logical interfaces associated with the Kerberos configuration for SVMs.

**Service Principal Name**

Specifies the Service Principal Name (SPN) that matches the Kerberos configuration.

**Realm**

Specifies the name of the Kerberos realm associated with the Kerberos configuration.

**Kerberos Status**

Specifies whether Kerberos is enabled.

## DNS/DDNS Services

You can use System Manager to manage DNS/DDNS services.

### Enabling or disabling DNS and DDNS

You can use System Manager to enable or disable DNS on a storage system. After enabling DNS, you can enable DDNS.

**Before you begin**

The DNS server administrator must have made the necessary changes in the DNS server for the DDNS functionality to work.

**About this task**

DNS and DDNS are disabled by default.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **DNS/DDNS**.
5. In the **DNS/DDNS Services** window, click **Edit**.
6. In the **Edit DNS/DDNS Settings** dialog box, enable DNS and DDNS services:
  - a. Select the **DNS service** check box.
  - b. Select the **DDNS service** check box.

You can disable DNS and DDNS by clearing the respective check box.

7. Click **OK**.

**Related references**

[DNS/DDNS Services window](#) on page 303

**Editing DNS and DDNS settings**

You can maintain host information centrally using DNS. You can use System Manager to add or modify the DNS domain name of your storage system. You can also enable DDNS on your storage system to update the name server automatically in the DNS server.

**Before you begin**

- You must have set up a CIFS server or Active Directory account for the Storage Virtual Machine (SVM) for secure DDNS to work.
- The DNS server administrator must have made the necessary changes in the DNS server for the DDNS functionality to work.  
Secure DDNS must be enabled on both Data ONTAP and in the DNS server.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **DNS/DDNS**.
5. Click **Edit**.
6. In the **Edit DNS/DDNS Settings** dialog box, select the **DNS service** check box to enable DNS.
7. In the DNS Domains and Name Servers areas, add or modify the DNS domain names and the IP addresses.
8. Select the **DDNS service** check box to enable DDNS.  
You can enable DDNS only if DNS is enabled.
  - a. Select the **Enable Secure DDNS** check box to enable secure DDNS.
  - b. Specify the FQDN and time to live values for the DDNS service.  
By default, time to live is set to 24 hours and FQDN is set to *SVM name . domain name*.
9. Click **OK**.

**Related references**

[DNS/DDNS Services window](#) on page 303

**DNS/DDNS Services window**

The DNS/DDNS Services window enables you to view the current DNS and DDNS settings for your system.

**Command buttons****Edit**

Opens the Edit DNS/DDNS Settings dialog box, which you can use to add or modify DNS or DDNS details. You can also enable or disable DNS or DDNS.

**Refresh**

Updates the information in the window.

**Related tasks**

[Enabling or disabling DNS and DDNS](#) on page 302

[Editing DNS and DDNS settings](#) on page 303

## Users

You can use System Manager to create and manage Storage Virtual Machine (SVM) user accounts.

### Adding SVM user accounts

You can use System Manager to add a Storage Virtual Machine (SVM) user account and specify a login user method to access the storage system.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **SVM User Details** pane, click **Users**.
5. Click **Add**.
6. Type the user name and password that the user uses to connect to the storage system and confirm the password.
7. Add one or more user login methods, and then click **Add**.

### Changing the password for SVM user accounts

You can use System Manager to reset the password for a Storage Virtual Machine (SVM) user account.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **SVM User Details** pane, click **Users**.
5. Select the user account for which you want to modify the password, and then click **Reset Password**.
6. In the **Reset Password** dialog box, type the new password, confirm the new password, and then click **Change**.



## Editing SVM user accounts

You can use System Manager to edit a Storage Virtual Machine (SVM) user account by modifying the user login methods to access the storage system.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **SVM User Details** pane, click **Users**.
5. Select the user account that you want to modify, and then click **Edit**.
6. Modify one or more user login methods, and then click **Modify**.

## Locking or unlocking SVM user accounts

You can either lock or unlock Storage Virtual Machine (SVM) user accounts by using System Manager.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **SVM User Details** pane, click **Users**.
5. In the **Users** window, select the user account whose account status you want to modify, and then click either **Lock** or **Unlock**, as required.

## Users window

You can use the Users window to manage user accounts, reset a user's password, or display information about all user accounts.

### Command buttons

#### Add

Opens the Add User dialog box, which enables you to add user accounts.

#### Edit

Opens the Modify User dialog box, which enables you to modify user login methods.

**Note:** It is best to use a single role for all access and authentication methods of a user account.

#### Delete

Enables you to delete a selected user account.

#### Change Password

Opens the Change Password dialog box, which enables you to reset the user password.

#### Lock

Locks the user account.

**Refresh**

Updates the information in the window.

**Users list**

The area below the users list displays detailed information about the selected user.

**User**

Displays the name of the user account.

**Account Locked**

Displays whether the user account is locked.

**User Login Methods area****Application**

Displays the access method that a user can use to access the storage system. The supported access methods include the following:

- System console (console)
- HTTP(S) (http)
- Data ONTAP API (ontapi)
- Service Processor (service-processor)
- SSH (ssh)

**Authentication**

Displays the default supported authentication method, which is “password”.

**Role**

Displays the role of a selected user.

## Roles

You can use System Manager to create and manage roles.

### Adding roles

You can use System Manager to add an access-control role and specify the command or command directory that the role's users can access. You can also control the level of access the role has to the command or command directory and specify a query that applies to the command or command directory.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **SVM User Details** pane, click **Roles**.
5. Click **Add**.
6. In the **Add Role** dialog box, specify the role name and add the role attributes.

7. Click **Add**.

## Editing roles

You can use System Manager to modify an access-control role's access to a command or command directory and restrict a user's access to only a specified set of commands.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **SVM User Details** pane, click **Roles**.
5. Select the role that you want to modify, and then click **Edit**.
6. Modify the role attributes, and then click **Modify**.

## Predefined roles for SVM administrators

The predefined roles for SVM administrators should meet most of your needs. You can create custom roles as necessary. By default, an SVM administrator is assigned the predefined **vsadmin** role.

The following table lists the predefined roles for SVM administrators:

Role name	Capabilities
vsadmin	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Managing volumes, except volume moves</li> <li>• Managing quotas, qtrees, Snapshot copies, and files</li> <li>• Managing LUNs</li> <li>• Performing SnapLock operations, except privileged delete</li> <li>• Configuring protocols: NFS, CIFS, iSCSI, and FC, including FCoE</li> <li>• Configuring services: DNS, LDAP, and NIS</li> <li>• Monitoring jobs</li> <li>• Monitoring network connections and network interface</li> <li>• Monitoring the health of the SVM</li> </ul>
vsadmin-volume	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Managing volumes, including volume moves</li> <li>• Managing quotas, qtrees, Snapshot copies, and files</li> <li>• Managing LUNs</li> <li>• Configuring protocols: NFS, CIFS, iSCSI, and FC, including FCoE</li> <li>• Configuring services: DNS, LDAP, and NIS</li> <li>• Monitoring network interface</li> <li>• Monitoring the health of the SVM</li> </ul>

Role name	Capabilities
vsadmin-protocol	<ul style="list-style-type: none"> <li>Managing own user account local password and key information</li> <li>Configuring protocols: NFS, CIFS, iSCSI, and FC, including FCoE</li> <li>Configuring services: DNS, LDAP, and NIS</li> <li>Managing LUNs</li> <li>Monitoring network interface</li> <li>Monitoring the health of the SVM</li> </ul>
vsadmin-backup	<ul style="list-style-type: none"> <li>Managing own user account local password and key information</li> <li>Managing NDMP operations</li> <li>Making a restored volume read/write</li> <li>Managing SnapMirror relationships and Snapshot copies</li> <li>Viewing volumes and network information</li> </ul>
vsadmin-snaplock	<ul style="list-style-type: none"> <li>Managing own user account local password and key information</li> <li>Managing volumes, except volume moves</li> <li>Managing quotas, qtrees, Snapshot copies, and files</li> <li>Performing SnapLock operations, including privileged delete</li> <li>Configuring protocols: NFS and CIFS</li> <li>Configuring services: DNS, LDAP, and NIS</li> <li>Monitoring jobs</li> <li>Monitoring network connections and network interface</li> </ul>
vsadmin-readonly	<ul style="list-style-type: none"> <li>Managing own user account local password and key information</li> <li>Monitoring the health of the SVM</li> <li>Monitoring network interface</li> <li>Viewing volumes and LUNs</li> <li>Viewing services and protocols</li> </ul>

**Related concepts**

[Roles](#) on page 86

**Roles window**

You can use the Roles window to manage roles for user accounts.

**Command buttons****Add**

Opens the Add Role dialog box, which enables you to create an access-control role and specify the command or command directory that the role's users can access.

**Edit**

Opens the Edit Role dialog box, which enables you to add or modify role attributes.

**Refresh**

Updates the information in the window.

**Roles list**

The roles list provides a list of roles that are available to be assigned to users.

**Role Attributes area**

The details area displays the role attributes, such as the command or command directory that the selected role can access, the access level, and the query that applies to the command or command directory.

## UNIX

You can use System Manager to maintain a list of local UNIX users and groups for each Storage Virtual Machine (SVM).

### UNIX window

You can use the UNIX window to maintain a list of local UNIX users and groups for each Storage Virtual Machine (SVM). You can use local UNIX users and groups for authentication and name mappings.

**Groups tab**

You can use the Groups tab to add, edit, or delete UNIX groups that are local to an SVM.

**Command buttons****Add Group**

Opens the Add Group dialog box, which enables you to create UNIX groups that are local to SVMs. Local UNIX groups are used with local UNIX users.

**Edit**

Opens the Edit Group dialog box, which enables you to edit a group ID.

**Delete**

Deletes the selected group.

**Refresh**

Updates the information in the window.

**Groups list****Group Name**

Displays the name of the group.

**Group ID**

Displays the ID of the group.

**Users tab**

You can use the **Users** tab to add, edit, and delete UNIX users that are local to SVMs.

**Command buttons****Add User**

Opens the Add User dialog box, which enables you to create UNIX users that are local to SVMs.

**Edit**

Opens the Edit User dialog box, which enables you to edit the User ID, UNIX group to which the user belongs, and the full name of the user.

**Delete**

Deletes the selected user.

**Refresh**

Updates the information in the window.

**Users list****User Name**

Displays the name of the user.

**User ID**

Displays the ID of the user.

**Full Name**

Displays the full name of the user.

**Primary Group ID**

Displays the ID of the group to which the user belongs.

**Primary Group Name**

Displays the name of the group to which the user belongs.

## Windows

You can use System Manager to create and manage Windows groups and user accounts.

### Creating a local Windows group

You can create local Windows groups that can be used for authorizing access to data contained in the Storage Virtual Machine (SVM) over an SMB connection by using System Manager. You can also assign privileges that define the user rights or capabilities that a member of the group has when performing administrative activities.

**Before you begin**

CIFS server must be configured for the SVM.

**About this task**

- You can specify a group name with or without the local domain name.  
The local domain is the name of the CIFS server for the SVM. For example, if the CIFS server name of the SVM is “CIFS\_SERVER” and you want to create an “engineering” group, you can specify either “engineering” or “CIFS\_SERVER\engineering” as the group name.  
The following rules apply when using a local domain as part of the group name:
  - You can only specify the local domain name for the SVM to which the group is applied.  
For example, if the local CIFS server name is “CIFS\_SERVER”, you cannot specify “CORP\_SERVER\group1” as the group name.
  - You cannot use “BUILTIN” as a local domain in the group name.  
For example, you cannot create a group with “BUILTIN\group1” as the name.
  - You cannot use an Active Directory domain as a local domain in the group name.

For example, you cannot create a group named “AD\_DOM\group1”, where “AD\_DOM” is the name of an Active Directory domain.

- You cannot use a group name that already exists.
- The group name must meet the following requirements:
  - Must not exceed 256 characters
  - Must not end in a period
  - Must not include commas
  - Must not include any of the following printable characters: " / \ [ ] : | < > + = ; ? \* @
  - Must not include characters in the ASCII range 1 through 31, which are non-printable

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**
5. In the **Groups** tab, click **Create**.
6. In the **Create Group** dialog box, specify a name for the group and a description that helps you identify this new group.
7. Assign a set of privileges to the group.  
You can select the privileges from the predefined set of supported privileges.
8. Click **Add** to add users to this group.
9. In the **Add Members to Group** dialog box, perform one of the following actions:
  - Specify the Active Directory user or Active Directory group to be added to a particular local group.
  - Select the users from the list of available local users in the SVM.
  - Click **OK**.
10. Click **Create**.

### Result

The local Windows group is created and is listed in the Groups window.

### Related references

[Windows window](#) on page 322

## Editing local Windows group properties

You can manage local group membership by adding and removing a local or Active Directory user or Active Directory group by using System Manager. You can modify the privileges assigned to a group and the description of a group to easily identify the group.

### About this task

You must keep the following in mind when adding or removing members to a local Windows group:

- You cannot add or remove users to the special *Everyone* group.
- You cannot add a local Windows group to another local Windows group.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**
5. In the **Groups** tab, click **Edit**.
6. Specify a name for the group and a description to identify this new group.
7. Assign a set of privileges to the group.  
You can select the privileges from the predefined set of supported privileges.
8. Click **Add** to add users to this group.
9. In the **Add Members** window, perform one of the following actions:
  - Specify the Active Directory user or Active Directory group to be added to a particular local group.
  - Select the users from the list of available local users in the SVM.
10. Click **Edit**.

### Result

The local Windows group settings are modified and the changes are displayed in the **Groups** tab.

### Related references

[Windows window](#) on page 322

## Adding user accounts to a Windows local group

You can add a local or an Active Directory user, or an Active Directory group, if you want users to have the privileges associated with that group by using System Manager.

### Before you begin

- The group must already exist before you can add a user to it.
- The user must already exist before you can add the user to a group.



**About this task**

You must keep the following in mind when adding members to a local Windows group:

- You cannot add users to the special *Everyone* group.
- You cannot add a local Windows group to another local Windows group.
- You cannot add a user account that contains a space in the user name by using System Manager. You can either rename the user account or add the user account by using the command-line interface (CLI).

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**
5. In the **Groups** tab, select the group to which you want to add a user, and then click **Add Members**.
6. In the **Add Members** window, perform one of the following actions:
  - Specify the Active Directory user or Active Directory group to be added to a particular local group.
  - Select the users from the list of available local users in the SVM.
7. Click **OK**.

**Result**

The user you added is listed in the Users tab of the **Groups** tab.

**Related references**

[Windows window](#) on page 322

## Renaming a local Windows group

You can use System Manager to rename a local Windows group to identify it more easily.

**About this task**

- The new group name must remain in the same domain as the old group name.
- The group name must meet the following requirements:
  - Must not exceed 256 characters
  - Must not end in a period
  - Must not include commas
  - Must not include any of the following printable characters: " / \ [ ] : | < > + = ; ? \* @
  - Must not include characters in the ASCII range 1 through 31, which are non-printable

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**
5. In the **Groups** tab, select the group you want to rename, and then click **Rename**.
6. In the **Rename Group** window, specify a new name for the group.

**Result**

The local group name is changed and is listed with the new name in the Groups window.

**Related references**

[Windows window](#) on page 322

**Deleting a local Windows group**

You can use System Manager to delete a local Windows group from a Storage Virtual Machine (SVM) if it is no longer required for determining access rights to data contained on the SVM or for assigning SVM user rights (privileges) to group members.

**About this task**

- Removing a local group removes its membership records.
- The file system is not altered.  
Windows Security Descriptors on files and directories that refer to this group are not adjusted.
- The special “Everyone” group cannot be deleted.
- Built-in groups, such as BUILTIN\Administrators and BUILTIN\Users, cannot be deleted.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**
5. In the **Groups** tab, select the group you want to delete, and then click **Delete**.
6. Click **Delete**.

**Result**

The local group is deleted along with its membership records.

**Related references**

[Windows window](#) on page 322

## Creating a local Windows user account

You can use System Manager to create a local Windows user account that can be used to authorize access to data contained in the Storage Virtual Machine (SVM) over an SMB connection. You can also use local Windows user accounts for authentication when creating a CIFS session.

### Before you begin

- The CIFS server must be configured for the SVM.

### About this task

A local Windows user name must meet the following requirements:

- Must not exceed 20 characters
- Must not end in a period
- Must not include commas
- Must not include any of the following printable characters: " / \ [ ] : | < > + = ; ? \* @
- Must not include characters in the ASCII range 1 through 31, which are non-printable

The password must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters: ~ ! @ # 0 ^ & \* \_ - + = ` \ | ( ) [ ] ; , ' < > , . ? /

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**.
5. In the **Users** tab, click **Create**.
6. Specify a name for the local user.
7. Specify the full name of the local user and a description that helps you identify this new user.
8. Enter a password for the local user and confirm the password.  
The password must meet the password requirements.
9. Click **Add** to assign group memberships to this user.
10. In the **Add Groups** window, select the groups from the list of available groups in the SVM.
11. Select **Disable this account** to disable this account after the user is created.

**12. Click **Create**.****Result**

The local Windows user account is created and is assigned membership to the selected groups. The user account is listed in the **Users** tab.

**Related references**

[Windows window](#) on page 322

**Editing the local Windows user properties**

You can use System Manager to modify a local Windows user account if you want to change an existing user's full name or description, and if you want to enable or disable the user account. You can also modify the group memberships assigned to the user account.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**
5. In the **Users** tab, click **Edit**.
6. In the **Modify User** window, make the necessary changes.
7. Click **Modify**.

**Result**

The local Windows user account attributes are modified and is displayed in the **Users** tab.

**Related references**

[Windows window](#) on page 322

**Assigning group memberships to a user account**

You can use System Manager to assign group membership to a user account if you want a user to have privileges associated with that group.

**Before you begin**

- The group must exist before you can add a user to it.
- The user must exist before you can add the user to a group.

**About this task**

You cannot add users to the special *Everyone* group.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.

3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**.
5. In the **Users** tab, select the user account to which you want to assign group memberships, and then click **Add to Group**.
6. In the **Add Groups** window, select the groups to which you want to add the user account.
7. Click **OK**.

### Result

The user account is assigned membership for all the selected groups and has privileges associated with these groups.

### Related references

[Windows window](#) on page 322

## Renaming a local Windows user

You can use System Manager to rename a local Windows user account to identify it more easily.

### About this task

- The new user name must be created in the same domain as the previous user name.
- The user name must meet the following requirements:
  - Must not exceed 20 characters
  - Must not end in a period
  - Must not include commas
  - Must not include any of the following printable characters: " / \ [ ] : | < > + = ; ? \* @
  - Must not include characters in the ASCII range 1 through 31, which are non-printable

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**
5. In the **Users** tab, select the user that you want to rename, and then click **Rename**.
6. In the **Rename User** window, specify a new name for the user.
7. Confirm the new name, and then click **Rename**.

### Result

The user name is changed and the new name is listed in the **Users** tab.

### Related references

[Windows window](#) on page 322

## Resetting the password of a Windows local user

You can use System Manager to reset the password of a Windows local user. For example, you might want to reset the password if the password is compromised or if the user has forgotten the password.

### About this task

The password must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters: ~ ! @ # 0 ^ & \* \_ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.
4. In the **Host Users and Groups** pane, click **Windows**.
5. In the **Users** tab, select the user whose password you want to reset, and then click **Set Password**.
6. In the **Reset Password** dialog box, set a new password for the user.
7. Confirm the new password, and then click **Reset**.

### Related references

[Windows window](#) on page 322

## Deleting a local Windows user account

You can use System Manager to delete a local Windows user account from a Storage Virtual Machine (SVM) if it is no longer required for local CIFS authentication to the CIFS server of the SVM or for determining access rights to data contained in the SVM.

### About this task

- Standard users such as Administrator cannot be deleted.
- Data ONTAP removes references to this user from the local-group database, from the local-user-membership, and from the user-rights database.

### Steps

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **SVM Settings** tab.

4. In the **Host Users and Groups** pane, click **Windows**.
5. In the **Users** tab, select the user account that you want to delete, and then click **Delete**.
6. Click **Delete**.

### Result

The local user account is deleted along with its group membership entries.

### Related references

[Windows window](#) on page 322

## Using local users and groups for authentication and authorization

You can create local users and groups on the Storage Virtual Machine (SVM). The CIFS server can use local users for CIFS authentication and can use both local users and groups for authorization when determining both share and file and directory access rights.

Local group members can be local users, domain users and groups, and domain machine accounts.

Local users and groups can also be assigned privileges. Privileges control access to SVM resources and can override the permissions that are set on objects. A user or member of a group that is assigned a privilege is granted the specific rights that the privilege allows.

**Note:** Privileges do not provide clustered Data ONTAP general administrative capabilities.

### Related references

[Windows window](#) on page 322

## Local users and groups concepts

You should know what local users and groups are, and some basic information about them, before determining whether to configure and use local users and groups in your environment.

### Local user

A user account with a unique security identifier (SID) that has visibility only on the Storage Virtual Machine (SVM) on which it is created. Local user accounts have a set of attributes, including user name and SID. A local user account authenticates locally on the CIFS server using NTLM authentication.

User accounts have several uses:

- Used to grant *User Rights Management* privileges to a user.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

### Local group

A group with a unique SID has visibility only on the SVM on which it is created. Groups contain a set of members. Members can be local users, domain users, domain groups, and domain machine accounts. Groups can be created, modified, or deleted.

Groups have several uses:

- Used to grant *User Rights Management* privileges to its members.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

**Local domain**

A domain that has local scope, which is bounded by the SVM. The local domain's name is the CIFS server name. Local users and groups are contained within the local domain.

**Security identifier (SID)**

A SID is a variable-length numeric value that identifies Windows-style security principals. For example, a typical SID takes the following form:  
S-1-5-21-3139654847-1303905135-2517279418-123456.

**NTLM authentication**

A Microsoft Windows security method used to authenticate users on a CIFS server.

**Cluster replicated database (RDB)**

A replicated database with an instance on each node in a cluster. Local user and group objects are stored in the RDB.

**Reasons for creating local users and local groups**

There are several reasons for creating local users and local groups on your Storage Virtual Machine (SVM). For example, you can access a CIFS server by using a local user account if the domain controllers are unavailable, or you may want to use local groups to assign privileges.

You can create one or more local user accounts for the following reasons:

- You want the ability to authenticate and log in to the CIFS server if the domain controllers are unavailable.  
Local users can authenticate with the CIFS server by using NTLM authentication when the domain controller is down, or when network problems prevent your CIFS server from contacting the domain controller.
- You want to assign *User Rights Management* privileges to a local user.  
*User Rights Management* is the ability for a CIFS server administrator to control what rights the users and groups have on the SVM. You can assign privileges to a user by assigning the privileges to the user's account, or by making the user a member of a local group that has those privileges.

**Note:** A CIFS server can be part of either an Active Directory domain or a workgroup. A CIFS server operates as a member server in an Active Directory domain.

You can create one or more local groups for the following reasons:

- You want to control access to file and folder resources by using local groups for share and file-access control.
- You want to create local groups with customized *User Rights Management* privileges.  
Some built-in user groups have predefined privileges. To assign a customized set of privileges, you can create a local group and assign the necessary privileges to that group. You can then add local users, domain users, and domain groups to the local group.

**What local privileges are**

Privileges are well-known rights that can be granted to local and domain users and groups to perform *User Rights Management* tasks on the CIFS server. You cannot create privileges. You can only add or remove existing privileges.

**List of supported privileges**

Data ONTAP has a predefined set of supported privileges. Certain predefined local groups have some of these privileges added to them by default. You can also add or remove privileges from the



predefined groups or create new local users or groups and add privileges to the groups that you created or to existing domain users and groups.

The following table lists the supported privileges on the Storage Virtual Machine (SVM) and provides a list of BUILTIN groups with assigned privileges:

Privilege name	Default security setting	Description
<b>SeTcbPrivilege</b>	None	Act as part of the operating system
<b>SeBackupPrivilege</b>	<b>BUILTIN\Administrators</b> , <b>BUILTIN\Backup Operators</b>	Back up files and directories, overriding any ACLs
<b>SeRestorePrivilege</b>	<b>BUILTIN\Administrators</b> , <b>BUILTIN\Backup Operators</b>	Restore files and directories, overriding any ACLs
<b>SeTakeOwnershipPrivilege</b>	<b>BUILTIN\Administrators</b>	Take ownership of files or other objects
<b>SeSecurityPrivilege</b>	<b>BUILTIN\Administrators</b>	Manage auditing This includes viewing, dumping, and clearing the security log.
<b>SeChangeNotifyPrivilege</b>	<b>BUILTIN\Administrators</b> , <b>BUILTIN\Backup Operators</b> , <b>BUILTIN\Power Users</b> , <b>BUILTIN\Users</b> , <b>Everyone</b>	Bypass traverse checking Users with this privilege are not required to have traverse (x) permissions to traverse folders, symlinks, or junctions.

## Predefined BUILTIN groups and default privileges

You can assign membership of a local user or domain user to a predefined set of BUILTIN groups provided by Data ONTAP. Predefined groups have predefined privileges assigned.

The following table describes the predefined groups:

Predefined BUILTIN group	Default privileges
<b>BUILTIN\Administrators</b> RID 544 When first created, the local <b>Administrator</b> account, with a RID of 500, is automatically made a member of this group. When the Storage Virtual Machine (SVM) is joined to a domain, the <b>domain\Domain Admins</b> group is added to the group. If the SVM leaves the domain, the <b>domain\Domain Admins</b> group is removed from the group.	<ul style="list-style-type: none"> <li>• <b>SeBackupPrivilege</b></li> <li>• <b>SeRestorePrivilege</b></li> <li>• <b>SeSecurityPrivilege</b></li> <li>• <b>SeTakeOwnershipPrivilege</b></li> <li>• <b>SeChangeNotifyPrivilege</b></li> </ul>

Predefined BUILTIN group	Default privileges
<b>BUILTIN\Power Users</b> RID 547 When first created, this group does not have any members. Members of this group have the following characteristics: <ul style="list-style-type: none"> <li>• Can create and manage local users and groups.</li> <li>• Cannot add themselves or any other object to the <b>BUILTIN\Administrators</b> group.</li> </ul>	<b>SeChangeNotifyPrivilege</b>
<b>BUILTIN\Backup Operators</b> RID 551 When first created, this group does not have any members. Members of this group can override read and write permissions on files or folders if they are opened with backup intent.	<ul style="list-style-type: none"> <li>• <b>SeBackupPrivilege</b></li> <li>• <b>SeRestorePrivilege</b></li> <li>• <b>SeChangeNotifyPrivilege</b></li> </ul>
<b>BUILTIN\Users</b> RID 545 When first created, this group does not have any members (besides the implied <b>Authenticated Users</b> special group). When the SVM is joined to a domain, the <b>domain\Domain Users</b> group is added to this group. If the SVM leaves the domain, the <b>domain\Domain Users</b> group is removed from this group.	<b>SeChangeNotifyPrivilege</b>
<b>Everyone</b> SID S-1-1-0 This group includes all users, including guests (but not anonymous users). This is an implied group with an implied membership.	<b>SeChangeNotifyPrivilege</b>

## Windows window

You can use the Windows window to maintain a list of local Windows users and groups for each Storage Virtual Machine (SVM) on the cluster. You can use the local Windows users and groups for authentication and name mappings.

- [Users tab](#) on page 322
- [Groups tab](#) on page 323

### Users tab

You can use the Users tab to view the Windows users that are local to an SVM.

### Command buttons

#### Create

Opens the Create User dialog box, which enables you to create a local Windows user account that can be used to authorize access to data contained in the SVM over an SMB connection.

**Edit**

Opens the Edit User dialog box, which enables you to edit local Windows user properties, such as group memberships and the full name. You can also enable or disable the user account.

**Delete**

Opens the Delete User dialog box, which enables you to delete a local Windows user account from an SVM if it is no longer required.

**Add to Group**

Opens the Add Groups dialog box, which enables you to assign group membership to a user account if you want the user to have privileges associated with that group.

**Set Password**

Opens the Reset Password dialog box, which enables you to reset the password of a Windows local user. For example, you might want to reset the password if the password is compromised or if the user has forgotten the password.

**Rename**

Opens the Rename User dialog box, which enables you to rename a local Windows user account to more easily identify it.

**Refresh**

Updates the information in the window.

**Users list****Name**

Displays the name of the local user.

**Full Name**

Displays the full name of the local user.

**Account Disabled**

Displays whether the local user account is enabled or disabled.

**Description**

Displays the description for this local user.

**Users Details Area****Group**

Displays the list of groups in which the user is a member.

**Groups tab**

You can use the Groups tab to add, edit, or delete Windows groups that are local to an SVM.

**Command buttons****Create**

Opens the Create Group dialog box, which enables you to create local Windows groups that can be used for authorizing access to data contained in SVMs over an SMB connection.

**Edit**

Opens the Edit Group dialog box, which enables you to edit the local Windows group properties, such as privileges assigned to the group and the description of the group.

**Delete**

Opens the Delete Group dialog box, which enables you to delete a local Windows group from an SVM if it is no longer required.

**Add Members**

Opens the Add Members dialog box, which enables you to add local or Active Directory users, or Active Directory groups to the local Windows group.

**Rename**

Opens the Rename Group dialog box, which enables you to rename a local Windows group to more easily identify it.

**Refresh**

Updates the information in the window.

**Groups list****Name**

Displays the name of the local group.

**Description**

Displays the description for this local group.

**Groups Details Area****Privileges**

Displays the list of privileges associated with the selected group.

**Users**

Displays the list of local users associated with the selected group.

**Related concepts**

[Using local users and groups for authentication and authorization](#) on page 319

**Related tasks**

[Creating a local Windows group](#) on page 310

[Editing local Windows group properties](#) on page 312

[Adding user accounts to a Windows local group](#) on page 312

[Renaming a local Windows group](#) on page 313

[Deleting a local Windows group](#) on page 314

[Creating a local Windows user account](#) on page 315

[Editing the local Windows user properties](#) on page 316

[Assigning group memberships to a user account](#) on page 316

[Renaming a local Windows user](#) on page 317

[Resetting the password of a Windows local user](#) on page 318

[Deleting a local Windows user account](#) on page 318

## Name mapping

You can use System Manager to specify name mapping entries to map users from different platforms.

## How name mappings are used

Data ONTAP uses name mapping to map CIFS identities to UNIX identities, Kerberos identities to UNIX identities, and UNIX identities to CIFS identities. It needs this information to obtain user credentials and provide proper file access regardless of whether they are connecting from an NFS client or a CIFS client.

Name mapping is usually required due to the multiprotocol nature of Data ONTAP, which supports CIFS and NFS client access to the same data. Data stored on Storage Virtual Machines (SVMs) with FlexVol volumes uses either UNIX- or NTFS-style permissions. To authorize a client, the credentials must match the security style. Consider the following scenarios:

If a CIFS client wants to access data with UNIX-style permissions, Data ONTAP cannot directly authorize the client because it cannot use CIFS credentials with UNIX-style permissions. To properly authorize the client request, Data ONTAP must first map the CIFS credentials to the appropriate UNIX credentials so that it can then use the UNIX credentials to compare them to the UNIX-style permissions.

If an NFS client wants to access data with NTFS-style permissions, Data ONTAP cannot directly authorize the client because it cannot use UNIX credentials with NTFS-style permissions. To properly authorize the client request, Data ONTAP must first map the UNIX credentials to the appropriate NTFS credentials so that it can then use the NTFS credentials to compare them to the NTFS-style permissions.

There are two exceptions where you do not have to use name mapping:

- You configure a pure UNIX environment and do not plan to use CIFS access or NTFS security style on volumes.  
In this scenario, name mapping is not required because Data ONTAP can use the UNIX credentials of the NFS clients to directly compare them to the UNIX-style permissions.
- You configure the default user to be used instead.  
In this scenario, name mapping is not required because instead of mapping every individual client credential all client credentials are mapped to the same default user.

Note that you can use name mapping only for users, not for groups. It is not possible to map CIFS users to a group ID (GID), or UNIX users to a group in the Active Directory (AD). Similarly, it is not possible to map a GID to a group or a user in AD, or an AD group to a UNIX UID or GID.

However, you can map a group of individual users to a specific user. For example, you can map all AD users that start or end with the word SALES to a specific UNIX user and to the user's UID. As a result, you can rename certain users in AD and use regular expressions to effectively emulate group actions. This type of mapping also works in reverse.

## How name mapping works

Data ONTAP goes through a number of steps when attempting to map user names. They include checking the local name mapping database and LDAP, trying the user name, and using the default user if configured. If the name mapping matches with the pattern but the replacement string is null, the mapping is explicitly denied to the user.

When Data ONTAP has to map credentials for a user, it first checks the local name mapping database and LDAP server for an existing mapping. Whether it checks one or both and in which order is determined by the name service configuration of the Storage Virtual Machine (SVM).

- For Windows to UNIX mapping  
If no mapping is found, Data ONTAP checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided that it is configured. If the default UNIX user is not configured and Data ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

- For UNIX to Windows mapping

If no mapping is found, Data ONTAP tries to find a Windows account that matches the UNIX name in the CIFS domain. If this does not work, it uses the default CIFS user, provided that it is configured. If the default CIFS user is not configured and Data ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

## Name mapping conversion rules

A Data ONTAP system keeps a set of conversion rules for each Storage Virtual Machine (SVM). Each rule consists of two pieces: a *pattern* and a *replacement*. Conversions start at the beginning of the appropriate list and perform a substitution based on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX `sed` program.

It is possible to allow NFS access to volumes with NTFS security style for users in a different domain from the one that the storage system belongs to, provided that the proper name mapping rule exists. If the name mapping matches with the pattern but the replacement string is null, the mapping is explicitly denied to the user.

If a user matches a rule to map to a user in a different domain, the domain must be trusted. For successful mapping to users in other domains for both SMB and NFS access, there must be a bidirectional trust relationship between the domains.

If a user matches a rule but the user cannot authenticate in the other domain because it is untrusted, the mapping fails.

The SVM automatically discovers all bidirectional trusted domains, which are used for multi-domain user mapping searches. Alternatively, you can configure a list of preferred trusted domains that are used for name mapping searches instead of the list of automatically discovered trusted domains.

Regular expressions are not case-sensitive when mapping from Windows to UNIX. However, they are case-sensitive for Kerberos-to-UNIX and UNIX-to-Windows mappings.

As an example, the following rule converts the Windows user named “jones” in the domain named “ENG” into the UNIX user named “jones”:

Pattern	Replacement
ENG\\jones	jones

Note that the backslash is a special character in regular expressions and must be escaped with another backslash.

The caret (^), underscore (\_), and ampersand (&) characters can be used as prefixes for digits in replacement patterns. These characters specify uppercase, lowercase, and initial-case transformations, respectively. For instance:

- If the initial pattern is `(.+)` and the replacement pattern is `\1`, then the string `jOe` is mapped to `jOe` (no change).
- If the initial pattern is `(.+)` and the replacement pattern is `\_1`, then the string `jOe` is mapped to `joe`.
- If the initial pattern is `(.+)` and the replacement pattern is `\^1`, then the string `jOe` is mapped to `JOE`.
- If the initial pattern is `(.+)` and the replacement pattern is `\&1`, then the string `jOe` is mapped to `Joe`.

If the character following a backslash-underscore (`\_`), backslash-caret (`\^`), or backslash-ampersand (`\&`) sequence is not a digit, then the character following the backslash is used verbatim.

The following example converts any Windows user in the domain named “ENG” into a UNIX user with the same name in NIS:

Pattern	Replacement
ENG\\(.+)	\1

The double backslash (\\) matches a single backslash. The parentheses denote a subexpression but do not match any characters themselves. The period matches any single character. The asterisk matches zero or more of the previous expression. In this example, you are matching ENG\ followed by one or more of any character. In the replacement, \1 refers to whatever the first subexpression matched. Assuming the Windows user ENG\jones, the replacement evaluates to jones; that is, the portion of the name following ENG\.

**Notes:**

- If you are using the CLI, you must delimit all regular expressions with double quotation marks (").  
For instance, to enter the regular expression (.)+ in the CLI, type "(.)+" at the command prompt. Quotation marks are not required in the Web UI.
- If you create a name mapping with the pattern ENG\\John\$, then the user mapping fails to match the Windows account named "ENG\\John\$".  
That is because the pattern is a UNIX regular expression, and "\$" is a pattern that matches the end of a string. In this case, a literal dollar sign (\$) should match, so the pattern should escape the \$ by prefixing it with a backslash (\); in this example, ENG\\John\$. Any verbatim name mapping pattern, which has a special meaning in a regular expression, must have an escape sequence (\).

For further information about regular expressions, see your UNIX system administration documentation, the online UNIX documentation for *sed* or *regex*, or *Mastering Regular Expressions*, published by O'Reilly and Associates.

## How group mapping supports multiprotocol access to Infinite Volumes

Group mapping improves the accuracy of permissions that appear when NFSv4.1 clients display the ACL of a file or directory that has NTFS file permissions. If an Infinite Volume supports both NFSv4.1 ACLs and SMB, you should configure group mapping, which is similar to user mapping.

### Why group mapping is necessary

Groups are often used in ACLs to simplify security management. However, groups in multiple Windows domains cannot be easily translated to the groups of a single NFSv4.1 domain.

Mapping groups from Windows to UNIX ensures that group names appear when NFSv4.1 ACLs are displayed on NFSv4.1 clients.

If a Windows group is not mapped to a UNIX group and a default UNIX group is not configured, the Windows group is displayed to an NFSv4.1 client as nobody (specifically `nobody@v4-id-domain`).

### What group mapping is required

If an Infinite Volume supports both SMB and NFSv4.1 ACLs, you should perform the following configurations:

- Create a Windows-to-UNIX mapping for every Windows group.
- Define a default UNIX group that is used when no mapping exists for a Windows group and the lowercase name of the Windows group is not a valid group name in the UNIX domain.

### Comparison of user and group mapping

Group mapping and user mapping share the following similarities:

- They can both be defined either using Data ONTAP or using LDAP.
- If they are defined using Data ONTAP, they are defined in a similar way and using the same conversion rules.  
For information about conversion rules in user and group mappings, see either the *NFS Reference* or the *CIFS Reference*.

Group mapping is unique in the following ways:

- It is available only on Storage Virtual Machines (SVMs) with Infinite Volume, not SVMs with FlexVol volumes.
- It is necessary only if an SVM is configured for both SMB and NFSv4.1, including NFSv4.1 ACLs.
- It does not affect access; it affects only what NFSv4.1 clients display.  
During access checks, a user's group membership is determined in the same way on all SVMs.
- It is necessary only in one direction—from Windows to UNIX.  
UNIX groups do not have to be mapped to Windows groups.

## Name Mapping window

You can use the Name Mapping window to specify the name mapping entries to map users from different platforms. If an Infinite Volume supports both NFSv4.1 ACLs and SMB, you can also configure group mappings.

### Name Mappings

You can create and use name mappings to map your UNIX users to Windows users, Windows users to UNIX users, or Kerberos users to UNIX users.

### Command buttons

#### Add

Opens the Add Name Mapping Entry dialog box, which enables you to create a name mapping on Storage Virtual Machines (SVMs).

#### Edit

Opens the Edit Name Mapping Entry dialog box, which enables you to edit a name mapping on SVMs.

#### Delete

Opens the Delete Name Mapping Entries dialog box, which enables you to delete a name mapping entry.

#### Swap

Opens the Swap Name Mapping Entries dialog box, which enables you to interchange positions of the two selected name mapping entries.

#### Refresh

Updates the information in the window.

### Name mappings list

#### Position

Specifies the name mapping's position in the priority list. Name mappings are applied in the order in which they occur in the priority list.

#### Pattern

Specifies the user name pattern that must be matched.



**Replacement**

Specifies the replacement pattern for the user name.

**Direction**

Specifies the direction of the name mapping. Possible values are `krb_unix` for a Kerberos-to-UNIX name mapping, `win_unix` for a Windows-to-UNIX name mapping, and `unix_win` for a UNIX-to-Windows name mapping.

**Group Mappings**

If an Infinite Volume supports both NFSv4.1 ACLs and SMB, you can create and use group mappings to map your UNIX groups to Windows groups, Windows groups to UNIX groups, or Kerberos groups to UNIX groups.

**Command buttons****Add**

Opens the Add Group Mapping Entry dialog box, which enables you to create a group mapping on SVMs.

**Edit**

Opens the Edit Group Mapping Entry dialog box, which enables you to edit the group mapping on SVMs.

**Delete**

Opens the Delete Group Mapping Entries dialog box, which enables you to delete a group mapping entry.

**Swap**

Opens the Swap Group Mapping Entries dialog box, which enables you to interchange positions of the two selected group mapping entries.

**Refresh**

Updates the information in the window.

**Group mappings list****Position**

Specifies the group mapping's position in the priority list. Group mappings are applied in the order in which they occur in the priority list.

**Pattern**

Specifies the user name pattern that must be matched.

**Replacement**

Specifies the replacement pattern for the user names.

**Direction**

Specifies the direction of the group mapping. Possible values are `krb_unix` for a Kerberos-to-UNIX group mapping, `win_unix` for a Windows-to-UNIX group mapping, and `unix_win` for a UNIX-to-Windows group mapping.

## Managing data protection

---

You can use System Manager to protect your data by creating and managing mirror relationships, vault relationships, and mirror and vault relationships. You can also create and manage the Snapshot policies and schedules.

### Mirror relationships

You can use System Manager to create and manage mirror relationships by using the mirror policy.

#### Creating a mirror relationship from a destination SVM

You can use System Manager to create a mirror relationship from the destination Storage Virtual Machine (SVM), and to assign a policy and schedule to the mirror relationship. The mirror copy enables quick availability of data if the data on the source volume is corrupted or lost.

##### Before you begin

- The source cluster must be running ONTAP 8.2.2 or later.
- The SnapMirror license must be enabled on the source cluster and the destination cluster.
- While mirroring a volume, if you create a SnapLock volume, then the SnapMirror and SnapLock licenses must be installed on both the source cluster and destination cluster.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination aggregate must have free space available .
- A source volume of type read/write (rw) must exist.
- If the destination volume exists, the capacity of the destination volume must be greater than or equal to the capacity of the source volume.
- If the destination volume exists, the volume must not be the destination for any other mirror relationship.
- The destination volume must not be the root volume of a storage system.
- For Infinite Volumes, the destination SVM must not contain a read/write Infinite Volume or an Infinite Volume with storage classes.
- If the source Infinite Volume and destination Infinite Volume share aggregates with other Infinite Volumes or FlexVol volumes in the same cluster, sufficient shared aggregate space must be available for the destination Infinite Volume.  
If the source Infinite Volume and destination Infinite Volume do not share aggregates with other Infinite Volumes or FlexVol volumes in the same cluster, you can create the same number and size of aggregates for the destination volume as those used by the source volume.

##### About this task

- You cannot use System Manager to create a SnapMirror relationship if the source volume is an Infinite Volume with storage classes.  
Instead, you should use OnCommand Workflow Automation.
- System Manager does not support a cascade relationship.

For example, a destination volume in a relationship cannot be the source volume in another relationship.

- You cannot create a mirror relationship between a sync-source SVM and a sync-destination SVM in a MetroCluster configuration.
- You can create a mirror relationship between sync-source SVMs in a MetroCluster configuration.
- You can create a mirror relationship from a volume on a sync-source SVM to a volume on a data-serving SVM.
- You can create a mirror relationship from a volume on a data-serving SVM to a data protection (DP) volume on a sync-source SVM.
- You can create a mirror relationship between SnapLock volumes of the same type only.  
For example, if the source volume is a SnapLock Enterprise volume, then the destination volume must also be a SnapLock Enterprise volume.
- You can use System Manager to only view the FlexGroup volume relationships.

### Steps

1. Click **Protection > Relationships**.
2. In the **Relationships** window, click **Create**.
3. In the **Browse SVM** dialog box, select an SVM for the destination volume.
4. In the **Create Protection Relationship** dialog box, select **Mirror** from the **Relationship Type** drop-down list.
5. Optional: Select the **Create version-flexible mirror relationship** check box to create a mirror relationship that is independent of the ONTAP version running on the source and destination clusters, and to back up the Snapshot copies from the source volume.  
If you select this option, the SnapLock volumes will not be displayed.
6. Specify the cluster, the SVM, and the source volume.
7. If the selected SVM is not peered, use the **Authenticate** link to enter the credentials of the remote cluster and create the SVM peer relationship.  
If the names of the local SVM and remote SVM are identical, or if the local SVM is already in a peer relationship with another remote SVM of the same name, or if the local SVM contains a data SVM of the same name, the Enter Alias Name for SVM dialog box is displayed.
8. Optional: Enter an alias name for the remote SVM in the **Enter Alias Name for SVM** dialog box.
9. For FlexVol volumes, create a new destination volume or select an existing volume:

If you want to...	Do the following...
Create a new volume	<ul style="list-style-type: none"> <li>• If you want to change the default name, which is displayed in the format <i>source_SVM_name_source_volume_name_mirror</i>, specify a new name, and select the containing aggregate for the destination volume.</li> <li>• Select <b>Default</b>, <b>Thin provisioned</b> or <b>Thick provisioned</b> for the volume.</li> </ul> <p><b>Note:</b> For AFF storage systems, thin provisioning is default, and for other storage systems, thick provisioning is default.</p>

If you want to...	Do the following...
Select an existing volume	Select the <b>Select Volume</b> option.  Only those volumes with the same language attribute as that of the source volume are listed.

For Infinite Volumes, you can create a destination volume only if the destination SVM does not contain a volume.

**10.** Select an existing policy or create a new policy:

If you want to...	Do the following...
Select an existing policy	Select a mirror policy from the list.
Create a new policy	<ol style="list-style-type: none"> <li>Click <b>Create Policy</b>.</li> <li>Specify a policy name, and set the schedule transfer priority. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to normal.</li> <li>Select the <b>Transfer All Source Snapshot Copies</b> check box to include the “all_source_snapshots” rule to the mirror policy, which will enable you to back up all the Snapshot copies from the source volume.</li> <li>Select the <b>Enable Network Compression</b> check box to compress the data that is being transferred.</li> <li>Click <b>Create</b>.</li> </ol>

**11.** Specify a schedule for the relationship:

If...	Do the following...
You want to assign an existing schedule	From the list of schedules, select an existing schedule.
You want to create a new schedule	<ol style="list-style-type: none"> <li>Click <b>Create Schedule</b>.</li> <li>Specify a name for the schedule.</li> <li>Select <b>Basic</b> or <b>Advanced</b>. <ul style="list-style-type: none"> <li>Basic: You can select this option to specify only the day of the week, time, and the transfer interval.</li> <li>Advanced: You can select this option to specify a cron-style schedule.</li> </ul> </li> <li>Click <b>Create</b>.</li> </ol>
You do not want to assign a schedule	Select <b>None</b> .

**12.** Optional: Select **Initialize Relationship** to initialize the mirror relationship.

**13.** Click **Create**.

**Result**

If you chose to create a new destination volume, then a new destination volume of type *dp* is created, with the language attribute set to match the language attribute of the source volume.

A mirror relationship is created between the source volume and the destination volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.

#### Related references

[Protection window](#) on page 364

## Deleting mirror relationships

You can delete a mirror relationship and permanently end the mirror relationship between the source and destination volumes. When a mirror relationship is deleted, the base Snapshot copy on the source volume is deleted.

#### About this task

It is a best practice to break the mirror relationship before deleting the relationship.

#### Steps

1. Click **Protection > Relationships**.
2. Select the mirror relationship that you want to delete and click **Delete**.
3. Select the confirmation check boxes to delete the mirror relationship and to release the base Snapshot copies, and then click **Delete**.
4. Optional: If you are deleting mirror relationship between Infinite Volumes, click **Run in Background** to run the operation in the background.

#### Result

The relationship is deleted and the base Snapshot copy on the source volume is deleted.

#### Related references

[Protection window](#) on page 364

## Editing mirror relationships

You can use System Manager to edit a mirror relationship either by selecting an existing policy or schedule in the cluster, or by creating a new policy or schedule. However, you cannot edit the parameters of an existing policy or schedule.

#### About this task

- You cannot edit a mirror relationship created between a volume in Data ONTAP 8.2.1 and a volume in Data ONTAP 8.3 or later.
- You can modify the relationship type of a version-flexible mirror relationship, vault relationship, or mirror and vault relationship by modifying the policy type.

#### Steps

1. Click **Protection > Relationships**.
2. Select the mirror relationship for which you want to modify the policy or schedule, and then click **Edit**.
3. In the **Edit Relationship** dialog box, select an existing policy or create a new policy:

If you want to...	Do the following...
Select an existing policy	Click <b>Browse</b> , and then select an existing policy.
Create a new policy	<ol style="list-style-type: none"> <li>Click <b>Create Policy</b>.</li> <li>Specify a name for the policy.</li> <li>Set the priority for scheduled transfers. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to Normal.</li> <li>Select the <b>Transfer All Source Snapshot Copies</b> check box to include the “all_source_snapshots” rule to the mirror policy, which enables you to back up all the Snapshot copies from the source volume.</li> <li>Select the <b>Enable Network Compression</b> check box to compress the data that is being transferred.</li> <li>Click <b>Create</b>.</li> </ol>

4. Specify a schedule for the relationship:

If...	Do the following...
You want to assign an existing schedule	From the list of schedules, select an existing schedule.
You want to create a new schedule	<ol style="list-style-type: none"> <li>Click <b>Create Schedule</b>.</li> <li>Specify a name for the schedule.</li> <li>Select either <b>Basic</b> or <b>Advanced</b>: <ul style="list-style-type: none"> <li>Basic specifies only the day of the week, time, and the transfer interval.</li> <li>Advanced creates a cron-style schedule.</li> </ul> </li> <li>Click <b>Create</b>.</li> </ol>
You do not want to assign a schedule	Select <b>None</b> .

5. Click **OK** to save the changes.

#### Related references

[Protection window](#) on page 364

## Initializing mirror relationships

When you start a mirror relationship for the first time, you have to initialize the relationship. Initializing a relationship consists of a complete baseline transfer of data from the source volume to the destination. You can use System Manager to initialize a mirror relationship if you have not already initialized the relationship while creating it.

#### About this task

You cannot initialize a mirror relationship if the Infinite Volume has storage classes.

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror relationship that you want to initialize.
3. Click **Operations > Initialize**.
4. Select the confirmation check box and click **Initialize**.
5. Optional: If you are initializing a mirror relationship between Infinite Volumes, click **Run in Background** to run the operation in the background.
6. Verify the status of the mirror relationship in the **Protection** window.

### Result

A Snapshot copy is created and transferred to the destination. This Snapshot copy is used as a baseline for subsequent incremental Snapshot copies.

### Related references

[Protection window](#) on page 364

## Updating mirror relationships

You can initiate an unscheduled mirror update of the destination. You might have to perform a manual update to prevent data loss due to an upcoming power outage, scheduled maintenance, or data migration.

### Before you begin

The mirror relationship must be in a Snapmirrored state.

### About this task

For Infinite Volumes with storage classes, if new constituents have been added to the source Infinite Volume since the mirror relationship was created, you cannot use to update the destination Infinite Volume.

Instead, you should use OnCommand Workflow Automation.

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror relationship for which you want to update the data, and click **Operations > Update**.
3. Choose one of the following options:
  - Select **On demand** to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
  - Select **Select Snapshot copy** and specify the Snapshot copy that you want to transfer.
4. Optional: Select **Limit transfer bandwidth to** to limit the network bandwidth used for transfers and specify the maximum transfer speed.
5. Click **Update**.
6. Optional: If you are initiating data transfers on an Infinite Volume, click **Run in Background** to run the operation in the background.

It takes longer to update an Infinite Volume than a FlexVol volume.

7. Verify the transfer status in the **Details** tab.

#### Related references

[Protection window](#) on page 364

## Quiescing mirror relationships

Use System Manager to quiesce a mirror destination to stabilize the destination before creating a Snapshot copy. The quiesce operation enables active mirror transfers to finish and disables future transfers for the mirroring relationship.

#### About this task

You can quiesce only mirror relationships that are in the Snapmirrored state.

#### Steps

1. Click **Protection > Relationships**.
2. Select the mirror relationship that you want to quiesce.
3. Click **Operations > Quiesce**.
4. Select the confirmation check box and click **Quiesce**.
5. Optional: If you are quiescing data transfers on an Infinite Volume, click **Run in Background** to run the operation in the background.

It takes longer to quiesce data transfers of an Infinite Volume than of a FlexVol volume.

#### Related references

[Protection window](#) on page 364

## Resuming mirror relationships

You can resume a quiesced mirror relationship. When you resume the relationship, normal data transfer to the mirror destination is resumed and all the mirror activities are restarted.

#### About this task

If you have quiesced a broken mirror relationship from the command-line interface (CLI), you cannot resume the relationship from System Manager. You must use the CLI to resume the relationship.

#### Steps

1. Click **Protection > Relationships**.
2. Select the mirror relationship that you want to resume.
3. Click **Operations > Resume**.
4. Select the confirmation check box and click **Resume**.
5. Optional: If you are resuming data transfer on an Infinite Volume, click **Run in Background** to run the operation in the background.

It takes longer to resume data transfer of an Infinite Volume than of a FlexVol volume.



**Result**

Data transfer to the mirror destination is resumed for the selected mirror relationship.

**Related references**

[Protection window](#) on page 364

**Breaking SnapMirror relationships**

You must break the mirror relationship if a mirror source becomes unavailable and you want client applications to be able to access the data from the mirror destination. After the mirror relationship is broken, the destination volume type changes from DP to RW.

**Before you begin**

- The SnapMirror destination must be in the quiesced or idle state.
- The destination volume must be already mounted on the destination Storage Virtual Machine (SVM) namespace.

**About this task**

You can use the destination volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.

**Steps**

1. Click **Protection > Relationships**.
2. Select the mirror relationship that you want to break.
3. Click **Operations > Break**.
4. Select the confirmation check box and click **Break**.

**Result**

The data protection SnapMirror relationship is broken. The destination volume type changes from data protection (DP) read-only to read/write. The system stores the base Snapshot copy for the data protection mirror relationship for later use.

For Infinite Volumes, a new mirror is created on the volume if the namespace mirror constituent does not already exist. The namespace mirror constituent is required on the destination volume to provide data protection to the namespace constituent.

**Related references**

[Protection window](#) on page 364

**Resynchronizing mirror relationships**

You can reestablish a mirror relationship that was broken earlier. You can perform a resynchronization operation to recover from a disaster that disabled the source volume. For Infinite Volumes, the resynchronization operation recovers the volume and its constituents.

**Before you begin**

The source and destination clusters and the source and destination Storage Virtual Machines (SVMs) must be in peer relationships.

**About this task**

- When you perform a resynchronization operation, the contents on the mirror destination are overwritten by the contents on the source.  
**Attention:** The resynchronization operation can cause loss of newer data written to the destination volume after the base Snapshot copy was created.
- If the Last Transfer Error field in the Protection window recommends a resynchronization operation, you must first break the relationship and then perform the resynchronization operation.
- For Infinite Volumes with storage classes, if new constituents have been added to the source Infinite Volume since the mirror relationship was created, you cannot use System Manager to resynchronize the mirror relationship.  
Instead, you should use OnCommand Workflow Automation.

**Steps**

1. Click **Protection > Relationships**.
2. Select the mirror relationship that you want to resynchronize.
3. Click **Operations > Resync**.
4. Select the confirmation check box and click **Resync**.
5. Optional: If you are resynchronizing a mirror relationship between Infinite Volumes, click **Run in Background** to run the operation in the background.

**Related references**

[Protection window](#) on page 364

**Reverse resynchronizing mirror relationships**

You can use System Manager to reestablish a mirror relationship that was previously broken. In a reverse resynchronization operation, you reverse the functions of the source and destination.

**Before you begin**

The source volume must be online.

**About this task**

- You can use the destination volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.
- When you perform reverse resynchronization, the contents on the mirror source are overwritten by the contents on the destination.  
**Attention:** This operation can cause data loss on the source.
- When you perform reverse resynchronization, the mirror policy of the relationship is set to DPDefault and the mirror schedule is set to None.
- You cannot use System Manager to perform a reverse resynchronization operation in the following scenarios:
  - For Infinite Volumes with storage classes, if new constituents have been added to the source Infinite Volume since the mirror relationship was created.  
You should use OnCommand Workflow Automation instead.

- For a mirror relationship between Infinite Volumes, if the cluster peer relationship is in an unhealthy state.  
You should use the command-line interface (CLI) instead.

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror relationship that you want to reverse.
3. Click **Operations > Reverse Resync**.
4. Select the confirmation check box, and click **Reverse Resync**.
5. Optional: If you are reverse resynchronizing a mirror relationship between Infinite Volumes, click **Run in Background** to run the operation in the background.

### Related references

[Protection window](#) on page 364

## Aborting a mirror transfer

You can abort a volume replication operation before the data transfer is complete. You can abort a scheduled update, a manual update, or an initial data transfer.

### Steps

1. Click **Protection > Relationships**.
2. Select the relationship for which you want to stop the data transfer, and click **Operations > Abort**.
3. Select the **Yes, I want to abort the transfer** check box to confirm the operation.
4. Optional: Select the **Keep any partially transferred data** check box to retain the data that is already transferred to the destination volume.
5. Click **Abort**.
6. Optional: If you are aborting data transfers on an Infinite Volume, click **Run in Background** to run the operation in the background.

It takes longer to abort data transfers of Infinite Volumes than of a FlexVol volume.

The transfer status is displayed as “Aborting” until the operation is complete and displayed as “Idle” after the operation is complete.

### Related references

[Protection window](#) on page 364

## Restoring a volume in a mirror relationship

For a version-independent mirror relationship, you can use System Manager to restore Snapshot copies to a source volume or other volumes if the source data is corrupted and is no longer usable. You can replace the original data with the Snapshot copies in the destination volume.

### Before you begin

- The SnapMirror license must be enabled on both the source and the destination clusters or the nodes that contain the source and destination volumes.

- The source and destination clusters must be in a healthy peer relationship.
- The source aggregate or any other aggregate that you select for the restore operation must be a 64-bit aggregate.

#### About this task

- You cannot restore a volume that is in a mirror relationship between a source Storage Virtual Machine (SVM) and a destination SVM in a MetroCluster configuration.
- You can restore a mirror relationship between sync-source SVMs in a MetroCluster configuration.
- You can restore a mirror relationship from a volume on a sync-source SVM to a default SVM.
- You can restore a mirror relationship from a volume on a default SVM to a DP volume on a sync-source SVM.

#### Steps

1. Click **Protection > Relationships**.
2. Select the mirror relationship, and then click **Operations > Restore**.
3. In the **Restore** dialog box, restore the data to the source volume in the mirror relationship or select any other volume:

If you want to restore to...	Do the following...
The source volume	<ol style="list-style-type: none"> <li>a. Select <b>Source volume</b>.</li> <li>b. Go to Step 7.</li> </ol>
Any other volume	Select <b>Other volume</b> , and then select the cluster and SVM from the list.

4. Restore the data to a new volume or to an existing volume:

If you want to restore to...	Do the following...
A new volume	If you want to change the default name, displayed in the format <i>destination_SVM_name_destination_volume_name_</i> restore, specify a new name, and then select the containing aggregate for the volume.
An existing volume	<p>Select the <b>Select Volume</b> option.</p> <p>You must select a volume other than the source volume, or a read/write volume with some data in it and with a common Snapshot copy.</p> <p>Only those volumes with the same language attribute as the source volume are listed.</p>

5. Select the latest Snapshot copy or select the specific Snapshot copy that you want to restore.
6. Select the confirmation check box to restore the volume from the Snapshot copy.
7. Optional: Select the **Enable Network Compression** check box to compress the data that is being transferred during the restore operation.
8. Click **Restore**.

## Components of a mirror relationship

In its simplest configuration, a mirror relationship is between a source volume and a destination volume and data is replicated to the destination volume using Snapshot copies.

Typically, the source volume is a read-write volume that clients can access and modify. The destination volume is a read-only volume that exports a Snapshot copy to clients for read-only access. The only time the source volume is not a read-write volume is in a cascade configuration where the source volume is a destination of one mirror relationship and the source of another mirror relationship.

Snapshot copies are used by the source volume to update destination volumes. Snapshot copies are transferred from the source volume to the destination volume using an automated schedule or manually; therefore, mirror copies are updated asynchronously.

## How SnapMirror works

You can create a data protection mirror relationship to a destination within a cluster to protect your data. For greater disaster protection, you can also create a mirror relationship to a destination in a different cluster in a different location.

A data protection mirror configuration consists of a source volume that can be replicated to one or more destination volumes. Each data protection mirror relationship is independent from the other.

**Note:** The destination volume must be running the same Data ONTAP version as or a later version than the source volume.

Snapshot copies are used to update destination volumes. Snapshot copies are transferred from the source volume to the destination volume by using an automated schedule or manually; therefore, mirrors are updated asynchronously.

You can create data protection mirror relationships to destinations on the same aggregate as the source volume, and on the same Storage Virtual Machine (SVM) or on a different SVM. For greater protection, you can create the relationships to destinations on a different aggregate, which enables you to recover from any failure of the source volume's aggregate. However, these two configurations do not protect against a cluster failure.

To protect against a cluster failure, you can create a data protection mirror relationship in which the source volume is on one cluster and the destination volume is on a different cluster. If the cluster on which the source volume resides experiences a disaster, you can direct user clients to the destination volume on the cluster peer until the source volume is available again.

## Uses for data protection mirror copies

You can create data protection mirror copies to back up data for archiving, recover data when disasters occur, and distribute data to various sites.

## Providing disaster recovery on Infinite Volumes using mirroring technology

Stored data is susceptible to disaster, either through hardware failure or environmental catastrophe. You can use mirroring technology on Infinite Volumes to create an identical second set of data to replace the primary set of data, in case something happens to the primary set of data.

You can create a data protection mirror relationship from a source Infinite Volume on one cluster to a destination Infinite Volume on a different cluster to provide asynchronous disaster recovery. Infinite Volumes support bidirectional data exchange between two sites and multiple-mirror fanout deployments.

You cannot create a data protection mirror relationship between two Infinite Volumes on the same cluster, and you cannot create a data protection mirror relationship between a FlexVol volume and an Infinite Volume.

## Vault relationships

You can use System Manager to create and manage vault relationships by using the vault policy.

### Creating a vault relationship from a destination SVM

You can use System Manager to create a vault relationship from the destination Storage Virtual Machine (SVM), and to assign a vault policy to create a backup vault. In the event of data loss or corruption on a system, backed-up data can be restored from the backup vault destination.

#### Before you begin

- The source cluster must be running ONTAP 8.2.2 or later.
- The SnapVault license or SnapMirror license must be enabled on both the source cluster and the destination cluster.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination aggregate must have available space.
- The source aggregate and the destination aggregate must be 64-bit aggregates.
- A vault (XDP) policy must exist.  
If a vault policy does not exist, you must create one or accept the default vault policy (XDPEndpoint) that is automatically assigned.
- The capacity of the destination volume must be greater than or equal to the capacity of the source volume.
- If autogrow is disabled, the free space on the destination volume must be at least five percent more than the used space on the source volume.

#### About this task

- System Manager does not support a cascade relationship.  
For example, a destination volume in a relationship cannot be the source volume in another relationship.
- You cannot create a vault relationship between a sync-source SVM and a sync-destination SVM in a MetroCluster configuration.
- You can create a vault relationship between sync-source SVMs in a MetroCluster configuration.
- You can create a vault relationship from a volume on a sync-source SVM to a volume on a data-serving SVM.
- You can create a vault relationship from a volume on a data-serving SVM to a data protection (DP) volume on a sync-source SVM.
- You can create a vault relationship only between a non-SnapLock (primary) volume and a Snaplock destination (secondary) volume.
- You can use System Manager to only view the FlexGroup volume relationships.

## Steps

1. Click **Protection > Relationships**.
2. In the **Relationships** window, click **Create**.
3. In the **Browse SVM** dialog box, select an SVM for the destination volume.
4. In the **Create Protection Relationship** dialog box, select **Vault** from the **Relationship Type** drop-down list.
5. Specify the cluster, the SVM, and the source volume.
6. If the selected SVM is not peered, use the **Authenticate** link to enter the credentials of the remote cluster, and create an SVM peer relationship.

If the name of the local SVM and remote SVM are identical, or if the local SVM is in a peer relationship with another remote SVM of the same name, or if the local SVM contains a data SVM of the same name, the Enter Alias Name for SVM dialog box is displayed.

7. Optional: Enter an alias name for the remote SVM in the **Enter Alias Name for SVM** dialog box.
8. Create a new destination volume or select an existing volume:

If you want to...	Do the following...
Create a new volume	<ol style="list-style-type: none"> <li>a. If you want to change the default name, which is displayed in the format <i>source_SVM_name_source_volume_name_vault</i>, specify a new name, and select the containing aggregate for the destination volume.</li> <li>b. Select <b>Enable dedupe</b> to enable deduplication on the new destination volume. If deduplication is disabled on the source volume, then the check box for the new volume is selected by default.</li> </ol>
Select an existing volume	Select the <b>Select Volume</b> option.  <b>Note:</b> Only those volumes with the same language attribute as that of the source volume are listed.

9. If you are creating a SnapLock volume, specify the default retention period.  
The default retention period can be set to any value between 1 day through 70 years or Infinite.
10. Select an existing policy or create a new policy:

If you want to...	Do the following...
Select an existing policy	Select a vault policy from the list.  You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.

If you want to...	Do the following...
Create a new policy	<ol style="list-style-type: none"> <li>a. Click <b>Create Policy</b>.</li> <li>b. Specify a policy name, and set the schedule transfer priority. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to normal.</li> <li>c. Select the <b>Enable Network Compression</b> check box to compress the data that is being transferred.</li> <li>d. Click <b>Create</b>.</li> </ol> <p>You can also specify the SnapMirror label and destination retention count for the vault policy. For the new SnapMirror label to be effective, you must ensure that a Snapshot copy with the same label is created on the source volume.</p>

**11. Specify a schedule for the relationship:**

If...	Do the following...
You want to assign an existing schedule	From the list of schedules, select an existing schedule.
You want to create a new schedule	<ol style="list-style-type: none"> <li>a. Click <b>Create Schedule</b>.</li> <li>b. Specify a name for the schedule.</li> <li>c. Select <b>Basic</b> or <b>Advanced</b>. <ul style="list-style-type: none"> <li>• Basic: You can select this option to specify only the day of the week, time, and the transfer interval.</li> <li>• Advanced: You can select this option to specify a cron-style schedule.</li> </ul> </li> <li>d. Click <b>Create</b>.</li> </ol>
You do not want to assign a schedule	Select <b>None</b> .

**12. Optional: Select **Initialize Relationship** to initialize the vault relationship.**

**13. Click **Create**.**

**Result**

If you chose to create a new destination volume, a volume of type *dp* is created with the following default settings:

- Autogrow is enabled.
- Deduplication is enabled or disabled according to the user preference, or the source volume deduplication setting.
- Compression is disabled.
- The language attribute is set to match the language attribute of the source volume.

A vault relationship is created between the destination volume and the source volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.



**Related references**

[Protection window](#) on page 364

**Deleting vault relationships**

You can use System Manager to end a vault relationship between a source and destination volume, and release the Snapshot copies from the source.

**About this task**

Releasing the relationship permanently removes the base Snapshot copies used by the vault relationship on the source volume. To re-create the vault relationship, you must run the resynchronization operation from the source volume by using the command-line interface (CLI).

**Steps**

1. Click **Protection > Relationships**.
2. Select the volume for which you want to delete the vault relationship, and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

You can also select the release base Snapshot copies check box to delete the base Snapshot copies used by the vault relationship on the source volume.

If the relationship is not released, then you must use the CLI to run the release operation on the source cluster to delete the base Snapshot copies that were created for the vault relationship from the source volume.

**Related references**

[Protection window](#) on page 364

**Editing vault relationships**

You can use System Manager to edit a vault relationship either by selecting an existing policy or schedule in the cluster, or by creating a new policy or schedule. However, you cannot edit the parameters of an existing policy or schedule.

**Before you begin**

The source and destination clusters must be in a healthy peer relationship.

**Steps**

1. Click **Protection > Relationships**.
2. Select the vault relationship for which you want to modify the policy or schedule, and then click **Edit**.
3. In the **Edit Relationship** dialog box, select the appropriate action:

If you want to...	Do the following...
Select an existing policy	Click <b>Browse</b> , and then select an existing policy.  You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.

If you want to...	Do the following...
Create a new policy	<ol style="list-style-type: none"> <li>a. Click <b>Create Policy</b>.</li> <li>b. Specify a name for the policy.</li> <li>c. Set the priority for scheduled transfers. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to Normal.</li> <li>d. Select the <b>Enable Network Compression</b> check box to compress the data that is being transferred.</li> <li>e. Specify a SnapMirror label and destination retention count for the vault policy. You must ensure that a Snapshot copy with the same label is created on the source volume for the new SnapMirror label to be effective.</li> <li>f. Click <b>Create</b>.</li> </ol>

4. Specify a schedule for the relationship:

If...	Do the following...
You want to assign an existing schedule	Select an existing schedule from the list.
You want to create a new schedule	<ol style="list-style-type: none"> <li>a. Click <b>Create Schedule</b>.</li> <li>b. Specify a name for the schedule.</li> <li>c. Select one of the following options: <ul style="list-style-type: none"> <li>• <b>Basic</b> You can select this option to specify only the day of the week, time, and the transfer interval.</li> <li>• <b>Advanced</b> You can select this option to specify a cron-style schedule.</li> </ul> </li> <li>d. Click <b>Create</b>.</li> </ol>
You do not want to assign a schedule	Select <b>None</b> .

5. Click **OK**.

**Related references**

[Protection window](#) on page 364

## Initializing a vault relationship

You can use System Manager to initialize a vault relationship if you have not already initialized it while creating the relationship. A baseline transfer of data is initiated from the source FlexVol volume to the destination FlexVol volume.

**Before you begin**

The source and destination clusters must be in a healthy peer relationship.

**Steps**

1. Click **Protection > Relationships**.
2. Select the relationship you want to initialize, and click **Operations > Initialize**.
3. In the **Initialize** window, click **Initialize**.

**Result**

A Snapshot copy is created and transferred to the destination.

This Snapshot copy is used as a baseline for subsequent incremental Snapshot copies.

**Related references**

[Protection window](#) on page 364

**Updating a vault relationship**

You can use System Manager to manually initiate an unscheduled incremental update. You might require a manual update to prevent data loss due to an upcoming power outage, scheduled maintenance, or data migration.

**Before you begin**

The vault relationship must be initialized.

**Steps**

1. Click **Protection > Relationships**.
2. Select the relationship for which you want to update the data, and click **Operations > Update**.
3. Choose one of the following options:
  - Select **As Per Policy** to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
  - Select **Select Snapshot copy** and specify the Snapshot copy that you want to transfer.
4. Optional: Select **Limit transfer bandwidth to** to limit the network bandwidth that is used for transfers and specify the maximum transfer speed.
5. Click **Update**.
6. Verify the transfer status in the **Details** tab.

**Related references**

[Protection window](#) on page 364

**Quiescing a vault relationship**

You can use System Manager to disable data transfers to the destination FlexVol volume by quiescing the vault relationship.

**Steps**

1. Click **Protection > Relationships**.
2. Select the relationship for which you want to stop the scheduled data transfers, and click **Operations > Quiesce**.

3. In the **Quiesce** window, click **Quiesce**.

#### Result

If there is no transfer in progress, the transfer status is displayed as Quiesced. If a transfer is in progress, the transfer is not affected, and the transfer status is displayed as Quiescing until the transfer is complete.

#### Related references

[Protection window](#) on page 364

## Resuming a vault relationship

You can resume a quiesced vault relationship by using System Manager. When you resume the relationship, normal data transfer to the destination FlexVol volume is resumed and all vault activities are restarted.

#### Steps

1. Click **Protection > Relationships**.
2. Select the relationship for which you want to resume the data transfer, and click **Operations > Resume**.
3. In the **Resume** window, click **Resume**.

#### Result

Normal data transfers are resumed. If there is a scheduled transfer for the relationship, the transfer is started from the next schedule.

#### Related references

[Protection window](#) on page 364

## Aborting a Snapshot copy transfer

You can use System Manager to abort or stop a data transfer that is currently in progress.

#### Steps

1. Click **Protection > Relationships**.
2. Select the relationship for which you want to stop the data transfer, and click **Operations > Abort**.
3. Select the **Yes, I want to abort the transfer** check box to confirm the operation.
4. Optional: Select the **Keep any partially transferred data** check box to retain the data that is already transferred to the destination volume.
5. Click **Abort**.

#### Result

The transfer status is displayed as “Aborting” until the operation is complete and displayed as “Idle” after the operation is complete.

## Related references

[Protection window](#) on page 364

## Restoring a volume in a vault relationship

You can use System Manager to restore Snapshot copies to a source or other volumes if the source data is corrupted and is no longer usable. You can replace the original data with the Snapshot copies in the destination volume.

### Before you begin

- The SnapMirror license must be enabled on both the source and the destination storage systems or the nodes that contain the source and destination volumes.
- The source and destination clusters must be in a healthy peer relationship.
- The source aggregate or the other aggregate that you select for the restore operation must be a 64-bit aggregate.

### About this task

- You cannot restore a volume that is in a vault relationship between a source Storage Virtual Machine (SVM) and a destination SVM in a MetroCluster configuration.
- You can restore a vault relationship between sync-source SVMs in a MetroCluster configuration.
- You can restore a vault relationship from a volume on a sync-source SVM to a default SVM.
- You can restore a vault relationship from a volume on a default SVM to a DP volume on a sync-source SVM.

### Steps

1. Click **Protection > Relationships**.
2. Select the vault relationship, and then click **Operations > Restore**.
3. In the **Restore** dialog box, restore the data to the source volume in the vault relationship or select any other volume:

If you want to restore to...	Do the following...
The source volume	<ol style="list-style-type: none"> <li>a. Select <b>Source volume</b>.</li> <li>b. Go to Step 6.</li> </ol>
Any other volume	Select <b>Other volume</b> , and select the cluster and SVM from the list.

4. Restore the data to a new volume or select any existing volume:

If you want to...	Do the following...
Create a new volume	If you want to change the default name, displayed in the format <i>destination_SVM_name_destination_volume_name_</i> restore, specify a new name and select the containing aggregate for the volume.

If you want to...	Do the following...
Select an existing volume	<p>Select the <b>Select Volume</b> option.</p> <p>You must select a volume other than the source volume, or a read/write volume with some data in it and with a common Snapshot copy.</p> <p>Only those volumes with the same language attribute as the source volume are listed.</p>

5. Select the latest Snapshot copy or select the specific Snapshot copy that you want to restore.
6. Select the confirmation check box to restore the volume from the Snapshot copy.
7. Optional: Select the **Enable Network Compression** check box to compress the data that is being transferred during the restore operation.
8. Click **Restore**.

#### Related references

[Protection window](#) on page 364

## What a SnapVault backup is

A SnapVault backup is a collection of Snapshot copies on a FlexVol volume that you can restore data from if the primary data is not usable. Snapshot copies are created based on a Snapshot policy. The SnapVault backup backs up Snapshot copies based on its schedule and SnapVault policy rules.

A SnapVault backup is a disk-to-disk backup solution that you can also use to offload tape backups. In the event of data loss or corruption on a system, backed-up data can be restored from the SnapVault secondary volume with less downtime and uncertainty than is associated with conventional tape backup and restore operations.

The following terms are used to describe SnapVault backups:

#### baseline transfer

An initial complete backup of a primary storage volume to a corresponding volume on the secondary system.

#### secondary volume

A volume to which data is backed up from a primary volume. Such a volume can be a secondary or tertiary (and onward) destination in a cascade or fanout backup configuration. The SnapVault secondary system maintains Snapshot copies for long-term storage and possible restore operations.

#### incremental transfer

A follow-up backup to the secondary system that contains only the changes to the primary data since the last transfer action.

#### SnapMirror label

An attribute that identifies Snapshot copies for the purpose of selection and retention in SnapVault backups. Each SnapVault policy configures the rules for selecting Snapshot copies on the primary volume and transferring the Snapshot copies that match a given SnapMirror label.

#### Snapshot copy

The backup images on the source volume that are created manually or automatically as scheduled by an assigned policy. Baseline Snapshot copies contain a copy of the entire source data being protected; subsequent Snapshot copies contain differential copies of the source data. Snapshot copies can be stored on the source volume or on a different destination volume in a different Storage Virtual Machine (SVM) or cluster.

Snapshot copies capture the state of volume data on each source system. For SnapVault and mirror relationships, this data is transferred to destination volumes.

### **primary volume**

A volume that contains data that is to be backed up. In cascade or fanout backup deployments, the primary volume is the volume that is backed up to a SnapVault backup, regardless of where in the chain the SnapVault source is. In a cascade chain configuration in which A has a mirror relationship to B and B has a SnapVault relationship to C, B serves as the source for the SnapVault backup even though it is a secondary destination in the chain.

### **SnapVault relationship**

A backup relationship, configured as a SnapVault relationship, between a primary volume and a secondary volume.

### **Related references**

[Protection window](#) on page 364

## **How a SnapVault backup works**

Backing up volumes to a SnapVault backup involves starting the baseline transfers, making scheduled incremental transfers, and restoring data upon request.

### **Baseline transfers**

In general, baseline transfers work as follows:

A baseline transfer occurs when you initialize the SnapVault relationship. When you do this, Data ONTAP creates a new Snapshot copy. Data ONTAP transfers the Snapshot copy from the primary volume to the secondary volume. This Snapshot copy is the baseline of the volume at the time of the transfer and is a complete transfer, not an incremental transfer. As a result, none of the other Snapshot copies on the primary volume are transferred as part of the initial SnapVault transfer, regardless of whether they match rules specified in the SnapVault policy.

### **Incremental transfers**

The source system creates incremental Snapshot copies of the source volume as specified by the Snapshot policy that is assigned to the primary volume. Each Snapshot copy for a specific volume contains a label that is used to identify it.

The SnapVault secondary system selects and retrieves specifically labeled incremental Snapshot copies, according to the rules that are configured for the SnapVault policy that is assigned to the SnapVault relationship. The Snapshot label is retained to identify the backup Snapshot copies.

Snapshot copies are retained in the SnapVault backup for as long as is needed to meet your data protection requirements. The SnapVault relationship does not configure a retention schedule, but the SnapVault policy does specify number of Snapshot copies to retain.

### **SnapVault backup updates**

At the end of each Snapshot copy transfer session, which can include transferring multiple Snapshot copies, the most recent incremental Snapshot copy in the SnapVault backup is used to establish a new common base between the primary and secondary volumes and is exported as the active file system.

### **Data restore**

If data needs to be restored to the primary volume or to a new volume, the SnapVault secondary transfers the specified data from the SnapVault backup.

## Which data gets backed up and restored from a SnapVault backup

You create SnapVault relationships to back up and restore volumes. You can select the Snapshot copies that the SnapVault relationship uses to backup and restore volumes.

The SnapVault operation backs up a specified volume on the primary system to the associated volume on the SnapVault secondary system. If necessary, data is restored from the SnapVault secondary volume back to the associated primary volume or to a different volume.

The Snapshot policy assigned to the source volume specifies when Snapshot copies are performed. The SnapVault policy assigned to the SnapVault relationship specifies which of the source volume Snapshot copies are replicated to the SnapVault backup.

If the destination volume is a FlexClone volume, the volume retains two more Snapshot copies than the number you configure in the policy. This occurs because the volume retains the FlexClone Snapshot copy and an exported Snapshot copy. For example, if your policy specifies to retain three Snapshot copies, five Snapshot copies are retained (three specified Snapshot copies, one FlexClone Snapshot copy, and one exported Snapshot copy).

In SAN environments, LUN identifiers are preserved on the SnapVault secondary volume.

The secondary system uses slightly more disk space and directories than the source system.

## How SnapVault backups work with data compression

SnapVault relationships preserve storage efficiency when replicating data from the source to the SnapVault secondary volume except when additional data compression is enabled.

If additional compression is enabled on the SnapVault secondary volume, storage efficiency is affected as follows:

- Storage efficiency is not preserved for data transfers between the primary and secondary volumes.
- You can return to replicating data while preserving storage efficiency by turning off additional data compression and then executing the `snapmirror update` command with the `-enable-storage-efficiency` parameter set to `true`.

## SnapVault backup limitations

When planning SnapVault relationships, you must keep in mind what is supported and what is not supported.

The following limitations apply to SnapVault backups:

- 32-bit aggregates are not supported.  
Clustered Data ONTAP systems do not support the SnapVault backup feature for volumes in 32-bit aggregates.
- A SnapVault secondary volume cannot be the secondary volume for multiple primary volumes.  
A volume can be the secondary for one SnapVault relationship only. However, that same volume can be the source for other relationships.
- SnapVault backups are not supported on Infinite Volumes.

## Guidelines for planning Snapshot copy schedule and retention for SnapVault backups

It is important to plan the Snapshot copy transfer schedule and retention for your SnapVault backups.

When planning SnapVault relationships, consider the following guidelines:



- Before you create a SnapVault policy, you should create a table to plan which Snapshot copies you want replicated to the SnapVault secondary volume and how many of each you want to keep. For example:
  - Hourly (periodically throughout the day)  
Does the data change often enough throughout the day to make it worthwhile to replicate a Snapshot copy every hour, every two hours, or every four hours?
  - Nightly  
Do you want to replicate a Snapshot copy every night or just workday nights?
  - Weekly  
How many weekly Snapshot copies is it useful to keep in the SnapVault secondary volume?
- The primary volume should have an assigned Snapshot policy that creates Snapshot copies at the intervals you need, and labels each Snapshot copy with the appropriate `snapmirror-label` attribute name.
- The SnapVault policy assigned to the SnapVault relationship should select the Snapshot copies you want from the primary volume, identified by the `snapmirror-label` attribute name, and specify how many Snapshot copies of each name you want to keep on the SnapVault secondary volume.

#### Sample transfer schedule and retention

<code>snapmirror-label</code> attribute value	Source volume: Snapshot copy schedule	Primary volume: Snapshot copies retained	SnapVault secondary volume: Snapshot copies retained
<b>weekly</b>	Every Saturday at 19:00	4	8
<b>nightly</b>	Every Monday through Friday at 19:00	10	60
<b>hourly</b>	Every hour from 07:00 through 18:00	11	120
Total	n/a	25	188

## Data protection for SVM namespace and root information

Backups to secondary volumes in SnapVault relationships between FlexVol volumes replicate only volume data, not the Storage Virtual Machine (SVM) namespace or root information.

SnapVault relationships replicate only volume data. If you want to back up an entire SVM to a SnapVault secondary volume, you must first create SnapVault relationships for every volume in the SVM.

To provide data protection of the SVM namespace information, you must manually create the namespace on the SnapVault secondary immediately after the first data transfer is completed for all of the volumes in the SVM and while the source SVM volumes are still active. When subsequent changes are made to the namespace on the source SVM, you must manually update the namespace on the destination SVM.

You cannot create the namespace for an SVM on a SnapVault secondary volume if only a subset of the SVM volumes are in a SnapVault relationship, or if only a subset of the SVM volumes have completed the first data transfer.

## Mirror and vault relationships

You can use System Manager to create and manage mirror and vault relationships by using the mirror and vault policy.

### Creating a mirror and vault relationship from a destination SVM

You can use System Manager to create a mirror and vault relationship from the destination Storage Virtual Machine (SVM). Creating this relationship enables you to better protect your data by periodically transferring data from the source volume to the destination volume. It also enables you to retain data for long periods by creating backups of the source volume.

#### Before you begin

- The destination cluster must be running ONTAP 8.3.2 or later.
- The SnapMirror license must be enabled on both the source cluster and destination cluster that contain the source volume and destination volume.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination aggregate must have available space.
- The source aggregate and destination aggregate must be 64-bit aggregates.
- A source volume of type read/write (rw) must already exist.
- If the destination volume exists, the capacity of the destination volume must be greater than or equal to the capacity of the source volume.
- The destination volume must not be the root volume of a storage system.
- If the destination volume exists, the volume must not be the destination for any other mirror relationship.
- If autogrow functionality is disabled, the free space on the destination volume must be at least five percent more than the used space on the source volume.

#### About this task

- System Manager does not support a cascade relationship.  
For example, a destination volume in a relationship cannot be the source volume in another relationship.
- You cannot create a mirror and vault relationship between a sync-source SVM and a sync-destination SVM in a MetroCluster configuration.
- You can create a mirror and vault relationship between sync-source SVMs in a MetroCluster configuration.
- You can create a mirror and vault relationship from a volume on a sync-source SVM to a volume of a data-serving SVM.
- You can create a mirror and vault relationship from a volume on a data-serving SVM to a DP volume on a sync-source SVM.
- The destination volume that is created for a mirror relationship is not thin provisioned.
- You can use System Manager to only view the FlexGroup volume relationships.

## Steps

1. Click **Protection > Relationships**.
2. In the **Relationships** window, click **Create**.
3. In the **Browse SVM** dialog box, select an SVM for the destination volume.
4. In the **Create Protection Relationship** dialog box, select **Mirror and Vault** from the **Relationship Type** drop-down list.
5. Specify the cluster, the SVM, and the source volume.
6. If the selected SVM is not peered, use the **Authenticate** link to enter the credentials of the remote cluster and create the SVM peer relationship.

If the names of the local SVM and remote SVM are identical, or if the local SVM is already in a peer relationship with another remote SVM of the same name, or if the local SVM contains a data SVM of the same name, the Enter Alias Name for SVM dialog box is displayed.

7. Optional: Enter an alias name for the remote SVM in the **Enter Alias Name for SVM** dialog box.
8. Create a new destination volume or select an existing volume:

If you want to...	Do the following...
Create a new volume	<ol style="list-style-type: none"> <li>a. If you want to change the default name, which is displayed in the format <code>source_SVM_name_source_volume_name_mirror_vault</code>, specify a new name, and select the containing aggregate for the destination volume.</li> <li>b. Select <b>Enable dedupe</b> to enable deduplication on the new destination volume. If deduplication is disabled on the source volume, then the check box for the new volume is selected by default.</li> </ol>
Select an existing volume	Select the <b>Select Volume</b> option.  <b>Note:</b> Only those volumes with the same language attribute as the source volume are listed.

9. Select an existing policy or create a new policy:

If you want to...	Do the following...
Select an existing policy	Click <b>Browse</b> , and then select a mirror and vault policy.  You can select the policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.

If you want to...	Do the following...
Create a new policy	<ol style="list-style-type: none"> <li>Click <b>Create Policy</b>.</li> <li>Specify a policy name, and set the schedule transfer priority. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to normal.</li> <li>Select the <b>Enable Network Compression</b> check box to compress the data that is being transferred.</li> <li>Click <b>Create</b>.</li> </ol> <p>You can also specify the SnapMirror label and destination retention count for the policy. For the new SnapMirror label to be effective, you must ensure that a Snapshot copy with the same label is created on the source volume.</p>

10. Specify a schedule for the relationship:

If...	Do the following...
You want to assign an existing schedule	From the list of schedules, select an existing schedule.
You want to create a new schedule	<ol style="list-style-type: none"> <li>Click <b>Create Schedule</b>.</li> <li>Specify a name for the schedule.</li> <li>Select <b>Basic</b> or <b>Advanced</b>. <ul style="list-style-type: none"> <li>Basic: You can select this option to specify only the day of the week, time, and the transfer interval.</li> <li>Advanced: You can select this option to specify a cron-style schedule.</li> </ul> </li> <li>Click <b>Create</b>.</li> </ol>
You do not want to assign a schedule	Select <b>None</b> .

11. Optional: Select **Initialize Relationship** to initialize the relationship.

12. Click **Create**.

## Deleting mirror and vault relationships

You can use System Manager to end a mirror and vault relationship between a source and destination volume, and release the Snapshot copies from the source volume.

### About this task

- It is a best practice to break the mirror and vault relationship before deleting the relationship.
- To re-create the relationship, you must run the resynchronization operation from the source volume by using the command-line interface (CLI).

### Steps

- Click **Protection > Relationships**.
- Select the mirror and vault relationship that you want to delete and click **Delete**.

3. Select the confirmation check box, and then click **Delete**.

You can also select the release base Snapshot copies check box to delete the base Snapshot copies used by the mirror and vault relationship on the source volume.

If the relationship is not released, then you must use the CLI to run the release operation on the source cluster to delete the base Snapshot copies that were created for the mirror and vault relationship from the source volume.

### Result

The relationship is deleted and the base Snapshot copies on the source volume are permanently deleted.

## Editing mirror and vault relationships

You can use System Manager to edit a mirror and vault relationship by modifying the selected policy or schedule. However, you cannot edit the parameters of an existing policy or schedule.

### Before you begin

The source and destination clusters must be in a healthy peer relationship.

### About this task

You can modify the relationship type of a version-flexible mirror relationship, vault relationship, or mirror and vault relationship by modifying the policy type.

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror and vault relationship that you want to modify, and then click **Edit**.
3. In the **Edit Relationship** dialog box, select the appropriate action:

If you want to...	Do the following...
Select an existing policy	<p>Click <b>Browse</b>, and then select an existing policy.</p> <p>You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.</p>
Create a new policy	<ol style="list-style-type: none"> <li>a. Click <b>Create Policy</b>.</li> <li>b. Specify a name for the policy.</li> <li>c. Set the priority for scheduled transfers. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to Normal.</li> <li>d. Select the <b>Enable Network Compression</b> check box to compress the data that is being transferred.</li> <li>e. Specify a SnapMirror label and destination retention count for the vault policy. You must ensure that a Snapshot copy with the same label is created on the source volume for the new SnapMirror label to be effective.</li> <li>f. Click <b>Create</b>.</li> </ol>

4. Specify a schedule for the relationship:

If...	Do the following...
You want to assign an existing schedule	Click <b>Browse</b> , and then select an existing schedule.
You want to create a new schedule	<ol style="list-style-type: none"> <li>a. Click <b>Create Schedule</b>.</li> <li>b. Specify a name for the schedule.</li> <li>c. Select one of the following options: <ul style="list-style-type: none"> <li>• <b>Basic</b> You can select this option to specify only the day of the week, time, and the transfer interval.</li> <li>• <b>Advanced</b> You can select this option to specify a cron style schedule.</li> </ul> </li> <li>d. Click <b>Create</b>.</li> </ol>
You do not want to assign a schedule	Select <b>None</b> .

5. Click **OK**.

## Initializing mirror and vault relationships

You can use System Manager to initialize a mirror and vault relationship if you have not already initialized the relationship while creating it. When you initialize a relationship, a complete baseline transfer of data is performed from the source volume to the destination.

### Before you begin

The source and destination clusters must be in a healthy peer relationship.

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror and vault relationship that you want to initialize, and then click **Operations > Initialize**.
3. Select the confirmation check box, and then click **Initialize**.
4. Verify the status of the relationship in the **Protection** window.

### Result

A Snapshot copy is created and transferred to the destination.

This Snapshot copy is used as a baseline for subsequent incremental Snapshot copies.

## Updating mirror and vault relationships

You can use System Manager to manually initiate an unscheduled incremental update. You might require a manual update to prevent data loss due to an upcoming power outage, scheduled maintenance, or data migration.

### Before you begin

The mirror and vault relationship must be initialized and in a Snapmirrored state.

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror relationship for which you want to update the data, and then click **Operations > Update**.
3. Choose one of the following options:
  - Select **As Per Policy** to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
  - Select **Select Snapshot copy** and specify the Snapshot copy that you want to transfer.
4. Optional: Select **Limit transfer bandwidth to** to limit the network bandwidth that is used for transfers, and then specify the maximum transfer speed.
5. Click **Update**.
6. Verify the transfer status in the **Details** tab.

## Quiescing mirror and vault relationships

You can use System Manager to quiesce a destination volume to stabilize the destination before creating a Snapshot copy. The quiesce operation enables active data transfers to finish and disables future transfers for the mirror and vault relationship.

### Before you begin

The mirror and vault relationship must be in a Snapmirrored state.

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror and vault relationship that you want to quiesce, and then click **Operations > Quiesce**.
3. Select the confirmation check box, and then click **Quiesce**.

### Result

If there is no transfer in progress, the transfer status is displayed as Quiesced. If a transfer is in progress, the transfer is not affected, and the transfer status is displayed as Quiescing until the transfer is complete.

## Resuming mirror and vault relationships

If you have a quiesced mirror and vault relationship, you can resume the relationship by using System Manager. When you resume the relationship, normal data transfer to the destination volume is resumed and all the protection activities are restarted.

### About this task

If you have quiesced a broken mirror and vault relationship from the command-line interface (CLI), you cannot resume the relationship from System Manager. You must use the CLI to resume the relationship.

### Steps

1. Click **Protection > Relationships**.

2. Select the mirror and vault relationship that you want to resume, and then click **Operations > Resume**.
3. Select the confirmation check box, and then click **Resume**.

#### Result

Normal data transfers are resumed. If there is a scheduled transfer for the relationship, the transfer is started from the next schedule.

## Breaking mirror and vault relationships

You can use System Manager to break the mirror and vault relationship if a source volume becomes unavailable and you want client applications to access the data from the destination volume. You can use the destination volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.

#### Before you begin

- The mirror and vault relationship must be in the Quiesced or Idle state.
- The destination volume must be already mounted on the destination Storage Virtual Machine (SVM) namespace.

#### Steps

1. Click **Protection > Relationships**.
2. Select the mirror and vault relationship that you want to break, and then click **Operations > Break**.
3. Select the confirmation check box, and then click **Break**.

#### Result

The mirror and vault relationship is broken. The destination volume type changes from data protection (DP) read-only to read/write. The system stores the base Snapshot copy for the relationship for later use.

## Resynchronizing mirror and vault relationships

You can use System Manager to reestablish a mirror and vault relationship that was broken earlier. You can perform a resynchronization operation to recover from a disaster that disabled the source volume. For Infinite Volumes, the resynchronization operation recovers the volume and its constituents.

#### Before you begin

The source and destination clusters and the source and destination Storage Virtual Machines (SVMs) must be in peer relationships.

#### About this task

- When you perform a resynchronization operation, the contents on the destination volume are overwritten by the contents on the source.
 

**Attention:** The resynchronization operation can cause loss of newer data written to the destination volume after the base Snapshot copy was created.
- If the Last Transfer Error field in the Protection window recommends a resynchronization operation, you must first break the relationship and then perform the resynchronization operation.



### Steps

1. Click **Protection > Relationships**.
2. Select the mirror and vault relationship that you want to resynchronize, and then click **Operations > Resync**.
3. Select the confirmation check box, and then click **Resync**.

## Reverse resynchronizing mirror and vault relationships

You can use System Manager to reestablish a mirror and vault relationship that was previously broken. In a reverse resynchronization operation, the functions of the source and destination volumes are reversed. You can use the destination volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.

### Before you begin

The source volume must be online.

### About this task

- When you perform reverse resynchronization, the contents on the source volume are overwritten by the contents on the destination volume.  
**Attention:** The reverse resynchronization operation can cause data loss on the source volume.
- When you perform reverse resynchronization, the policy of the relationship is set to MirrorAndVault and the schedule is set to None.

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror and vault relationship that you want to reverse, and then click **Operations > Reverse Resync**.
3. Select the confirmation check box, and then click **Reverse Resync**.

## Aborting mirror and vault relationships

You can abort a volume replication operation if you want to stop the data transfer. You can abort a scheduled update, a manual update, or an initial data transfer.

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror and vault relationship for which you want to stop the data transfer, and then click **Operations > Abort**.
3. Select the **Yes, I want to abort the transfer** check box to confirm the operation.
4. Optional: Select the **Keep any partially transferred data** check box to retain the data that is already transferred to the destination volume.
5. Click **Abort**.

### Result

The transfer status is displayed as “Aborting” until the operation is complete and displayed as “Idle” after the operation is complete.

## Restoring a volume in a mirror and vault relationship

You can use System Manager to restore Snapshot copies to a source volume or other volumes if the source data is corrupted and is no longer usable. You can replace the original data with the Snapshot copies in the destination volume.

### Before you begin

- The SnapMirror and SnapVault licenses must be enabled on both the source and the destination clusters or the nodes that contain the source and destination volumes.
- The source and destination clusters must be in a healthy peer relationship.
- The source aggregate or any other aggregate that you select for the restore operation must be a 64-bit aggregate.

### About this task

- You cannot restore a volume that is in a mirror and vault relationship between a source Storage Virtual Machine (SVM) and a destination SVM in a MetroCluster configuration.
- You can restore a mirror and vault relationship for the following configurations:
  - Between sync-source SVMs in a MetroCluster configuration
  - From a volume on a sync-source SVM to a default SVM
  - From a volume on a default SVM to a DP volume on a sync-source SVM

### Steps

1. Click **Protection > Relationships**.
2. Select the mirror and vault relationship that you want to restore, and then click **Operations > Restore**.
3. In the **Restore** dialog box, restore the data to the source volume in the relationship or select any other volume:

If you want to restore to...	Do the following...
The source volume	<ol style="list-style-type: none"> <li>a. Select <b>Source volume</b>.</li> <li>b. Go to step 6 to select the confirmation check box.</li> </ol>
Any other volume	Select <b>Other volume</b> , and then select the cluster and the SVM.

4. Restore the data to a new volume or to an existing volume:

If you want to restore to...	Do the following...
A new volume	If you want to change the default name, displayed in the format <i>destination_SVM_name_destination_volume_name_</i> restore, specify a new name, and then select the containing aggregate for the volume.
An existing volume	<p>Select the <b>Select Volume</b> option.</p> <p>You must select a volume other than the source volume, or a read/write volume with some data in it and with a common Snapshot copy.</p> <p>Only those volumes with the same language attribute as the source volume are listed.</p>

5. Select either the latest Snapshot copy or a specific Snapshot copy that you want to restore.
6. Select the confirmation check box to restore the volume from the Snapshot copy.
7. Optional: Select the **Enable Network Compression** check box to compress the data that is being transferred during the restore operation.
8. Click **Restore**.

## What lag time is

Lag time is the amount of time by which the destination system lags behind the source system.

The lag time is the difference between the current time and the timestamp of the Snapshot copy that was last successfully transferred to the destination system. The lag time will always be at least as much as the duration of the last successful transfer, unless the clocks on the source and destination systems are not synchronized. The lag time can be negative if the time zone of the destination system is behind the time zone of the source system.

## Types of data protection relationships

Depending on your data protection and backup requirements, OnCommand System Manager provides different types of protection relationships that enable you to protect data against accidental, malicious, or disaster-induced loss of data.

### Mirror relationship (SnapMirror license required)

A mirror relationship provides asynchronous disaster recovery. Data protection mirror relationships enable you to periodically create Snapshot copies of data on one volume; copy those Snapshot copies to a partner volume (the destination volume), usually on another cluster; and retain those Snapshot copies. The mirror copy on the destination volume ensures quick availability and restoration of data from the time of the latest Snapshot copy, if the data on the source volume is corrupted or lost.

For mirror relationships, the version of Data ONTAP that is running on the destination cluster must be the same or a later version than the one running on the source cluster. However, version-flexible mirror relationships are not dependent on the Data ONTAP version; therefore, you can create a version-flexible mirror relationship with a destination cluster that is either running a later version of Data ONTAP than the source cluster or an earlier version of Data ONTAP than the source cluster.

**Note:** The version-flexible mirror relationship feature is available only from Data ONTAP 8.3; therefore, you cannot have a version-flexible mirror relationship with a volume earlier than Data ONTAP 8.3.

Mirror relationships are valid for FlexVol volumes and Infinite Volumes.

### Vault relationship (SnapVault license required)

A vault relationship provides storage-efficient and long-term retention of backups. Vault relationships enable you to back up selected Snapshot copies of volumes to a destination volume and retain the backups.

Vault relationships are valid only for FlexVol volumes.

### Mirror and vault relationship (SnapMirror and SnapVault licenses required)

A mirror and vault relationship provides data protection by periodically transferring data from the source volume to the destination volume and also facilitates long-term retention of data by creating backups of the source volume.

**Note:** The mirror and vault relationship feature is available only from Data ONTAP 8.3.2; therefore, you cannot have a mirror and vault relationship with a volume earlier than Data ONTAP 8.3.2.

A mirror and vault relationship is valid only for FlexVol volumes.

## Protection window

You can use the Protection window to create and manage mirror, vault, and mirror vault relationships and to display details about these relationships. The Protection window does not display load-sharing (LS) and transition relationships (TDP).

Namespace mirrors and constituents are not displayed for mirror relationships on Infinite Volumes.

- [Command buttons](#) on page 364
- [Protection relationships list](#) on page 364
- [Details area](#) on page 365

### Command buttons

#### Create

Opens the Create Protection Relationship dialog box, which you can use to create a mirror, vault, or mirror and vault relationship from a destination volume.

System Manager does not display any Storage Virtual Machine (SVM) configured for disaster recovery (DR) in the Create Protection Relationship dialog box.

You cannot create vault relationships for Infinite Volumes and mirror relationships for Infinite Volumes with storage classes.

#### Edit

Opens the Edit Protection Relationship dialog box, which you can use to edit the schedule and policy of a relationship.

For a vault relationship, mirror and vault relationship, or version-flexible mirror relationship, you can modify the relationship type by modifying the policy type.

#### Delete

Opens the Delete Protection Relationship dialog box, which you can use to delete a relationship.

### Operations

Displays the operations that can be performed on a protection relationship.

#### Refresh

Updates the information in the window.

### Protection relationships list

#### Source Storage Virtual Machine

Displays the SVM that contains the volume from which data is mirrored or vaulted in a relationship.

#### Source Volume

Displays the volume from which data is mirrored or vaulted in a relationship.

#### Destination Volume

Displays the volume to which data is mirrored or vaulted in a relationship.

**Is Healthy**

Displays whether the relationship is healthy or not.

**Relationship State**

Displays the state of the relationship, such as Snapmirrored, Uninitialized, or Broken Off.

**Transfer Status**

Displays the relationship status, such as Idle, Transferring, or Aborting.

**Relationship Type**

Displays the type of relationship, such as Mirror, Vault, or Mirror and Vault.

**Lag Time**

Displays the difference between the current time and the timestamp of the Snapshot copy that was last transferred successfully to the destination storage system. It indicates the time difference between the data that is currently on the source system and the latest data stored on the destination system. The value that is displayed can be positive or negative. The value is negative if the time zone of the destination system is behind the time zone of the source storage system.

**Policy Name**

Displays the name of the policy that is assigned to the relationship.

**Policy Type**

Displays the type of policy that is assigned to the relationship. The policy type can be Vault, Mirror Vault, or Asynchronous Mirror.

**Details area****Details tab**

Displays general information about the selected relationship, such as the source and destination clusters, data transfer rate, state of the relationship, details about the network compression ratio, data transfer status, type of current data transfer, type of last data transfer, latest Snapshot copy, and timestamp of the latest Snapshot copy.

**Policy Details tab**

Displays details about the policy that is assigned to the selected protection relationship. It also displays the SnapMirror label and the Snapshot copy schedules in the source volume that match the specified label.

**Snapshot Copies tab**

Displays the count of Snapshot copies with the SnapMirror label attribute for the selected protection relationship and the timestamp of the latest Snapshot copy.

**Related concepts**

[What a SnapVault backup is](#) on page 350

**Related tasks**

[Creating a mirror relationship from a source SVM](#) on page 185

[Creating a mirror relationship from a destination SVM](#) on page 330

[Deleting mirror relationships](#) on page 333

[Editing mirror relationships](#) on page 333

[Initializing mirror relationships](#) on page 334

[Updating mirror relationships](#) on page 335

[Quiescing mirror relationships](#) on page 336

[Resuming mirror relationships](#) on page 336

[Breaking SnapMirror relationships](#) on page 337  
[Resynchronizing mirror relationships](#) on page 337  
[Reverse resynchronizing mirror relationships](#) on page 338  
[Aborting a mirror transfer](#) on page 339  
[Creating a vault relationship from a source SVM](#) on page 188  
[Creating a vault relationship from a destination SVM](#) on page 342  
[Deleting vault relationships](#) on page 345  
[Editing vault relationships](#) on page 345  
[Initializing a vault relationship](#) on page 346  
[Updating a vault relationship](#) on page 347  
[Quiescing a vault relationship](#) on page 347  
[Resuming a vault relationship](#) on page 348  
[Aborting a Snapshot copy transfer](#) on page 348  
[Restoring a volume in a vault relationship](#) on page 349

## Snapshot policies

You can use System Manager to create and manage Snapshot policies in your storage system.

### Creating Snapshot policies

You can create a Snapshot policy in System Manager to specify the maximum number of Snapshot copies that can be automatically created and the frequency of creating them.

#### Steps

1. Click **Protection > Snapshot Policies**.
2. Click **Create**.
3. In the **Create Snapshot Policy** dialog box, specify the policy name.
4. Click **Add**, and then specify the schedule name, the maximum number of Snapshot copies that you want to retain, and the SnapMirror label name.

The maximum number of Snapshot copies that can be retained by the specified schedules must not exceed 254.

5. Click **OK**, and then click **Create**.

### Editing Snapshot policies

You can modify the details of an existing Snapshot policy, such as the schedule name, SnapMirror label, or the maximum number of Snapshot copies that are created by using the Edit Snapshot Policy dialog box in System Manager.

#### About this task

For an Infinite Volume, scheduled Snapshot copies cannot occur more often than at an hourly rate.

#### Steps

1. Click **Protection > Snapshot Policies**.
2. In the **Snapshot Policies** window, select the Snapshot policy that you want to modify and click **Edit**.

3. In the **Edit Snapshot Policy** dialog box, select the schedule that you want to modify and click **Edit**.
4. Click **OK**.
5. Verify the changes you made to the selected Snapshot policy in the **Edit Snapshot Policy** dialog box and click **Save**.

## Deleting Snapshot policies

You can use System Manager to delete Snapshot policies. If you delete a Snapshot policy that is being used by one or more volumes, Snapshot copies of the volume or volumes are no longer created according to the deleted policy.

### Before you begin

You must have dissociated the Snapshot policy from each volume that uses it.

### Steps

1. Click **Protection > Snapshot Policies**.
2. Select the Snapshot policy and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

## About Snapshot policies

When applied to a volume, a Snapshot policy specifies a schedule or schedules according to which Snapshot copies are created and specifies the maximum number of Snapshot copies that each schedule can create. A Snapshot policy can include up to five schedules.

For vault relationships, the SnapMirror Label attribute is used to select Snapshot copies on the source volumes. Only Snapshot copies with the labels configured in the vault policy rules are replicated in backup vault operations. The Snapshot policy assigned to the source volume must include the SnapMirror Label attribute.

## Snapshot Policies window

You can use the Snapshot Policies window to manage Snapshot policy tasks, such as adding, editing, and deleting Snapshot policies.

### Command buttons

#### Create

Opens the Create Snapshot Policy dialog box, which enables you to add backup schedules and specify the maximum number of Snapshot copies to be retained in a policy.

#### Edit

Opens the Edit Snapshot Policy dialog box, which enables you to modify the frequency at which Snapshot copies should be created and the maximum number of Snapshot copies to be retained.

#### Delete

Opens the Delete dialog box, which enables you to delete the selected Snapshot policy.

#### View as

Enables you to view the Snapshot policies either as a list or as a tree.

**Status**

Opens the menu, which you can use to either enable or disable the selected Snapshot policy.

**Refresh**

Updates the information in the window.

**Snapshot policy list****Policy/Schedule Name**

Specifies the name of the Snapshot policy and the schedules in the policy.

**Storage Virtual Machine**

Specifies the name of the Storage Virtual Machine (SVM) to which the Snapshot copies belong.

**Status**

Specifies the status of the Snapshot policy, which can be Enabled or Disabled.

**Maximum Snapshots to be retained**

Specifies the maximum number of Snapshot copies to be retained.

**SnapMirror Label**

Specifies the name of the SnapMirror label attribute of the Snapshot copy generated by the backup schedule.

## Schedules

You can use System Manager to create and manage schedules in your storage system.

### Creating schedules

You can create schedules to run a job at a specific time or at regular periods by using System Manager.

**About this task**

When you create a schedule in a MetroCluster configuration, it is a best practice to create an equivalent schedule on the cluster in the surviving site as well.

**Steps**

1. Click **Protection > Schedules**.
2. Click **Create**.
3. In the **Create Schedule** dialog box, specify the schedule name.
4. Create a schedule based on your requirements:

If you want to create...	Do this...
A daily or a specific schedule on certain days	Select <b>Basic</b> , and specify the schedule and recurrence details (in hours and minutes).
A schedule that runs at a specific interval	Select <b>Interval</b> , and specify the schedule and recurrence details (in days, hours, and minutes).
A schedule that runs at a specific period	Select <b>Advanced</b> , and specify the schedule and recurrence details (in months, days, weekdays, hours, and minutes).



5. Click **Create**.

## Editing schedules

You can make changes to a previously created cron schedule or an interval schedule if it does not meet your requirements by using System Manager. You can modify schedule details such as recurring days and hours, interval options, and advanced cron options.

### About this task

When you edit a schedule in a MetroCluster configuration, it is a best practice to edit the equivalent schedule on the surviving site cluster as well.

### Steps

1. Click **Protection > Schedules**.
2. Select the schedule that you want to modify and click **Edit**.
3. In the **Edit Schedule** dialog box, modify the schedule by performing the appropriate action:

If you select the schedule option as...	Do this..
Basic	Specify the recurring days and recurring schedule details.
Interval	Specify the interval options in days, hours, and minutes.
Advanced	Specify the advanced cron options in months, days, week days (if applicable), hours, and minutes.

4. Click **OK**.

## Deleting schedules

You can use System Manager to delete the schedules that run specific storage management tasks.

### Steps

1. Click **Protection > Schedules**.
2. Select the schedule that you want to delete and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

## Schedules

You can configure many tasks (for instance, volume Snapshot copies and mirror replications) to run on specified schedules. Schedules that are run at specified schedules are known as *cron* schedules because of their similarity to UNIX *cron* schedules. Schedules that are run at intervals are known as *interval* schedules.

You can manage schedules in the following ways:

- Creating a cron schedule or an interval schedule
  - Displaying information about all the schedules
  - Modifying a cron schedule or an interval schedule
  - Deleting a cron schedule or an interval schedule
- You cannot delete a schedule that is currently in use by a running job.

The cluster administrator can perform all the schedule management tasks.

## Schedules window

You can use the Schedules window to manage scheduled tasks, such as creating, displaying information about, modifying, and deleting schedules.

### Command buttons

#### Create

Opens the Create Schedule dialog box, which enables you to create time-based and interval schedules.

#### Edit

Opens the Edit Schedule dialog box, which enables you to edit the selected schedules.

#### Delete

Opens the Delete Schedule dialog box, which enables you to delete the selected schedules.

#### Refresh

Updates the information in the window.

### Schedules list

#### Name

Specifies the name of the schedule.

#### Type

Specifies the type of the schedule—time-based or interval-based.

### Details area

The details area displays information about when a selected schedule is run.

## Copyright information

---

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

**RESTRICTED RIGHTS LEGEND:** Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark information

---

Active IQ, AltaVault, Arch Design, ASUP, AutoSupport, Campaign Express, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlexArray, FlexCache, FlexClone, FlexGroup, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, Fueled by SolidFire, GetSuccessful, Helix Design, LockVault, Manage ONTAP, MetroCluster, MultiStore, NetApp, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANscreen, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, SolidFire Helix, StorageGRID, SyncMirror, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## How to send comments about documentation and receive update notifications

---

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

[doccomments@netapp.com](mailto:doccomments@netapp.com)

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

# Index

## A

- ABE
  - enabling [221](#)
- aborting
  - a mirror and vault relationship [361](#)
  - a mirror relationship [339](#)
- absolute symbolic links
  - how SMB clients can access UNIX [265](#)
- access
  - modifying for roles [88](#)
  - stopping share [220](#)
  - user accounts [86](#)
- access control
  - adding roles [306](#)
- access-based enumeration
  - See* ABE
- access-control roles
  - adding [87](#)
  - predefined roles for cluster administrators [88](#)
  - predefined roles for SVM administrators [307](#)
- accessing
  - a cluster by using OnCommand System Manager browser-based graphic interface [28](#), [30](#)
- accounts
  - changing passwords for cluster user [85](#)
- ACLs
  - file permissions, SMB [327](#)
- activating
  - quotas [253](#)
- Active Directory
  - adding users [312](#)
- adapters
  - FC/FCoE, editing the settings [104](#)
- adding
  - AutoSupport email recipients [154](#)
  - capacity disks to aggregates [116](#)
  - CIFS server preferred domain controllers [263](#)
  - cluster user accounts [85](#)
  - disks to storage pools [128](#)
  - export rules [277](#)
  - group memberships to users [316](#)
  - home directory path for CIFS [259](#)
  - initiators [232](#)
  - LDAP client configuration [294](#)
  - members to local Windows groups [312](#)
  - NIS domains [293](#)
  - preferred domain controllers [263](#)
  - roles [87](#), [306](#)
  - rules to export policies [278](#)
  - Snapshot policies [366](#)
  - SSDs to aggregates [114](#)
  - SSDs to HDDs for converting to Flash Pool aggregates [39](#)
  - users to local Windows groups [312](#)
  - VLAN interfaces [100](#)
- additional information
  - about ONTAP [21](#)
- admin SVMs
  - described [164](#)
- administration
  - adding SVM user accounts [304](#)
  - configuring details of SVM administrators [59](#)
  - delegating to SVM administrators [49](#)
- administrators
  - predefined roles for cluster [88](#)
  - predefined roles for SVM [307](#)
- Advanced Drive Partitioning [129](#)
  - See also* storage pools
- aggregate overcommitment
  - for Infinite Volumes, about [201](#)
- aggregates
  - adding capacity disks to [116](#)
  - assigning array LUNs to [142](#)
  - assigning disks to increase capacity [37](#)
  - assigning to SVMs with Infinite Volume [50](#)
  - changing the RAID group while adding capacity disks [117](#)
  - considerations for sizing RAID groups [138](#)
  - considerations when moving volumes in a Flash Pool aggregate [205](#)
  - considerations when moving volumes in HDD [205](#)
  - creating LUNs [229](#)
  - creating storage pools [127](#)
  - deleting [113](#)
  - deleting storage pools [128](#)
  - description and characteristics of [119](#)
  - editing the settings [112](#)
  - Flash Pool, how they work [120](#)
  - how storage pools increase cache allocation flexibility for Flash Pool [129](#)
  - how you use storage pools with Flash Pool [129](#)
  - managing [112](#)
  - mirrored, explained [123](#)
  - mirroring [118](#)
  - modifying RAID group size [113](#)
  - modifying RAID type [113](#)
  - moving volumes [183](#)
  - provisioning cache by adding SSDs [114](#)
  - provisioning storage by creating [38](#)
  - provisioning storage by creating Flash Pool [39](#)
  - provisioning storage by creating HDD and SSD [38](#)
  - provisioning storage by creating SnapLock Compliance [41](#)
  - provisioning storage by creating SnapLock Enterprise [41](#)
  - reassigning array LUNs to nodes [143](#)
  - reassigning disks to increase capacity [134](#)
  - requirements and best practices for using storage pools with Flash Pool [130](#)
  - requirements for data protection mirror relationships [123](#)
  - requirements for Infinite Volumes [122](#)
  - rules for mixing array LUNs in [145](#)
  - viewing information about [119](#)
  - zeroing spare array LUNs [143](#)
  - zeroing spare disks [38](#)
- Aggregates window

- using to create, manage, and display information about aggregates [124](#)
- alerts
  - acknowledging system health [150](#)
  - dashboard for viewing details [57](#)
  - deleting system health [151](#)
  - introduction to monitoring system health [150](#)
  - responding to [152](#)
  - suppressing system health [151](#)
- aliases
  - creating an iSCSI [270](#)
- All Flash FAS clusters
  - creating LUNs during initial setup [225](#)
- all-share cache
  - creating for BranchCache configuration [261](#)
- application-specific LUN settings
  - for Oracle and SQL [226](#)
- application-specific volume settings
  - examples for Oracle and Oracle RAC [215](#)
- applications
  - provision storage over NFS [214](#)
- array LUNs
  - assigning [142](#)
  - considerations for sizing RAID groups for [138](#)
  - erasing data from [143](#)
  - formatting [143](#)
  - managing [142](#)
  - reassigning to nodes [143](#)
  - zeroing [143](#)
- Array LUNs window
  - using to assign ownership [145](#)
- assigning
  - array LUNs [142](#)
  - disks to nodes [37](#)
  - export policies to qtrees [248](#)
  - group memberships to users [316](#)
- ASUP
  - See* AutoSupport
- ATA drives
  - how ONTAP reports disk types [135](#)
- authentication
  - changing the default method for iSCSI initiators [272](#)
  - how ONTAP handles NFS client [269](#)
  - Kerberos [300](#)
  - modifying the security style for iSCSI initiators [272](#)
  - requirements for using Kerberos with NFS [300](#)
  - using local users and groups for [319](#)
- authorization
  - using local users and groups for [319](#)
- autogrow
  - editing volume settings [169](#)
- AutoSupport
  - editing settings [34](#)
  - email recipients, adding [154](#)
  - enabling or disabling [154](#)
  - generating data for a single node or all nodes [155](#)
  - setting up [154](#)
  - testing the configuration [155](#)
  - viewing summary [155](#)
- AutoSupport messages
  - severity types [156](#)
- AutoSupport notifications
  - managing [154](#)
- AutoSupport window
  - using to view and edit AutoSupport settings [156](#)
- available health monitors
  - for clusters [151](#)
- B**
- backups
  - SnapVault, how they work [351](#)
- baseline transfers
  - defined [350](#)
- benefits
  - of storage efficiency [203](#)
  - of using SVMs [165](#)
- best practices
  - for using storage pools [130](#)
- BranchCache
  - about using to cache SMB shares at branch offices [266](#)
  - deleting the configuration [263](#)
  - enabling [221](#)
  - modifying settings [262](#)
  - setting up [261](#)
  - what happens when you delete the configuration [266](#)
- breaking
  - mirror and vault relationships [360](#)
  - SnapMirror relationships [337](#)
- broadcast domains
  - creating [36](#)
  - deleting [92](#)
  - introduction to configuring for SVM traffic [93](#)
  - managing [92](#)
  - modifying the settings [92](#)
  - types of, defined [93](#)
- browser-based
  - graphic interface, accessing a cluster by using OnCommand System Manager [28](#), [30](#)
- BSAS drives
  - how ONTAP reports disk types [135](#)
- BUILTIN groups
  - predefined local [321](#)
- C**
- cache
  - increasing for Flash Pool aggregates by adding SSDs [115](#)
  - provisioning by adding SSDs [114](#)
  - provisioning to aggregates by adding SSDs [114](#)
- cache disks
  - viewing details about [134](#)
- cache size
  - adding disks to storage pools to increase [128](#)
- cache storage
  - requirements and best practices for using storage pools for Flash Pool aggregate [130](#)
- caching
  - configuring BranchCache for [261](#)
- capacity
  - dashboard for viewing details [57](#)
- capacity disks
  - adding to aggregates [116](#)

- viewing details about [134](#)
- carriers
  - determining when to remove multi-disk [138](#)
  - spare requirements for multi-disk [138](#)
- cascade configurations
  - networking requirements for cluster peering [63](#)
- changing
  - export policies [218](#)
  - RAID type and RAID group size [113](#)
  - the default authentication method for iSCSI initiators [272](#)
- CHAP
  - defined [274](#)
- CIFS
  - adding the home directory [259](#)
  - configuring on the SVM [44](#)
  - creating a local Windows user account [315](#)
  - creating home directory shares [221](#)
  - deleting the home directory [260](#)
  - deleting the home directory path [260](#)
  - editing general properties [259](#)
  - enabling or disabling a group policy [261](#)
  - Kerberos authentication [300](#)
  - reloading the group policy [261](#)
  - resetting domain controllers [260](#)
  - setting up [258](#)
  - stopping share access [220](#)
  - updating group policy configuration [260](#)
  - updating the group policy [260](#)
  - viewing domain information [264](#)
- CIFS protocol
  - managing [257](#)
- CIFS servers
  - adding preferred domain controllers [263](#)
  - configuring BranchCache on [261](#)
  - deleting preferred domain controllers [264](#)
  - modifying BranchCache configurations for [262](#)
  - modifying the IP addresses of preferred domain controllers [264](#)
  - using local users and groups for authentication and authorization [319](#)
  - using privileges to manage access to resources [319](#)
- CIFS shares
  - creating [219](#)
- CIFS window
  - using to manage CIFS [266](#)
- client access
  - adding rules to export policies [278](#)
  - creating export policies [277](#)
  - creating export policy for [277](#)
  - setting up CIFS [258](#)
- client authentication
  - how ONTAP handles [269](#)
- clients
  - adding an LDAP configuration [294](#)
  - associating LDAP clients with SVMs [296](#)
  - deleting active LDAP [297](#)
  - deleting an LDAP configuration [295](#)
  - editing LDAP client configuration [295](#)
  - viewing LDAP configuration [84](#)
- clones
  - creating, of LUNs [233](#)
- cluster
  - creating manually [24](#)
  - cluster administrators
    - predefined roles for [88](#)
  - cluster details
    - dashboard for viewing details [57](#)
  - cluster LIFs
    - role for [98](#)
  - cluster management
    - creating a cluster [22](#)
  - cluster management LIFs
    - role for [98](#)
  - cluster peer relationships
    - deleting [66](#)
    - requirements for [63](#)
  - cluster peers
    - creating relationships between [65](#)
    - definition of intercluster networking [67](#)
    - managing [63](#)
    - modifying the passphrase [66](#)
  - cluster performance
    - dashboard for viewing details [57](#)
  - cluster setup
    - setting up a network [25](#)
  - cluster switch health monitors
    - about [151](#)
  - cluster time
    - managing [79](#)
  - cluster update
    - managing [74](#)
  - cluster update window
    - using to perform automated cluster upgrade [78](#)
    - using to perform nondisruptive cluster upgrade [78](#)
  - cluster user accounts
    - adding [85](#)
    - changing passwords for [85](#)
    - editing [85](#)
  - cluster-management interfaces
    - creating [31](#)
  - clusters
    - adding a user account for [85](#)
    - changing passwords for [31](#)
    - creating LUNs during initial setup [225](#)
    - creating network interfaces for managing [31](#)
    - creating peer relationships [65](#)
    - dashboard for viewing details [57](#)
    - deleting a peer relationship [66](#)
    - description of [56](#)
    - locking or unlocking user accounts [86](#)
    - managing [56](#)
    - managing time [79](#)
    - modifying the intercluster interfaces of remote [66](#)
    - monitoring the health of [59](#)
    - naming requirements for cluster peering [63](#)
    - nondisruptively updating, using System Manager [75](#)
    - understanding how nondisruptive update is performed [77](#)
    - understanding quorum and epsilon [56](#)
    - updating the name [31](#)
    - when to use IPspaces to separate client traffic [91](#)
  - comments
    - how to send feedback about documentation [373](#)
  - communities
    - specifying information for SNMP [81](#)



- compatible spare disks
    - what they are [121](#)
  - ComplianceClock time
    - initializing [146](#)
  - compression
    - configuring on a volume [181](#)
    - editing the settings [169](#)
  - configuration
    - creating a Kerberos realm [298](#)
    - managing [59](#)
    - modifying a Kerberos realm [299](#)
  - configuration updates window
    - using to manage cluster, SVM, and node configuration updates [60](#)
  - configurations
    - cascade, for cluster peering [63](#)
    - fan-out, for cluster peering [63](#)
  - configuring
    - basic details of the SVM [42](#)
    - BranchCache [261](#)
    - CIFS and NFS on the SVM [44](#)
    - DNS on the SVM [42](#)
    - FC protocol [48](#)
    - FCoE protocol [48](#)
    - iSCSI protocol [46](#)
    - log levels and inactivity timeout value [28](#)
  - considerations
    - when using thin provisioning with Infinite Volumes [201](#)
  - constituents
    - and Snapshot copies [198](#)
    - for infinite Volumes [122](#)
  - contact personnel
    - specifying information for SNMP [81](#)
  - continuous availability
    - enabling or disabling for shares [221](#)
  - controllers
    - adding CIFS server preferred domain [263](#)
  - conventions
    - network port naming [102](#)
  - conversion rules
    - name mapping [326](#)
  - core files
    - spare disk requirement for [137](#)
  - creating
    - a cluster by using OnCommand System Manager [22](#)
    - a cluster peer relationship [65](#)
    - a Kerberos realm [298](#)
    - a mirror and vault relationship from a destination SVM [354](#)
    - a mirror relationship from a destination SVM [330](#)
    - a vault relationship from a destination SVM [342](#)
    - aggregates [38](#)
    - an Infinite Volume [52](#)
    - broadcast domains [36](#)
    - CIFS shares [219](#)
    - cluster
      - setting up [24](#)
    - cluster manually [24](#)
    - cluster-management interfaces [31](#)
    - export policies [277](#)
    - Flash Pool aggregates [38, 39](#)
    - FlexClone files [173](#)
    - FlexClone volumes [172](#)
    - FlexGroup volumes [193](#)
    - FlexVol volumes [51](#)
    - HDD and SSD aggregates [38](#)
    - home directory shares [221](#)
    - initiator groups [231](#)
    - interface groups [100](#)
    - IPspaces [36](#)
    - iSCSI aliases [270](#)
    - local Windows groups [310](#)
    - LUN clones [233](#)
    - LUNs [229](#)
    - LUNs during initial setup [225](#)
    - mirror and vault relationships from a source volume [190](#)
    - mirror policies [285](#)
    - mirror relationships from a source SVM [185](#)
    - mirror vault policies [285](#)
    - network interfaces [94](#)
    - node-management interfaces [33](#)
    - port sets [232](#)
    - QoS policy groups [288](#)
    - qtrees [246](#)
    - quotas [251](#)
    - schedules [368](#)
    - setting up
      - cluster [24](#)
    - SnapLock Compliance aggregates [41](#)
    - SnapLock Compliance volumes [54](#)
    - SnapLock Enterprise aggregates [41](#)
    - SnapLock Enterprise volumes [54](#)
    - Snapshot copies [175](#)
    - Snapshot policies [366](#)
    - storage pools [127](#)
    - subnets [37](#)
    - vault policies [285](#)
    - vault relationships from a source SVM [188](#)
    - Windows local users [315](#)
  - creating a cluster
    - AutoSupport messages [22](#)
    - event notifications [22](#)
  - customization
    - ways to perform, of window layout [19](#)
  - cutover
    - manually triggering the phase [184](#)
- ## D
- dashboard
    - using to monitor cluster health and performance [59](#)
    - using to monitor SVM health and performance [159](#)
  - dashboard icons
    - described [18](#)
  - Dashboard window
    - using to view cluster and storage object details [57](#)
    - using to view SVM details [159](#)
  - data compression
    - how SnapVault backups work with [352](#)
  - data compression's interoperability
    - with deduplication [204](#)
  - data LIFs
    - enabling management access for [96](#)
    - role for [98](#)

- data protection
  - managing relationships [330](#)
  - managing Snapshot policies and schedules [330](#)
  - mirror relationships [341](#)
  - using the Protection window for [364](#)
- data protection mirror copies
  - providing disaster recovery for Infinite Volumes [341](#)
- data protection mirror relationships
  - aggregate requirements [123](#)
  - aggregate requirements for Infinite Volumes [123](#)
- data protection mirrors
  - FlexVol volumes [341](#)
  - uses for [341](#)
- data protection relationships
  - mirror [363](#)
  - mirror and vault [363](#)
  - overview of types of [363](#)
  - vault [363](#)
  - version-flexible mirror [363](#)
- data protection volumes
  - editing properties of [171](#)
- data SVMs
  - described [164](#)
- datastores
  - NFS, creating for VMware [193](#)
- date and time window
  - using to view and modify date and time settings [80](#)
- DDNS
  - enabling [303](#)
  - enabling or disabling [302](#)
- deactivating
  - quotas [253](#)
- dedicated SSDs
  - adding to Flash Pool aggregates [115](#)
- deduplication
  - adding efficiency policies on a volume for [282](#)
  - changing schedule [182](#)
  - configuring on a volume [181](#)
  - editing the schedule [169](#)
  - FlexVol volumes
    - guidelines for using deduplication [204](#)
  - guidelines for using [204](#)
  - running on volumes [183](#)
- default initiator security
  - editing [271](#)
- default predefined efficiency policy
  - understanding [284](#)
- default privileges
  - predefined BUILTIN group [321](#)
- define
  - volume encryption [196](#)
  - volume granular encryption [196](#)
- definitions
  - local privileges [320](#)
  - local users and groups [319](#)
- delegating
  - SVMs administration [59](#)
  - SVMs to administrators [49](#)
- deleting
  - active LDAP clients [297](#)
  - aggregates [113](#)
  - BranchCache configuration [263](#)
  - BranchCache configuration, what happens when you [266](#)
  - broadcast domains [92](#)
  - efficiency policies [283](#)
  - export policies [278](#)
  - export policy rules [280](#)
  - FlexGroup volumes [195](#)
  - FlexVol volumes [171](#)
  - home directory path [260](#)
  - Infinite Volumes [171](#)
  - initiator groups [231](#)
  - initiators from an initiator group [232](#)
  - IPspaces [90](#)
  - Kerberos realm configurations [299](#)
  - LDAP client configuration [295](#)
  - licenses [69](#)
  - local Windows groups [314](#)
  - LUNs [231](#)
  - mirror and vault relationships [356](#)
  - mirror policies [286](#)
  - mirror relationships [333](#)
  - mirror vault policies [286](#)
  - network interfaces [96](#)
  - port sets [233](#)
  - preferred domain controllers [264](#)
  - protection policies [286](#)
  - QoS policy groups [288](#)
  - qtrees [247](#)
  - quotas [252](#)
  - schedules [369](#)
  - Snapshot copies [179](#)
  - Snapshot policies [367](#)
  - storage pools [128](#)
  - subnets [94](#)
  - SVM [161](#)
  - vault policies [286](#)
  - VLANs [102](#)
  - Windows local user accounts [318](#)
- deleting rules
  - export policies [280](#)
- demo license
  - description of [71](#)
- destination Infinite Volumes
  - aggregate requirements for [123](#)
- destination volumes
  - components of a mirror relationship [341](#)
- DHCP
  - assigning IP addresses to Service Processors [61](#)
- directory shares
  - creating home [221](#)
- disabling
  - AutoSupport settings [154](#)
  - CIFS group policy [261](#)
  - DNS and DDNS [302](#)
  - efficiency policies [283](#)
  - Flash Cache [148](#)
  - iSCSI service on the interfaces [270](#)
  - NFS [268](#)
  - SNMP [81](#)
  - SNMP traps [81](#)
- disabling user accounts
  - local Windows users [316](#)
- disaster recovery

- for Infinite Volumes using mirroring [341](#)
  - disk ownership
    - application to array LUNs [144](#)
    - application to disks [144](#)
  - disk RPM
    - rules for displaying [122](#)
  - disk shelves
    - configuration requirements for multi-disk carrier [138](#)
  - disk space
    - hard limits for [254](#)
    - soft limits for [254](#)
  - disk types
    - rules for displaying [122](#)
  - disks
    - adding to storage pools [128](#)
    - adding, to increase the size of aggregates [116](#)
    - assigning to nodes [37](#)
    - changing the RAID group when adding HDDs to aggregates [117](#)
    - dashboard for viewing details [57](#)
    - description of compatible spare [121](#)
    - erasing data from [38](#)
    - formatting [38](#)
    - how available for Data ONTAP use [144](#)
    - how hot spares are calculated [121](#)
    - how ONTAP reports types [135](#)
    - managing [134](#)
    - minimum required hot spare [137](#)
    - mirroring aggregates [118](#)
    - RAID drive types, defined [135](#)
    - reassigning to nodes [134](#)
    - spare requirements for multi-disk carrier [138](#)
    - viewing
      - disk information [134](#)
      - viewing information [134](#)
      - why you add to storage pools [132](#)
    - zeroing [38](#)
  - Disks window
    - using to view disk details [140](#)
  - disks, hot spares
    - how they work [136](#)
  - distinct IP address spaces
    - when to use IPspaces to define [91](#)
  - DMAs
    - incremental tape backups of Infinite Volumes, using Snapshot copies and SnapDiff [200](#)
  - DNS
    - configuring on the SVM [42](#)
    - editing settings [31](#), [303](#)
    - enabling or disabling [302](#)
  - DNS/DDNS services
    - managing [302](#)
  - DNS/DDNS Services window
    - using to view DNS and DDNS settings [303](#)
  - documentation
    - how to receive automatic notification of changes to [373](#)
    - how to send feedback about [373](#)
  - domain controllers
    - adding preferred [263](#)
    - editing the IP address of preferred [264](#)
    - resetting [260](#)
    - viewing information about [264](#)
  - domain information
    - viewing [264](#)
  - domain names
    - DNS, editing [31](#), [303](#)
  - domains
    - creating broadcast [36](#)
    - deleting broadcast [92](#)
    - editing NIS [293](#)
    - introduction to configuring broadcast, for SVM traffic [93](#)
    - NIS, adding [293](#)
  - downgrades
    - obtaining ONTAP software images [77](#)
  - drive types
    - RAID, defined [135](#)
  - drives
    - considerations for sizing RAID groups for [138](#)
    - See also* disks
- ## E
- editing
    - active LDAP clients [296](#)
    - aggregate settings [112](#)
    - AutoSupport settings [34](#)
    - BranchCache settings [262](#)
    - broadcast domain settings [92](#)
    - cluster name [31](#)
    - cluster user accounts [85](#)
    - data protection volumes [171](#)
    - default security settings [271](#)
    - DNS domain name [303](#)
    - DNS domain names [31](#)
    - Ethernet port properties [101](#)
    - FC/FCoE adapter settings [104](#)
    - FlexGroup volumes [194](#)
    - FlexVol volume properties [169](#)
    - Infinite Volume properties [169](#)
    - initiator groups [237](#)
    - initiator name [237](#)
    - intercluster interfaces [66](#)
    - interface group settings [101](#)
    - IP address of preferred domain controllers [264](#)
    - IP addresses of preferred domain controllers [264](#)
    - IPspace name [90](#)
    - Kerberos configurations [301](#)
    - LUNs [233](#)
    - mirror and vault relationships [357](#)
    - mirror policies [286](#)
    - mirror relationships [333](#)
    - mirror vault policies [286](#)
    - network interfaces [96](#)
    - NFS settings [268](#)
    - NIS domains [293](#)
    - node name [32](#)
    - port sets [237](#)
    - QoS policy groups [289](#)
    - qtrees [247](#)
    - quotas [252](#)
    - RAID type and RAID group size [113](#)
    - schedules [369](#)
    - Service Processor settings [62](#)
    - share settings [221](#)

- Snapshot policies [366](#)
  - subnet settings [93](#)
  - SVM properties [160](#)
  - SVMs user accounts [305](#)
  - the cluster peer passphrase [66](#)
  - the security style for iSCSI initiators [272](#)
  - the status of a FlexGroup volume [195](#)
  - the status of a volume [174](#)
  - vault policies [286](#)
  - vault relationships [345](#)
  - VLAN settings [101](#)
  - effective ONTAP disk types
    - mixing HDDs [120](#)
  - efficiency
    - benefits of storage [203](#)
  - efficiency policies
    - adding for a volume to run deduplication [282](#)
    - deleting [283](#)
    - described [284](#)
    - disabling [283](#)
    - editing [283](#)
    - enabling [283](#)
    - enabling or disabling [283](#)
    - managing [282](#)
    - modifying for a volume [169](#)
    - settings in the Efficiency Policy window for managing [284](#)
  - Efficiency Policies window
    - fields in the [284](#)
  - efficiency policies, predefined
    - understanding inline-only and default [284](#)
  - email messages
    - editing for AutoSupport [34](#)
    - setting up AutoSupport [154](#)
  - emails
    - adding recipients for AutoSupport messages [154](#)
  - enabling
    - AutoSupport settings [154](#)
    - CIFS group policy [261](#)
    - DDNS [303](#)
    - DNS [31](#)
    - DNS and DDNS [302, 303](#)
    - efficiency policies [283](#)
    - Flash Cache [148](#)
    - iSCSI service on the interfaces [270](#)
    - management access for LIFs [96](#)
    - NFS [268](#)
    - SNMP [81](#)
    - SNMP traps [81](#)
    - storage efficiency [171](#)
    - storage efficiency on a volume [181](#)
  - enabling user accounts
    - local Windows users [316](#)
  - encrypt data
    - while accessing this share [221](#)
  - entitlement risk
    - for licenses [71](#)
    - licenses [71](#)
    - node-locked licenses [71](#)
  - entitlement risks
    - managing licenses [70](#)
  - epsilon
    - understanding cluster [56](#)
  - Ethernet
    - editing port properties [101](#)
  - Ethernet ports
    - managing [100](#)
  - evaluation license
    - description of [71](#)
  - event log
    - viewing [149](#)
  - event notification
    - viewing [149](#)
  - events
    - severity of [149](#)
    - viewing [149](#)
  - Events window
    - viewing event log [149](#)
    - viewing event notification [149](#)
  - existing storage pools
    - considerations for adding SSDs to [132](#)
  - expanding
    - FlexGroup volumes [194](#)
  - expiry dates
    - extending Snapshot copies [178](#)
  - export policies
    - adding export rules to [277](#)
    - adding rules [278](#)
    - assigning new or existing for qtrees [247](#)
    - assigning to qtrees [248](#)
    - changing [218](#)
    - creating [277](#)
    - deleting [278](#)
    - deleting export rules [280](#)
    - how they control client access to qtrees [280](#)
    - how they control client access to volumes [280](#)
    - managing [277](#)
    - renaming [278](#)
  - Export Policies window
    - using to manage export policies and rules [281](#)
  - export policy rules
    - deleting [280](#)
    - editing
      - access protocols and details [279](#)
      - export policy rules [279](#)
    - editing client specification, access protocols, and access details [279](#)
  - export rules
    - adding to export policies [277, 278](#)
  - exporting
    - qtrees [248](#)
  - extending
    - expiry date of Snapshot copies [178](#)
  - external services
    - requirements for using Kerberos with NFS [300](#)
- ## F
- fabric health monitors
    - about [151](#)
  - fan-out configurations
    - networking requirements for cluster peering [63](#)
  - FC
    - configuring on the SVM [48](#)
    - starting or stopping [275](#)
  - FC SAN optimized LUNs

- creating during cluster setup [225](#)
  - FC/FCoE
    - changing the node name [276](#)
    - editing adapter settings [104](#)
  - FC/FCoE adapters
    - managing [104](#)
  - FC/FCoE protocols
    - managing [275](#)
  - FC/FCoE window [277](#)
  - FCAL drives
    - how ONTAP reports disk types [135](#)
  - FCoE
    - configuring on the SVM [48](#)
    - converged network adapters [277](#)
    - data center bridging [277](#)
    - Ethernet switch [277](#)
    - starting or stopping [275](#)
    - traditional FC [277](#)
  - FCP
    - changing node name [276](#)
    - defined [276](#)
    - nodes defined [276](#)
  - feedback
    - how to send comments about documentation [373](#)
  - Fibre Channel protocol
    - starting or stopping [275](#)
  - file permissions
    - NFSv4.1 ACLs [327](#)
    - SMB ACLs [327](#)
  - files
    - creating FlexClone [173](#)
    - hard limits for [254](#)
    - rules for assigning to Storage QoS policy groups [291](#)
    - soft limits for [254](#)
  - firewalls
    - requirements for cluster peering [63](#)
  - Flash Cache
    - enabling or disabling [148](#)
    - how it improves performance [148](#)
    - managing [148](#)
    - read workload [148](#)
  - Flash Cache window [148](#)
  - Flash Pool aggregate
    - managing [158](#)
  - Flash Pool aggregates
    - considerations when moving volumes in [205](#)
    - creating [39](#)
    - creating storage pools [127](#)
    - deleting storage pools [128](#)
    - how storage pools increase cache allocation flexibility for [129](#)
    - how they work [120](#)
    - how you use storage pools with [129](#)
    - increasing the size by adding SSDs [115](#)
    - provisioning cache by adding SSDs [114](#)
    - provisioning storage by creating [38](#)
    - requirements and best practices for using storage pools with [130](#)
    - using the statistics window [158](#)
  - Flash Pool SSD partitioning
    - how it increases cache allocation flexibility for Flash Pool aggregates [129](#)
  - Flash Pool Statistics window
    - using to monitor Flash Pool aggregates [158](#)
  - FlexClone files
    - creating [173](#)
  - FlexClone volumes
    - creating [172](#)
    - space guarantees and [200](#)
    - splitting from the parent volume [173](#)
    - viewing the hierarchy [174](#)
  - FlexGroup volume
    - changing the status [195](#)
  - FlexGroup volume status
    - changing [195](#)
  - FlexGroup volumes
    - creating [193](#)
    - deleting [195](#)
    - editing [194](#)
    - expanding [194](#)
    - resizing [194](#)
    - viewing information about [196](#)
  - FlexVol volumes
    - about [196](#)
    - creating [51](#)
    - creating Snapshot copies [175](#)
    - creating SVMs with [42](#)
    - deleting [171](#)
    - editing properties [169](#)
    - how moving them works [119](#), [206](#)
    - how volume guarantees work with [199](#)
    - initializing a vault relationship [346](#)
    - mirror relationships for [341](#)
    - moving [118](#)
    - moving from an SVM [183](#)
    - renaming Snapshot copies [179](#)
    - rules for assigning to Storage QoS policy groups [291](#)
    - setting reserve for Snapshot copies [176](#)
    - SnapVault backup limitations [352](#)
    - thick provisioning for [199](#)
    - unmounting [218](#)
    - which data gets backed up and restored from [352](#)
    - with SVMs, explained [162](#)
  - fractional reserve
    - editing the volume [169](#)
  - FSAS drives
    - how ONTAP reports disk types [135](#)
  - full-mesh connectivity
    - description [63](#)
- ## G
- gateway addresses
    - editing the subnet [93](#)
  - generating
    - AutoSupport
      - monitoring storage system health [155](#)
      - AutoSupport data for nodes [155](#)
  - getting started tasks
    - for System Manager [22](#)
  - group mappings
    - Infinite Volumes [327](#)
  - group memberships
    - of local Windows users, removing [316](#)
  - group policies
    - enabling or disabling for CIFS [261](#)

- reloading [261](#)
- group policy
  - updating CIFS [260](#)
- groups
  - adding users, Windows local [312](#)
  - assigning to a user account [316](#)
  - deleting, Window local [314](#)
  - local, creating on Windows [310](#)
  - local, renaming on Windows [313](#)
  - predefined local BUILTIN [321](#)
- guarantees, volume
  - how they work with FlexVol volumes [199](#)
- guidelines
  - for creating LIFs [99](#)
  - for using deduplication [204](#)
  - for using LUN types [239](#)
  - for working with FlexVol volumes containing LUNs [238](#)
  - for working with Snapshot copies of Infinite Volumes [197](#)

## H

- HA pairs
  - monitoring [35](#)
- hard limits
  - editing quota [252](#)
  - for files and disk space for quotas [254](#)
- hardware model
  - of an HA node, viewing [35](#)
- hash stores
  - BranchCache, modifying the size of [262](#)
  - specifying path and maximum size for BranchCache configuration [261](#)
- HBA [274](#)
- HDD aggregates
  - considerations when moving volumes in [205](#)
- HDD RAID groups
  - sizing considerations for [138](#)
- HDDs
  - changing the RAID group of, when adding to aggregates [117](#)
  - compatible disk types [120](#)
  - converting existing aggregate to a Flash Pool aggregate [39](#)
  - creating aggregates [38](#)
  - using effective disk types for mixing [120](#)
- HDDs and SSDs
  - adding to aggregates [116](#)
- health
  - monitoring clusters [59](#)
  - monitoring SVMs [159](#)
- health alerts
  - acknowledging system [150](#)
  - deleting system [151](#)
  - suppressing system [151](#)
- health monitoring
  - introduction to system [150](#)
  - ways to respond to alerts [152](#)
- health monitors
  - available cluster [151](#)
- Help
  - about the [16](#)

- high availability
  - managing [68](#)
- High Availability window
  - using the view details of HA pairs [68](#)
- home directories
  - how ONTAP enables dynamic SMB [222](#)
- home directory
  - adding for CIFS [259](#)
  - deleting for CIFS [260](#)
- home directory shares
  - creating [221](#)
- host operating systems
  - guidelines for using LUN multiprotocol type [239](#)
- hot spare disks
  - how they work [136](#)
- hot spares
  - how System Manager works with [121](#)
  - minimum needed [137](#)

## I

- icons used in the dashboard
  - described [18](#)
- icons used in the interface
  - described [18](#)
- ifgroups
  - See* interface groups
- igroups
  - defined [241](#)
  - requirements for creating [242](#)
  - ways to limit LUN access in a virtualized environment with [242](#)
- inactivity timeout
  - configuring [28](#)
- incremental tape backup
  - of Infinite Volumes [200](#)
- incremental transfers
  - defined [350](#)
- Infinite Volumes
  - aggregate requirements [122](#)
  - aggregate requirements for data protection mirror relationships [123](#)
  - creating [52](#)
  - creating Snapshot copies [175](#)
  - definition of [197](#)
  - deleting [171](#)
  - editing properties [169](#)
  - group mappings [327](#)
  - guidelines for Snapshot copies [197](#)
  - how SnapDiff supports [200](#)
  - namespace constituent [122](#)
  - setting reserve for Snapshot copies [176](#)
  - support for incremental tape backup [200](#)
  - with SVMs, explained [162](#)
- information
  - how to send feedback about improving documentation [373](#)
- initial setup
  - clusters, creating LUNs [225](#)
- initializing
  - a vault relationship [346](#)
  - ComplianceClock time [146](#)
  - mirror and vault relationships [358](#)

- mirror relationships [334](#)
  - initiator groups
    - adding initiators [232](#)
    - creating [231](#)
    - deleting [231](#)
    - deleting initiators [232](#)
    - editing [237](#)
    - editing initiators [237](#)
    - name rules [242](#)
    - naming [242](#)
    - ostype of [242](#)
    - requirements for creating [242](#)
    - type [242](#)
    - viewing [238](#)
  - initiator security
    - viewing iSCSI [273](#)
  - initiators
    - adding [232](#)
    - adding security for iSCSI [271](#)
    - changing the default authentication method for iSCSI [272](#)
    - changing the name [237](#)
    - deleting from an initiator group [232](#)
    - editing the security style for iSCSI [272](#)
    - setting default security for iSCSI [273](#)
  - inline compression
    - configuring on a volume [181](#)
  - inline-only predefined efficiency policy
    - understanding [284](#)
  - intercluster connectivity
    - creating network interfaces for [31](#), [94](#)
  - intercluster interfaces
    - modifying [66](#)
  - intercluster LIFs
    - role for [98](#)
  - intercluster networking
    - definition of cluster peer [67](#)
  - interconnect status
    - viewing [35](#)
  - interface groups
    - creating [100](#)
    - defined [102](#)
    - editing the settings [101](#)
  - interface icons
    - described [18](#)
  - interfaces
    - deleting broadcast domains [92](#)
    - deleting subnets [94](#)
    - deleting VLANs [102](#)
    - enabling or disabling iSCSI service [270](#)
    - graphic, accessing a cluster by using OnCommand System Manager browser-based [28](#), [30](#)
    - logical, migrating to a different port [97](#)
    - modifying, network [96](#)
  - invalid state
    - Snapshot copies [198](#)
  - IP address disabled
    - setting up a network [26](#)
  - IP address range enabled
    - using for setting up a network [25](#)
  - IP addresses
    - assigning to multiple Service Processors [61](#)
    - editing for a Service Processor [62](#)
    - editing the subnet [93](#)
    - introduction to configuring pools of, into subnets [104](#)
    - modifying for domain controllers [264](#)
    - requirements for cluster peering [63](#)
    - when to use IPspaces to define distinct spaces [91](#)
  - IPspace
    - modifying [66](#)
  - IPspaces
    - creating [36](#)
    - default [91](#)
    - deleting [90](#)
    - explained [91](#)
    - managing [90](#)
    - properties of [91](#)
    - renaming [90](#)
    - requirements for cluster peering [63](#)
    - SVMs created by default [91](#)
    - when to use to separate client traffic [91](#)
  - iSCSI
    - changing the default authentication method for initiators [272](#)
    - configuring on the SVM [46](#)
    - creating aliases [270](#)
    - disabling on the interfaces [270](#)
    - editing the security style for initiators [272](#)
    - enabling on the interfaces [270](#)
    - explained [274](#)
    - initiator security [274](#)
    - initiator security, viewing [273](#)
    - nodes defined [274](#)
    - setting security for initiators [273](#)
  - iSCSI initiators
    - adding security [271](#)
  - iSCSI protocol
    - managing [269](#)
  - iSCSI service
    - starting [273](#)
    - stopping [273](#)
  - iSCSI window
    - using to manage iSCSI settings [275](#)
- ## J
- Job window [157](#)
  - jobs
    - about [157](#)
    - managing [157](#)
- ## K
- Kerberos
    - authentication [300](#)
    - creating a realm configuration [298](#)
    - editing configurations [301](#)
    - introduction to using with NFS for strong security [300](#)
    - modifying a realm configuration [299](#)
    - requirements for external services [300](#)
  - Kerberos interface services
    - managing [301](#)
  - Kerberos Interface window



- using to manage Kerberos configuration [301](#)
- Kerberos realm configurations
  - creating [298](#)
  - deleting [299](#)
  - editing [299](#)
- Kerberos realm services
  - creating [298](#)
- Kerberos Realm window
  - using to manage Kerberos realms [300](#)
- keys
  - managing licenses [70](#)

## L

- lag time [363](#)
- LDAP
  - adding a client configuration [294](#)
  - associating clients with SVMs [296](#)
  - deleting a client configuration [295](#)
  - deleting active clients [297](#)
  - editing client configuration [295](#)
  - fields in the LDAP configuration window [297](#)
  - fields in the LDAP window [296](#)
  - using [84](#)
  - viewing information about clients [84](#)
- LDAP client services
  - managing [294](#)
- LDAP clients
  - viewing [84](#)
- LDAP configuration
  - using to edit or delete active LDAP clients [297](#)
- LDAP configuration services
  - managing [296](#)
- LDAP server
  - managing [84](#)
- LDAP window
  - using to create LDAP clients [84](#), [296](#)
- license
  - FC [276](#)
- license types
  - and entitlement risk [71](#)
- licenses
  - adding [34](#)
  - deleting [69](#)
  - managing [69](#), [70](#)
- Licenses window
  - using to add or remove licenses [73](#)
- LIFs
  - creating [94](#)
  - creating for cluster management [31](#)
  - creating for node management [33](#)
  - defined [97](#)
  - editing network interfaces [96](#)
  - guidelines for creating [99](#)
  - introduction to configuring subnets to make creation easier [104](#)
  - migrating to a different port [97](#)
  - modifying intercluster [66](#)
  - port hierarchy of [97](#)
  - ports that can host [97](#)
  - roles for [98](#)
- limitations
  - SnapVault backup [352](#)
- limits
  - editing quota hard and soft limits [252](#)
- links
  - how SMB clients can access UNIX symbolic [265](#)
- lists
  - of supported privileges [320](#)
- local accounts
  - on Windows, deleting [318](#)
- local groups
  - creating on Windows [310](#)
  - predefined BUILTIN [321](#)
  - reasons for creating [320](#)
  - renaming on Windows [313](#)
- local links
  - how SMB clients can access UNIX symbolic [265](#)
- local privileges
  - defined [320](#)
- local users
  - creating on Windows [315](#)
  - on Windows, changing the password [318](#)
  - reasons for creating [320](#)
  - renaming on Windows [317](#)
- local users and groups
  - defined [319](#)
  - how they are used [319](#)
  - reasons for creating [320](#)
  - using for authentication and authorization [319](#)
- local Windows groups
  - adding members [312](#)
  - modifying the description [312](#)
  - modifying the privileges [312](#)
  - removing members [312](#)
- local Windows users
  - assigning group memberships [316](#)
  - disabling user accounts [316](#)
  - enabling user accounts [316](#)
  - modifying the description [316](#)
  - removing group memberships [316](#)
- locking
  - cluster user accounts [86](#)
  - SVM user accounts [305](#)
- log files
  - viewing [29](#)
- log levels
  - configuring [28](#)
- logical storage
  - managing [159](#)
- LUN clones
  - creating [233](#)
  - described [241](#)
- LUN size
  - for Oracle and SQL application types [226](#)
- LUNs
  - assigning them to Storage QoS [236](#)
  - bringing them online [234](#)
  - creating [229](#)
  - creating clones [233](#)
  - creating during initial setup [225](#)
  - deleting [231](#)
  - editing [233](#)
  - guidelines for host operating system type [239](#)
  - guidelines for working with FlexVol volumes with [238](#)



- initiator hosts [241](#)
  - managing [225](#)
  - moving [234](#)
  - non-space-reserved, described [239](#)
  - resizing [241](#)
  - rules for assigning to Storage QoS policy groups [291](#)
  - settings for different application types [226](#)
  - size and type [239](#)
  - space reservation, affect on how space is set aside for [239](#)
  - space reservations disabled [239](#)
  - space reservations enabled [239](#)
  - space-reserved, described [239](#)
  - taking offline [234](#)
  - viewing information about [238](#)
  - viewing initiator groups [238](#)
  - ways to limit access in a virtualized environment with port sets and igroups [242](#)
  - LUNs (array)
    - how available for Data ONTAP use [144](#)
    - ONTAP RAID groups with [139](#)
    - RAID protection for [137](#)
    - rules for mixing in an aggregate [145](#)
  - LUNs window
    - using to manage LUNs [243](#)
  - LUNs, array
    - assigning [142](#)
    - reassigning spares to nodes [143](#)
- ## M
- management devices
    - remote, understanding the Service Processor [62](#)
  - managing
    - local Windows group memberships [312](#)
    - SVM [164](#)
  - mappings, name
    - conversion rules [326](#)
  - master license
    - description of [71](#)
  - membership
    - group, assigning to users [316](#)
  - messages, AutoSupport
    - severity types [156](#)
  - MetroCluster configurations
    - adding licenses [34](#)
  - migrating
    - LIFs to a different port [97](#)
  - mirror and vault
    - creating a relationship from a source volume [190](#)
    - deleting a relationship [356](#)
    - editing a relationship [357](#)
  - mirror and vault relationship
    - creating from a destination SVM [354](#)
  - mirror and vault relationships
    - aborting [361](#)
    - breaking [360](#)
    - deleting [356](#)
    - initializing [358](#)
    - managing [354](#)
    - overview [363](#)
    - quiescing [359](#)
    - restoring Snapshot copies [362](#)
    - resuming [359](#)
    - resynchronizing [360](#)
    - updating [358](#)
    - using the Protection window for managing [364](#)
  - mirror d vault relationships
    - reverse resynchronizing [361](#)
  - mirror policies
    - deleting [286](#)
    - editing [286](#)
  - mirror relationships
    - aborting [339](#)
    - breaking [337](#)
    - components of [341](#)
    - data protection [341](#)
    - deleting [333](#)
    - initializing [334](#)
    - managing [330](#)
    - overview [363](#)
    - quiescing [336](#)
    - restoring Snapshot copies [339](#)
    - resuming [336](#)
    - resynchronizing [337](#)
    - reverse resynchronizing [338](#)
    - updating [335](#)
    - using the Protection window for managing [364](#)
  - mirror vault policies
    - deleting [286](#)
    - editing [286](#)
  - mirrored aggregates
    - explained [123](#)
  - mirroring
    - aggregates [118](#)
  - mirrors
    - creating a relationship from a destination SVM [330](#)
    - creating relationships from source SVM [185](#)
    - editing a relationship [333](#)
  - modifying
    - a Kerberos realm [299](#)
    - aggregate settings [112](#)
    - BranchCache settings [262](#)
    - broadcast domain settings [92](#)
    - CIFS properties [259](#)
    - data LIFs [96](#)
    - Ethernet port properties [101](#)
    - export policy names [278](#)
    - FC/FCoE adapter settings [104](#)
    - intercluster interfaces [66](#)
    - interface group settings [101](#)
    - IP addresses of preferred domain controllers [264](#)
    - IPspace [66](#)
    - IPspace name [90](#)
    - Kerberos configurations [301](#)
    - LDAP client configuration [295](#)
    - local Windows group description [312](#), [316](#)
    - mirror and vault relationships [357](#)
    - mirror relationships [333](#)
    - password for SVM user accounts [304](#)
    - privileges for local Windows groups [312](#)
    - quotas [252](#)
    - RAID group to which disks are added [117](#)
    - RAID type and RAID group size [113](#)
    - roles [307](#)
    - schedules [369](#)

- Service Processor settings [62](#)
- Snapshot policies [366](#)
- subnet settings [93](#)
- the cluster peer passphrase [66](#)
- the security style for iSCSI initiators [272](#)
- the share settings [221](#)
- the status of a FlexGroup volume [195](#)
- the status of a volume [174](#)
- user login methods [85](#)
- vault relationships [345](#)
- monitoring
  - HA pairs [35](#)
  - node connectivity, introduction to [150](#)
  - switches, introduction to [150](#)
  - system connectivity, introduction to [150](#)
- mounting
  - volumes [217](#)
- moving
  - LUNs [234](#)
  - volumes [118](#)
  - volumes from an SVM [183](#)
- MSATA drives
  - how ONTAP reports disk types [135](#)
- MTU settings
  - editing broadcast domain [92](#)
  - modifying the size [101](#)
- multi-disk carrier shelves
  - configuration requirements for [138](#)
- multi-disk carriers
  - determining when to remove [138](#)
  - spare requirements for [138](#)
- multiprotocol types
  - LUNs, guidelines for using [239](#)

## N

- name mapping
  - how it works [325](#)
  - managing [324](#)
- Name Mapping window [328](#)
- name mappings
  - conversion rules [326](#)
  - how used [325](#)
- name rules
  - igroups [242](#)
- name services
  - how ONTAP uses [165](#)
- namespace constituents
  - and thin provisioning [201](#)
  - definition [122](#)
- Namespace window
  - managing [217](#)
  - using to manage NAS namespace [219](#)
- namespaces
  - data protection for SVM [353](#)
- naming conventions
  - network port [102](#)
- NAS optimized volumes
  - creating for Oracle application [214](#)
- NDU
  - .See nondisruptive updates
- NetApp Support Site
  - obtaining ONTAP software images [77](#)

- network
  - creating broadcast domains [36](#)
  - creating subnets [37](#)
  - creating VLANs [100](#)
  - full-mesh connectivity described [63](#)
  - requirements for cluster peering [63](#)
- network interfaces
  - creating [94](#)
  - creating IPspaces [36](#)
  - creating VLANs [100](#)
  - deleting [96](#)
  - deleting IPspaces [90](#)
  - managing [94](#)
  - modifying the settings [96](#)
- network mask
  - editing for a Service Processor [62](#)
- network ports
  - introduction to grouping into broadcast domains for SVM traffic [93](#)
  - types of [102](#)
- Network Time Protocol
  - .See NTP
- Network window
  - using to create, edit, delete, or view details of network components [104](#)
- networks
  - dashboard for viewing details [57](#)
  - managing [90](#)
  - setting up [36](#)
  - setting up to manage clusters, nodes, Service Processors [25](#)
- new storage pools
  - considerations for adding SSDs to [132](#)
- NFS
  - configuring on the SVM [44](#)
  - editing the settings [268](#)
  - how ONTAP handles client authentication [269](#)
- NFS datastore
  - creating for VMware [193](#)
- NFS protocol
  - managing [268](#)
- NFS window
  - using to display and configure NFS settings [269](#)
- NIS
  - adding domains [293](#)
  - editing domains [293](#)
  - managing domains [293](#)
- NIS domains
  - editing [293](#)
  - managing [293](#)
- NIS window
  - using to view NIS settings [294](#)
- NL-SAS drives
  - how ONTAP reports disk types [135](#)
- node connectivity health monitors
  - about [151](#)
- node management
  - creating a cluster [22](#)
- node management LIFs
  - guidelines for creating [99](#)
  - role for [98](#)
- node names
  - changing for FC/FCoE [276](#)

- node status
  - viewing [35](#)
- node SVMs
  - described [164](#)
- node-locked license
  - description of [71](#)
- node-management interfaces
  - creating [33](#)
- nodes
  - assigning disks [37](#)
  - creating network interfaces for managing [33](#)
  - description of [57](#)
  - FCP [276](#)
  - generating AutoSupport data [155](#)
  - iSCSI [274](#)
  - managing [146](#)
  - moving volumes [183](#)
  - reassigning array LUNs [143](#)
  - reassigning disks to [134](#)
  - single-node cluster
    - See single-node clusters
  - updating the name [32](#)
  - viewing AutoSupport data [155](#)
- Nodes window
  - content and purpose of [147](#)
- non-root aggregates
  - adding capacity disks to [116](#)
- nondisruptive updates
  - how it works [77](#)
  - performing for clusters using System Manager [75](#)
- nondisruptive volume move
  - moving between aggregates or nodes [183](#)
  - performing [118](#)
- NTP
  - managing the cluster time with [79](#)

## O

- offlining
  - LUNs [234](#)
- OnCommand System Manager
  - accessing a cluster by using browser-based graphic interface [28, 30](#)
  - creating a cluster [22](#)
- OnCommand System Managercreating a cluster
  - setting up a cluster [24](#)
- online Help
  - about [16](#)
- ONTAP
  - additional conceptual information [21](#)
  - additional information [21](#)
- ONTAP disk types
  - comparison with industry standard [135](#)
- ONTAP software images
  - obtaining [77](#)
  - selecting for nondisruptive update [75](#)
- operating mode
  - modifying BranchCache [262](#)
- oplocks
  - enabling [221](#)
  - enabling or disabling for qtrees [247](#)
- opportunistic locks
  - See oplocks

- options
  - setting when creating qtrees [249](#)
- Oracle application
  - creating volumes [214](#)
  - provisioning storage [214](#)
- Oracle RAC
  - example volume settings [215](#)
  - LUN settings [226](#)
- Oracle RAC application
  - creating volumes [214](#)
  - provisioning storage [214](#)

## P

- pages
  - ways to customize the windows of storage object [19](#)
- PAM
  - See Flash Cache
- partial state
  - Snapshot copies [198](#)
- partitioning
  - how Flash Pool SSD increases cache allocation flexibility for [129](#)
- passphrases
  - modifying [66](#)
- passwords
  - changing cluster user account [85](#)
  - changing for a local Windows user [318](#)
  - changing for cluster [31](#)
  - changing for SVM user accounts [304](#)
- peer relationships
  - creating cluster [65](#)
  - deleting cluster [66](#)
  - requirements for clusters [63](#)
- peers
  - modifying the passphrase of cluster [66](#)
- peers window
  - using to manage peer relationships [67](#)
- per-share cache
  - creating for BranchCache configuration [261](#)
- performance
  - dashboard for viewing SVM details [159](#)
  - monitoring clusters [59](#)
  - monitoring SVMs [159](#)
- physical ports
  - defined [102](#)
- physical storage
  - managing [112](#)
- plexes
  - mirrored aggregate, explained [123](#)
- policies
  - assigning export, to qtrees [248](#)
  - assigning QoS policy groups [184, 236](#)
  - creating mirror [285](#)
  - creating mirror vault [285](#)
  - creating QoS policy groups [288](#)
  - creating vault [285](#)
  - deleting efficiency [283](#)
  - deleting export [278](#)
  - editing protection policies [286](#)
  - editing QoS policy groups [289](#)
  - efficiency policy described [284](#)

- introduction to managing data protection using SnapMirror [287](#)
  - reloading group [261](#)
  - renaming export [278](#)
  - Snapshot copy schedule and retention planning guidelines for SnapVault backups [352](#)
  - Snapshot, about [367](#)
  - policies, efficiency
    - editing [283](#)
  - policies, export
    - changing [218](#)
  - policies, predefined efficiency
    - understanding inline-only and default [284](#)
  - policy groups
    - assigning, QoS [184](#), [236](#)
    - creating, QoS [288](#)
    - deleting, QoS [288](#)
    - editing, QoS [289](#)
    - how maximum throughput works [290](#)
    - rules for assigning storage objects to [291](#)
    - types of [290](#)
    - what they are [290](#)
  - pools
    - considerations for when to use SSD storage [131](#)
    - IP address, introduction to configuring subnets of [104](#)
    - requirements and best practices for using storage [130](#)
  - port hierarchy
    - of LIFs [97](#)
  - port sets
    - creating [232](#)
    - deleting [233](#)
    - editing [237](#)
    - ways to limit LUN access in a virtualized environment with [242](#)
  - ports
    - adding or removing in interface groups [101](#)
    - editing broadcast domain [92](#)
    - editing Ethernet properties [101](#)
    - migrating LIFs to different [97](#)
    - naming conventions for [102](#)
    - network, introduction to grouping into broadcast domains for SVM traffic [93](#)
    - requirements for cluster peering [63](#)
    - that can host LIFs [97](#)
    - types of network [102](#)
  - portsets
    - See port sets
  - pre-update checks
    - validating the cluster before updating [75](#)
  - predefined
    - BUILTIN local groups [321](#)
  - predefined efficiency policies
    - understanding inline-only and default [284](#)
  - predefined roles
    - for cluster administrators [88](#)
    - for SVM administrators [307](#)
  - preferred domain controllers
    - adding [263](#)
    - deleting [264](#)
    - editing the IP address [264](#)
  - prerequisites
    - for configuring a cluster using System Manager [30](#)
  - primary volumes
    - defined [350](#)
  - privileges
    - defined, local [320](#)
    - list of supported local [320](#)
    - predefined BUILTIN group default [321](#)
  - protection policies
    - creating [285](#)
    - deleting [286](#)
    - editing [286](#)
    - managing [285](#)
  - Protection policies window
    - using to create, manage, and view details of policies [287](#)
  - Protection window
    - using to create and manage mirror, vault, and mirror vault relationships [364](#)
  - protocols
    - configuring CIFS and NFS on the SVM [44](#)
    - dashboard for viewing details [159](#)
  - provision storage
    - creating volumes for Oracle application [214](#)
  - provisioning storage
    - by creating HDD and SSD aggregates [38](#)
    - by creating volumes for Oracle application [214](#)
    - creating aggregates or Flash Pool aggregates [38](#)
    - creating Flash Pool aggregates [39](#)
    - creating SnapLock Compliance aggregates [41](#)
    - creating SnapLock Enterprise aggregates [41](#)
    - for Oracle application [214](#)
- ## Q
- QoS
    - See Storage QoS
  - QoS policy groups
    - managing [288](#)
  - QoS Policy Groups window
    - using to manage and view details about policy groups [292](#)
  - qtrees
    - about [248](#)
    - assigning an export policy to [248](#)
    - assigning new or existing export policies [247](#)
    - creating [246](#)
    - creating LUNs [229](#)
    - creating quotas [251](#)
    - deleting [247](#)
    - editing the security style [247](#)
    - enabling or disabling oplocks [247](#)
    - exporting [248](#)
    - how export policies control client access to [280](#)
    - options [249](#)
    - security style [249](#)
    - viewing information [248](#)
  - Qtrees
    - managing [246](#)
  - Qtrees window
    - using to manage qtrees [250](#)
  - Quality of Service
    - See Storage QoS
  - quiescing
    - mirror and vault relationships [359](#)

- mirror relationships [336](#)
- vault relationships [347](#)
- quorum
  - understanding cluster [56](#)
- quotas
  - activating or deactivating [253](#)
  - creating [251](#)
  - default quotas
    - description of [254](#)
  - deleting [252](#)
  - description of default [254](#)
  - description of group [254](#)
  - description of qtree [254](#)
  - description of user [254](#)
  - editing [252](#)
  - limits for [254](#)
  - management of [255](#)
  - managing [251](#)
  - qtree quotas
    - description of [254](#)
  - resizing [253](#)
  - security style changes [255](#)
  - user quotas
    - description of [254](#)
  - viewing information about [253](#)
- Quotas window
  - using to manage quotas [256](#)
- R**
- RAID
  - drive types defined [135](#)
- RAID group sizes
  - modifying [113](#)
- RAID groups
  - changing [117](#)
  - changing while adding capacity disks [117](#)
  - editing the size of [112](#)
  - how hot spares are calculated [121](#)
  - naming convention [119](#)
  - sizing considerations for [138](#)
  - with array LUNs, considerations [139](#)
- RAID protection
  - for array LUNs [137](#)
- RAID types
  - editing [112](#)
  - modifying [113](#)
- RAID0
  - how Data ONTAP uses for array LUNs [137](#)
  - use by Data ONTAP [137](#)
- raw device mapping [241](#)
- RBAC
  - predefined roles for cluster administrators [88](#)
  - predefined roles for SVM administrators [307](#)
- RDM [241](#)
- read workload statistics
  - Flash Cache [148](#)
- reassigning
  - array LUNs to nodes [143](#)
  - disks to nodes [134](#)
- relationships
  - components of mirror [341](#)
  - mirror and vault, creating from a destination SVM [354](#)
  - mirror and vault, creating from a source volume [190](#)
  - mirror and vault, reverse resynchronizing [361](#)
  - mirror, creating from a destination SVM [330](#)
  - mirror, creating from a source SVM [185](#)
  - mirror, reverse resynchronizing [338](#)
  - vault, creating from a destination SVM [342](#)
  - vault, creating from a source SVM [188](#)
- relationships, mirror and vault
  - aborting [361](#)
  - breaking [360](#)
  - initializing [358](#)
  - quiescing [359](#)
  - restoring a volume [362](#)
  - resuming [359](#)
  - resynchronizing [360](#)
  - reverse resynchronizing [361](#)
  - updating [358](#)
- relative symbolic links
  - how SMB clients can access UNIX [265](#)
- remote management devices
  - understanding the Service Processor [62](#)
- removing
  - multi-disk carriers, determining when it is safe [138](#)
  - preferred domain controllers [264](#)
- removing members
  - to local Windows groups [312](#)
- renaming
  - IPspaces [90](#)
  - local Windows groups [313](#)
  - local Windows users [317](#)
- requirements
  - cluster naming when peering [63](#)
  - firewall for cluster peering [63](#)
  - for using storage pools [130](#)
  - Infinite Volumes, aggregate [122](#)
  - IP addresses for cluster peering [63](#)
  - IPspaces for cluster peering [63](#)
  - network for cluster peering [63](#)
  - ports for cluster peering [63](#)
  - subnets for cluster peering [63](#)
- resetting
  - the password for Windows local users [318](#)
- resizing
  - FlexGroup volumes [194](#)
  - options for resizing volumes [205](#)
  - quotas [253](#)
  - volumes [180](#)
- respond to
  - alerts [152](#)
  - system health alerts [152](#)
- restarting
  - a vault relationship [348](#)
  - mirror and vault relationships [359](#)
  - mirror relationships [336](#)
- restoring
  - a volume from Snapshot copies [177](#)
  - a volume in a mirror and vault relationship [362](#)
  - to a volume in a mirror relationship [339](#)
  - to a volume in a vault relationship [349](#)
- resuming
  - a vault relationship [348](#)

- mirror and vault relationships [359](#)
- mirror relationships [336](#)
- resync
  - reverse resynchronizing mirror and vault relationships [361](#)
  - reverse resynchronizing mirror relationships [338](#)
- resynchronizing
  - mirror and vault relationships [360](#)
  - mirror relationships [337](#)
- reverse resynchronizing
  - mirror and vault relationships [361](#)
  - mirror relationships [338](#)
- reversions
  - obtaining ONTAP software images [77](#)
- role-based access control
  - predefined roles for cluster administrators [88](#)
  - predefined roles for SVM administrators [307](#)
- roles
  - adding [87](#), [306](#)
  - for LIFs [98](#)
  - managing [87](#), [306](#)
  - modifying an access-control role's access [307](#)
  - modifying the attributes [88](#)
  - predefined for cluster administrators [88](#)
  - predefined for SVM administrators [307](#)
- Roles window [89](#), [308](#)
- root aggregates
  - adding capacity disks to [116](#)
- root information
  - data protection for SVM [353](#)
- RPM
  - rules for displaying disk [122](#)
- rules
  - applied for displaying disk types and disk RPM [122](#)
- rules, conversion
  - name mapping [326](#)

## S

- SAN environments
  - which LUN data is backed up to SnapVault backups [352](#)
- SAS drives
  - how ONTAP reports disk types [135](#)
- SATA drives
  - how ONTAP reports disk types [135](#)
- schedules
  - changing deduplication [182](#)
  - creating [368](#)
  - deleting [369](#)
  - editing [369](#)
  - guidelines for planning Snapshot copy [352](#)
  - setting up for creating Snapshot copies [177](#)
- schedules window [370](#)
- secondary volumes
  - defined [350](#)
- security
  - adding for iSCSI initiators [271](#)
  - editing the default settings [271](#)
  - modifying roles [307](#)
  - requirements for using Kerberos with NFS [300](#)
  - setting the default for iSCSI initiators [273](#)
  - viewing iSCSI initiator [273](#)
- security style
  - editing the volume [169](#)
- security styles
  - changing quotas [255](#)
  - editing for qtrees [247](#)
- server keys
  - specifying for BranchCache configuration [261](#)
- Service Processor
  - managing [61](#)
- Service Processors
  - assigning IP addresses globally [61](#)
  - editing the settings [62](#)
  - understanding [62](#)
- service processors window
  - using to view and edit Service Processors [62](#)
- setting
  - the time zone [35](#)
- setting up
  - AutoSupport [154](#)
  - BranchCache [261](#)
  - CIFS [258](#)
  - cluster environment [22](#)
  - clusters
    - setting up [30](#)
  - logical storage
    - setting up [42](#)
  - physical storage
    - setting up [37](#)
  - the cluster [30](#)
  - the network [36](#)
- setting up a cluster
  - by using the template file in your data center [22](#)
  - using OnCommand System Manager in your data center [24](#)
- setting up a network
  - by using OnCommand System Manager [25](#)
  - for managing cluster, nodes, Services Processors [25](#)
  - when the IP address range is disabled [26](#)
  - when the IP address range is enabled [25](#)
- setting up a support page
  - cluster setup [27](#)
  - using OnCommand System Manager [27](#)
- severity types
  - AutoSupport message [156](#)
- shared SSDs
  - See* storage pools
- shares
  - creating, CIFS [219](#)
  - disabling [220](#)
  - editing permissions and options [221](#)
  - managing [219](#)
- Shares window
  - using to manage shares [223](#)
- shelves
  - configuration requirements for multi-disk carrier [138](#)
- Simple Network Management Protocol
  - See* SNMP
- single-node clusters
  - description of [56](#)
- site license
  - description of [71](#)
- sizing
  - RAID groups, considerations for [138](#)

- SMB
  - about using BranchCache for caching at branch offices [266](#)
  - concepts [264](#)
  - configuring BranchCache on [261](#)
  - modifying BranchCache configurations for [262](#)
- SMB access
  - how to use UNIX symbolic links for [265](#)
- SMB encryption
  - setting up [258](#)
- SMB home directories
  - how ONTAP enables dynamic [222](#)
- SMB shares
  - how ONTAP enables dynamic home directories on [222](#)
- SnapDiff
  - defined [200](#)
  - how it works with namespace mirror constituents [200](#)
  - incremental tape backups of Infinite Volumes, using [200](#)
- SnapLock Compliance aggregates
  - creating [41](#)
- SnapLock Compliance volumes
  - creating [54](#)
- SnapLock Enterprise aggregates
  - creating [41](#)
- SnapLock Enterprise volumes
  - creating [54](#)
- SnapMirror
  - how it works [341](#)
- SnapMirror labels
  - defined [350](#)
- SnapMirror policies
  - introduction to managing data protection using [287](#)
- SnapMirror relationships
  - quiescing [336](#)
  - updating [335](#)
- SnapMirror volumes
  - FlexClone volumes considerations for [197](#)
- Snapshot copies
  - automatic scheduling [177](#)
  - creating [175](#)
  - creating policies for automatically creating [366](#)
  - defined [350](#)
  - deleting [179](#)
  - directory, making invisible [177](#)
  - extending expiry date [178](#)
  - guidelines for Infinite Volumes [197](#)
  - incremental tape backups of Infinite Volumes, using [200](#)
  - Infinite Volumes [198](#)
  - renaming [179](#)
  - restoring a volume from [177](#)
  - restoring to a source in a mirror and vault relationship or other volumes [362](#)
  - restoring to a source in a mirror relationship or other volumes [339](#)
  - restoring to a source in a vault relationship or other volumes [349](#)
  - setting reserve [176](#)
  - states [198](#)
  - used by SnapDiff to identify file and directory differences [200](#)
  - viewing list of [175](#)
- Snapshot copies of Infinite Volumes
  - guidelines for [197](#)
- Snapshot policies
  - about [367](#)
  - creating [366](#)
  - deleting [367](#)
  - editing [366](#)
  - managing [366](#)
- Snapshot policies window
  - using to add, edit and delete Snapshot policies [367](#)
- SnapVault
  - which data is backed up and restored from FlexVol volume [352](#)
- SnapVault backups
  - data protection for SVM namespace and root information [353](#)
  - guidelines for planning Snapshot copy schedule and retention for [352](#)
  - how they work [351](#)
  - how they work with data compression [352](#)
  - limitations for FlexVol volume backup [352](#)
- SnapVault relationships
  - defined [350](#)
- SNMP
  - enabling or disabling [81](#)
  - enabling or disabling SNMP traps [81](#)
  - introduction to managing on the cluster [82](#)
  - managing [81](#)
  - options to use for configuring [82](#)
  - specifying system location, contact personnel, and SNMP community information [81](#)
  - testing the trap host configuration [82](#)
- SNMP window
  - content and purpose of [83](#)
- soft limits
  - editing quota [252](#)
  - for files and disk space for quotas [254](#)
- software efficiency
  - achieving using FlexVol volumes [200](#)
- software entitlements
  - managing licenses [70](#)
- software images
  - selecting the ONTAP image for update [75](#)
- software images, ONTAP
  - obtaining [77](#)
- software licenses
  - adding [34](#)
- source volumes
  - components of a mirror relationship [341](#)
- SP
  - See* Service Processors
- space
  - resizing volumes for more space [180](#)
- space efficiency
  - configuring deduplication and data compression [181](#)
- space guarantees
  - See* volume guarantees
- space reservation
  - affect on how space is set aside for LUNs [239](#)
  - thick provisioning [201](#)



- thin provisioning [201](#)
- spare array LUNs
  - reassigning to nodes [143](#)
  - zeroing [143](#)
- spare disks
  - (compatible), described [121](#)
  - minimum needed [137](#)
  - reassigning to disks [134](#)
  - requirements for multi-disk carriers [138](#)
  - zeroing [38](#)
- splitting
  - FlexClone volumes [173](#)
- SPs
  - See* Service Processors
- SQL
  - LUN settings [226](#)
- SSD storage pools
  - See* storage pools
- SSDs
  - adding to HDDs for converting to Flash Pool aggregates [39](#)
  - adding to storage pools [128](#)
  - combining to create storage pools [127](#)
  - considerations for adding to existing storage pool versus new one [132](#)
  - considerations for when to use storage pools [131](#)
  - creating aggregates [38](#)
  - dedicated SSDs [114](#)
  - how ONTAP reports disk types [135](#)
  - how storage pools work [132](#)
  - how used in Flash Pool aggregates [120](#)
  - increasing the size of Flash Pool aggregates by adding [115](#)
  - provisioning cache by adding [114](#)
  - shared
    - See* storage pools
  - sizing considerations for RAID groups [138](#)
  - storage pools [114](#)
- standard license
  - description of [71](#)
- starting
  - FC or FCoE service [275](#)
  - iSCSI service [273](#)
  - SVMs [162](#)
- states
  - Snapshot copies [198](#)
- status
  - viewing node and interconnect [35](#)
- stopping
  - a mirror and vault relationship [361](#)
  - a mirror relationship [339](#)
  - a vault relationship [348](#)
  - FC or FCoE service [275](#)
  - iSCSI service [273](#)
  - SVMs [162](#)
- storage
  - provisioning by creating aggregates [38](#)
  - rules for mixing array LUNs in an aggregate [145](#)
- storage classes
  - aggregate overcommitment in Infinite Volumes with [201](#)
- storage efficiency
  - benefits of [203](#)
  - editing the settings [169](#)
  - enabling [171](#)
  - enabling on a volume [181](#)
  - how SnapVault backups work with data compression [352](#)
  - running deduplication [183](#)
- storage object pages
  - ways to customize the windows [19](#)
- storage pools
  - adding disks to [128](#)
  - adding SSDs as [115](#)
  - advantages of SSD [131](#)
  - assigning disks to increase capacity [37](#)
  - considerations for adding SSDs to new versus existing [132](#)
  - considerations for when to use SSD [131](#)
  - creating [127](#)
  - deleting [128](#)
  - disadvantages of SSD [131](#)
  - how they increase cache allocation for Flash Pool aggregates [129](#)
  - how they work [132](#)
  - how you use [129](#)
  - managing [127](#)
  - reassigning disks to increase capacity [134](#)
  - requirements and best practices for [130](#)
  - why you add disks to [132](#)
- Storage Pools window
  - using to create, display, and manage SSDs [132](#)
- storage provisioning
  - creating SnapLock aggregates [41](#)
- Storage QoS
  - assigning LUNs to [236](#)
  - assigning volumes to [184](#)
  - creating policy groups [288](#)
  - deleting policy groups [288](#)
  - editing policy groups [289](#)
  - how it helps [289](#)
  - how it works [290](#)
  - how maximum throughput works [290](#)
  - rules for assigning storage objects to policy groups [291](#)
  - types of policy groups [290](#)
  - types of workloads [290](#)
  - what it is [289](#)
  - workflow [289](#)
- storage system access
  - editing login methods [85](#)
- storage system dashboard icons
  - described [18](#)
- storage system location
  - specifying information for SNMP [81](#)
- strong security
  - requirements for using Kerberos with NFS [300](#)
- subnets
  - assigning IP addresses to Service Processors [61](#)
  - creating [37](#)
  - deleting [94](#)
  - introduction to configuring [104](#)
  - managing [93](#)
  - modifying the settings [93](#)
  - requirements for cluster peering [63](#)



- specifying the IP address for the network interface [94](#)
  - suggestions
    - how to send feedback about documentation [373](#)
  - supportability dashboard [20](#)
  - supported
    - local privileges [320](#)
  - SVM
    - FC traffic [276](#)
  - SVM administrators
    - capabilities of [164](#)
  - SVMs
    - adding CIFS server preferred domain controllers [263](#)
    - adding user accounts for [304](#)
    - associating LDAP clients with [296](#)
    - benefits of using [165](#)
    - changing the user account password [304](#)
    - configuring basic details [42](#)
    - configuring CIFS protocol [44](#)
    - configuring DNS [42](#)
    - configuring FC protocol [48](#)
    - configuring FCoE protocol [48](#)
    - configuring for SVM administrators [59](#)
    - configuring iSCSI protocol [46](#)
    - configuring NFS protocol [44](#)
    - creating in clusters [42](#)
    - creating LUNs during initial setup [225](#)
    - creating network interfaces for managing [94](#)
    - creating vault relationships from destination [342](#)
    - dashboard for viewing details [159](#)
    - data protection for namespace information [353](#)
    - data protection for root information [353](#)
    - delegating to SVM administrators [49](#)
    - deleting [161](#)
    - deleting active LDAP clients [297](#)
    - deleting preferred domain controllers on [264](#)
    - editing [160](#)
    - editing Kerberos configurations [301](#)
    - editing user accounts [305](#)
    - introduction to managing SNMP on the cluster [82](#)
    - locking or unlocking user accounts [305](#)
    - managing [159](#), [164](#)
    - managing user accounts [304](#)
    - monitoring the health of [159](#)
    - predefined roles for administrators [307](#)
    - predefined roles for cluster administrators [88](#)
    - setting up BranchCache on [261](#)
    - starting [162](#)
    - stopping [162](#)
    - types of [164](#)
    - unmounting FlexVol volumes from the namespace [218](#)
    - with FlexVol volumes, explained [162](#)
    - with Infinite Volume, explained [162](#)
  - SVMs SNMP
    - enabling or disabling [81](#)
  - SVMs window
    - using to manage SVMs [166](#)
  - SVMs with FlexVol volumes
    - creating [42](#)
    - explained [162](#)
    - rules for assigning to Storage QoS policy groups [291](#)
  - SVMs with Infinite Volume
    - aggregate requirements [122](#)
    - assigning aggregates to [50](#)
    - explained [162](#)
  - switch name services
    - how ONTAP uses [165](#)
  - switches
    - introduction to monitoring health of [150](#)
  - symbolic links
    - editing the settings of [221](#)
    - how SMB clients can access UNIX [265](#)
  - system alerts
    - managing [150](#)
  - System Alerts window
    - using to acknowledge, delete, or suppress alerts [153](#)
  - system connectivity health monitors
    - about [151](#)
  - system health
    - introduction to monitoring [150](#)
  - system health alerts
    - acknowledging [150](#)
    - deleting [151](#)
    - responding to [152](#)
    - suppressing [151](#)
  - system logging
    - about [29](#)
    - log levels [29](#)
  - System Manager
    - about [17](#)
    - OnCommand, accessing a cluster by using browser-based graphic interface [28](#), [30](#)
    - prerequisites for configuring a cluster [30](#)
    - tasks you can perform from [17](#)
  - System Manager log files
    - viewing [29](#)
  - system SVMs
    - described [164](#)
- ## T
- template file for creating a cluster
    - using to set up a cluster [22](#)
  - temporary license
    - description of [71](#)
  - testing
    - AutoSupport configuration [155](#)
    - trap host configuration [82](#)
  - thick provisioning
    - about [201](#)
  - thin provisioning
    - about [201](#)
    - for Infinite Volumes [201](#)
    - using FlexVol volumes [200](#)
  - threshold
    - disk space limits for [254](#)
  - time
    - managing the cluster [79](#)
  - time zone
    - setting it [35](#)
  - timeout
    - configuring inactivity [28](#)
  - trap hosts
    - testing the configuration [82](#)
  - traps

- enabling or disabling SNMP [81](#)
- troubleshooting
  - viewing log files [29](#)
- Twitter
  - how to receive automatic notification of documentation changes [373](#)
- two-node clusters
  - description of [56](#)
- types
  - overview of data protection relationships [363](#)
  - rules for displaying disk [122](#)

## U

- UI icons
  - described [18](#)
- understanding
  - how nondisruptive update is performed [77](#)
  - space reservation setting [239](#)
- UNIX
  - managing users and groups [309](#)
- UNIX users
  - editing the properties [259](#)
- unlocking
  - cluster user accounts [86](#)
  - SVM user accounts [305](#)
- unowned disks
  - assigning ownership [37](#)
- updates
  - batch and rolling update [77](#)
  - performing a nondisruptive upgrade through System Manager [75](#)
  - to mirror and vault relationships [358](#)
  - to mirror relationships [335](#)
- updating
  - cluster name [31](#)
  - the node name [32](#)
- upgrades
  - obtaining ONTAP software images [77](#)
  - See also* nondisruptive updates
- user accounts
  - adding for a cluster [85](#)
  - changing passwords for cluster [85](#)
  - changing the password for SVMs [304](#)
  - editing for a cluster [85](#)
  - editing SVM user accounts [305](#)
  - locking or unlocking on clusters [86](#)
  - locking or unlocking SVM [305](#)
  - managing [86](#)
  - predefined roles for cluster administrators [88](#)
  - predefined roles for SVM administrators [307](#)
  - SVM [304](#)
- user names
  - how mapping works [325](#)
- users
  - adding the home directory path for CIFS [259](#)
  - adding to Windows local group [312](#)
  - assigning group memberships [316](#)
  - changing the password, Windows local [318](#)
  - deleting, Window local [318](#)
  - local, creating on Windows [315](#)
  - local, renaming on Windows [317](#)
  - managing [85](#)

- users and groups
  - local, defined [319](#)
  - local, using for authentication and authorization [319](#)
- Users window
  - using to manage accounts, reset user passwords, and display information [86](#), [305](#)

## V

- valid state
  - Snapshot copies [198](#)
- validating
  - checking the cluster before an update [75](#)
- vault policies
  - deleting [286](#)
  - editing [286](#)
- vault relationships
  - initializing [346](#)
  - managing [342](#)
  - overview [363](#)
  - quiescing [347](#)
  - resuming [348](#)
  - stopping [348](#)
  - updating [347](#)
  - using the Protection window for managing [364](#)
- vaults
  - creating a relationship from a destination SVM [342](#)
  - creating a relationship from a source SVM [188](#)
  - deleting a relationship [345](#)
  - editing a relationship [345](#)
  - restoring a volume [349](#)
- versions
  - modifying BranchCache [262](#)
- viewing
  - aggregate information [119](#)
  - AutoSupport
    - viewing status [155](#)
  - AutoSupport data [155](#)
  - FlexClone volume hierarchy [174](#)
  - FlexGroup volume information [196](#)
  - initiator groups [238](#)
  - iSCSI initiator security [273](#)
  - LDAP client configuration [84](#)
  - log files [29](#)
  - LUN information [238](#)
  - qtree information [248](#)
  - quota information [253](#)
- virtual ports
  - constitute VLANs and interface groups [102](#)
- virtualized environments
  - ways to limit LUN access with port sets and igroups [242](#)
- VLANs
  - creating [100](#)
  - defined [102](#)
  - deleting [102](#)
  - editing the settings [101](#)
  - subdivide a physical port into multiple separate logical ports [102](#)
  - tagging [103](#)
- VMware
  - creating NFS datastore [193](#)
- volume guarantees

- effect on maximum FlexVol volume size [199](#)
  - how they work with FlexVol volumes [199](#)
  - volume move
    - manually triggering the cutover [184](#)
  - volume sizes
    - for Oracle application types, examples [215](#)
  - volume status
    - changing [174](#)
  - volumes
    - aborting a mirror and vault relationship [361](#)
    - aborting a mirror relationship [339](#)
    - adding efficiency policies to run deduplication [282](#)
    - changing the status [174](#)
    - components of a mirror relationship [341](#)
    - considerations when moving [205](#)
    - creating an export policy for client access to [277](#)
    - creating an Infinite Volume [52](#)
    - creating FlexClone [172](#)
    - creating FlexVol [51](#)
    - creating for Oracle application [214](#)
    - creating LUNs [229](#)
    - creating qtrees [246](#)
    - creating quotas [251](#)
    - creating SnapLock Compliance [54](#)
    - creating SnapLock Enterprise [54](#)
    - creating Snapshot copies [175](#)
    - data protection, editing [171](#)
    - deduplication
      - changing schedule [182](#)
    - deleting [171](#)
    - deleting Snapshot copies [179](#)
    - editing the properties [169](#)
    - enabling storage efficiency [181](#)
    - example settings for Oracle application types [215](#)
    - hiding the Snapshot copy directory [177](#)
    - how export policies control client access to [280](#)
    - how FlexVol volumes work [196](#)
    - how moving FlexVol volumes works [119](#), [206](#)
    - Infinite Volume defined [197](#)
    - managing [168](#)
    - manually triggering cutover for a volume move [184](#)
    - mounting [217](#)
    - moving LUNs across [234](#)
    - moving nondisruptively [118](#)
    - moving nondisruptively from an SVM [183](#)
    - options for resizing [205](#)
    - resizing [180](#)
    - restoring from Snapshot copies [177](#)
    - restoring Snapshot copies to volumes in mirror and vault relationships [362](#)
    - restoring Snapshot copies to volumes in mirror relationships [339](#)
    - resuming a vault relationship [348](#)
    - running deduplication [183](#)
    - scheduling Snapshot copies [177](#)
    - setting reserve for Snapshot copies [176](#)
    - SnapVault backup limitations for FlexVol [352](#)
    - stopping a vault relationship [348](#)
    - SVMs with FlexVol, explained [162](#)
    - SVMs with Infinite, explained [162](#)
    - unmounting FlexVol volumes [218](#)
    - updating a vault relationship [347](#)
    - viewing FlexClone hierarchy [174](#)
    - viewing list of Snapshot copies [175](#)
    - viewing the Snapshot copies [175](#)
    - which data gets backed up and restored from FlexVol [352](#)
  - Volumes window
    - using to manage FlexGroup volumes [206](#)
    - using to manage FlexVol volumes and Infinite Volumes [206](#)
    - using to manage volumes [206](#)
  - Vservers
    - See* SVMs
- ## W
- ways to respond to alerts
    - health monitoring [152](#)
  - web services
    - accessing a cluster by using OnCommand System Manager browser-based graphic interface [28](#), [30](#)
  - widelinks
    - how SMB clients can access UNIX symbolic [265](#)
  - window layouts
    - ways to customize [19](#)
  - Windows
    - managing [310](#)
  - Windows local groups
    - creating [310](#)
    - deleting [314](#)
    - renaming [313](#)
  - Windows local user accounts
    - deleting [318](#)
  - Windows local users
    - changing the password [318](#)
    - creating [315](#)
    - renaming [317](#)
  - Windows users
    - editing the properties [259](#)
  - Windows window [322](#)
  - workloads
    - types of [290](#)
    - what they are [290](#)
  - WWPNs
    - about configuring for LIFs [97](#)
- ## Z
- zeroing
    - array LUNs [143](#)
    - disks [38](#)