Configure the SnapCenter Server

SnapCenter software

NetApp
January 09, 2026

Table of Contents

Configure the SnapCenter Server

Add and provision the storage system

Add storage systems

You should set up the storage system that gives SnapCenter access to ONTAP storage, ASA r2 systems, or Amazon FSx for NetApp ONTAP to perform data protection and provisioning operations.

You can either add a stand-alone SVM or a cluster comprising of multiple SVMs. If you are using Amazon FSx for NetApp ONTAP, you can either add FSx admin LIF comprising of multiple SVMs using fsxadmin account or add FSx SVM in SnapCenter.

Before you begin

- You should have the required permissions in the Infrastructure Admin role to create storage connections.
- You should ensure that the plug-in installations are not in progress.

  Host plug-in installations must not be in progress while adding a storage system connection because the host cache might not be updated and databases status might be displayed in the SnapCenter GUI as “Not available for backup” or “Not on NetApp storage”.

- Storage system names should be unique.

  SnapCenter does not support multiple storage systems with the same name on different clusters. Each storage system that is supported by SnapCenter should have a unique name and a unique data LIF IP address.

About this task

- When you configure storage systems, you can also enable Event Management System (EMS) & AutoSupport features. The AutoSupport tool collects data about the health of your system and automatically sends the data to NetApp technical support, enabling them to troubleshoot your system.

  If you enable these features, SnapCenter sends AutoSupport information to the storage system and EMS messages to the storage system syslog when a resource is protected, a restore or clone operation finishes successfully, or an operation fails.

- If you are planning to replicate Snapshots to a SnapMirror destination or SnapVault destination, you must set up storage system connections for the destination SVM or Cluster as well as the source SVM or Cluster.

If you change the storage system password, scheduled jobs, on demand backup, and restore operations might fail. After you change the storage system password, you can update the password by clicking **Modify** in the Storage tab.

Steps

1. In the left navigation pane, click **Storage Systems**.
2. In the Storage Systems page, click **New**.

3. In the Add Storage System page, provide the following information:

For this field…	Do this…
Storage System	Enter the storage system name or IP address. Storage system names, not including the domain name, must have 15 or fewer characters, and the names must be resolvable. To create storage system connections with names that have more than 15 characters, you can use the Add-SmStorageConnectionPowerShell cmdlet. For storage systems with MetroCluster configuration (MCC), it is recommended to register both local and peer clusters for non-disruptive operations. SnapCenter does not support multiple SVMs with the same name on different clusters. Each SVM that is supported by SnapCenter must have a unique name. After adding the storage connection to SnapCenter, you should not rename the SVM or the Cluster using ONTAP. If SVM is added with a short name or FQDN then it has to be resolvable from both the SnapCenter and the plug-in host.
User name/Password	Enter the credentials of the storage user that has the required privileges to access the storage system.

For this field…	Do this…
Event Management System (EMS) & AutoSupport Settings	If you want to send EMS messages to the storage system syslog or if you want to have AutoSupport messages sent to the storage system for applied protection, completed restore operations, or failed operations, select the appropriate checkbox. When you select the **Send AutoSupport Notification for failed operations to storage system** checkbox, the **Log SnapCenter Server events to syslog** checkbox is also selected because EMS messaging is required to enable AutoSupport notifications.

4. Click **More Options** if you want to modify the default values assigned to platform, protocol, port, and timeout.
   a. In Platform, select one of the options from the drop-down list.

      If the SVM is the secondary storage system in a backup relationship, select the **Secondary** checkbox. When the **Secondary** option is selected, SnapCenter does not perform a license check immediately.

      If you have added SVM in SnapCenter then, user need to select the platform type from the dropdown manually.

   b. In Protocol, select the protocol that was configured during SVM or Cluster setup, typically HTTPS.
   c. Enter the port that the storage system accepts.

      The default port 443 typically works.

   d. Enter the time in seconds that should elapse before communication attempts are halted.

      The default value is 60 seconds.

   e. If the SVM has multiple management interfaces, select the **Preferred IP** checkbox, and then enter the preferred IP address for SVM connections.
   f. Click **Save**.
5. Click **Submit**.

Result

In the Storage Systems page, from the **Type** drop-down perform one of the following actions:

- Select **ONTAP SVMs** if you want to view all the SVMs that were added.

  If you have added FSx SVMs, the FSx SVMs are listed here.

- Select **ONTAP Clusters** if you want to view all the clusters that were added.

  If you have added FSx clusters using fsxadmin, the FSx clusters are listed here.

  When you click on the cluster name, all the SVMs that are part of the cluster are displayed in the Storage Virtual Machines section.

If a new SVM is added to the ONTAP cluster using ONTAP GUI, click **Rediscover** to view the newly added SVM.

After you finish

A cluster administrator must enable AutoSupport on each storage system node to send email notifications from all storage systems to which SnapCenter has access, by running the following command from the storage system command line:

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
-to enable -noteto enable
```

The Storage Virtual Machine (SVM) administrator has no access to AutoSupport.

Storage connections and credentials

Before performing data protection operations, you should set up the storage connections and add the credentials that the SnapCenter Server and the SnapCenter plug-ins will use.

Storage connections

The storage connections give the SnapCenter Server and SnapCenter plug-ins access to the ONTAP storage. Setting up these connections also involves configuring AutoSupport and Event Management System (EMS) features.

Credentials

- Domain administrator or any member of the administrator group

  Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the Username field are:

  - *NetBIOS\UserName*
  - *Domain FQDN\UserName*
  - *UserName@upn*
- Local administrator (for workgroups only)

  For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system.

  The valid format for the Username field is: *UserName*
- Credentials for individual resource groups

  If you set up credentials for individual resource groups and the username does not have full admin privileges, you must assign at least the resource group and backup privileges to the username.

Provision storage on Windows hosts

Create and manage igroups

You create initiator groups (igroups) to specify which hosts can access a given LUN on the storage system. You can use SnapCenter to create, rename, modify, or delete an igroup on a Windows host.

Create an igroup

You can use SnapCenter to create an igroup on a Windows host. The igroup will be available in the Create Disk or Connect Disk wizard when you map the igroup to a LUN.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Igroup**.
3. In the Initiator Groups page, click **New**.
4. In the Create Igroup dialog box, define the igroup:

In this field…	Do this…
Storage System	Select the SVM for the LUN you will map to the igroup.
Host	Select the host on which you want to create the igroup.
Igroup Name	Enter the name of the igroup.
Initiators	Select the initiator.
Type	Select the initiator type, iSCSI, FCP, or mixed (FCP and iSCSI).

5. When you are satisfied with your entries, click **OK**.

   SnapCenter creates the igroup on the storage system.

Rename an igroup

You can use SnapCenter to rename an existing igroup.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Igroup**.
3. In the Initiator Groups page, click in the **Storage Virtual Machine** field to display a list of available SVMs, and then select the SVM for the igroup you want to rename.

4. In the list of igroups for the SVM, select the igroup you want to rename and click **Rename**.
5. In the Rename igroup dialog box, enter the new name for the igroup and click **Rename**.

Modify an igroup

You can use SnapCenter to add igroup initiators to an existing igroup. While creating an igroup you can add only one host. If you want to create an igroup for a cluster, you can modify the igroup to add other nodes to that igroup.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Igroup**.
3. In the Initiator Groups page, click in the **Storage Virtual Machine** field to display a drop-down list of available SVMs, then select the SVM for the igroup you want to modify.
4. In the list of igroups, select an igroup and click **Add Initiator to igroup**.
5. Select a host.
6. Select the initiators and click **OK**.

Delete an igroup

You can use SnapCenter to delete an igroup when you no longer need it.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Igroup**.
3. In the Initiator Groups page, click in the **Storage Virtual Machine** field to display a drop-down list of available SVMs, then select the SVM for the igroup you want to delete.
4. In the list of igroups for the SVM, select the igroup you want to delete and click **Delete**.
5. In the Delete igroup dialog box, click **OK**.

   SnapCenter deletes the igroup.

Create and manage disks

The Windows host sees LUNs on your storage system as virtual disks. You can use SnapCenter to create and configure an FC-connected or iSCSI-connected LUN.

- SnapCenter supports only basic disks. The dynamic disks are not supported.
- For GPT only one data partition and for MBR one primary partition is allowed that has one volume formatted with NTFS or CSVFS and has one mount path.
- Supported partition styles: GPT, MBR; in a VMware UEFI VM, only iSCSI disks are supported

SnapCenter does not support renaming a disk. If a disk that is managed by SnapCenter is renamed, SnapCenter operations will not succeed.

View the disks on a host

You can view the disks on each Windows host you manage with SnapCenter.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Disks**.
3. Select the host from the **Host** drop-down list.

   The disks are listed.

View clustered disks

You can view clustered disks on the cluster that you manage with SnapCenter. The clustered disks are displayed only when you select the cluster from the Hosts drop-down.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Disks**.
3. Select the cluster from the **Host** drop-down list.

   The disks are listed.

Establish an iSCSI session

If you are using iSCSI to connect to a LUN, you must establish an iSCSI session before you create the LUN to enable communication.

Before you begin

- You must have defined the storage system node as an iSCSI target.
- You must have started the iSCSI service on the storage system. Learn more

About this task

You can establish an iSCSI session only between the same IP versions, either from IPv6 to IPv6, or from IPv4 to IPv4.

You can use a link-local IPv6 address for iSCSI session management and for communication between a host and a target only when both are in the same subnet.

If you change the name of an iSCSI initiator, access to iSCSI targets is affected. After changing the name, you might require to reconfigure the targets accessed by the initiator so that they can recognize the new name. You must ensure to restart the host after changing the name of an iSCSI initiator.

If your host has more than one iSCSI interface, once you have established an iSCSI session to SnapCenter using an IP address on the first interface, you cannot establish an iSCSI session from another interface with a different IP address.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **iSCSI Session**.
3. From the **Storage Virtual Machine** drop-down list, select the storage virtual machine (SVM) for the iSCSI target.
4. From the **Host** drop-down list, select the host for the session.
5. Click **Establish Session**.

   The Establish Session wizard is displayed.

6. In the Establish Session wizard, identify the target:

In this field…	Enter…
Target node name	The node name of the iSCSI target If there is an existing target node name, the name is displayed in read-only format.
Target portal address	The IP address of the target network portal
Target portal port	The TCP port of the target network portal
Initiator portal address	The IP address of the initiator network portal

7. When you are satisfied with your entries, click **Connect**.

   SnapCenter establishes the iSCSI session.

8. Repeat this procedure to establish a session for each target.

Create FC-connected or iSCSI-connected LUNs or disks

The Windows host sees the LUNs on your storage system as virtual disks. You can use SnapCenter to create and configure an FC-connected or iSCSI-connected LUN.

If you want to create and format disks outside of SnapCenter, only NTFS and CSVFS file systems are supported.

Before you begin

- You must have created a volume for the LUN on your storage system.

  The volume should hold LUNs only, and only LUNs created with SnapCenter.

  > ⓘ You cannot create a LUN on a SnapCenter-created clone volume unless the clone has already been split.

- You must have started the FC or iSCSI service on the storage system.
- If you are using iSCSI, you must have established an iSCSI session with the storage system.
- The SnapCenter Plug-ins Package for Windows must be installed only on the host on which you are

creating the disk.

About this task

- You cannot connect a LUN to more than one host unless the LUN is shared by hosts in a Windows Server failover cluster.
- If a LUN is shared by hosts in a Windows Server failover cluster that uses CSV (Cluster Shared Volumes), you must create the disk on the host that owns the cluster group.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Disks**.
3. Select the host from the **Host** drop-down list.
4. Click **New**.

   The Create Disk wizard opens.

5. In the LUN Name page, identify the LUN:

In this field…	Do this…
Storage System	Select the SVM for the LUN.
LUN path	Click **Browse** to select the full path of the folder containing the LUN.
LUN name	Enter the name of the LUN.
Cluster size	Select the LUN block allocation size for the cluster. Cluster size depends upon the operating system and applications.
LUN label	Optionally, enter descriptive text for the LUN.

6. In the Disk Type page, select the disk type:

Select…	If…
Dedicated disk	The LUN can be accessed by only one host. Ignore the **Resource Group** field.
Shared disk	The LUN is shared by hosts in a Windows Server failover cluster. Enter the name of the cluster resource group in the **Resource Group** field. You need to create the disk on only one host in the failover cluster.

Select…	If…
Cluster Shared Volume (CSV)	The LUN is shared by hosts in a Windows Server failover cluster that uses CSV. Enter the name of the cluster resource group in the **Resource Group** field. Make sure that the host on which you are creating the disk is the owner of the cluster group.

7. In the Drive Properties page, specify the drive properties:

Property	Description
Auto assign mount point	SnapCenter automatically assigns a volume mount point based on the system drive. For example, if your system drive is C:, auto assign creates a volume mount point under your C: drive (C:\scmnpt\). Auto assign is not supported for shared disks.
Assign drive letter	Mount the disk to the drive you select in the adjacent drop-down list.
Use volume mount point	Mount the disk to the drive path you specify in the adjacent field. The root of the volume mount point must be owned by the host on which you are creating the disk.
Do not assign drive letter or volume mount point	Choose this option if you prefer to mount the disk manually in Windows.
LUN size	Specify the LUN size; 150 MB minimum. Select MB, GB, or TB in the adjoining drop-down list.
Use thin provisioning for the volume hosting this LUN	Thin provision the LUN. Thin provisioning allocates only as much storage space as is needed at one time, allowing the LUN to grow efficiently to the maximum available capacity. Make sure there is enough space available on the volume to accommodate all the LUN storage you think you will need.

Property	Description
Choose partition type	Select GPT partition for a GUID Partition Table, or MBR partition for a Master Boot Record. MBR partitions might cause misalignment issues in Windows Server failover clusters. Unified extensible firmware interface (UEFI) partition disks are not supported.

8. In the Map LUN page, select the iSCSI or FC initiator on the host:

In this field…	Do this…
Host	Double-click the cluster group name to display a drop-down list that shows the hosts that belong to the cluster, and then select the host for the initiator. This field is displayed only if the LUN is shared by hosts in a Windows Server failover cluster.
Choose host initiator	Select **Fibre Channel** or **iSCSI**, and then select the initiator on the host. You can select multiple FC initiators if you are using FC with multipath I/O (MPIO).

9. In the Group Type page, specify whether you want to map an existing igroup to the LUN, or create a new igroup:

Select…	If…
Create new igroup for selected initiators	You want to create a new igroup for the selected initiators.
Choose an existing igroup or specify a new igroup for selected initiators	You want to specify an existing igroup for the selected initiators, or create a new igroup with the name you specify. Type the igroup name in the **igroup name** field. Type the first few letters of the existing igroup name to autocomplete the field.

10. In the Summary page, review your selections and then click **Finish**.

    SnapCenter creates the LUN and connects it to the specified drive or drive path on the host.

Resize a disk

You can increase or decrease the size of a disk as your storage system needs change.

About this task

- For thin provisioned LUN, the ONTAP lun geometry size is shown as the maximum size.
- For thick provisioned LUN, the expandable size (available size in the volume) is shown as the maximum size.
- LUNs with MBR-style partitions have a size limit of 2 TB.
- LUNs with GPT-style partitions have a storage system size limit of 16 TB.
- It is a good idea to make a Snapshot before resizing a LUN.
- If you need to restore a LUN from a Snapshot made before the LUN was resized, SnapCenter automatically resizes the LUN to the size of the Snapshot.

  After the restore operation, data added to the LUN after it was resized must be restored from a Snapshot made after it was resized.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Disks**.
3. Select the host from the Host drop-down list.

   The disks are listed.

4. Select the disk you want to resize and then click **Resize**.
5. In the Resize Disk dialog box, use the slider tool to specify the new size of the disk, or enter the new size in the Size field.

   If you enter the size manually, you need to click outside the Size field before the Shrink or Expand button is enabled appropriately. Also, you must click MB, GB, or TB to specify the unit of measurement.

6. When you are satisfied with your entries, click **Shrink** or **Expand**, as appropriate.

   SnapCenter resizes the disk.

Connect a disk

You can use the Connect Disk wizard to connect an existing LUN to a host, or to reconnect a LUN that has been disconnected.

Before you begin

- You must have started the FC or iSCSI service on the storage system.
- If you are using iSCSI, you must have established an iSCSI session with the storage system.
- You cannot connect a LUN to more than one host unless the LUN is shared by hosts in a Windows Server failover cluster.

- If the LUN is shared by hosts in a Windows Server failover cluster that uses CSV (Cluster Shared Volumes), then you must connect the disk on the host that owns the cluster group.
- The Plug-in for Windows needs to be installed only on the host on which you are connecting the disk.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Disks**.
3. Select the host from the **Host** drop-down list.
4. Click **Connect**.

   The Connect Disk wizard opens.

5. In the LUN Name page, identify the LUN to connect to:

In this field…	Do this…
Storage System	Select the SVM for the LUN.
LUN path	Click **Browse** to select the full path of the volume containing the LUN.
LUN name	Enter the name of the LUN.
Cluster size	Select the LUN block allocation size for the cluster. Cluster size depends upon the operating system and applications.
LUN label	Optionally, enter descriptive text for the LUN.

6. In the Disk Type page, select the disk type:

Select…	If…
Dedicated disk	The LUN can be accessed by only one host.
Shared disk	The LUN is shared by hosts in a Windows Server failover cluster. You need only connect the disk to one host in the failover cluster.
Cluster Shared Volume (CSV)	The LUN is shared by hosts in a Windows Server failover cluster that uses CSV. Make sure that the host on which you are connecting to the disk is the owner of the cluster group.

7. In the Drive Properties page, specify the drive properties:

Property	Description
Auto assign	Let SnapCenter automatically assign a volume mount point based on the system drive. For example, if your system drive is C:, the auto assign property creates a volume mount point under your C: drive (C:\scmnpt\). The auto assign property is not supported for shared disks.
Assign drive letter	Mount the disk to the drive you select in the adjoining drop-down list.
Use volume mount point	Mount the disk to the drive path you specify in the adjoining field. The root of the volume mount point must be owned by the host on which you are creating the disk.
Do not assign drive letter or volume mount point	Choose this option if you prefer to mount the disk manually in Windows.

8. In the Map LUN page, select the iSCSI or FC initiator on the host:

In this field…	Do this…
Host	Double-click the cluster group name to display a drop-down list that shows the hosts that belong to the cluster, then select the host for the initiator. This field is displayed only if the LUN is shared by hosts in a Windows Server failover cluster.
Choose host initiator	Select **Fibre Channel** or **iSCSI**, and then select the initiator on the host. You can select multiple FC initiators if you are using FC with MPIO.

9. In the Group Type page, specify whether you want to map an existing igroup to the LUN or create a new igroup:

Select…	If…
Create new igroup for selected initiators	You want to create a new igroup for the selected initiators.

Select…	If…
Choose an existing igroup or specify a new igroup for selected initiators	You want to specify an existing igroup for the selected initiators, or create a new igroup with the name you specify. Type the igroup name in the **igroup name** field. Type the first few letters of the existing igroup name to automatically complete the field.

10. In the Summary page, review your selections and click **Finish**.

    SnapCenter connects the LUN to the specified drive or drive path on the host.

Disconnect a disk

You can disconnect a LUN from a host without affecting the contents of the LUN, with one exception: If you disconnect a clone before it has been split off, you lose the contents of the clone.

Before you begin

- Make sure that the LUN is not in use by any application.
- Make sure that the LUN is not being monitored with monitoring software.
- If the LUN is shared, make sure to remove the cluster resource dependencies from the LUN and verify that all nodes in the cluster are powered on, functioning properly, and available to SnapCenter.

About this task

If you disconnect a LUN in a FlexClone volume that SnapCenter has created and no other LUNs on the volume are connected, SnapCenter deletes the volume. Before disconnecting the LUN, SnapCenter displays a message warning you that the FlexClone volume might be deleted.

To avoid automatic deletion of the FlexClone volume, you should rename the volume before disconnecting the last LUN. When you rename the volume, make sure that you change multiple characters than just the last character in the name.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Disks**.
3. Select the host from the **Host** drop-down list.

   The disks are listed.

4. Select the disk you want to disconnect, and then click **Disconnect**.
5. In the Disconnect Disk dialog box, click **OK**.

   SnapCenter disconnects the disk.

Delete a disk

You can delete a disk when you no longer need it. After you delete a disk, you cannot undelete it.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Disks**.
3. Select the host from the **Host** drop-down list.

   The disks are listed.
4. Select the disk you want to delete, and then click **Delete**.
5. In the Delete Disk dialog box, click **OK**.

   SnapCenter deletes the disk.

Create and manage SMB shares

To configure an SMB3 share on a storage virtual machine (SVM), you can use either the SnapCenter user interface or PowerShell cmdlets.

Best Practice: Using the cmdlets is recommended because it enables you to take advantage of templates provided with SnapCenter to automate share configuration.

The templates encapsulate best practices for volume and share configuration. You can find the templates in the Templates folder in the installation folder for the SnapCenter Plug-ins Package for Windows.

If you feel comfortable doing so, you can create your own templates following the models provided. You should review the parameters in the cmdlet documentation before creating a custom template.

Create an SMB share

You can use the SnapCenter Shares page to create an SMB3 share on a storage virtual machine (SVM).

You cannot use SnapCenter to back up databases on SMB shares. SMB support is limited to provisioning only.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Shares**.
3. Select the SVM from the **Storage Virtual Machine** drop-down list.
4. Click **New**.

   The New Share dialog opens.
5. In the New Share dialog, define the share:

In this field…	Do this…
Description	Enter descriptive text for the share.
Share name	Enter the share name, for example, test_share. The name you enter for the share will also be used as the volume name. The share name: • Must be a UTF-8 string. • Must not include the following characters: control characters from 0x00 to 0x1F (both inclusive), 0x22 (double quotes), and the special characters `\ / [ ] : (vertical bar) < > + = ; , ?`
Share path	• Click in the field to enter a new file system path, for example, /. • Double-click in the field to select from a list of existing file system paths.

6. When you are satisfied with your entries, click **OK**.

   SnapCenter creates the SMB share on the SVM.

Delete an SMB share

You can delete an SMB share when you no longer need it.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Shares**.
3. In the Shares page, click in the **Storage Virtual Machine** field to display a drop-down with a list of available storage virtual machines (SVMs), then select the SVM for the share you want to delete.
4. From the list of shares on the SVM, select the share you want to delete and click **Delete**.
5. In the Delete Share dialog box, click **OK**.

   SnapCenter deletes the SMB share from the SVM.

Reclaim space on the storage system

Although NTFS tracks the available space on a LUN when files are deleted or modified, it does not report the new information to the storage system. You can run the space reclamation PowerShell cmdlet on the Plug-in for Windows host to ensure that newly freed blocks are marked as available in storage.

If you are running the cmdlet on a remote plug-in host, you must have run the SnapCenterOpen-SMConnection cmdlet to open a connection to the SnapCenter Server.

Before you begin

- You must ensure that the space reclamation process has completed before performing a restore operation.
- If the LUN is shared by hosts in a Windows Server failover cluster, you must perform space reclamation on the host that owns the cluster group.
- For optimum storage performance, you should perform space reclamation as often as possible.

  You should ensure that the entire NTFS file system has been scanned.

About this task

- Space reclamation is time-consuming and CPU-intensive, so it is usually best to run the operation when storage system and Windows host usage is low.
- Space reclamation reclaims nearly all available space, but not 100 percent.
- You should not run disk defragmentation at the same time as you are performing space reclamation.

  Doing so can slow the reclamation process.

Step

From the application server PowerShell command prompt, enter the following command:

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_path is the drive path mapped to the LUN.

Provision storage using PowerShell cmdlets

If you do not want to use the SnapCenter GUI to perform host provisioning and space reclamation jobs, you can use the PowerShell cmdlets. You can use cmdlets directly or add them to scripts.

If you are running the cmdlets on a remote plug-in host, you must run the SnapCenter Open-SMConnection cmdlet to open a connection to the SnapCenter Server.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

If SnapCenter PowerShell cmdlets are broken due to removal of SnapDrive for Windows from the server, refer to SnapCenter cmdlets broken when SnapDrive for Windows is uninstalled.

Provision storage in VMware environments

You can use the SnapCenter Plug-in for Microsoft Windows in VMware environments to create and manage LUNs and manage Snapshots.

Supported VMware guest OS platforms

- Supported versions of Windows Server
- Microsoft cluster configurations

  Support for up to a maximum of 16 nodes supported on VMware when using the Microsoft iSCSI Software Initiator, or up to two nodes using FC

- RDM LUNs

  Support for a maximum of 56 RDM LUNs with four LSI Logic SCSI controllers for normal RDMS, or 42 RDM LUNs with three LSI Logic SCSI controllers on a VMware VM MSCS box-to-box Plug-in for Windows configuration

  Supports VMware ParaVirtual SCSI Controller. 256 disks can be supported on RDM disks.

VMware ESXi server-related limitations

- Installing the Plug-in for Windows on a Microsoft cluster on virtual machines using ESXi credentials is not supported.

  You should use your vCenter credentials when installing the Plug-in for Windows on clustered virtual machines.

- All clustered nodes must use the same target ID (on the virtual SCSI adapter) for the same clustered disk.
- When you create an RDM LUN outside of the Plug-in for Windows, you must restart the plug-in service to enable it to recognize the newly created disk.
- You cannot use iSCSI and FC initiators at the same time on a VMware guest OS.

Minimum vCenter privileges required for SnapCenter RDM operations

You should have the following vCenter privileges on the host to perform RDM operations in a guest OS:

- Datastore: Remove File
- Host: Configuration > Storage Partition Configuration
- Virtual Machine: Configuration

You must assign these privileges to a role at the Virtual Center Server level. The role to which you assign these privileges cannot be assigned to any user without root privileges.

After you assign these privileges, you can install the Plug-in for Windows on the guest OS.

Manage FC RDM LUNs in a Microsoft cluster

You can use the Plug-in for Windows to manage a Microsoft cluster using FC RDM LUNs, but you must first create the shared RDM quorum and shared storage outside the plug-in, and then add the disks to the virtual machines in the cluster.

Starting with ESXi 5.5, you can also use ESX iSCSI and FCoE hardware to manage a Microsoft cluster. The Plug-in for Windows includes out-of-box support for Microsoft clusters.

Requirements

The Plug-in for Windows provides support for Microsoft clusters using FC RDM LUNs on two different virtual machines that belong to two different ESX or ESXi servers, also known as cluster across boxes, when you meet specific configuration requirements.

- The virtual machines (VMs) must be running the same Windows Server version.
- ESX or ESXi server versions must be the same for each VMware parent host.
- Each parent host must have at least two network adapters.
- There must be at least one VMware Virtual Machine File System (VMFS) datastore shared between the two ESX or ESXi servers.
- VMware recommends that the shared datastore be created on an FC SAN.

  If necessary, the shared datastore can also be created over iSCSI.

- The shared RDM LUN must be in physical compatibility mode.
- The shared RDM LUN must be created manually outside of the Plug-in for Windows.

  You cannot use virtual disks for shared storage.

- A SCSI controller must be configured on each virtual machine in the cluster in physical compatibility mode:

  Windows Server 2008 R2 requires you to configure the LSI Logic SAS SCSI controller on each virtual machine. Shared LUNs cannot use the existing LSI Logic SAS controller if only one of its type exists and it is already attached to the C: drive.

  SCSI controllers of type paravirtual are not supported on VMware Microsoft clusters.

  When you add a SCSI controller to a shared LUN on a virtual machine in physical compatibility mode, you must select the **Raw Device Mappings** (RDM) option and not the **Create a new disk** option in the VMware Infrastructure Client.

- Microsoft virtual machine clusters cannot be part of a VMware cluster.
- You must use vCenter credentials and not ESX or ESXi credentials when you install the Plug-in for Windows on virtual machines that belongs to a Microsoft cluster.
- The Plug-in for Windows cannot create a single igroup with initiators from multiple hosts.

  The igroup containing the initiators from all ESXi hosts must be created on the storage controller prior to creating the RDM LUNs that will be used as shared cluster disks.

- Ensure that you create an RDM LUN on ESXi 5.0 using an FC initiator.

  When you create an RDM LUN, an initiator group is created with ALUA.

Limitations

The Plug-in for Windows supports Microsoft clusters using FC/iSCSI RDM LUNs on different virtual machines belonging to different ESX or ESXi servers.

This feature is not supported in releases before ESX 5.5i.

- The Plug-in for Windows does not support clusters on ESX iSCSI and NFS datastores.
- The Plug-in for Windows does not support mixed initiators in a cluster environment.

  Initiators must be either FC or Microsoft iSCSI, but not both.

- ESX iSCSI initiators and HBAs are not supported on shared disks in a Microsoft cluster.
- The Plug-in for Windows does not support virtual machine migration with vMotion if the virtual machine is part of a Microsoft cluster.
- The Plug-in for Windows does not support MPIO on virtual machines in a Microsoft cluster.

Create a shared FC RDM LUN

Before you can use FC RDM LUNs to share storage between nodes in a Microsoft cluster, you must first create the shared quorum disk and shared storage disk, and then add them to both virtual machines in the cluster.

The shared disk is not created using the Plug-in for Windows. You should create and then add the shared LUN to each virtual machine in the cluster. For information, see Cluster Virtual Machines Across Physical Hosts.

Add SnapCenter Standard controller-based licenses

A SnapCenter Standard controller-based license is required if you are using FAS, AFF, or ASA storage controllers.

The controller-based license has the following characteristics:

- SnapCenter Standard entitlement included with purchase of Premium or Flash Bundle (not with the base pack)
- Unlimited storage usage
- Added directly to the FAS, AFF, or ASA storage controller by using either ONTAP System Manager or the ONTAP CLI.

  You do not enter any license information in the SnapCenter user interface for the SnapCenter controller-based licenses.

- Locked to the controller's serial number

For information on the licenses required, see SnapCenter licenses.

Step 1: Verify if the SnapManager Suite license is installed

You can use the SnapCenter user interface to check if a SnapManager Suite license is installed on FAS, AFF, or ASA primary storage systems and identify which systems that need licenses. SnapManager Suite licenses apply only to FAS, AFF, and ASA SVMs or clusters on primary storage systems.

If you already have a SnapManager Suite license on your controller, SnapCenter automatically provides the Standard controller-based license entitlement. The names SnapManagerSuite license and SnapCenter Standard controller-based license are used interchangeably, but they refer to the same license.

Steps

1. In the left navigation pane, select **Storage Systems**.
2. In the Storage Systems page, from the **Type** drop-down, select whether to view all the SVMs or clusters that were added:
   - To view all of the SVMs that were added, select **ONTAP SVMs**.
   - To view all of the clusters that were added, select **ONTAP Clusters**.

     When you select the cluster name, all of the SVMs that are part of the cluster are displayed in the Storage Virtual Machines section.
3. In the Storage Connections list, locate the Controller License column.

   The Controller License column displays the following status:

   -  indicates that a SnapManager Suite license is installed on a FAS, AFF, or ASA primary storage system.
   -  indicates that a SnapManager Suite license is not installed on a FAS, AFF, or ASA primary storage system.
   - Not applicable indicates that a SnapManager Suite license is not applicable because the storage controller is on Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select, or Secondary storage platforms.

Step 2: Identify the licenses installed on the controller

You can use the ONTAP command line to view all the licenses installed on your controller. You should be a cluster administrator on the FAS, AFF, or ASA system.

The controller displays the SnapCenter Standard controller-based license as the SnapManagerSuite license.

Steps

1. Log in to the NetApp controller using the ONTAP command line.
2. Enter the license show command, and then view the output to see if the SnapManagerSuite license is installed.

Example output

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
Base              site     Cluster Base License     -

Serial Number: 1-81-00000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

In the example, the SnapManagerSuite license is installed, therefore, no additional SnapCenter licensing action is required.

Step 3: Retrieve the controller serial number

Get the controller serial number using the ONTAP command line. You must be a cluster administrator on the FAS, AFF, or ASA system to get your controller-based license serial number.

Steps

1. Log in to the controller using the ONTAP command line.
2. Enter the system show -instance command, and then review the output to locate the controller serial number.

Example output

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. Record the serial numbers.

Step 4: Retrieve the serial number of the controller-based license

If you are using FAS, ASA, or AFF storage, you can retrieve the SnapCenter controller-based license from the NetApp Support Site before you install it using the ONTAP command line.

Before you begin

- You should have a valid NetApp Support Site login credentials.

  If you do not enter valid credentials, the system does not return any information for your search.

- You should have the controller serial number.

Steps

1. Log in to the NetApp Support Site.
2. Navigate to **Systems** > **Software Licenses**.
3. In the Selection Criteria area, ensure Serial Number (located on back of unit) is selected, enter the controller serial number, and then select **Go!**.

   A list of licenses for the specified controller is displayed.

4. Locate and record the SnapCenter Standard or SnapManagerSuite license.

Step 5: Add controller-based license

You can use the ONTAP command line to add a SnapCenter controller-based license when you are using FAS, AFF, or ASA systems, and you have a SnapCenter Standard or SnapManagerSuite license.

Before you begin

- You should be a cluster administrator on the FAS, AFF, or ASA system.
- You should have the SnapCenter Standard or SnapManagerSuite license.

About this task

If you want to install SnapCenter on a trial basis with FAS, AFF, or ASA storage, you can obtain a Premium Bundle evaluation license to install on your controller.

If you want to install SnapCenter on a trial basis, you should contact your sales representative to obtain a Premium Bundle evaluation license to install on your controller.

Steps

1. Log in to the NetApp cluster using the ONTAP command line.
2. Add the SnapManagerSuite license key:

   ```
   system license add -license-code license_key
   ```

   This command is available at the admin privilege level.

3. Verify that the SnapManagerSuite license is installed:

   ```
   license show
   ```

Step 6: Remove the trial license

If you are using a controller-based SnapCenter Standard license and need to remove the capacity-based trial license (serial number ending with “50”), you should use MySQL commands to remove the trial license manually. The trial license cannot be deleted using the SnapCenter user interface.

Removing a trial license manually is only required if you are using a SnapCenter Standard controller-based license.

Steps

1. On the SnapCenter Server, open a PowerShell window to reset the MySQL password.
   a. Run the Open-SmConnection cmdlet to establish connection with the SnapCenter Server for a SnapCenterAdmin account.
   b. Run the Set-SmRepositoryPassword to reset the MySQL password.

      For information about the cmdlets, see SnapCenter Software Cmdlet Reference Guide.
2. Open the command prompt and run mysql -u root -p to log into MySQL.

   MySQL prompts you for the password. Enter the credentials you provided while resetting the password.
3. Remove the trial license from the database:

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

Configure High Availability

Configure SnapCenter Servers for High Availability

To support High Availability (HA) in SnapCenter running either on Windows or on Linux, you can install the F5 load balancer. F5 enables the SnapCenter Server to support active-passive configurations in up to two hosts that are in the same location. To use F5 Load Balancer in SnapCenter, you should configure the SnapCenter Servers and configure F5 load balancer.

You can also configure Network Load Balancing (NLB) to set up SnapCenter High Availability. You should manually configure NLB outside of SnapCenter installation for high availability.

For cloud environment, you can configure high availability using either Amazon Web Services (AWS) Elastic Load Balancing (ELB) and Azure load balancer.

Configure high availability using F5

For instruction to configure SnapCenter Servers for high availability using F5 load balancer, refer to How to configure SnapCenter Servers for high availability using F5 Load Balancer.

You must be a member of the Local Administrators group on the SnapCenter Servers (in addition to being assigned to the SnapCenterAdmin role) to use the following cmdlets for adding and removing F5 clusters:

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

  For more information, refer to SnapCenter Software Cmdlet Reference Guide.

Additional information

- After you install and configure SnapCenter for high availability, edit the SnapCenter desktop shortcut to point to the F5 cluster IP.
- If a failover occurs between SnapCenter Servers and if there is also an existing SnapCenter session, you must close the browser and log on to SnapCenter again.
- In load balancer setup (NLB or F5), if you add a host that is partially resolved by the NLB or F5 host and if the SnapCenter host is not able to reach out to this host, then the SnapCenter host page switches between hosts down and running state frequently. To resolve this issue, you should ensure that both the SnapCenter hosts are able to resolve the host in NLB or F5 host.
- SnapCenter commands for MFA settings should be executed on all the hosts. Relying party configuration should be done in the Active Directory Federation Services (AD FS) server using F5 cluster details. The host level SnapCenter UI access will be blocked after MFA is enabled.
- During failover, the audit log settings will not reflect on the second host. Hence, you should manually repeat the audit log settings on F5 passive host when it becomes active.

Configure high availability using Network Load Balancing (NLB)

You can configure Network Load Balancing (NLB) to set up SnapCenter High Availability. You should manually configure NLB outside of SnapCenter installation for high availability.

For information about how to configure Network Load Balancing (NLB) with SnapCenter refer to How to configure NLB with SnapCenter.

Configure high availability using AWS Elastic Load Balancing (ELB)

You can configure high availability SnapCenter environment in Amazon Web Services (AWS) by setting up two SnapCenter servers in separate availability zones (AZs) and configuring them for automatic failover. The architecture includes virtual private IP addresses, routing tables, and synchronization between active and standby MySQL databases.

Steps

1. Configure virtual private overlay IP in AWS. For information, refer to Configure virtual private overlay IP.
2. Prepare your Windows host
   a. Force IPv4 being prioritized above IPv6:
      - Location: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters

- Key: DisabledComponents
- Type: REG_DWORD
- Value: 0x20

b. Ensure that the fully qualified domain names can be resolved via DNS or via local host configuration to the IPv4 addresses.

c. Ensure that you do not have a system proxy configured.

d. Ensure that the administrator password is same on both the Windows Server when using a setup without an Active Directory and the servers are not in one domain.

e. Add virtual IP on both Windows Servers.

3. Create the SnapCenter cluster.

a. Start Powershell and connect to SnapCenter. `Open-SmConnection`

b. Create the cluster. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`

c. Add the secondary server. `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`

d. Get the high availability details. `Get-SmServerConfig`

4. Create the Lamda function to adjust the routing table in case the virtual private IP endpoint becomes unavailable, monitored by AWS CloudWatch. For information, refer to Create a Lambda function.

5. Create a monitor in CloudWatch to monitor the availability of the SnapCenter endpoint. An alarm is configured to trigger a Lambda function if the endpoint is unreachable. The Lambda function adjusts the routing table to redirect traffic to the active SnapCenter server. For information, refer to Create synthetic canaries.

6. Implement workflow using a step function as an alternative to CloudWatch monitoring, providing smaller failover times. The workflow includes a Lambda probe function to test the SnapCenter URL, a DynamoDB table for storing failure counts, and the Step Function itself.

a. Use a lambda function for probing the SnapCenter URL. For information, refer to Create Lambda function.

b. Create a DynamoDB table for storing the failure count between two Step Function iterations. For information, refer to Get started with DynamoDB table.

c. Create the Step Function. For information, refer to Step Function documentation.

d. Test a single step.

e. Test the complete function.

f. Create IAM Role and adjust permissions to be allowed to execute Lambda function.

g. Create schedule to trigger Step Function. For information, refer to Using Amazon EventBridge Scheduler to start a Step Functions.

Configure high availability using Azure load balancer

You can configure high availability SnapCenter environment using Azure load balancer.

Steps

1. Create virtual machines in a scale set using Azure portal. The Azure virtual machine scale set allows you to create and manage a group of load balanced virtual machines. The number of virtual machine

instances can automatically increase or decrease in response to demand or a defined schedule. For information, refer to Create virtual machines in a scale set using Azure portal.

2. After configuring the virtual machines, log into each virtual machine in VM set and install SnapCenter Server in both the nodes.
3. Create the cluster in host 1. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. Add the secondary server. `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. Obtain the high availability details. `Get-SmServerConfig`
6. If required, rebuild the secondary host. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. Failover to the second host. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== Switch from NLB to F5 for high availability

You can change your SnapCenter HA configuration from Network Load Balancing (NLB) to use F5 Load Balancer.

Steps

1. Configure SnapCenter Servers for high availability using F5. Learn more.
2. On the SnapCenter Server host, launch PowerShell.
3. Start a session by using the Open-SmConnection cmdlet, and then enter your credentials.
4. Update the SnapCenter Server to point to the F5 cluster IP address using the Update-SmServerCluster cmdlet.

   The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

High availability for the SnapCenter MySQL repository

MySQL replication is a feature of MySQL Server that enables you to replicate data from one MySQL database server (master) to another MySQL database server (slave). SnapCenter supports MySQL replication for high availability only on two Network Load Balancing-enabled (NLB-enabled) nodes.

SnapCenter performs read or write operations on the master repository and routes its connection to the slave repository when there is a failure on the master repository. The slave repository then becomes the master repository. SnapCenter also supports reverse replication, which is enabled only during failover.

If you want to use the MySQL high availability (HA) feature, you must configure Network Load Balancer (NLB) on the first node. The MySQL repository is installed on this node as part of the installation. While installing SnapCenter on the second node, you must join to the F5 of the first node and create a copy of the MySQL repository on the second node.

SnapCenter provides the *Get-SmRepositoryConfig* and *Set-SmRepositoryConfig* PowerShell cmdlets to manage MySQL replication.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

You must be aware of the limitations related to the MySQL HA feature:

- NLB and MySQL HA are not supported beyond two nodes.
- Switching from a SnapCenter standalone installation to an NLB installation or vice versa and switching from a MySQL standalone setup to MySQL HA are not supported.
- Automatic failover is not supported if the slave repository data is not synchronized with the master repository data.

  You can initiate a forced failover by using the *Set-SmRepositoryConfig* cmdlet.

- When failover is initiated, jobs that are running might fail.

  If failover happens because MySQL Server or SnapCenter Server is down, then any jobs that are running might fail. After failing over to the second node, all subsequent jobs run successfully.

For information about configuring high availability, see How to configure NLB and ARR with SnapCenter.

Configure role-based access control (RBAC)

Create a role

In addition to using the existing SnapCenter roles, you can create your own roles and customize the permissions.

To create your own roles, it is necessary to log in as the "SnapCenterAdmin" role.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Roles**.
3. Click ➕.
4. Specify a name and description for the new role.

   ⓘ Only the following special characters can be used in user names and group names: space ( ), hyphen (-), underscore (_), and colon (:).

5. Select **All members of this role can see other members' objects** to enable other members of the role to see resources such as volumes and hosts after they refresh the resources list.

   You should deselect this option if you do not want members of this role to see objects to which other members are assigned.

   ⓘ When this option is enabled, assigning users access to objects or resources is not required if users belong to the same role as the user who created the objects or resources.

6. In the Permissions page, select the permissions that you want to assign to the role, or click **Select All** to grant all permissions to the role.
7. Click **Submit**.

Add an NetApp ONTAP RBAC role using security login commands

You can use the security login commands to add a NetApp ONTAP RBAC role when your storage systems are running clustered ONTAP.

Before you begin

- Identify the task (or tasks) that you want to perform and the privileges required to perform these tasks.
- Grant privileges to commands and/or command directories.

  There are two levels of access for each command/command directory: all-access and read-only.

  You must always assign the all-access privileges first.

- Assign roles to users.
- Identify your configuration depending on whether your SnapCenter plug-ins are connected to the Cluster Administrator IP for the entire cluster or directly connected to a SVM within the cluster.

About this task

To simplify the configuration of these roles on storage systems, you can use the RBAC User Creator for NetApp ONTAP tool, which is posted on the NetApp Communities Forum.

This tool automatically handles setting up the ONTAP privileges correctly. For example, RBAC User Creator for NetApp ONTAP tool automatically adds the privileges in the correct order so that the all-access privileges appear first. If you add the read-only privileges first and then add the all-access privileges, ONTAP marks the all-access privileges as duplicates and ignores them.

If you later upgrade SnapCenter or ONTAP, you should re-run the RBAC User Creator for NetApp ONTAP tool to update the user roles you created previously. User roles created for an earlier version of SnapCenter or ONTAP do not work properly with upgraded versions. When you re-run the tool, it automatically handles the upgrade. You do not need to recreate the roles.

More information about setting up ONTAP RBAC roles, see the ONTAP 9 Administrator Authentication and RBAC Power Guide.

Steps

1. On the storage system, create a new role by entering the following command:

```
security login role create <role_name\> -cmddirname "command" -access all
–vserver <svm_name\>
```

   - svm_name is the name of the SVM. If you leave this blank, it defaults to cluster administrator.
   - role_name is the name you specify for the role.
   - command is the ONTAP capability.

You must repeat this command for each permission. Remember that all-access commands must be listed before read-only commands.

For information about the list of permissions, see ONTAP CLI commands for creating roles and assigning permissions.

2. Create a user name by entering the following command:

```
security login create -username <user_name\> -application ontapi -authmethod
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
"user_description"
```

   - user_name is the name of the user you are creating.
   - <password> is your password. If you do not specify a password, the system will prompt you for one.
   - svm_name is the name of the SVM.

3. Assign the role to the user by entering the following command:

```
security login modify username <user_name\> -vserver <svm_name\> -role
<role_name\> -application ontapi -application console -authmethod <password\>
```

   - <user_name> is the name of the user you created in Step 2. This command lets you modify the user to associate it with the role.
   - <svm_name> is the name of the SVM.
   - <role_name> is the name of the role you created in Step 1.
   - <password> is your password. If you do not specify a password, the system will prompt you for one.

4. Verify that the user was created correctly by entering the following command:

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

   user_name is the name of the user you created in Step 3.

Create SVM roles with minimum privileges

There are several ONTAP CLI commands you must run when you create a role for a new SVM user in ONTAP. This role is required if you configure SVMs in ONTAP to use with SnapCenter and you do not want to use the vsadmin role.

Steps

1. On the storage system, create a role and assign all the permissions to the role.

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```

   You should repeat this command for each permission.

2. Create a user and assign the role to that user.

```
security login create -user <user_name\> -vserver <svm_name\> -application
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. Unlock the user.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

ONTAP CLI commands for creating SVM roles and assigning permissions

There are several ONTAP CLI commands you should run to create SVM roles and assign permissions.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"volume clone split start" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

"nvme subsystem create" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

Create SVM roles for ASA r2 systems

There are several ONTAP CLI commands you must run to create a role for a new SVM user in ASA r2 systems. This role is required if you configure SVMs in ASA r2 systems to use with SnapCenter and you do not want to use the vsadmin role.

Steps

1. On the storage system, create a role and assign all the permissions to the role.

   ```
   security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
   -cmddirname <permission\>
   ```

   You should repeat this command for each permission.

2. Create a user and assign the role to that user.

   ```
   security login create -user <user_name\> -vserver <svm_name\> -application
   http -authmethod password -role <SVM_Role_Name\>
   ```

3. Unlock the user.

   ```
   security login unlock -user <user_name\> -vserver <svm_name\>
   ```

ONTAP CLI commands for creating SVM roles and assigning permissions

There are several ONTAP CLI commands you should run to create SVM roles and assign permissions.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"volume clone split stop" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname`

"nvme subsystem delete" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all
- security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name
- security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name

Create ONTAP cluster roles with minimum privileges

You should create an ONTAP cluster role with minimum privileges so that you do not have to use the ONTAP admin role to perform operations in SnapCenter. You can run several ONTAP CLI commands to create the ONTAP cluster role and assign minimum privileges.

Steps

1. On the storage system, create a role and assign all the permissions to the role.

```
security login role create –vserver <cluster_name\>- role <role_name\>
-cmddirname <permission\>
```

You should repeat this command for each permission.

2. Create a user and assign the role to that user.

```
security login create -user <user_name\> -vserver <cluster_name\> -application
ontapi http -authmethod password -role <role_name\>
```

3. Unlock the user.

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

ONTAP CLI commands for creating cluster roles and assigning permissions

There are several ONTAP CLI commands you should run to create cluster roles and assign permissions.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"lun igroup create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly`
- `security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all`
- `security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"snapmirror policy remove-rule" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume snapshot show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

Create ONTAP cluster roles for ASA r2 systems

You should create an ONTAP cluster role with minimum privileges so that you do not have to use the ONTAP admin role to perform operations in SnapCenter. You can run several ONTAP CLI commands to create the ONTAP cluster role and assign minimum privileges.

Steps

1. On the storage system, create a role and assign all the permissions to the role.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   You should repeat this command for each permission.

2. Create a user and assign the role to that user.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   http -authmethod password -role <role_name\>
   ```

3. Unlock the user.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

ONTAP CLI commands for creating cluster roles and assigning permissions

There are several ONTAP CLI commands you should run to create cluster roles and assign permissions.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"cluster show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"nvme namespace show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume restrict" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all`

Add a user or group and assign role and assets

To configure role-based access control for SnapCenter users, you can add users or groups and assign role. The role determines the options that SnapCenter users can access.

Before you begin

- You must have logged in as the "SnapCenterAdmin" role.
- You must have created the user or group accounts in Active Directory in the operating system or database. You cannot use SnapCenter to create these accounts.

You can include only the following special characters in user names and group names: space ( ), hyphen (-), underscore (_), and colon (:).

- SnapCenter includes several predefined roles.

  You can either assign these roles to the user or create new roles.

- AD Users and AD Groups that are added to SnapCenter RBAC must have the READ permission on the Users Container and the Computers Container in the Active Directory.
- After you assign a role to a user or group that contains the appropriate permissions, you must assign the user access to SnapCenter assets, such as hosts and storage connections.

  This enables users to perform the actions for which they have permissions on the assets that are assigned to them.

- You should assign a role to the user or group at some point to take advantage of RBAC permissions and efficiencies.
- You can assign assets like host, resource groups, policy, storage connection, plug-in, and credential to the user while creating the user or group.
- The minimum assets that you should assign an user to perform certain operations are as follows:

Operation	Assets assignment
Protect resources	host, policy
Backup	host, resource group, policy
Restore	host, resource group
Clone	host, resource group, policy
Clone lifecycle	host
Create a Resource Group	host

- When a new node is added to a Windows cluster or a DAG (Exchange Server Database Availability Group) asset and if this new node is assigned to a user, you must reassign the asset to the user or group to include the new node to the user or group.

  You should reassign the RBAC user or group to the cluster or DAG to include the new node to the RBAC user or group. For example, you have a two-node cluster and you have assigned an RBAC user or group to the cluster. When you add another node to the cluster, you should reassign the RBAC user or group to the cluster to include the new node for the RBAC user or group.

- If you are planning to replicate Snapshots, you must assign the storage connection for both the source and destination volume to the user performing the operation.

  You should add assets before assigning access to the users.

If you are using the SnapCenter Plug-in for VMware vSphere functions to protect VMs, VMDKs, or datastores, you should use the VMware vSphere GUI to add a vCenter user to a SnapCenter Plug-in for VMware vSphere role. For information about VMware vSphere roles, see Predefined roles packaged with SnapCenter Plug-in for VMware vSphere.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Users and Access** > .
3. In the Add Users/Groups from Active Directory or Workgroup page:

For this field…	Do this…
Access Type	Select either Domain or workgroup For Domain authentication type, you should specify the domain name of the user or group to which you want to add the user to a role. By default, it is pre-populated with the logged in domain name. You must register the untrusted domain in the **Settings** > **Global Settings** > **Domain Settings** page.
Type	Select either User or Group SnapCenter supports only security group and not the distribution group.
User Name	a. Type the partial user name, and then click **Add**. The user name is case-sensitive. b. Select the user name from the search list. When you add users from a different domain or an untrusted domain, you should type the user name fully because there is no search list for cross domain users. Repeat this step to add additional users or groups to the selected role.
Roles	Select the role to which you want to add the user.

4. Click **Assign**, and then in the Assign Assets page:

a. Select the type of asset from the **Asset** drop-down list.
b. In the Asset table, select the asset.

   The assets are listed only if the user has added the assets to SnapCenter.

c. Repeat this procedure for all of the required assets.
d. Click **Save**.

5. Click **Submit**.

After adding users or groups and assigning roles, refresh the resources list.

Configure audit log settings

Audit logs are generated for each and every activity of the SnapCenter Server. By default, audit logs are secured in the default installed location *C:\Program Files\NetApp\SnapCenter WebApp\audit*.

Audit logs are secured by means of generating digitally signed digest for each and every audit events to protect it from the unauthorized modification. The generated digest's are maintained in the separate audit checksum file and it under goes periodic integrity checks to ensure the integrity of the content.

You should have logged in as the "SnapCenterAdmin" role.

About this task

- Alerts are sent in the following scenarios:
  - Audit log integrity check schedule or Syslog server is enabled or disabled
  - Audit log integrity check, audit log, or Syslog server log failure
  - Low disk space
- Email is sent only when integrity check fails.
- You should modify both audit log directory and audit checksum log directory paths together. You cannot modify only one of them.
- When audit log directory and audit checksum log directory paths are modified, the integrity check cannot be performed on audit logs present in the earlier location.
- Audit log directory and Audit checksum log directory paths should be on the local drive of SnapCenter Server.

  Shared or network mounted drives are not supported.

- If UDP protocol is used in the Syslog server settings, errors due to port is down or unavailable cannot be captured as either an error or an alert in SnapCenter.
- You can use Set-SmAuditSettings and Get-SmAuditSettings commands to configure the audit logs.

  The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running Get-Help command_name. Alternatively, you can also refer the SnapCenter Software Cmdlet Reference Guide.

Steps

1. In the **Settings** page, navigate to **Settings** > **Global Settings** > **Audit log Settings**.
2. In the Audit log section, enter the details.
3. Enter the **Audit log directory** and **Audit checksum log directory**
   a. Enter the Maximum file size
   b. Enter the Maximum log files
   c. Enter the percentage of disk space usage to send an alert
4. (Optional) Enable **Log UTC time**.
5. (Optional) Enable **Audit Log Integrity Check Schedule** and click **Start Integrity Check** for on demand integrity check.

   You can also run **Start-SmAuditIntegrityCheck** command to start on demand integrity check.

6. (Optional) Enable Forwarded audit logs to remote syslog server and enter the Syslog Server details.

   You should import the certificate from the Syslog server into the 'Trusted Root' for TLS 1.2 protocol.

   a. Enter Syslog Server Host
   b. Enter Syslog Server Port
   c. Enter Syslog Server Protocol
   d. Enter RFC Format
7. Click **Save**.
8. You can see audit integrity checks and disk space checks by clicking **Monitor** > **Jobs**.

Configure secured MySQL connections with SnapCenter Server

You can generate Secure Sockets Layer (SSL) certificates and key files if you want to secure the communication between SnapCenter Server and MySQL Server in standalone configurations or Network Load Balancing (NLB) configurations.

Configure secured MySQL connections for standalone SnapCenter Server configurations

You can generate Secure Sockets Layer (SSL) certificates and key files, if you want to secure the communication between SnapCenter Server and MySQL Server. You must configure the certificates and key files in the MySQL Server and SnapCenter Server.

The following certificates are generated:

- CA certificate
- Server public certificate and private key file
- Client public certificate and private key file

Steps

1. Set up the SSL certificates and key files for MySQL servers and clients on Windows by using the openssl

command.

For information, see MySQL Version 5.7: Creating SSL Certificates and Keys Using openssl

> The common name value that is used for the server certificate, client certificate, and key files must each differ from the common name value that is used for the CA certificate. If the common name values are the same, the certificate and key files fail for servers that are compiled by using OpenSSL.

Best Practice: You should use the server fully qualified domain name (FQDN) as the common name for the server certificate.

2. Copy the SSL certificates and key files to the MySQL Data folder.

   The default MySQL Data folder path is `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Update the CA certificate, server public certificate, client public certificate, server private key, and client private key paths in the MySQL server configuration file (my.ini).

   The default MySQL server configuration file (my.ini) path is `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   > You must specify the CA certificate, server public certificate, and server private key paths in the [mysqld] section of the MySQL server configuration file (my.ini).

   You must specify the CA certificate, client public certificate, and client private key paths in the [client] section of the MySQL server configuration file (my.ini).

   The following example shows the certificates and key files copied to the [mysqld] section of the my.ini file in the default folder `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
key.pem"
```

   The following example shows the paths updated in the [client] section of the my.ini file.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
key.pem"
```

4. Stop the SnapCenter Server web application in the Internet Information Server (IIS).
5. Restart the MySQL service.
6. Update the value of the MySQLProtocol key in the SnapManager.Web.UI.dll.config file.

   The following example shows the value of the MySQLProtocol key updated in the SnapManager.Web.UI.dll.config file.

```
<add key="MySQLProtocol" value="SSL" />
```

7. Update the SnapManager.Web.UI.dll.config file with the paths that were provided in the [client] section of the my.ini file.

   The following example shows the paths updated in the [client] section of the my.ini file.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

8. Start the SnapCenter Server web application in the IIS.

Configure secured MySQL connections for HA configurations

You can generate Secure Sockets Layer (SSL) certificates and key files for both the High Availability (HA) nodes if you want to secure the communication between SnapCenter Server and MySQL servers. You must configure the certificates and key files in the MySQL servers and on the HA nodes.

The following certificates are generated:

- CA certificate

  A CA certificate is generated on one of the HA nodes, and this CA certificate is copied to the other HA

node.

- Server public certificate and server private key files for both the HA nodes
- Client public certificate and client private key files for both the HA nodes

Steps

1. For the first HA node, set up the SSL certificates and key files for MySQL servers and clients on Windows by using the openssl command.

   For information, see MySQL Version 5.7: Creating SSL Certificates and Keys Using openssl

   > The common name value that is used for the server certificate, client certificate, and key files must each differ from the common name value that is used for the CA certificate. If the common name values are the same, the certificate and key files fail for servers that are compiled by using OpenSSL.

   Best Practice: You should use the server fully qualified domain name (FQDN) as the common name for the server certificate.

2. Copy the SSL certificates and key files to the MySQL Data folder.

   The default MySQL Data folder path is C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

3. Update the CA certificate, server public certificate, client public certificate, server private key, and client private key paths in the MySQL server configuration file (my.ini).

   The default MySQL server configuration file (my.ini) path is C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini.

   > You must specify CA certificate, server public certificate, and server private key paths in the [mysqld] section of the MySQL server configuration file (my.ini).

   You must specify CA certificate, client public certificate, and client private key paths in the [client] section of the MySQL server configuration file (my.ini).

   The following example shows the certificates and key files copied to the [mysqld] section of the my.ini file in the default folder C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

The following example shows the paths updated in the [client] section of the my.ini file.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. For the second HA node, copy the CA certificate and generate server public certificate, server private key files, client public certificate, and client private key files. perform the following steps:
   a. Copy the CA certificate generated on the first HA node to the MySQL Data folder of the second NLB node.

      The default MySQL Data folder path is C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

      > You must not create a CA certificate again. You should create only the server public certificate, client public certificate, server private key file, and client private key file.

   b. For the first HA node, set up the SSL certificates and key files for MySQL servers and clients on Windows by using the openssl command.

      MySQL Version 5.7: Creating SSL Certificates and Keys Using openssl

      > The common name value that is used for the server certificate, client certificate, and key files must each differ from the common name value that is used for the CA certificate. If the common name values are the same, the certificate and key files fail for servers that are compiled by using OpenSSL.

      It is recommended to use the server FQDN as the common name for the server certificate.

   c. Copy the SSL certificates and key files to the MySQL Data folder.
   d. Update the CA certificate, server public certificate, client public certificate, server private key, and client private key paths in the MySQL server configuration file (my.ini).

      > You must specify the CA certificate, server public certificate, and server private key paths in the [mysqld] section of the MySQL server configuration file (my.ini).

      You must specify the CA certificate, client public certificate, and client private key paths in the [client] section of the MySQL server configuration file (my.ini).

      The following example shows the certificates and key files copied to the [mysqld] section of the my.ini file in the default folder C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

The following example shows the paths updated in the [client] section of the my.ini file.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

5. Stop the SnapCenter Server web application in the Internet Information Server (IIS) on both the HA nodes.
6. Restart the MySQL service on both the HA nodes.
7. Update the value of the MySQLProtocol key in the SnapManager.Web.UI.dll.config file for both the HA nodes.

   The following example shows the value of MySQLProtocol key updated in the SnapManager.Web.UI.dll.config file.

   ```
   <add key="MySQLProtocol" value="SSL" />
   ```

8. Update the SnapManager.Web.UI.dll.config file with the paths that you specified in the [client] section of the my.ini file for both the HA nodes.

   The following example shows the paths updated in the [client] section of the my.ini files.

   ```
   <add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
   ```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

9. Start the SnapCenter Server web application in the IIS on both the HA nodes.
10. Use the Set-SmRepositoryConfig -RebuildSlave -Force PowerShell cmdlet with the -Force option on one of the HA nodes to establish secured MySQL replication on both the HA nodes.

    Even if the replication status is healthy, the -Force option allows you to rebuild the slave repository.

Copyright information

Trademark information