Cluster Management Workflows for ONTAP® System Manager
Contents

ONTAP System Manager workflows .......................................................... 5
Setting up a cluster by using ONTAP System Manager ....................... 8
  Setting up a cluster by using the template file ................................. 9
  Setting up the cluster manually ....................................................... 11
  Creating a cluster .................................................................................. 11
  Setting up a network ............................................................................. 12
  Setting up a support page ..................................................................... 14
  Reviewing storage recommendations .................................................. 14
  Creating an SVM ................................................................................... 14

Setting up the network ........................................................................ 17
  Creating VLAN interfaces ................................................................. 18
  Creating interface groups ................................................................. 18
  Creating broadcast domains ............................................................... 19
  Creating subnets ................................................................................ 19
  Creating network interfaces .............................................................. 19

Assigning disks or array LUNs to nodes .............................................. 22
  Assigning disks to nodes .................................................................... 22
  Zeroing spare disks ............................................................................. 23
  Assigning array LUNs ......................................................................... 23
  Zeroing spare array LUNs ................................................................... 24

Managing FlexGroup volumes using System Manager ..................... 25
  Creating FlexGroup volumes ............................................................ 25

Resizing FlexGroup volumes using System Manager ....................... 28
  Resizing FlexGroup volumes ............................................................ 28

Assigning disks to existing aggregates .............................................. 30
  Adding capacity disks ....................................................................... 32
  Provisioning cache to aggregates by adding SSDs ............................ 33
  Creating a storage pool ...................................................................... 34

Provisioning cache through Flash Pool aggregates ............................ 36
  Provisioning cache to aggregates by adding SSDs ............................ 37
  Increasing the cache for Flash Pool aggregates by adding SSDs ........ 38
  Creating a storage pool ...................................................................... 38

Providing data resiliency by mirroring aggregates ......................... 40
  Provisioning storage through aggregates ....................................... 40
  Provisioning storage by creating an aggregate manually ................ 41
  Provisioning storage by creating a Flash Pool aggregate manually .... 42
  Mirroring aggregates ........................................................................ 43

Providing data access to qtrees using export policies ..................... 44
  Creating qtrees ................................................................................ 44
  Assigning export policies to qtrees ................................................... 45
  Creating an export policy .................................................................. 46
Adding rules to an export policy ................................................................. 46

**Configuring a Service Processor** .......................................................... 48
  Assigning IP addresses to Service Processors ........................................... 48
  Editing Service Processor settings ............................................................. 49

**Setting up a BranchCache configuration** ............................................. 50
  Setting up CIFS ....................................................................................... 50
  Setting up BranchCache ........................................................................... 51
  Editing share settings ............................................................................. 52

**Protecting data using mirror and vault relationship** ............................ 54
  Creating a mirror and vault relationship from a source SVM .................. 54
  Creating a mirror and vault relationship from a destination SVM ............ 56

**Protecting data using SnapLock** ......................................................... 59
  Adding licenses ..................................................................................... 60
  Provisioning storage by creating a SnapLock aggregate manually .......... 61
  Creating SnapLock volumes ................................................................. 62
  Mounting volumes ................................................................................. 66
  Creating a mirror or vault relationship from a source or destination SVM .... 67
    Creating a mirror relationship from a source SVM .................................. 67
    Creating a mirror relationship from a destination SVM ......................... 69
  Creating a vault relationship from a source SVM ..................................... 71
  Creating a vault relationship from a destination SVM ............................. 73

**Copyright** ............................................................................................ 76
**Trademark** ............................................................................................ 77
**How to send comments about documentation and receive update**
**notifications** ....................................................................................... 78
**Index** ................................................................................................. 79
ONTAP System Manager workflows

The workflow guide provides workflows for some of the new functions that are introduced in ONTAP System Manager.

Workflows that are introduced or enhanced in System Manager 9.6 are included in the Cluster Management Using OnCommand System Manager guide. The following workflow is introduced in System Manager 9.6:

MetroCluster switchover and switchback

Starting with System Manager 9.6, you can use MetroCluster switchover and switchback operations to allow one cluster site to take over the tasks of another cluster site. This capability allows you to facilitate maintenance or recovery from disasters.

Cluster management using System Manager

Workflows that are introduced or enhanced in System Manager 9.5 are included in the Cluster Management Using OnCommand System Manager guide. The following workflow is enhanced in System Manager 9.5:

Setting up NVMe protocol

In System Manager 9.5, when you set up the NVMe protocol for a storage virtual machine (SVM), you must ensure that at least one LIF is configured for each node in an HA pair.

Cluster management using System Manager

Workflows that are introduced or enhanced in System Manager 9.4 are included in the Cluster Management Using OnCommand System Manager guide. The following workflow is introduced in System Manager 9.4:

Setting up NVMe protocol

You can set up the NVMe protocol for a storage virtual machine (SVM) by using System Manager. After the NVMe protocol is enabled on the SVM, you can provision namespaces and assign the namespaces to a host and a subsystem.

Cluster management using System Manager

Workflows that are introduced or enhanced in System Manager 9.3 are included in the Cluster Management Using OnCommand System Manager guide. The following workflows are introduced in System Manager 9.3:

• Setting up SAML authentication
  You can set up Security Assertion Markup Language (SAML) authentication so that remote users are authenticated through a secure identity provider (IdP) before they log in to System Manager.

• Setting up peering
  Setting up peering involves creating intercluster logical interfaces (LIFs) on each node, creating cluster peering relationship, and creating SVM peering relationship.

Cluster management using System Manager

Workflows are provided for the following functionalities that were introduced or enhanced in System Manager 9.2:

Creating a cluster using System Manager on page 8

Provides information about creating a cluster manually or by using a template file, setting up the network, providing storage recommendation, creating an aggregate, and creating an SVM by using 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 8  
  Provides information about creating a cluster and setting up node management networks, cluster management networks, and AutoSupport messages and event notifications by using System Manager.

- **Managing FlexGroups** on page 25  
  Provides information about creating FlexGroup volumes, editing the properties of existing FlexGroup volumes, resizing FlexGroup volumes, changing the status of FlexGroup volumes, and deleting FlexGroup volumes.

- **Resizing FlexGroup volumes using System Manager** on page 28  
  Provides information about resizing FlexGroup volumes by resizing existing resources or adding new resources.

Workflows are provided for the following functionality that was introduced in System Manager 9.0:

- **Protecting data using SnapLock** on page 59  
  Provides information about using SnapLock volumes 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 22  
  Provides information about assigning disks and array LUNs to nodes.

- **Providing data resiliency by mirroring aggregates** on page 40  
  Provides information about mirroring aggregates by using the SyncMirror feature.

- **Protecting data using mirror and vault relationship** on page 54  
  Provides information about protecting data by using mirror and vault relationships.

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

- **Setting up the network** on page 17  
  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 30  
  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 36  
  Provides information about provisioning cache by creating Flash Pool aggregates or by converting existing aggregates to Flash Pool aggregates by adding SSDs.

- **Providing data access to qtrees using export policies** on page 44  
  Provides information about exporting a specific qtree on a volume by assigning export policies to the qtree.

- **Configuring a Service Processor** on page 48  
  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 50
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 included 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.
Setting up a cluster by using ONTAP System Manager

You can use ONTAP 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.
Setting up a cluster by using ONTAP System Manager

Choices

- Setting up a cluster by using the template file on page 9
- Setting up the cluster manually on page 11

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 event...
notifications. (Starting with ONTAP System Manager 9.6, AutoSupport is not supported.) 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 automatically 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:
If you want to... | Then...
---|---
Exit cluster setup without provisioning storage and creating an SVM | Click **Skip this step**.
Provision storage using aggregates and create an SVM | Click **Submit and Continue**.

You can edit the support details, if required.

11. Verify the details in the **Create Storage Virtual Machine (SVM)** window, and then click **Submit and Continue**.

You can edit the SVM name, select a different data protocol, and modify the Network Interface and Adapter Details, if required.

12. 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.

13. 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.

14. 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 event notifications.

### Creating a cluster

You can use ONTAP 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 each IP address range on a separate line, 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 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 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 event notifications, and for single-node clusters, configuring system backup.

**Before you begin**

You must have set up the cluster and network.

**Steps**

1. 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.

2. 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.

3. 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. |

| Enable FC/FCoE protocol | a. Select the **FC/FCoE** box.  
  b. Select the FC/FCoE ports for FC or FCoE protocols.  
  **Note**: Each node must have at least one correctly configured port for each protocol (FC and FCoE). |
If you want to... Then...

Enable NVMe protocol

a. Select the NVMe box.

   b. Select the NVMe ports for NVMe protocols.

   **Note:** At least one NVMe capable adapter must be available in one of the nodes to configure NVMe. Also, starting with ONTAP 9.5, at least one NVMe LIF must be configured for each node of a HA pair associated with the SVM. You can create a maximum of two NVMe LIFs for each node in the pair.

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.
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 18
   You can create a VLAN to maintain separate broadcast domains within the same network domain by using System Manager.

2. **Creating interface groups** on page 18
   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 19
   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 19
   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 19
   You can use System Manager to create a network interface or LIF to access data from storage virtual machines (SVMs), to manage SVMs and to provide an interface for intercluster connectivity.
Creating VLAN interfaces

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

Steps
1. Click Network > Ethernet Ports.
2. 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 interface group, or that host a VLAN.

Steps
1. Click Network > Ethernet Ports.
2. 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-mode, static multiple, or dynamic multimode (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, IP space, 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), to 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, DDNS is disabled if you configure the LIF for intercluster communication using iSCSI, NVMe, or FC/FCoE protocols, or for management access only.

- You can specify an IP address by using a subnet or by not 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 (CLI) to create a network interface in such cases.

- To create NVMeoF data LIF the SVM must already be set up, the NVMe service must already exist on the SVM and the NVMeoF capable adapters should be available.

- NVMe protocol is enabled only if the selected SVM has the NVMe service configured.

Steps

1. Click **Network > Network Interfaces**.

2. 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.

   **Note:** If you select the NVMe protocol, the rest of the protocols are disabled. If NAS (CIFS and NFS) protocols are supported then they remain available. The NVMe transports field is displayed when you select the NVMe protocol and FC-NVMe is shown as the transport protocol.

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 NVMe protocols.

7. Assign the IP address:
<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the IP address by using a subnet</td>
<td>a. Select <strong>Using a subnet</strong>.&lt;br&gt;&lt;br&gt;b. In the Add Details dialog box, select the subnet from which the IP address must be assigned.&lt;br&gt;For intercluster LIF, only the subnets that are associated with the selected IPspace are displayed.&lt;br&gt;&lt;br&gt;c. If you want to assign a specific IP address to the interface, select <strong>Use a specific IP address</strong>, and then type the IP address.&lt;br&gt;The IP address that you specify is added to the subnet if the IP address is not already present in the subnet range.&lt;br&gt;&lt;br&gt;d. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Specify the IP address manually without using a subnet</td>
<td>a. Select <strong>Without a subnet</strong>.&lt;br&gt;&lt;br&gt;b. In the Add Details dialog box, perform the following steps:&lt;br&gt;&lt;br&gt;   i. Specify the IP address and the network mask or prefix.&lt;br&gt;   ii. Optional: Specify the gateway.&lt;br&gt;   iii. If you do not want to use the default value for the Destination field, specify a new destination value.&lt;br&gt;   If you do not specify a destination value, the Destination field is populated with the default value based on the family of the IP address.&lt;br&gt;&lt;br&gt;   If a route does not exist, a new route is automatically created based on the gateway and destination.&lt;br&gt;&lt;br&gt;c. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

8. Select the required ports from the **Port** details area.<br><br>   • For data LIFs, the Port details area displays all of the ports from the broadcast domain that is associated with the IPspace of the SVM.<br>   • For intercluster LIFs, the Port details area displays all of the ports from the broadcast domain that is associated with the required IPspace.<br>   • The Port details area will display only NVMe capable adapters if the NVMe protocol is selected.<br><br>9. Optional: Select the **Dynamic DNS (DDNS)** check box to enable DDNS.<br><br>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.

Assigning disks to nodes:
1. Assigning disks to nodes
2. Zeroing spare disks

Assigning array LUNs to nodes:
1. Assigning array LUNs
2. Zeroing spare array LUNs

Assigning disks to nodes

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

About this task
- You can assign disks if the following conditions are true:
  - The container type of the selected disks must be “unassigned”.
  - The disks must be connected to nodes in an HA pair.
  - The disks must be visible to the node.
- For MetroCluster configurations, you cannot use System Manager to assign disks. You must use the command-line interface instead.
Steps
1. Click Storage > Aggregates & Disks > 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 Storage > Aggregates & Disks > 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 Storage > Aggregates & Disks > 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 Storage > Aggregates & Disks > 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 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 25
   A FlexGroup volume can contain many volumes that can be administered as a group instead of individually. You can use System Manager to create a FlexGroup volume by selecting specific aggregates or by selecting system-recommended aggregates.

Creating FlexGroup volumes

A FlexGroup volume can contain many volumes that can be administered as a group instead of individually. 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.
- Starting with System Manager 9.6, you can create FlexGroup volumes in a MetroCluster configuration.

Steps
1. Click Storage > Volumes.
2. Click Create > Create FlexGroup.
3. In the **Create FlexGroup** window, specify a name for the FlexGroup volume. By default, the aggregates are selected according to best practices.

4. Click the **Volume Encryption** button to enable encryption for the volume. This option is available only if you have enabled the Volume Encryption license and if the corresponding platform supports encryption.

   Turning on volume encryption might affect the cross-volume storage efficiency when the selected aggregates are encrypted.

5. Specify a size for the FlexGroup volume.
   **Note:** You must also specify the measurement units.

6. Enable the **FabricPool** toggle button to use FabricPool aggregates in the FlexGroup volume.
   - When you enable **FabricPool**, you can select the Tiering policy from the following choices in the drop-down menu:
     - **Snapshot-only**
       Moves the Snapshot copies of only those volumes that are currently not being referenced by the active file system. Snapshot-only policy is the default tiering policy.
     - **Auto**
       Moves the inactive (cold) data and the Snapshot copies from the active file system to the cloud tier.
     - **Backup (for System Manager 9.5)**
       Moves the newly transferred data of a data protection (DP) volume to the cloud tier.
     - **All (starting with System Manager 9.6)**
       Moves all data to the cloud tier.
     - **None**
       Prevents the data on the volume from being moved to a cloud tier.
   - If you leave **FabricPool** in the “not enabled” position, only non-FabricPool aggregates are included in the created FlexGroup volume, and the tiering policy is set to “None”.
   - If no FabricPool aggregates exist in the SVM, then **FabricPool** displays in the "not enabled" position and cannot be changed.
   - If only FabricPool aggregates exist in the SVM, then the **FabricPool** button is displays in the "enabled" position and cannot be changed.

7. If you want to specify particular aggregates, click (advanced options).

   The aggregates associated with the FlexGroup volume you are creating are selected by default, according to best practices. They are displayed next to the **Aggregates** label.

8. In the **Protection** section, perform the following actions:
   a. Enable the **Volume Protection** option.
   b. Select the **Replication** type.
      **Note:** The **Synchronous** replication type is not supported for FlexGroup volumes.
   c. Click **Help me Choose**, if you do not know the replication type and relationship type.
      - Specify the values and click **Apply**.
        The replication type and the relationship type is automatically selected based on the values specified.
d. Select the relationship type.
   The relationship types can be mirror, vault, or mirror and vault.

e. Select a cluster and an SVM for the destination volume.
   If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then
   only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered
   SVMs and permitted SVMs are listed.

f. Modify the volume name suffix as required.

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 28
   You can use System Manager to resize a FlexGroup volume by resizing existing resources or by adding new resources.

Resizing FlexGroup volumes

You can use System Manager to resize a FlexGroup volume by resizing existing resources or by 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 Storage > Volumes.
2. From the drop-down menu in the SVM field, select All SVMs.
3. Select the FlexGroup volume that you want to resize, and then click More Actions > Resize.
4. In the Resize FlexGroup Volume window, specify the size to which you want to resize the FlexGroup volume.
By default, existing aggregates are used to resize the FlexGroup volume. Starting with System Manager 9.6, the minimum size that is allowed for the volume is displayed next to the size fields.

**Note:** If you want to expand the FlexGroup volume by adding new resources, click (advanced options).

5. Specify the percentage of the Snapshot copy reserve.

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).
Steps

1. **Adding capacity disks** on page 32
   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 33
   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 34
   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 might cause performance issues.

If you add disks that are larger in size than the disks that are 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 sized disks remain in the new RAID group, the disks are not 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 of the disks in the range of 669 GB through 781 GB are eligible for selection. For all of 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.

• Shared disks support two RAID types: RAID DP and RAID-TEC.

• You cannot use SSDs with storage pool.

• If the RAID group 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 type 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 Applications & Tiers > Storage Tiers.
2. In the Storage Tiers window, select the aggregate to which you want to add capacity disks, and then click More Actions > Add Capacity.

3. Specify the following information in the Add Capacity dialog box:
   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 of the 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 then provision 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.

About this task
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 **Applications & Tiers** > **Storage Tiers**.
   • Click **Storage** > **Aggregates & Disks** > **Aggregates**.

2. In the **Storage Tiers** window, select the aggregate, and then click **More Actions** > **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>
</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.

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 **Storage > Aggregates & Disks > 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 37
   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 38
   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 38
   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 of the 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 then provision 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.

About this task

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 Applications & Tiers > Storage Tiers.
   - Click Storage > Aggregates & Disks > Aggregates.

2. In the Storage Tiers window, select the aggregate, and then click More Actions > 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>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 Change.</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 Save.</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.

### 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 **Storage** > **Aggregates & Disks** > **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 Storage > Aggregates & Disks > 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 based on storage recommendations or manually depending on your requirement. You can create Flash Pool aggregates, SnapLock aggregates, and a FabricPool-enabled aggregates 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 then 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 manually

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

Before you begin
All of the 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 available RAID type.

Steps
1. Create an aggregate by using one of the following methods:
   • Click Applications & Tiers > Storage Tiers > Add Aggregate.
   • Click Storage > Aggregate & Disks > Aggregates > Create.
2. Enable the Manually Create Aggregate option to create an aggregate.
3. To create an aggregate:
   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.
         Shared disks support two RAID types: RAID DP and RAID-TEC.
      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 for MetroCluster configurations.
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 manually

You can use System Manager to create a Flash Pool aggregate manually, 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 the platform-specific best practices and workload-specific best practices for the Flash Pool aggregate SSD tier size and configuration.
- All of the HDDs must be in the zeroed state.
- If you want to add SSDs to the aggregate, all of the existing SSDs and dedicated SSDs must be of the same size.

About this task

- You cannot use partitioned SSDs while creating a 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. Create an aggregate by using one of the following methods:
   - Click Applications & Tiers > Storage Tiers > Add Aggregate.
   - Click Storage > Aggregate & Disks > Aggregates > Create.
2. Enable the Manually Create Aggregate option to create an aggregate.
3. In the Create Aggregate window, specify the name of the aggregate, the disk type, and the number of disks or partitions to include for the HDDs 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 for MetroCluster configurations.
5. Click Use Flash Pool Cache with this aggregate.
6. Specify the cache source:

<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 Storage pools 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...

<table>
<thead>
<tr>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated SSDs</td>
</tr>
<tr>
<td>a. Select <strong>Dedicated SSDs</strong> as the Cache Source.</td>
</tr>
<tr>
<td>b. Select the SSD size and the number of SSDs to include in the aggregate.</td>
</tr>
<tr>
<td>c. Modify the RAID configuration, if required:</td>
</tr>
<tr>
<td>i. Click <strong>Change</strong>.</td>
</tr>
<tr>
<td>ii. In the Change RAID Configuration dialog box, specify the RAID type and the RAID group size.</td>
</tr>
<tr>
<td>iii. Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

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 to 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 a Flash Pool aggregate when the cache source is storage pool.

**Steps**
1. Choose one of the following methods:
   - Click **Applications & Tiers > Storage Tiers**.
   - Click **Storage > Aggregates & Disks > Aggregates**.
2. Select the aggregate that you want to mirror, and then click **More 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 44

  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 45

  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 a 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 Storage > Qtrees.

2. From the drop-down menu in the SVM field, select the storage virtual machine (SVM) on which you want to create a qtree.

3. Click Create.

4. In the Details tab of the Create Qtree dialog box, type a name for the qtree.
5. Select the volume to which you want to add the qtree.
   The Volume browse list includes only the volumes that are online.

6. If you want to disable opportunistic locks (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.

7. If you want to change the default inherited security style, select a new security style.
   The default security style of the qtree is the security style of the volume that contains the qtree.

8. If you want to change the default inherited export policy, either select an existing export policy or create an export policy.
   The default export policy of the qtree is the export policy that is assigned to the volume that contains the qtree.
   *Creating an export policy* on page 46

9. 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.

10. Click **Create**.

11. Verify that the qtree that 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 the qtree. You can assign an export policy to one or more qtrees from the Qtrees window.

**Steps**

1. Click **Storage > Qtrees**.

2. From the drop-down menu in the SVM field, select the storage virtual machine (SVM) on which the qtrees that you want to export reside.

3. Select one or more qtrees for which you want to assign an export policy, and then click **Change Export Policy**.

4. In the **Export Policy** dialog box, either create an export policy or select an existing export policy.
   *Creating an export policy* on page 46

5. Click **Save**.

6. Verify that the export policy and its related export rules that you assigned to the qtrees are displayed in the **Details** tab of the appropriate qtrees.
Creating an export policy

You can use System Manager to create an export policy so that clients can access specific volumes.

Steps
1. Click Storage > SVMs.
2. Select the SVM, and then click SVM Settings.
3. In the Policies pane, click Export Policies.
4. Click Create.
5. In the Create Export Policy dialog box, specify a name for the export policy.
6. If you want to create an export policy by copying the rules from an existing export policy, select the Copy Rules from check box, and then select the storage virtual machine (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.
7. In the Export Rules area, click Add to add rules to the export policy.
   Adding rules to an export policy on page 46
8. Click Create.
9. Verify that the export policy that you created is displayed in the Export Policies window.

Related tasks
Creating qtrees on page 44
Assigning export policies to qtrees on page 45

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 Storage > SVMs.
2. Select the SVM, and then click SVM Settings.
3. In the Policies pane, click Export Policies.
4. Select the export policy to which you want to add rules, and from the Export Rules tab, click Add.
5. 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 symbol (@); 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 are treated as a host name.

You can enter the IPv4 address 0.0.0.0/0 to provide access to all of 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.

6. Click OK.

7. Verify that the export rule that you added is displayed in the **Export Rules** tab for the selected export policy.

**Related tasks**

*Creating an export policy* on page 46
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 48
   You can use System Manager to assign IP addresses to all of your Service Processors at the same time and to use these Service Processors to monitor and manage various system parameters of your storage systems.
2. Editing Service Processor settings on page 49
   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 of your Service Processors at the same time and to use these Service Processors to monitor and manage various system parameters of your storage systems.

Steps
1. Click Configuration > Cluster > Configuration Updates.
2. In the Service Processor window, click Global Settings.
3. In the Global Settings dialog box, choose the source for assigning the IP addresses:

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

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

Steps

1. Click **Configuration > Cluster > Service Processor**.
2. In the **Service Processor** window, select the Service Processor that you want to modify, and then click **Edit**.
3. In the **Edit Service Processor** dialog box, make the required 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 50
   You can use System Manager to enable and configure CIFS servers to allow CIFS clients to access the files on the cluster.

2. **Setting up BranchCache** on page 51
   You can use System Manager to configure BranchCache on a CIFS-enabled storage virtual machine (SVM) to enable the caching of content on computers that are local to the requesting clients.

3. **Editing share settings** on page 52
   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). Starting with System Manager 9.6, continuous availability is supported for FlexGroup volumes.

**Setting up CIFS**

You can use System Manager to enable and configure CIFS servers to allow CIFS clients to access the 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 by 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 that is 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 the CIFS protocol.

**Steps**

1. Click **Storage > SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Configuration** tab, click **Set up**.
4. In the **General** tab of the **CIFS Server Setup** dialog box, specify the NetBIOS name and the Active Directory domain details.
5. Click the **Options** tab, and then perform the following actions:
   - In the SMB settings area, select or clear the SMB signing check box and the SMB encryption check box, as required.
   - Specify the default UNIX user.
   - In the WINS Servers area, add the required IP address.
6. Click **Set up**.

### Setting up BranchCache

You can use System Manager to configure BranchCache on a CIFS-enabled storage virtual machine (SVM) to enable the caching of content on computers that are local to the 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.
- You can create an all-shares BranchCache configuration if you want to offer caching services for all of the content that is contained within all of 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 that is contained within selected SMB shares on the CIFS server.

**Steps**

1. Click **Storage > SVMs**.
2. Select the SVM, and then click SVM Settings.

3. In the BranchCache tab, click Set Up.

4. 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 a 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 of the versions that are supported by the client are selected.

5. 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). Starting with System Manager 9.6, continuous availability is supported for FlexGroup volumes.

Steps

1. Click Storage > Shares.

2. Select the share that you want to modify from the list of shares, and then click Edit.

3. 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 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 then assign permissions to specify the type of access.
   c. In the Options tab, select the required options.

4. Click Save and Close.
5. 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. This relationship 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 the source cluster and destination cluster.

Note:
For some platforms, it is not mandatory for the source cluster to have the SnapMirror license enabled if the destination cluster has the SnapMirror license and Data Protection Optimization (DPO) license enabled.

After the DPO license is enabled on the destination cluster, you must refresh the browser of the source cluster to enable the Protect option.

- The source cluster and destination cluster must be in a healthy peer relationship.
- The source SVM and destination SVM must be in a healthy peer relationship, or the destination SVM must have permission to peer.
- The destination aggregate must have space available.
- The source aggregate and the destination aggregate must be 64-bit aggregates.
- FlexVol volumes must be online and of type read/write.
- The SnapLock aggregate type must be the same.
- A maximum of 25 volumes can be protected in one selection.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must be enabled on the remote cluster.

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.
- If encryption is enabled on the source volume and the destination cluster is running a version of ONTAP software earlier than ONTAP 9.3, then encryption is disabled on the destination volume by default.
- SVMs that are peered only for FlexCache applications and do not have peering permissions for SnapMirror applications are not shown in the list of SVMs in this task. You can use the ONTAP System Manager 9.6 enhanced peering workflow to give permission to, or peer to, these SVMs. You then can select them in this task to create a protection relationship.

Steps

1. Click Storage > Volumes.
2. From the drop-down menu in the SVM field, select All SVMs.
3. Select the volumes for which you want to create mirror and vault relationships, and then click More Actions > Protect.
   - The Protect option is available only for a read/write volume.
4. Select the Replication type:
If you selected the replication type as… | Do this…
---|---
Asynchronous | a. **Optional**: If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**.

b. Select the relationship type.
The relationship type can be mirror, vault, or mirror and vault.

c. Select a cluster and an SVM.
If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.

d. Modify the volume name suffix, if required.

Synchronous | a. **Optional**: If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**.

b. Select the synchronization policy.
The synchronization policy can be **StrictSync** or **Sync**.

c. Select a cluster and an SVM.
If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.

d. Modify the volume name suffix, if required.

5. **Optional**: Click 🔄, update the protection policy and protection schedule, select **FabricPool-enabled aggregate**, and then initialize the protection relationship.

6. Click **Save**.

**Related information**

*Data Protection Power Guide*

---

**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.
- SnapMirror license must be enabled on the source cluster and destination cluster.

**Note**: For some platforms, it is not mandatory for the source cluster to have the SnapMirror license enabled if the destination cluster has the SnapMirror license and Data Protection Optimization (DPO) license enabled.
• The source cluster and destination cluster must be in a healthy peer relationship.
• The destination SVM must have space available.
• The source aggregate and destination aggregate must be 64-bit aggregates.
• A source volume of type read/write (rw) must already exist.
• The SnapLock aggregate type must be the same.
• If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which SAML authentication is enabled, password-based authentication must be enabled on the remote cluster.

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.
• A maximum of 25 volumes can be protected in one selection.

Steps
1. Click Protection > Volume 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.
   If the specified cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the specified cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.
6. Enter a volume name suffix.
   The volume name suffix is appended to the source volume names to generate the destination volume names.
7. Optional: Click Browse, and then change the 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.
8. Select a schedule for the relationship from the list of existing schedules.
9. Optional: Select Initialize Relationship to initialize the relationship.
10. Enable FabricPool-enabled aggregates, and then select an appropriate tiering policy.

11. Click **Validate** to verify whether the selected volumes have matching labels.

12. Click **Create**.

**Related information**

*Data Protection Power Guide*
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 60
   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 manually** on page 61
   You can use System Manager to create a SnapLock Compliance aggregate or a SnapLock Enterprise aggregate manually. You can create SnapLock volumes on these aggregates, which provide “write once, read many” (WORM) capabilities.

3. **Creating SnapLock volumes** on page 62
   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 66
   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 67
   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 Cloud Volumes ONTAP license. The Cloud Volumes ONTAP license is not listed in the license page. System Manager does not raise any alert about the entitlement risk status of the Cloud Volumes ONTAP license.

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

Steps

1. Click Configuration > Cluster > Licenses.

2. Click Add.

3. 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>
<tbody>
<tr>
<td>Add a license for a specific ONTAP service</td>
<td>a. Enter the software license key.</td>
</tr>
<tr>
<td></td>
<td>You can add multiple licenses by entering the software license keys separated by commas.</td>
</tr>
<tr>
<td></td>
<td>b. Click Add.</td>
</tr>
<tr>
<td>Add a capacity based license</td>
<td>a. Click Browse, and then select the capacity based license file.</td>
</tr>
<tr>
<td></td>
<td>b. Click Add.</td>
</tr>
<tr>
<td>Add a license for a specific ONTAP service and add a capacity-based license</td>
<td>a. Enter the software license key.</td>
</tr>
<tr>
<td></td>
<td>You can add multiple licenses by entering the software license keys separated by commas.</td>
</tr>
<tr>
<td></td>
<td>b. Click Browse, and then select the capacity based license file.</td>
</tr>
<tr>
<td></td>
<td>c. Click Add.</td>
</tr>
</tbody>
</table>

The new license is added.

The Add License Status dialog box displays the list of licenses that were added successfully. The dialog box also displays the license keys of the licenses that were not added and the reason why the licenses were not added.

4. Click Close.
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 manually**

You can use System Manager to create a SnapLock Compliance aggregate or a SnapLock Enterprise aggregate manually. 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 aggregates are 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 AFF platform.

**Steps**

1. Create a SnapLock aggregate by using one of the following methods:
   - Click **Applications & Tiers > Storage Tiers > Add Aggregate**.
   - Click **Storage > Aggregate & Disks > Aggregates > Create**.
2. Enable the **Manually Create Aggregate** option to create an aggregate.
3. To create a SnapLock aggregate:
   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 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.
         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:** You must ensure that the current system time is correct. The ComplianceClock is set based on the system clock. Once the ComplianceClock 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 for MetroCluster configurations.

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 by using System Manager, and you must have enabled “key-manager setup” by 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 Cloud Volumes ONTAP.
- If encryption is enabled on the source volume and if the destination cluster is running a version of ONTAP software earlier than ONTAP 9.3, then encryption is disabled on the destination volume by default.

**Steps**

1. Click **Storage > Volumes**.
2. Click **Create > Create FlexVol**.
3. Browse and select the storage virtual machine (SVM) in which you want to create the volume.
4. 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 the volume.
5. Select the container 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.

6. Select the **Volume Encryption** checkbox 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.

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

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

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

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

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

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

10. Optional: Make the required 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 that is required for running deduplication, the volume is created, and deduplication is not enabled.

11. Select the **SnapLock** tab, and then perform the following steps:

    a. Optional: Specify the autocommit period.

       The file in the volume remains unchanged for the period that you specify before the file is committed to the WORM state. To set files to the WORM state manually, you must select **Not specified** as the autocommit setting.

       The values must be in the range of 5 minutes to 10 years.

    b. Specify the minimum retention period and maximum retention period.

       The values must be in the range of 1 day through 70 years or **Infinite**.

    c. Select the default retention period.

       The default retention period must be within the specified minimum retention period and maximum retention period.

12. Optional: Select the **Manage Storage Quality of Service** checkbox in the **Quality of Service** tab to enable storage QoS for the FlexVol volume in order to manage workload performance.

13. Create a storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the FlexVol volume.
<table>
<thead>
<tr>
<th>If you want to…</th>
<th>Do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a storage QoS policy group</td>
<td>a. Select <strong>New Policy Group</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Specify the policy group name.</td>
</tr>
<tr>
<td></td>
<td>c. Specify the minimum throughput limit.</td>
</tr>
<tr>
<td></td>
<td>• In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems.</td>
</tr>
<tr>
<td></td>
<td>• You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate.</td>
</tr>
<tr>
<td></td>
<td>• If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>d. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit.</td>
</tr>
<tr>
<td></td>
<td>• The minimum throughput limit and the maximum throughput limit must be of the same unit type.</td>
</tr>
<tr>
<td></td>
<td>• If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS, B/s, KB/s, MB/s, and so on.</td>
</tr>
<tr>
<td></td>
<td>• If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value. This value is case-sensitive. The unit that you specify does not affect the maximum throughput.</td>
</tr>
</tbody>
</table>
If you want to… | Do this…
---|---
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.

- In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems.

- You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate.

- If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value.

   This value is case-sensitive.

c. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does 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, 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.

   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.

14. Enable **Volume Protection** in the **Protection** tab to protect the volume:

15. In the **Protection** tab, select the **Replication** type:

<table>
<thead>
<tr>
<th>If you selected the replication type as…</th>
<th>Do this…</th>
</tr>
</thead>
</table>
| Asynchronous | a. **Optional**: If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**.

   b. Select the relationship type.

   The relationship type can be mirror, vault, or mirror and vault.

   c. Select a cluster and an SVM for the destination volume.

   If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.

   d. Modify the volume name suffix, if required. |
If you selected the replication type as… | Do this…
---|---
Synchronous | a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**.

  b. Select the synchronization policy.

  The synchronization policy can be **StrictSync** or **Sync**.

  c. Select a cluster and an SVM for the destination volume.

  If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.

  d. Modify the volume name suffix, if required.

16. Click **Create**.

17. 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 a 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 **Storage > Junction Path**.

2. From the drop-down menu in the **SVM** field, select the SVM on which you want to mount a volume.

3. Click **Mount**, and then select the volume that is to be mounted.

4. Optional: If you want to change the default junction name, specify a new name.

5. Click **Browse**, and then select the junction path to which you want to mount the volume.

6. Click **OK**, and then click **Mount**.

7. 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 67
• Creating a mirror relationship from a destination SVM on page 69
• Creating a vault relationship from a source SVM on page 71
• Creating a vault relationship from a destination SVM on page 73

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 destination cluster.

  Note:

  ◦ For some platforms, it is not mandatory for the source cluster to have the SnapMirror license enabled if the destination cluster has the SnapMirror license and Data Protection Optimization (DPO) license enabled.
  ◦ After the DPO license is enabled on the destination cluster, you must refresh the browser of the source cluster to enable the Protect option.

• While mirroring a SnapLock volume, the SnapMirror license must be installed on both the source cluster and destination cluster, and the SnapLock license must be installed on the destination cluster.

• The source cluster and destination cluster and the source SVM and destination SVM must be in a healthy peer relationship.

• The destination aggregate must have space available.

• FlexVol volumes must be online and of type read/write.

• The SnapLock aggregate type must be the same on both clusters.

• A maximum of 25 volumes can be protected in one selection.

• If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must be enabled on the remote cluster.
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 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.

- If encryption is enabled on the source volume and the destination cluster is running a version of ONTAP software earlier than ONTAP 9.3, then encryption is disabled on the destination volume by default.

- SVMs that are peered only for FlexCache applications and do not have peering permissions for SnapMirror applications are not shown in the list of SVMs in this task. You can use the ONTAP System Manager 9.6 enhanced peering workflow to give permission to, or peer to, these SVMs. You then can select them in this task to create a protection relationship.

Steps

1. Click Storage > Volumes.

2. From the drop-down menu in the SVM field, select All SVMs.

3. Select the volumes for which you want to create mirror relationships, and then click More Actions > Protect.
   The Protect option is available only for a read/write volume.

4. Select the Replication type:

<table>
<thead>
<tr>
<th>If you selected the replication type as…</th>
<th>Do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asynchronous</td>
<td>a. Optional: If you do not know the replication type and relationship type, click Help me Choose, specify the values, and then click Apply.</td>
</tr>
<tr>
<td></td>
<td>b. Select the relationship type.</td>
</tr>
<tr>
<td></td>
<td>The relationship type can be mirror, vault, or mirror and vault.</td>
</tr>
<tr>
<td></td>
<td>c. Select a cluster and an SVM.</td>
</tr>
<tr>
<td></td>
<td>If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.</td>
</tr>
<tr>
<td></td>
<td>d. Modify the volume name suffix, if required.</td>
</tr>
</tbody>
</table>
If you selected the replication type as...

<table>
<thead>
<tr>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronous</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

5. Optional: Click \( \text{Update} \), update the protection policy and protection schedule, select **FabricPool-enabled aggregate**, and then initialize the protection relationship.

6. Click **Save**.

**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 FlexVol volume, then a peer relationship is created between the two SVMs if the relationship does not already exist.

A mirror relationship is created between the source volume and the destination volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.

**Related information**

*Data Protection Power Guide*

**Creating a mirror relationship from a destination SVM**

You can use ONTAP 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 destination cluster.
  
  **Note:** For some platforms, it is not mandatory for the source cluster to have the SnapMirror license enabled if the destination cluster has the SnapMirror license and Data Protection Optimization (DPO) license enabled.

- While mirroring a volume, if you select a SnapLock volume as the source, then the SnapMirror license and SnapLock license must be installed on the destination cluster.
• The source cluster and destination cluster must be in a healthy peer relationship.
• The destination SVM must have space available.
• A source volume of type read/write (rw) must exist.
• The FlexVol volumes must be online and must be of type read/write.
• The SnapLock aggregate type must be of the same type.
• If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must be enabled on the remote cluster.

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 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 must ensure that the destination SVM has aggregates of the same SnapLock type available.
• The destination volume that is created for a mirror relationship is not thin provisioned.
• A maximum of 25 volumes can be protected in one selection.
• You cannot create a mirror relationship between SnapLock volumes if the destination cluster is running a version of ONTAP that is older than the ONTAP version that the source cluster is running.

Steps
1. Click Protection > Volume Relationships.
2. In the Volume 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. Specify the cluster, the SVM, and the source volume.
   If the specified cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the specified cluster is running ONTAP 9.3 or later, permitted SVMs are listed.
6. For FlexVol volumes, specify a volume name suffix.
The volume name suffix is appended to the source volume names to generate the destination volume names.

7. Optional: Click Browse, and then change the mirror policy.

8. Select a schedule for the relationship from the list of existing schedules.

9. Optional: Select Initialize Relationship to initialize the mirror relationship.

10. Enable FabricPool-enabled aggregates, and then select an appropriate tiering policy.

11. Click Create.

Result

If you chose to create a destination volume, a destination volume of type dp is created, with the language attribute set to match the language attribute of the source volume.

A mirror relationship is created between the source volume and the destination volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.

Related information

Data Protection Power Guide

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.

  Note:
  - For some platforms, it is not mandatory for the source cluster to have the SnapVault license or the SnapMirror license enabled if the destination cluster has the SnapVault license or the SnapMirror license, and the Data Protection Optimization (DPO) license enabled.
  - After the DPO license is enabled on the destination cluster, you must refresh the browser of the source cluster to enable the Protect option.

- The source cluster and destination cluster and the source SVM and destination SVM must be in a healthy peer relationship.

- The destination aggregate must have space available.

- 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 a vault policy or accept the default vault policy (named XDPDefault) that is automatically assigned.

- FlexVol volumes must be online and of type read/write.

- The SnapLock aggregate type must be the same.

- A maximum of 25 volumes can be protected in one selection.
• If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must be enabled on the remote cluster.

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 lock-vault relationship only between a non-SnapLock (primary) volume and a SnapLock destination (secondary) volume.

• If encryption is enabled on the source volume and the destination cluster is running a version of ONTAP software earlier than ONTAP 9.3, then encryption is disabled on the destination volume by default.

Steps

1. Click Storage > Volumes.
2. From the drop-down menu in the SVM field, select All SVMs.
3. Select the volumes for which you want to create vault relationships, and then click More Actions > Protect.
   
   The Protect option is available only for a read/write volume.
4. Select the Replication type:

<table>
<thead>
<tr>
<th>If you selected the replication type as...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asynchronous</td>
<td></td>
</tr>
<tr>
<td>a. Optional: If you do not know the replication type and relationship type, click Help me Choose, specify the values, and then click Apply.</td>
<td></td>
</tr>
<tr>
<td>b. Select the relationship type.</td>
<td></td>
</tr>
<tr>
<td>The relationship type can be mirror, vault, or mirror and vault.</td>
<td></td>
</tr>
<tr>
<td>c. Select a cluster and an SVM.</td>
<td></td>
</tr>
<tr>
<td>If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.</td>
<td></td>
</tr>
<tr>
<td>d. Modify the volume name suffix, if required.</td>
<td></td>
</tr>
<tr>
<td>Synchronous</td>
<td></td>
</tr>
<tr>
<td>a. Optional: If you do not know the replication type and relationship type, click Help me Choose, specify the values, and then click Apply.</td>
<td></td>
</tr>
<tr>
<td>b. Select the synchronization policy.</td>
<td></td>
</tr>
<tr>
<td>The synchronization policy can be StrictSync or Sync.</td>
<td></td>
</tr>
<tr>
<td>c. Select a cluster and an SVM.</td>
<td></td>
</tr>
<tr>
<td>If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.</td>
<td></td>
</tr>
<tr>
<td>d. Modify the volume name suffix, if required.</td>
<td></td>
</tr>
</tbody>
</table>
5. Optional: Click 📑, update the protection policy and protection schedule, enable SnapLock properties on the destination volume, select a FabricPool-enabled aggregate, and then initialize the protection relationship.

6. Click Save.

Related information

Data Protection Power Guide

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.
- SnapVault license or SnapMirror license must be enabled on both the source cluster and the destination cluster.
  
  **Note:** For some platforms, it is not mandatory for the source cluster to have the SnapVault license or the SnapMirror license enabled if the destination cluster has the SnapVault license or the SnapMirror license, and DPO license enabled.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination SVM must have space available.
- The source aggregate and the destination aggregate must be 64-bit aggregates.
- A source volume of type read/write (rw) must exist.
- A vault (XDP) policy must exist.
  If a vault policy does not exist, you must create a vault policy or accept the default vault policy (XDPDefault) that is automatically assigned.
- FlexVol volumes must be online and read/write.
- The SnapLock aggregate type must be the same.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which SAML authentication is enabled, password-based authentication must be enabled on the remote cluster.

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.

• A maximum of 25 volumes can be protected in one selection.

Steps
1. Click Protection > Volume 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.
   If the specified cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the specified cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.
6. Enter a volume name suffix.
   The volume name suffix is appended to the source volume names to generate the destination volume names.
7. 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.
8. Optional: Click Browse, and then change the vault policy.
9. Select a schedule for the relationship from the list of existing schedules.
10. Optional: Select Initialize Relationship to initialize the vault relationship.
11. Enable SnapLock aggregates, and then select a SnapLock Compliance aggregate or a SnapLock Enterprise aggregate.
12. Enable FabricPool-enabled aggregates, and then select an appropriate tiering policy.
13. Click Validate to verify whether the selected volumes have matching labels.
14. Click Create.

Result
If you chose to create a destination volume, a volume of type dp is created with the following default settings:

• Autogrow is enabled.
• Deduplication is enabled or disabled according to the user preference or the source volume deduplication setting.
• Compression is disabled.
• The language attribute is set to match the language attribute of the source volume.

A vault relationship is created between the destination volume and the source volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.
Related information

Data Protection Power Guide
Copyright

Copyright © 2019 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).
Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

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., 1395 Crossman Ave., 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 52
access-based enumeration
   See ABE
adding
   export rules 46
   rules to export policies 46
   VLAN interfaces 18
aggregates
   adding capacity disks to 32
   assigning array LUNs to 23
   assigning disks to increase capacity 22
   creating storage pools 34, 38
   Flash Pool, workflow for provisioning cache 36
   mirroring 43
   provisioning cache by adding SSDs 33, 37
   provisioning storage based on storage recommendations 40
   provisioning storage by creating HDD and SSD 41
   provisioning storage by creating manually 40
   workflow for assigning disks to existing 30
   workflow for mirroring data 40
   zeroing spare array LUNs 24
   zeroing spare disks 23
all-share cache
   creating for BranchCache configuration 51
array LUNs
   assigning 23
   erasing data from 24
   formatting 24
   zeroing 24
assigning
   array LUNs 23
   disks to nodes 22
   export policies to qtrees 45

B

BranchCache
   enabling 52
   setting up 51
   workflow for configuring 50
broadcast domains
   creating 19

C

cache
   increasing for Flash Pool aggregates by adding SSDs 38
   provisioning to aggregates by adding SSDs 33, 37
 caching
   configuring BranchCache for 51
capacity disks
   adding to aggregates 32
CIFS
   setting up 50
   workflow for configuring BranchCache 50
CIFS servers
   configuring BranchCache on 51
client access
   adding rules to export policies 46
   creating export policies 46
   creating export policy for 46
   setting up CIFS 50
cluster
   creating manually 11
cluster setup
   prerequisites and workflow for using OnCommand System Manager 8
   setting up a network 12
clusters
   setting up by using the template file 9
comments
   how to send feedback about documentation 78
configuring
   BranchCache 51
continuous availability
   enabling or disabling for shares 52
creating
   a mirror and vault relationship from a destination SVM 56
   a vault relationship from a destination SVM 73
   broadcast domains 19
   cluster
      setting up 11
      cluster manually 11
      export policies 46
      interface groups 18
      qtrees 44
      setting up
         cluster 11
      storage pools 34, 38
      subnets 19

D

Data ONTAP
   workflow for setting up a network 17
dedicated SSDs
   adding to Flash Pool aggregates 38
disks
   assigning to nodes 22
   erasing data from 23
   formatting 23
   increasing the size of aggregates by adding 32
   mirroring aggregates 43
   zeroing 23
documentation
   how to receive automatic notification of changes to 78
   how to send feedback about 78
domains
   creating broadcast 19
E
editing
share settings 52
shares, workflow to enable BranchCache 50
encrypt data
while accessing this share 52
export policies
adding export rules to 46
adding rules 46
assigning to qtrees 45
creating 46
workflow for assigning to qtrees 44
export rules
adding to export policies 46
exporting
qtrees 45
Express Guides
System Manager workflows in 5

F
FabricPool-enabled aggregates
provisioning storage by creating 40
feedback
how to send comments about documentation 78
Flash Pool aggregates
creating manually 42
creating storage pools 34, 38
increasing the size by adding SSDs 38
provisioning storage by creating 40, 42
workflow for provisioning cache 36
FlexGroup volumes
creating 25
managing workflow 25
resizing 28
flowcharts
Service Processor configuration workflow 48
setting up a network 17
setting up the BranchCache configuration 50
workflow for assigning array LUNs to nodes 22
workflow for assigning disks to existing aggregates 30
workflow for assigning disks to nodes 22
workflow for assigning export policies to qtrees 44
workflow for mirroring aggregates 40
workflow for protecting data using mirror and vault relationship 54
workflow for provisioning SSD cache 36

H
hash stores
specifying path and maximum size for BranchCache configuration 51
HDD aggregates
converting existing aggregate to a Flash Pool aggregate 42
creating manually 41
HDDs and SSDs
adding to aggregates 32

I
ifgroups
See interface groups
information
how to send feedback about improving documentation 78
interface groups
creating 18
IP address disabled
setting up a network 13
IP address range enabled
using for setting up a network 12
IP addresses
assigning to multiple Service Processors 48
editing for a Service Processor 49

L
licenses
adding 60
LIFs
creating to access data from SVMs 19
LUNs, array
assigning 23

M
MetroCluster configurations
adding licenses 60
mirror and vault
creating a relationship from a source volume 54
mirror and vault relationship
creating from a destination SVM 56
mirror and vault relationships
creating from a source volume 54
workflow for protecting data 54
workflow for providing data protection 54
mirror relationships
creating from a destination SVM 69
creating from a source SVM 67
mirroring aggregates
workflow for providing data resiliency 40
mirrors
creating relationships from source SVM 67
modifying
share settings 52

N
network
creating broadcast domains 19
creating subnets 19
creating VLAN interfaces 18
setup workflow 17
network interfaces
creating to access data from SVMs 19
creating VLANS 18
network masks
editing for a Service Processor 49
networks
setting up to manage clusters, nodes, Service Processors
nodes
assigning disks
workflow for assigning array LUNs to
workflow for assigning disks to
non-root aggregates
adding capacity disks to
OnCommand System Manager
prerequisites and workflow for setting up a cluster using
ONTAP System Manager
creating a cluster
setting up a cluster
oplocks
enabling
per-share cache
creating for BranchCache configuration
policies
assigning export, to qtrees
prerequisites
for setting up a cluster using OnCommand System Manager
qtrees
assigning an export policy to
creating
exporting
workflow for assigning export policies
relationships
mirror and vault, creating from a destination SVM
vault, creating from a destination SVM
reviewing
storage recommendations
root aggregates
adding capacity disks to
server keys
specifying for BranchCache configuration
Service Processors
assigning IP addresses globally
configuration workflow
editing the settings for
setting up
BranchCache
CIFS
setting up a cluster
using ONTAP System Manager in your data center
setting up a network
by using ONTAP System Manager
for managing cluster, nodes, Services Processors
when the IP address range is disabled
when the IP address range is enabled
setting up a support page
cluster setup
using ONTAP System Manager
shares
editing permissions and options
SMB
configuring BranchCache on
SMB encryption
setting up
SnapLock aggregates
provisioning storage by creating
SnapLock Compliance aggregates
creating manually
provisioning storage by manually creating
SnapLock Compliance volumes
creating
SnapLock Enterprise aggregates
creating manually
provisioning storage by manually creating
SnapLock Enterprise volumes
creating
SnapLock for SnapMirror
workflow
SnapLock for SnapVault
workflow
SnapMirror
workflow
SnapVault
workflow
software licenses
adding
spare array LUNs
zeroing
spare disks
zeroing
SSD aggregates
creating manually
SSDs
adding to HDDs for converting to Flash Pool
aggregates
combining to create storage pools
dedicated SSDs
increasing the size of Flash Pool aggregates by adding
provisioning cache by adding
storage pools
workflow for provisioning cache
storage
provisioning by creating aggregates manually
storage pools
adding SSDs as
assigning disks to increase capacity
creating
storage provisioning
by creating Flash Pool aggregates
by creating HDD aggregates and SSD aggregates manually 
manually creating SnapLock aggregates 
manually creating SnapLock Compliance aggregates 
manually creating SnapLock Enterprise aggregates 
storage recommendations 
provisioning storage by creating aggregates 
reviewing 
subnets 
creating 
suggestions 
how to send feedback about documentation 
SVMs 
creating for serving data 
creating mirror relationships from destination or source 
creating network interfaces of LIFs to access 
creating vault relationships from destination 
creating vault relationships from source or destination 
setting up BranchCache on 
symbolic links 
editing the settings of 
System Manager 
creating FlexGroup volumes with 
System Manager workflows 
in the release 
T 
template files using to step up a cluster 
Twitter 
how to receive automatic notification of documentation changes 
U 
unowned disks 
assigning ownership 
V 
vault relationships 
creating from a source SVM 
vaults 
creating a relationship from a destination SVM 
creating a relationship from a source SVM 
VLAN interfaces 
creating 
volumes 
creating an export policy for client access to 
creating qtrees 
mounting 
W 
workflow 
managing FlexGroup volumes 
resizing FlexGroup 
workflows 
assigning array LUNs to existing aggregates 
assigning disks to existing aggregates 
cluster setup using OnCommand System Manager 
configuring a Service Processor 
creating SnapLock for SnapMirror relationships 
creating SnapLock for SnapVault relationships 
in System Manager 
providing data access to qtrees by using export policies 
providing data protection by creating mirror and vault relationships 
providing data resiliency by mirroring aggregates 
provisioning SSD cache through Flash pool aggregates 
setting up a network 
setting up the BranchCache configuration 
Z 
zeroing 
array LUNs 
disks