Cluster Management Workflows for OnCommand® System Manager

June 2017 | 215-11440-C0
doccomments@netapp.com
Updated forONTAP 9.2
# Contents

OnCommand System Manager workflows ................................. 5

Setting up a cluster by using OnCommand System Manager ........ 7
- Setting up a cluster by using the template file .......................... 8
- Setting up the cluster manually ............................................. 10
  - Creating a cluster .............................................................. 10
  - Setting up a network ......................................................... 11
  - Setting up a support page .................................................. 13
  - Reviewing storage recommendations .................................. 13
- Creating an SVM ............................................................... 14

Performing a nondisruptive cluster update ............................. 16
- Obtaining ONTAP software images ....................................... 16
- Updating the cluster nondisruptively ..................................... 17

Setting up the network ....................................................... 20
- Creating VLAN interfaces .................................................. 21
- Creating interface groups .................................................... 21
- Creating broadcast domains ............................................... 22
- Creating subnets ............................................................... 22
- Creating network interfaces ............................................... 22

Assigning disks or array LUNs to nodes ................................. 25
- Assigning disks to nodes ..................................................... 25
- Zeroing spare disks ........................................................... 26
- Assigning array LUNs ........................................................ 26
- Zeroing spare array LUNs .................................................... 27

Managing storage tiers by using FabricPool ............................ 28
- Adding an external capacity tier .......................................... 29
- Attaching an aggregate to external capacity tier .................... 30
- Provisioning storage by creating a FabricPool ....................... 30
- Changing the tiering policy of a volume ............................... 31

Managing FlexGroup volumes using System Manager ............. 32
- Creating FlexGroup volumes .............................................. 32

Resizing FlexGroup volumes using System Manager ............... 34
- Resizing FlexGroup volumes .............................................. 34

Assigning disks to existing aggregates ................................. 36
- Adding capacity disks ....................................................... 38
- Provisioning cache to aggregates by adding SSDs .................. 39
- Creating a storage pool ...................................................... 40

Provisioning cache through Flash Pool aggregates ................. 42
- Provisioning cache to aggregates by adding SSDs .................. 43
- Increasing the cache for Flash Pool aggregates by adding SSDs 44
- Creating a storage pool ...................................................... 44

Providing data resiliency by mirroring aggregates .................. 46
OnCommand System Manager workflows

The workflow guide provides workflows for some of the new functionalities introduced in OnCommand System Manager.

Workflows are provided for the following functionalities that were introduced or enhanced in System Manager 9.1:

- **Creating a cluster using System Manager** on page 7
  Provides information about creating a cluster, setting up node management and cluster management networks, and AutoSupport messages and event notifications using System Manager.

- **Managing FlexGroups** on page 32
  Provides information about creating FlexGroup volumes, editing the properties of the existing FlexGroup volumes, resizing FlexGroup volumes, changing the status of FlexGroup volumes, and deleting FlexGroup volumes.

- **Resizing FlexGroup volumes using System Manager** on page 34
  Provides information about resizing FlexGroup volumes by resizing existing resources or adding new resources.

Workflows are provided for the following functionalities that were introduced or enhanced in System Manager 9.0:

- **Protecting data using SnapLock** on page 66
  Provides information about using SnapLock for data protection.

Workflows are provided for the following functionalities that were introduced or enhanced in System Manager 8.3.2:

- **Assigning disks or array LUNs to nodes** on page 25
  Provides information about assigning disks and array LUNs to nodes.

- **Providing data resiliency by mirroring aggregates** on page 46
  Provides information about mirroring aggregates using the SyncMirror feature.

- **Protecting data using mirror and vault relationship** on page 60
  Provides information about protecting data using mirror and vault relationships.

Workflows are provided for the following functionalities that were introduced or enhanced in System Manager 8.3.1:

- **Performing a nondisruptive cluster update** on page 16
  Provides information about performing a nondisruptive cluster update.

- **Setting up the network** on page 20
  Provides information about configuring network components during and after cluster setup to manage and access data from your SVMs.

- **Assigning disks to existing aggregates** on page 36
  Provides information about adding disks (capacity or cache) to increase the size of aggregates to provide storage for one or more volumes.

Workflows are provided for the following functionalities that were introduced or enhanced in System Manager 8.3:

- **Provisioning cache through Flash Pool aggregates** on page 42
Provides information about provisioning cache by creating Flash Pool aggregates or converting existing aggregates to Flash Pool aggregates by adding SSDs.

- **Providing data access to qtrees using export policies** on page 50
  Provides information about exporting a specific qtree on a volume by assigning export policies to it.

- **Configuring a Service Processor** on page 54
  Provides information about configuring a Service Processor (SP) to monitor and manage various system parameters of your storage systems.

- **Setting up the BranchCache configuration** on page 56
  Provides information about setting up the BranchCache configuration on a CIFS-enabled SVM and about enabling BranchCache on shares to enable caching of content on computers that are local to the requesting clients.

System Manager 8.3 and later versions also include the following functionalities that are covered in the workflows in the *Express Guides*:

- Creating cluster peer relationships
  Provides information about creating authenticated cluster peer relationships among clusters to enable the clusters to communicate with each other so that you can replicate data between volumes in different clusters.

- Creating an SVM and configuring protocols for data access
  Provides information about creating an SVM and configuring CIFS, NFS, iSCSI, and FC/FCoE protocols on the SVM to serve data to the clients.

- Disaster recovery using SnapMirror relationships
  Provides information about configuring and monitoring SnapMirror relationships between peered clusters for volume disaster recovery.

- Volume backup using SnapVault relationships
  Provides information about configuring SnapVault relationships between volumes that are located in different clusters to back up and restore data when the data is corrupted or lost.

*NetApp Documentation: Clustered Data ONTAP Express Guides*
Setting up a cluster by using OnCommand System Manager

You can use OnCommand System Manager to set up the cluster automatically by using a template file, or manually by entering values in a guided setup.

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 version.
- All of the nodes must be healthy, and cabling for the nodes must be set up.
- The cabling and connectivity must be 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

Setting up a cluster manually includes creating a cluster, setting up node management and cluster management networks, setting up AutoSupport messages and event notifications, and creating SVMs per storage recommendations.
Choices

- Setting up a cluster by using the template file on page 8
- Setting up the cluster manually on page 10

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 window 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 cluster 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 and Continue**.
   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 and Continue**.
   You can edit the network details, if required.
9. Verify the details in the **Support** window, and then click **Submit and Continue**.
   You can edit the support details, if required.
10. Verify the details in the **Storage** window, and then create aggregates or exit the cluster setup:
<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit cluster setup without provisioning storage and creating an SVM</td>
<td>Click <strong>Skip this step</strong>.</td>
</tr>
<tr>
<td>Provision storage using aggregates and create an SVM</td>
<td>Click <strong>Submit and Continue</strong>.</td>
</tr>
</tbody>
</table>

You can edit the support details, if required.

11. If you have clicked **Skip this step** on the **Storage** window, view the details on the **Summary** window, and then click **Manage your Cluster** to launch System Manager.

12. If you have clicked **Submit and Continue** on the **Storage** window, verify the details in the **SVM** window, and then click **Submit and Continue**.

   You can edit the **SVM** details, if required.

13. Verify all the details in the **Summary** window, and then click **Provision an Application** to provision storage for applications, or click **Manage your Cluster** to complete the cluster setup process and launch System Manager, or click **Export Configuration** to download the configuration file.

### 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 window 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. Enter the password for the cluster.
5. Optional: Enter the feature license keys.

6. Click **Submit**.

**After you finish**
Enter the network details in the Network page to continue with the cluster setup.

### 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**.

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

**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.

### 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.
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 and continue.

After you finish
View the storage recommendations and create SVMs to continue with the cluster setup.

Reviewing storage recommendations

Using the Storage window, you can review the storage recommendations that are provided for creating aggregates.

Before you begin
You must have set up the cluster, network, and the support details.

About this task
You can create data aggregates per the storage recommendations or you can skip this step and create data aggregates at a later time using System Manager.

Choices
• To create data aggregates as per the storage recommendations, click Submit and Continue.
• To create data aggregates at a later time using System Manager, click Skip this step.

After you finish
If you opted to create aggregates per the storage recommendations, you must create a Storage Virtual Machine (SVM) to continue with the cluster setup.
## Creating an SVM

You can use the Storage Virtual Machine (SVM) window to create fully configured SVMs. The SVMs serve data after storage objects are created on these SVMs.

### Before you begin

- You must have created an aggregate and the aggregate must be online
- You must have ensured that the aggregate has sufficient space for the SVM root volume

### Steps

1. Enter a name for the SVM.
2. Select data protocols for the SVM:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| Enable CIFS protocol by configuring the CIFS server using an Active Directory | a. Select the **Active Directory** box.  
   b. Enter the Active Directory administrator name.  
   c. Enter the Active Directory administrator password.  
   d. Enter a name for the CIFS server.  
   e. Enter a name for the Active Directory domain.  
   f. Depending on your requirements, select the **One data LIF on this SVM** or **One data LIF per node on this SVM** box.  
   g. Provide data LIF details such as IP address, netmask, gateway, and port.  
   h. Provide DNS details. |
| Enable CIFS protocol by configuring the CIFS server using a workgroup | a. Select the **Workgroup** box.  
   b. Enter a name for the workgroup.  
   c. Enter a name for the CIFS server.  
   d. Depending on your requirements, select the **One data LIF on this SVM** or **One data LIF per node on this SVM** check box.  
   e. Provide data LIF details such as IP address, netmask, gateway, and port. |
| Enable NFS protocol | a. Select the **NFS** box.  
   b. Depending on your requirements, select the **One data LIF on this SVM** or **One data LIF per node on this SVM** check box.  
   c. Provide data LIF details such as IP address, netmask, gateway, and port. |
| Enable iSCSI protocol | a. Select the **iSCSI** box.  
   b. Provide data LIF details such as IP address, netmask, gateway, and port. |
<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable FC/FCoE protocol</td>
<td>a. Select the FC/FCoE box.</td>
</tr>
<tr>
<td></td>
<td>b. Select the FC/FCoE ports for FC or FCoE protocols.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Each node must have at least one correctly configured port</td>
</tr>
<tr>
<td></td>
<td>for each protocol (FC and FCoE).</td>
</tr>
</tbody>
</table>

3. Optional: Click the Advanced Options icon and provide details to configure advanced options such as the default language, security style, CIFS server details, and NFS details.

4. Click **Submit and Continue** to create the SVM.

**After you finish**

If you have clicked **Submit and Continue**, you must verify the details that you have provided in the Summary window, and then click **Manage your Cluster** to launch System Manager, or click **Provision an Application** to provision storage applications, or click **Export Configuration** to download the configuration file.
Performing a nondisruptive cluster update

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.

Steps

1. **Obtaining ONTAP software images** on page 16
   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.

2. **Updating the cluster nondisruptively** on page 17
   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.

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 from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served.

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.

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:
<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new software image</td>
<td>a. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Select an available image</td>
<td>Choose one of the listed images.</td>
</tr>
</tbody>
</table>

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:

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

   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.
Setting up the network

After the IPspace is created, you can use System Manager to set up the network for accessing data from Storage Virtual Machines (SVMs) and managing SVMs. You must create a broadcast domain by using any type of port (VLANs, physical ports, or interface groups) and then create a subnet and a network interface.

Steps

1. Creating VLAN interfaces on page 21
   You can create a VLAN for maintaining separate broadcast domains within the same network domain by using System Manager.

2. Creating interface groups on page 21
   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.

3. Creating broadcast domains on page 22
   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.

4. Creating subnets on page 22
   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.

5. Creating network interfaces on page 22
   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.
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.

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.
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**.

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**.

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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| Associate the network interface with a data LIF | a. Select Serves Data.  
b. Select the SVM for the network interface. |
| Associate the network interface with an intercluster LIF | a. Select Intercluster Connectivity.  
b. Select the IPspace for the network interface. |
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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| Specify the IP address using a subnet | a. Select Using a subnet.  
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.  
c. If you want to assign a specific IP address to the interface, select Use a specific IP address, 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.  
d. Click OK. |
If you want to...

<table>
<thead>
<tr>
<th>Specifying the IP address manually without using a subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Then...</td>
</tr>
<tr>
<td>a. Select <strong>Without a subnet.</strong></td>
</tr>
<tr>
<td>b. In the Add Details dialog box, perform the following steps:</td>
</tr>
<tr>
<td>i. Specify the IP address and network mask or prefix.</td>
</tr>
<tr>
<td>ii. Optional: Specify the gateway. The destination field is populated with the default value based on the family of the IP address.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>c. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

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

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

10. Click **Create**.
Assigning disks or array LUNs to nodes

You can use System Manager to assign the ownership of unassigned disks and unassigned array LUNs to nodes to increase the size of the aggregates.

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.

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.

Choices

- Assign disks to nodes:
  1. Assigning disks to nodes on page 25
  2. Zeroing spare disks on page 26
- Assign array LUNs to nodes:
  1. Assigning array LUNs on page 26
  2. Zeroing spare array LUNs on page 27
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.

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.

**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.
Managing storage tiers by using FabricPool

Storing data in tiers can enhance the efficiency of your storage system. You manage storage tiers by using FabricPool. It stores data in a tier based on whether the data is frequently accessed.

**Before you begin**

- You must be running ONTAP 9.2 or later
- You must have all flash (all SSD) aggregates

**Steps**

1. **Adding an external capacity tier** on page 29
   You can use System Manager to add an external capacity tier to an SSD aggregate or a VMDISK aggregate. External capacity tiers provide storage for infrequently used data.

2. **Attaching an aggregate to external capacity tier** on page 30
   You can use System Manager to attach an all flash aggregate to an external capacity tier. External capacity tier provides storage for infrequently used data.

3. **Provisioning storage by creating a FabricPool** on page 30
You can use System Manager to create a FabricPool or to convert an existing SSD aggregate to a FabricPool by attaching an external capacity tier to the SSD aggregate.

4. Changing the tiering policy of a volume on page 31
   You can use System Manager to change the default tiering policy of a FabricPool.

Adding an external capacity tier

You can use System Manager to add an external capacity tier to an SSD aggregate or a VMDISK aggregate. External capacity tiers provide storage for infrequently used data.

Before you begin

- You must have the access key ID and secret key to connect to the object store.
- You must have created a bucket inside the object store.
- Network connectivity must exist between the cluster and the external capacity tier.
- If communication between the external capacity tier and cluster is encrypted using SSL/TLS, the required certificates must be installed.
- If you are using StorageGRID Webscale as an object store, a StorageGRID Webscale CA certificate must be installed on the cluster.

About this task

The supported object stores that can be used as external capacity tiers are StorageGRID Webscale and Amazon AWS S3.

Note: If you want to use Amazon AWS S3 as an external capacity tier, you must have the FabricPool capacity license.

Steps

1. Click the Storage Tiers tab.
2. Click Add External Capacity Tier.
   The Add External Capacity Tier window is displayed.
3. In the External Capacity Provider field, select the external capacity tier that you want to add.
4. Enter the server name that hosts the external capacity tier, the port to access the external capacity tier, the access key ID of the external capacity tier, the secret key of the external tier, and the container name.
5. Enable the SSL button if you want to transfer the data securely to the external capacity tier.
6. From the IPspace list, select the IPspace that is used to connect to the external capacity tier.
7. Click Save to save the external capacity tier.
8. Optional: Click Save and Attach Aggregates to save the external capacity tier and to attach aggregates to it.
Attaching an aggregate to external capacity tier

You can use System Manager to attach an all flash aggregate to an external capacity tier. External capacity tier provides storage for infrequently used data.

**Before you begin**

You must have added an external capacity tier in the cluster.

**Steps**

1. Click **Storage Tiers**.
   
   External capacity tiers that are added to System Manager are displayed.

2. In the **Used in Aggregates** column, click **Attach Aggregates**.
   
   The Attach Aggregates window is displayed.

3. Select the aggregate that you want to attach.

4. If you want to update the tiering policy of the volumes that are on the selected aggregates, click **View and Update Tiering Policy for Volumes**.

5. Click the **Change Tiering Policy** list, and then update the tiering policy.

6. Click **Save**.

Provisioning storage by creating a FabricPool

You can use System Manager to create a FabricPool or to convert an existing SSD aggregate to a FabricPool by attaching an external capacity tier to the SSD aggregate.

**Before you begin**

- You must have created an external capacity tier and attached it to the cluster in which the SSD aggregate resides.
- An on-premises external capacity tier must be present.
- A dedicated network connection must exist between the external capacity tier and the aggregate.

**About this task**

- Supported external capacity tiers are StorageGRID Webscale and Amazon AWS S3.

  **Note:** If you want to use Amazon AWS S3 as an external capacity tier, you must have the FabricPool capacity license.

- FabricPool is not supported on ONTAP Select and MetroCluster configurations.

**Steps**

1. Choose one of the following methods:
   
   - Click the **Storage Tiers** tab.
   
   - 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.
      
      **Note:** Only all flash (all SSD) aggregates support FabricPool.
      
      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**.

4. Select the **FabricPool** box, and then select an external capacity tier from the list.

5. Click **Create**.

### Changing the tiering policy of a volume

You can use System Manager to change the default tiering policy of a FabricPool.

**Steps**

1. Click the **SVMs** tab.
2. Select the SVM, and then click **Manage**.
3. Click the **Volumes** tab.
4. Select the volume, and then click **Actions > Change Tiering Policy**.
5. Change the tiering policy from the **Tiering Policy** list, and then click **Save**.
Managing FlexGroup volumes using System Manager

You can use System Manager to create FlexGroup volumes as per the best practices, or by manually selecting the aggregates.

Steps
1. Creating FlexGroup volumes on page 32
   You can use System Manager to create a FlexGroup volume by selecting specific aggregates or by selecting system recommended aggregates.

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.
- You cannot create FlexGroup volumes in a MetroCluster configuration.

Steps
1. Click the SVMs tab.
2. Select the SVM, and then click Manage.
3. Click the Volumes tab.
4. Click Create > Create FlexGroup.
5. In the **Create FlexGroup** window, specify a name for the FlexGroup volume.

6. Select **Recommended per best practices** or select **Select aggregates** and choose the required aggregates.

7. Optional: Select the space reserve.

8. Specify a size for the FlexGroup volume.

9. Click **Create** to create the FlexGroup volume.
Resizing FlexGroup volumes using System Manager

You can use System Manager to resize FlexGroup volumes by resizing the existing resources or adding new resources.

Steps
1. Resizing FlexGroup volumes on page 34
   You can use System Manager to resize a FlexGroup volume by resizing existing resources or adding new resources.

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 aggregate that you are using for expansion.

Steps
1. Click the SVMs tab.
2. Select the SVM, and then click Manage.
3. Click the Volumes tab.
4. Select the FlexGroup volume that you want to resize, and then click Actions > Resize.
5. Select a resize option:
<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resize using existing resources</td>
<td>a.  Click <strong>Resizing using the existing resources.</strong></td>
</tr>
<tr>
<td></td>
<td>b.  Specify the size to which you want to resize the FlexGroup volume.</td>
</tr>
<tr>
<td></td>
<td>c.  Specify the percentage of Snapshot reserve.</td>
</tr>
<tr>
<td>Expand by adding new resources</td>
<td>a.  Click <strong>Expanding by adding new resources.</strong></td>
</tr>
<tr>
<td></td>
<td>b.  Select the aggregates that you want to use for adding resources.</td>
</tr>
<tr>
<td></td>
<td>c.  Specify the size to which you want to expand the FlexGroup volume.</td>
</tr>
<tr>
<td></td>
<td>d.  Specify the percentage of Snapshot reserve.</td>
</tr>
</tbody>
</table>

6. Click **Resize** to resize the FlexGroup volume.
Assigning disks to existing aggregates

You can increase the size of existing aggregates by adding disks (HDDs or SSDs) or increase the cache for existing Flash Pool aggregates by adding storage pools or dedicated SSDs (cache disks).

1. Provision capacity through HDDs.
2. Add capacity:
   - Add HDDs.
   - Modify the attributes, if necessary.
Steps

1. **Adding capacity disks** on page 38
   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.

2. **Provisioning cache to aggregates by adding SSDs** on page 39
   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.

3. **Creating a storage pool** on page 40
   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.
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. Choose one of the following methods:
   • Click the Storage Tiers tab.
• Click Hardware and Diagnostics > Aggregates.

2. In the Storage Tiers window, select the aggregate to which you want to add capacity disks, and then click Actions > 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.

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.

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. Choose one of the following methods:
   • Click the **Storage Tiers** tab.
   • Click **Hardware and Diagnostics > Aggregates**.

2. In the **Storage Tiers** window, select the aggregate, and then click **Actions > Add Cache**.

3. In the **Add Cache** dialog box, perform the appropriate action:

<table>
<thead>
<tr>
<th>If you select the cache source as...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage pools</td>
<td>a. Select the storage pool from which cache can be obtained.</td>
</tr>
<tr>
<td></td>
<td>b. Specify the cache size.</td>
</tr>
<tr>
<td></td>
<td>c. Modify the RAID type, if required.</td>
</tr>
<tr>
<td>Dedicated SSDs</td>
<td>Select the SSD size and the number of SSDs to include, and optionally modify the RAID configuration:</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Change</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. In the Change RAID Configuration dialog box, specify the RAID type and RAID group size, and then click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

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.

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**.
Provisioning cache through Flash Pool aggregates

You can provision cache by creating a Flash Pool aggregate or convert an existing aggregate to a Flash Pool aggregate by adding SSDs. You can create a new HDD aggregate (if one does not exist already) and add cache through dedicated SSDs or storage pools.

Steps
1. **Provisioning cache to aggregates by adding SSDs** on page 43
   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.

2. **Increasing the cache for Flash Pool aggregates by adding SSDs** on page 44
   You can add SSDs as either storage pools or dedicated SSDs to increase the size of a Flash Pool aggregate by using System Manager.

3. **Creating a storage pool** on page 44
   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.
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. Choose one of the following methods:
   - Click the Storage Tiers tab.
   - Click Hardware and Diagnostics > Aggregates.

2. In the Storage Tiers window, select the aggregate, and then click Actions > Add Cache.

3. In the Add Cache dialog box, perform the appropriate action:

<table>
<thead>
<tr>
<th>If you select the cache source as...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| **Storage pools**                    | a. Select the storage pool from which cache can be obtained.  
                                        b. Specify the cache size.  
                                        c. Modify the RAID type, if required. |
| **Dedicated SSDs**                   | Select the SSD size and the number of SSDs to include, and optionally modify the RAID configuration:  
                                        a. Click Change.  
                                        b. In the Change RAID Configuration dialog box, specify the RAID type and RAID group size, and then click Save. |

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.

### 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**

1. Click Hardware and Diagnostics > Aggregates.
2. In the Aggregates window, select the Flash Pool aggregate, and then click Add Cache.
3. In the Add Cache dialog box, perform the appropriate action:

<table>
<thead>
<tr>
<th>If you selected the cache source as...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage pools</td>
<td>Select the storage pool from which cache can be obtained, and specify the cache size.</td>
</tr>
<tr>
<td>Dedicated SSDs</td>
<td>Select the SSD size and the number of SSDs to include.</td>
</tr>
</tbody>
</table>

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.

### 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.
Providing data resiliency by 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 when connecting to disks and array LUNs.

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.
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. Choose one of the following methods:
   - Click the Storage Tiers tab.
   - 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. Choose one of the following methods:
   - Click the **Storage Tiers** tab.
   - 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:

<table>
<thead>
<tr>
<th>If you want to select the cache source as...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage pools</td>
<td>a. Select <strong>Storage pools</strong> as the Cache Source.</td>
</tr>
<tr>
<td></td>
<td>b. Select the storage pool from which the cache can be obtained, and then specify the cache size.</td>
</tr>
<tr>
<td></td>
<td>c. Modify the RAID type, if required.</td>
</tr>
</tbody>
</table>
If you want to select the cache source as... Then...

Dedicated SSDs

a. Select *Dedicated SSDs* as the Cache Source.

b. Select the SSD size and the number of SSDs to include in the aggregate.

c. Modify the RAID configuration, if required:

   i. Click *Change*.

   ii. In the Change RAID Configuration dialog box, specify the RAID type and the RAID group size.

   iii. Click *Save*.

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.

**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. Choose one of the following methods:

   - Click the *Storage Tiers* tab.

   - Click *Hardware and Diagnostics > Aggregates*.

2. Select the aggregate that you want to mirror, and then click *Actions > Mirror*.

3. In the *Mirror this aggregate* dialog box, click *Mirror* to initiate the mirroring.
Providing data access to qtrees using export policies

You can export a qtree by assigning an export policy to it. This enables you to export a specific qtree on a volume and make it directly accessible to clients instead of exporting the entire volume.

**Choices**

- Assign export policies to new qtrees.
  
  *Creating qtrees* on page 50

  When creating a qtree, you can create a new export policy and add rules to it or select an existing export policy.

- Assign export policies to existing qtrees.
  
  *Assigning export policies to qtrees* on page 51

  When assigning an export policy to existing qtrees, you can create a new export policy and add rules to it or select an existing export policy.

**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.

   *Creating an export policy* on page 52

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.

**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 52

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.
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.
   Adding rules to an export policy on page 52
9. Click Create.
10. Verify that the export policy you created is displayed in the Export Policies window.

Related tasks

Creating qtrees on page 50
Assigning export policies to qtrees on page 51

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.

Related tasks
   Creating an export policy on page 52
Configuring a Service Processor

You can configure a Service Processor to monitor and manage various system parameters of your storage systems. Configuring a Service Processor involves assigning IP addresses to all the Service Processors and modifying the settings. If required, you can assign IP addresses to the selected Service Processors.

Steps

1. Assigning IP addresses to Service Processors on page 54
   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.

2. Editing Service Processor settings on page 55
   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.

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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Select the option...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign IP addresses automatically from a DHCP server</td>
<td>DHCP</td>
</tr>
<tr>
<td>Assign IP addresses from a subnet</td>
<td>Subnet</td>
</tr>
<tr>
<td>Manually provide IP addresses</td>
<td>Manual Assignment</td>
</tr>
</tbody>
</table>
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.
Setting up a BranchCache configuration

You can configure BranchCache on a CIFS-enabled Storage Virtual Machine (SVM) and enable BranchCache on the required shares to enable caching of content on computers local to requesting clients.

Steps

1. Setting up CIFS on page 56
   You can use System Manager to enable and configure CIFS servers to allow CIFS clients to access files on the cluster.

2. Setting up BranchCache on page 57
   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.

3. Editing share settings on page 58
   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).

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.

**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.

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.
Protecting data using mirror and vault relationship

You can create a mirror and vault relationship using the MirrorVault policy to protect your data by periodically transferring data from the source volume to the destination volume. The relationship also enables you to retain data for long periods by creating backups of the source volume.

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 Actions > 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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new volume</td>
<td>a. If you want to change the default name, which is displayed in the format source_SVM_name_source_volume_name_mirror_vault, specify a new name, and then select the containing aggregate for the destination volume.</td>
</tr>
<tr>
<td></td>
<td>b. Select Enable dedupe to enable deduplication on the new destination volume.</td>
</tr>
<tr>
<td></td>
<td>If deduplication is disabled on the source volume, then the check box for the new volume is selected by default.</td>
</tr>
<tr>
<td>If you want to...</td>
<td>Do the following...</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| Select an existing volume | Select the **Select Volume** option.  
**Note:** Only those volumes with the same language attribute as the source volume are listed. |

10. Select an existing policy or create a new policy:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
</table>
| Select an existing policy | Click **Browse**, 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 | a. Click **Create Policy**.  
b. 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.  
c. Select the **Enable Network Compression** check box to compress the data that is being transferred.  
d. Click **Create**.  
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. |

11. Specify a schedule for the relationship:

<table>
<thead>
<tr>
<th>If...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You want to assign an existing schedule</td>
<td>From the list of schedules, select an existing schedule.</td>
</tr>
</tbody>
</table>
| You want to create a new schedule | a. Click **Create Schedule**.  
b. Specify a name for the schedule.  
c. Select **Basic** or **Advanced**.  
• Basic: You can select this option to specify only the day of the week, time, and the transfer interval.  
• Advanced: You can select this option to specify a cron-style schedule.  
d. Click **Create**. |
| You do not want to assign a schedule | Select **None**. |

12. Optional: Select **Initialize Relationship** to initialize the relationship.

13. Click **Create**.
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:

<table>
<thead>
<tr>
<th>If you want to…</th>
<th>Do the following…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new volume</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>b. Select <strong>Enable dedupe</strong> to enable deduplication on the new destination volume.</td>
</tr>
<tr>
<td></td>
<td>If deduplication is disabled on the source volume, then the check box for the new volume is selected by default.</td>
</tr>
</tbody>
</table>

   Select an existing volume | Select the **Select Volume** option. |
   | Note: Only those volumes with the same language attribute as the source volume are listed. |

9. Select an existing policy or create a new policy:

<table>
<thead>
<tr>
<th>If you want to…</th>
<th>Do the following…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select an existing policy</td>
<td>Click <strong>Browse</strong>, and then select a mirror and vault policy.</td>
</tr>
<tr>
<td></td>
<td>You can select the policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.</td>
</tr>
</tbody>
</table>

   Create a new policy | a. Click **Create Policy**. |
   |                   | 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. |
   |                   | c. Select the **Enable Network Compression** check box to compress the data that is being transferred. |
   |                   | d. Click **Create**. |

   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.
10. Specify a schedule for the relationship:

<table>
<thead>
<tr>
<th>If…</th>
<th>Do the following…</th>
</tr>
</thead>
<tbody>
<tr>
<td>You want to assign an existing schedule</td>
<td>From the list of schedules, select an existing schedule.</td>
</tr>
</tbody>
</table>
| You want to create a new schedule | a. Click [Create Schedule].  
  b. Specify a name for the schedule.  
  c. Select [Basic] or [Advanced].  
    • Basic: You can select this option to specify only the day of the week, time, and the transfer interval.  
    • Advanced: You can select this option to specify a cron-style schedule.  
  d. Click [Create]. |
| You do not want to assign a schedule | Select [None]. |

11. Optional: Select **Initialize Relationship** to initialize the relationship.

12. Click [Create].
Protecting data using SnapLock

The SnapLock feature provides write once, read many (WORM) protection and a retention date to all files or data in the volumes that provides tamper-free backups. The SnapLock feature is most commonly used with unstructured data in the files on file systems. After the backup is complete, you can commit the backed-up files to WORM using a third-party application.

Steps

1. **Adding licenses** on page 67
   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.

2. **Provisioning storage by creating a SnapLock aggregate** on page 68
   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.

3. **Creating SnapLock volumes** on page 69
   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.

4. **Mounting volumes** on page 72
   You can use System Manager to mount volumes to a junction in the Storage Virtual Machine (SVM) namespace.

5. **Creating a mirror or vault relationship from a source or destination SVM** on page 72
   You can use System Manager to create a SnapMirror relationship or SnapVault relationship between a source volume and destination volume from a source Storage Virtual Machine (SVM) or destination SVM and assign a policy to mirror or vault data. In the event of data loss or corruption, the backed-up data can be restored.
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 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 ONTAP Cloud license. The ONTAP Cloud license is not listed in the license page. System Manager does not raise any alert about the entitlement risk status of the ONTAP Cloud license.

• You can upload only capacity based licenses. The capacity based licences are of “json” type.

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, perform the appropriate steps:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Add a license for a specific ONTAP service | a. Enter the software license key. You can add multiple licenses by entering the software license keys, separated by commas.  
 b. Click Add. |
| Add a capacity based license | a. Click Browse and select the capacity based license file.  
 b. Click Add. |
| Add a license for a specific ONTAP service and add a capacity based license | a. Enter the software license key. You can add multiple licenses by entering the software license keys, separated by commas.  
 b. Click Browse and select the capacity based license file.  
 c. Click Add. |

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.

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.
• 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. Choose one of the following methods:
   • Click the Storage Tiers tab.
   • 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.

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.
• For creating an encrypted volume, you must have installed the volume encryption license using System Manager and enabled “key-manager setup” using the command-line interface (CLI). You must refresh your web browser after enabling “key-manager setup”.

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.
• You cannot encrypt a volume in ONTAP Cloud.

Steps

1. Click the SVMs tab.
2. Select the SVM, and then click Manage.
3. Click the Volumes tab.
4. Click Create > Create FlexVol.
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 Encrypted check box to enable encryption for the volume.
   This option is available only if you have enabled the Volume Encryption license and if the corresponding platform is capable of supporting encryption.
8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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 | a. Select **New Policy Group**.
 | b. Specify the policy group name.
 | c. Specify the minimum throughput limit.
 | If you do not specify the minimum throughput value or when the minimum throughput value is set to 0, the system automatically displays “None” as the value and this value is case-sensitive.
 | d. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group do not exceed the specified throughput limit.
 | • The minimum throughput limit and the maximum throughput limit must be of the same unit type.
 | • If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPs and B/s, KB/s, MB/s, and so on.
 | • If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value and this value is case-sensitive. The unit that you specify does not affect the maximum throughput.

Select an existing policy group | a. Select **Existing Policy Group**, and then click **Choose** to select an existing policy group from the Select Policy Group dialog box.
 | b. Specify the minimum throughput limit.
 | If you do not specify the minimum throughput value or when the minimum throughput value is set to 0, the system automatically displays “None” as the value and this value is case-sensitive.
 | c. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group do not exceed the specified throughput limit.
 | • The minimum throughput limit and the maximum throughput limit must be of the same unit type.
 | • If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPs and B/s, KB/s, MB/s, and so on.
 | • If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value and this value is case-sensitive. The unit that you specify does not affect the maximum throughput.
 | If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.

15. Click **Create**.
16. 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.
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.

Creating a mirror or vault relationship from a source or destination SVM

You can use System Manager to create a SnapMirror relationship or SnapVault relationship between a source volume and destination volume from a source Storage Virtual Machine (SVM) or destination SVM and assign a policy to mirror or vault data. In the event of data loss or corruption, the backed-up data can be restored.

About this task

You can perform one of the following tasks depending on whether you want to create a SnapMirror or SnapVault relationship from a source or destination SVM:

- Creating a mirror relationship from a source SVM on page 73
- Creating a mirror relationship from a destination SVM on page 75
- Creating a vault relationship from a source SVM on page 78
- Creating a vault relationship from a destination SVM on page 81
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 **Actions > 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 `source_SVM_name_source_volume_name_mirror`, specify a new name, and select the containing aggregate for the destination volume. |
    | Select an existing volume | Select the **Select Volume** option.  
   
   **Note:** 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 |  
   
   **a.** Click **Create Policy**.  
   
   **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.  
   
   **c.** Select the **Transfer All Source Snapshot Copies** 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.  
   
   **d.** Select the **Enable Network Compression** check box to compress the data that is being transferred.  
   
   **e.** Click **Create**. |

12. Specify a schedule for the relationship:
### If...  

<table>
<thead>
<tr>
<th>If...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You want to assign an existing schedule</td>
<td>From the list of schedules, select an existing schedule.</td>
</tr>
</tbody>
</table>
| You want to create a new schedule | a. Click **Create Schedule**.  
b. Specify a name for the schedule.  
c. Select either **Basic** or **Advanced**.  
  - Basic: You can select this option to specify only the day of the week, time, and the transfer interval.  
  - Advanced: You can select this option to specify a cron-style schedule.  
d. Click **Create**. |
| You do not want to assign a schedule | Select **None**. |

---

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.

**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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
</table>
| Create a new volume | • If you want to change the default name, which is displayed in the format `source_SVM_name_source_volume_name_mirror`, specify a new name, and select the containing aggregate for the destination volume.  
  • Select Default, Thin provisioned or Thick provisioned for the volume.  
  **Note:** For AFF storage systems, thin provisioning is default, and for other storage systems, thick provisioning is default. |
| Select an existing volume | Select the **Select Volume** 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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select an existing policy</td>
<td>Select a mirror policy from the list.</td>
</tr>
</tbody>
</table>
| Create a new policy | a. Click **Create Policy**.  
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.  
c. Select the **Transfer All Source Snapshot Copies** 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.  
d. Select the **Enable Network Compression** check box to compress the data that is being transferred.  
e. Click **Create**. |

11. Specify a schedule for the relationship:

<table>
<thead>
<tr>
<th>If...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You want to assign an existing schedule</td>
<td>From the list of schedules, select an existing schedule.</td>
</tr>
</tbody>
</table>
If... | Do the following...
--- | ---
You want to create a new schedule | a. Click Create Schedule.  
b. Specify a name for the schedule.  
c. Select Basic or Advanced.  
• Basic: You can select this option to specify only the day of the week, time, and the transfer interval.  
• Advanced: You can select this option to specify a cron-style schedule.  
d. Click Create.
You do not want to assign a schedule | Select None.

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.

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 **Actions > 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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new volume</td>
<td>a. If you want to change the default name, which is displayed in the format <code>source_SVM_name_source_volume_name_vault</code>, specify a new name, and select the containing aggregate for the destination volume.</td>
</tr>
<tr>
<td></td>
<td>b. Select <strong>Enable dedupe</strong> to enable deduplication on the new destination volume.</td>
</tr>
<tr>
<td></td>
<td>If deduplication is disabled on the source volume, then the check box for the new volume is selected by default.</td>
</tr>
<tr>
<td>Select an existing volume</td>
<td>Select the <strong>Select Volume</strong> option.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Only those volumes with the same language attribute as that of the source volume are listed.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select an existing policy</td>
<td>Select a vault policy from the list.</td>
</tr>
<tr>
<td></td>
<td>You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.</td>
</tr>
</tbody>
</table>
If you want to... | Do the following...
---|---
Create a new policy | a. Click Create Policy.
  
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.
  
c. Select the Enable Network Compression check box to compress the data that is being transferred.
  
d. Click Create.
  
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.

12. Specify a schedule for the relationship:

<table>
<thead>
<tr>
<th>If...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You want to assign an existing schedule</td>
<td>From the list of schedules, select an existing schedule.</td>
</tr>
</tbody>
</table>
| You want to create a new schedule | a. Click Create Schedule.
  
b. Specify a name for the schedule.
  
c. Select Basic or Advanced.
    
    • Basic: You can select this option to specify only the day of the week, time, and the transfer interval.
    
    • Advanced: You can select this option to specify a cron-style schedule.
  
d. Click Create.
  
You do not want to assign a schedule | Select None. |


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.
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 (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 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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new volume</td>
<td>a. If you want to change the default name, which is displayed in the format <code>source_SVM_name_source_volume_name_vault</code>, specify a new name, and select the containing aggregate for the destination volume.</td>
</tr>
<tr>
<td></td>
<td>b. Select <strong>Enable dedupe</strong> to enable deduplication on the new destination volume.</td>
</tr>
<tr>
<td></td>
<td>If deduplication is disabled on the source volume, then the check box for the new volume is selected by default.</td>
</tr>
<tr>
<td>Select an existing volume</td>
<td>Select the <strong>Select Volume</strong> option.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Only those volumes with the same language attribute as that of the source volume are listed.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select an existing policy</td>
<td>Select a vault policy from the list.</td>
</tr>
<tr>
<td></td>
<td>You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.</td>
</tr>
<tr>
<td>Create a new policy</td>
<td>a. Click <strong>Create Policy</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Specify a policy name, and set the schedule transfer priority.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>c. Select the <strong>Enable Network Compression</strong> check box to compress the data that is being transferred.</td>
</tr>
<tr>
<td></td>
<td>d. Click <strong>Create</strong>.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

11. Specify a schedule for the relationship:
<table>
<thead>
<tr>
<th>If...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You want to assign an existing schedule</td>
<td>From the list of schedules, select an existing schedule.</td>
</tr>
<tr>
<td>You want to create a new schedule</td>
<td>a. Click <strong>Create Schedule</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Specify a name for the schedule.</td>
</tr>
<tr>
<td></td>
<td>c. Select <strong>Basic</strong> or <strong>Advanced</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Basic: You can select this option to specify only the day of the week, time, and the transfer interval.</td>
</tr>
<tr>
<td></td>
<td>• Advanced: You can select this option to specify a cron-style schedule.</td>
</tr>
<tr>
<td></td>
<td>d. Click <strong>Create</strong>.</td>
</tr>
<tr>
<td>You do not want to assign a schedule</td>
<td>Select <strong>None</strong>.</td>
</tr>
</tbody>
</table>

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.
Copyright information

Copyright © 1994–2017 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, Element, Fitness, Flash Accel, Flash Cache, Flash Pool, FlexArray, FlexCache, FlexClone, 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.

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

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 58
access-based enumeration
  See ABE
adding
capacity disks to aggregates 38
export rules 52
rules to export policies 52
SSDs to aggregates 39, 43
SSDs to HDDs for converting to Flash Pool aggregates 48
VLAN interfaces 21
aggregates
  adding capacity disks to 38
  assigning array LUNs to 26
  assigning disks to increase capacity 25
  creating storage pools 40, 44
Flash Pool, workflow for provisioning cache 42
  managing storage tiers by using FabricPool, introduction 28
  mirroring 49
  provisioning cache by adding SSDs 39, 43
  provisioning storage by creating 46
  provisioning storage by creating Flash Pool 48
  provisioning storage by creating HDD and SSD 47
  provisioning storage by creating SnapLock Compliance 68
  provisioning storage by creating SnapLock Enterprise 68
  workflow for assigning disks to existing 36
  workflow for mirroring data 46
  zeroing spare array LUNs 27
  zeroing spare disks 26
all-share cache
  creating for BranchCache configuration 57
array LUNs
  assigning 26
  erasing data from 27
  formatting 27
  zeroing 27
assigning
  array LUNs 26
  disks to nodes 25
  export policies to qtrees 51
attaching
  SSDs to external capacity tier for converting to FabricPool 30

B

BranchCache
  enabling 58
  setting up 57
  workflow for configuring 56
broadcast domains
  creating 22

C

cache
  increasing for Flash Pool aggregates by adding SSDs 44
  provisioning to aggregates by adding SSDs 39, 43

caching
  configuring BranchCache for 57
  capacity disks
    adding to aggregates 38
CIFS
  setting up 56
  workflow for configuring BranchCache 56
CIFS servers
  configuring BranchCache on 57
client access
  adding rules to export policies 52
  creating export policies 52
  creating export policy for 52
  setting up CIFS 56
cluster
  creating manually 10
  cluster setup
    prerequisites and workflow for using OnCommand System Manager 7
    setting up a network 11
clusters
  nondisruptively updating, using System Manager 17
  workflow for a nondisruptive update 16
comments
  how to send feedback about documentation 86
configuring
  BranchCache 57
continuous availability
  enabling or disabling for shares 58
creating
  a mirror and vault relationship from a destination SVM 63
  a mirror relationship from a destination SVM 75
  a vault relationship from a destination SVM 81
  aggregates 46
  broadcast domains 22
  cluster
    setting up 10
  cluster manually 10
  export policies 52
FabricPool 30
  Flash Pool aggregates 46, 48
  FlexGroup volumes 32
  HDD and SSD aggregates 47
  interface groups 21
  mirror and vault relationships from a source volume 60
  mirror relationships from a source SVM 73
  network interfaces 22
qtrees 50
setting up
  cluster 10
  SnapLock Compliance aggregates 68
SnapLock Compliance volumes 69
SnapLock Enterprise aggregates 68
SnapLock Enterprise volumes 69
storage pools 40, 44
subnets 22
vault relationships from a source SVM 78

D
Data ONTAP
  workflow for setting up a network 20
dedicated SSDs
  adding to Flash Pool aggregates 44
DHCP
  assigning IP addresses to Service Processors 54
disks
  adding, to increase the size of aggregates 38
  assigning to nodes 25
  erasing data from 26
  formatting 26
  mirroring aggregates 49
  zeroing 26
documentation
  how to receive automatic notification of changes to 86
  how to send feedback about 86
domains
  creating broadcast 22
downgrades
  obtaining ONTAP software images 16

E
editing
  Service Processor settings 55
  share settings 58
  shares, workflow to enable BranchCache 56
encrypt data
  while accessing this share 58
expanding
  FlexGroup volumes 34
export policies
  adding export rules to 52
  adding rules 52
  assigning to qtrees 51
  creating 52
  workflow for assigning to qtrees 50
export rules
  adding to export policies 52
exporting
  qtrees 51
express guides
  System Manager workflows in 5
external capacity tier
  attaching an aggregate 30
external capacity tiers
  adding 29
  using to store infrequently used data 29

F
FabricPool
  creating 30
FabricPools
  managing storage tiers by using, introduction 28
feedback
  how to send comments about documentation 86
Flash Pool aggregates
  creating 48
  creating storage pools 40, 44
  increasing the size by adding SSDs 44
  provisioning storage by creating 46
  workflow for provisioning cache 42
FlexGroup volumes
  creating 32
  expanding 34
  managing workflow 32
  resizing 34
flowcharts
  Service Processor configuration workflow 54
  setting up a network 20
  setting up the BranchCache configuration 56
  workflow for assigning array LUNs to nodes 25
  workflow for assigning disks to existing aggregates 36
  workflow for assigning disks to nodes 25
  workflow for assigning export policies to qtrees 50
  workflow for mirroring aggregates 46
  workflow for nondisruptive cluster update 16
  workflow for protecting data using mirror and vault relationship 60
  workflow for provisioning SSD cache 42

H
hash stores
  specifying path and maximum size for BranchCache configuration 57
HDDs
  converting existing aggregate to a Flash Pool aggregate 48
  creating aggregates 47
HDDs and SSDs
  adding to aggregates 38

I
ifgroups
  See interface groups
information
  how to send feedback about improving documentation 86
intercluster connectivity
  creating network interfaces for 22
interface groups
  creating 21
IP address disabled
  setting up a network 12
IP address range enabled
  using for setting up a network 11
IP addresses
  assigning to multiple Service Processors 54
  editing for a Service Processor 55
L
licenses
  adding 67
LIFs
  creating 22
LUNs, array
  assigning 26

M
MetroCluster configurations
  adding licenses 67
mirror and vault
  creating a relationship from a source volume 60
mirror and vault relationship
  creating from a destination SVM 63
mirror and vault relationships
  workflow for protecting data 60
  workflow for providing data protection 60
mirroring
  aggregates 49
mirroring aggregates
  workflow for providing data resiliency 46
mirrors
  creating a relationship from a destination SVM 75
  creating relationships from source SVM 73
modifying
  Service Processor settings 55
  the share settings 58
mounting
  volumes 72

N
NDU
  See nondisruptive updates
NetApp Support Site
  obtaining ONTAP software images 16
network
  creating broadcast domains 22
  creating subnets 22
  creating VLANs 21
  setup workflow 20
network interfaces
  creating 22
  creating VLANs 21
network mask
  editing for a Service Processor 55
networks
  setting up to manage clusters, nodes, Service Processors 11
nodes
  assigning disks 25
  workflow for assigning array LUNs to 25
  workflow for assigning disks to 25
non-root aggregates
  adding capacity disks to 38
nondisruptive updates
  performing for clusters using System Manager 17
  workflow for updating clusters 16

O
OnCommand System Manager
  prerequisites and workflow for setting up a cluster using 7
OnCommand System Manager creating a cluster
  setting up a cluster 10
ONTAP software images
  obtaining 16
  selecting for nondisruptive update 17
oplocks
  enabling 58

P
per-share cache
  creating for BranchCache configuration 57
policies
  assigning export, to qtrees 51
pre-update checks
  validating the cluster before updating 17
prerequisites
  for setting up a cluster using OnCommand System Manager 7
provisioning storage
  by creating a FabricPool 30
  by creating HDD and SSD aggregates 47
  creating aggregates or Flash Pool aggregates 46
  creating Flash Pool aggregates 48
  creating SnapLock Compliance aggregates 68
  creating SnapLock Enterprise aggregates 68

Q
qtrees
  assigning an export policy to 51
  creating 50
  exporting 51
  workflow for assigning export policies 50

R
relationships
  mirror and vault, creating from a destination SVM 63
  mirror and vault, creating from a source volume 60
  mirror, creating from a destination SVM 75
  mirror, creating from a source SVM 73
  vault, creating from a destination SVM 81
  vault, creating from a source SVM 78
resizing
  FlexGroup volumes 34
reversions
  obtaining ONTAP software images 16
reviewing
  storage recommendations 13
root aggregates
  adding capacity disks to 38

S
server keys
specifying for BranchCache configuration 57
Service Processors
assigning IP addresses globally 54
configuration workflow 54
editing the settings 55
setting up
BranchCache 57
CIFS 56
setting up a cluster
by using the template file in your data center 8
using OnCommand System Manager in your data center 10
setting up a network
by using OnCommand System Manager 11
for managing cluster, nodes, Services Processors 11
when the IP address range is disabled 12
when the IP address range is enabled 11
setting up a support page
cluster setup 13
using OnCommand System Manager 13
shares
editing permissions and options 58
SMB
configuring BranchCache on 57
SMB encryption
setting up 56
SnapLock Compliance aggregates
creating 68
SnapLock Compliance volumes
creating 69
SnapLock Enterprise aggregates
creating 68
SnapLock Enterprise volumes
creating 69
SnapLock for SnapMirror
workflow 66
SnapLock for SnapVault
workflow 66
SnapMirror
workflow 66
SnapVault
workflow 66
software images
selecting the ONTAP image for update 17
software images, ONTAP
obtaining 16
software licenses
adding 67
spare array LUNs
zeroing 27
spare disks
zeroing 26
SPs
See Service Processors
SSDs
adding to HDDs for converting to Flash Pool aggregates 48
combining to create storage pools 40, 44
creating aggregates 47
dedicated SSDs 39, 43
increasing the size of Flash Pool aggregates by adding 44
provisioning cache by adding 39, 43
storage pools 39, 43
workflow for provisioning cache 42
storage
provisioning by creating aggregates 47
storage pools
adding SSDs as 44
assigning disks to increase capacity 25
creating 40, 44
storage provisioning
creating SnapLock aggregates 68
storage recommendations
reviewing 13
storage tiers
managing by using FabricPool, introduction 28
subnets
assigning IP addresses to Service Processors 54
creating 22
specifying the IP address for the network interface 22
suggestions
how to send feedback about documentation 86
SVMs
creating 14
creating mirror relationships from destination or source 72
creating network interfaces for managing 22
creating vault relationships from destination 81
creating vault relationships from source or destination 72
setting up BranchCache on 57
using for serving data 14
symbolic links
editing the settings of 58
System Manager
workflows in the 8.3 release 5
workflows in the 8.3.1 release 5
workflows in the 8.3.2 release 5
T

template file for creating a cluster
using to set up a cluster 8
Twitter
how to receive automatic notification of documentation changes 86
U
unowned disks
assigning ownership 25
updates
performing a nondisruptive upgrade through System Manager 17
upgrades
obtaining ONTAP software images 16
See also nondisruptive updates
V
validating
checking the cluster before an update 17
vaults
creating a relationship from a destination SVM 81
creating a relationship from a source SVM 78

VLANs
creating 21
volume
using for changing tiering policy 31
volumes
creating an export policy for client access to 52
creating qtrees 50
creating SnapLock Compliance 69
creating SnapLock Enterprise 69
mounting 72

W
workflow
managing FlexGroup volumes 32
resizing FlexGroup 34
workflows
assigning array LUNs to existing aggregates 25
assigning disks to existing aggregates 25, 36
cluster setup using OnCommand System Manager 7
configuring a Service Processor 54

creating SnapLock for SnapMirror relationships 66
creating SnapLock for SnapVault relationships 66
for nondisruptive cluster update 16
in System Manager 8.3 5
in System Manager 8.3.1 5
in System Manager 8.3.2 5
in System Manager 9.0 5
in System Manager 9.1 5
providing data access to qtrees by using export policies 50
providing data protection by creating mirror and vault relationships 60
providing data resiliency by mirroring aggregates 46
provisioning SSD cache through Flash pool aggregates 42
setting up a network 20
setting up the BranchCache configuration 56

Z
zeroing
array LUNs 27
disks 26