SnapCenter Server installation

SnapCenter Software 4.5

NetApp
July 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/snapcenter-45/install/install_workflow.html on July 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

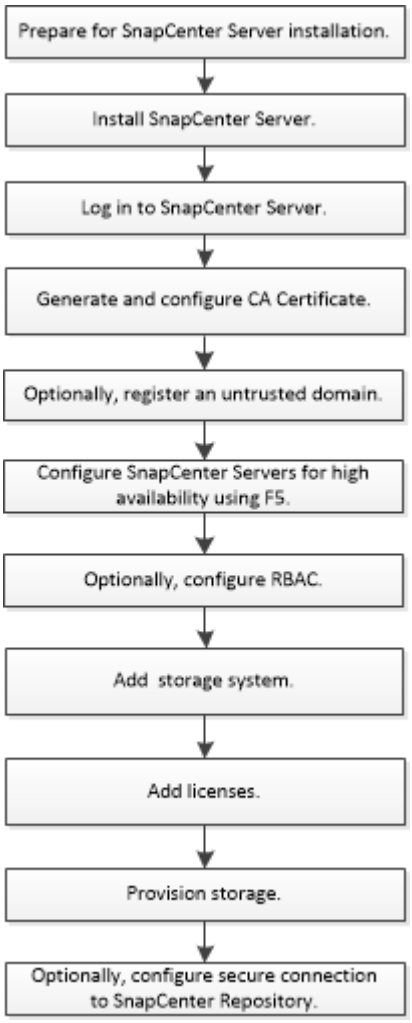
SnapCenter Server installation . . . 1
- Installation workflow . . . 1
- Prepare for installing the SnapCenter Server . . . 1
  - Domain and workgroup requirements . . . 1
  - Space and sizing requirements . . . 2
  - SAN host requirements . . . 3
  - Supported storage systems and applications . . . 3
  - Supported browsers . . . 4
  - Connection and port requirements . . . 4
  - SnapCenter licenses . . . 7
  - Authentication methods for your credentials . . . 9
  - Storage connections and credentials . . . 11
- Install the SnapCenter Server . . . 11
- Log in to SnapCenter . . . 12
  - Modify the SnapCenter default GUI session timeout . . . 14
  - Secure the SnapCenter web server by disabling SSL 3.0 . . . 14
- Configure CA Certificate . . . 15
  - Generate CA Certificate CSR file . . . 15
  - Import CA certificates . . . 15
  - Get the CA certificate thumbprint . . . 16
  - Configure CA certificate with Windows host plug-in services . . . 16
  - Configure CA certificate with SnapCenter site . . . 17
  - Enable CA certificates for SnapCenter . . . 18
- Register untrusted Active Directory domains . . . 18
- Configure High Availability . . . 19
  - Configure SnapCenter Servers for High Availability using F5 . . . 19
  - Configure Microsoft Network Load Balancer manually . . . 20
  - Switch from NLB to F5 for high availability . . . 21
  - High availability for the SnapCenter MySQL repository . . . 21
  - Export SnapCenter certificates . . . 22
- Configure role-based access control (RBAC) . . . 23
  - Add a user or group and assign role and assets . . . 23
  - Create a role . . . 25
  - Add an ONTAP RBAC role using security login commands . . . 26
  - Create SVM roles with minimum privileges . . . 28
  - Create ONTAP cluster roles with minimum privileges . . . 32
  - Configure IIS Application Pools to enable Active Directory read permissions . . . 38
- Add storage systems . . . 38
- Add SnapCenter Standard controller-based licenses . . . 42
  - Prerequisites to add controller-based license . . . 42
  - Add controller-based license . . . 46
- Add SnapCenter Standard capacity-based licenses . . . 47
  - Prerequisites to add capacity-based license . . . 48

Add capacity-based license . . . 49
Provision your storage system . . . 51
Provision storage on Windows hosts . . . 51
Provision storage in VMware environments . . . 66
Configure secured MySQL connections with SnapCenter Server . . . 68
Configure secured MySQL connections for standalone SnapCenter Server configurations . . . 68
Configure secured MySQL connections for HA configurations . . . 70
Features enabled on your Windows host during installation . . . 74

SnapCenter Server installation

Installation workflow

The workflow shows the different tasks required to install and configure the SnapCenter Server.



Prepare for installing the SnapCenter Server

Domain and workgroup requirements

The SnapCenter Server can be installed on systems that are either in a domain or in workgroup. The user used for installation should have admin privileges on the machine in case of both workgroup and domain.

For installing SnapCenter Server and SnapCenter plug-ins on Windows hosts, you should use one of the following:

- **Active Directory domain**

  You must use a Domain user with local administrator rights. The Domain user must be a member of the

local Administrator group on the Windows host.

- **Workgroups**

  You must use a local account that has local administrator rights.

While domain trusts, multi-domain forests, and cross-domain trusts are supported, cross-forest domains are not supported. The Microsoft documentation about Active Directory Domains and Trusts contains more information.

> After installing the SnapCenter Server, you should not change the domain in which the SnapCenter host is located. If you remove the SnapCenter Server host from the domain it was in when the SnapCenter Server was installed and then try to uninstall SnapCenter Server, the uninstall operation fails.

Space and sizing requirements

Before you install the SnapCenter Server, you should be familiar with the space and sizing requirements. You should also apply the available system and security updates.

Item	Requirements
Operating Systems	Microsoft Windows Only English, German, Japanese, and simplified Chinese version of the operating systems are supported. For the latest information about supported versions, see NetApp Interoperability Matrix Tool.
Minimum CPU count	4 cores
Minimum RAM	8 GB The MySQL Server buffer pool uses 20 percent of the total RAM.
Minimum hard drive space for the SnapCenter Server software and logs	4 GB If you have the SnapCenter repository in the same drive where SnapCenter Server is installed, then it is recommended to have 10 GB.

Item	Requirements
Minimum hard drive space for the SnapCenter repository	6 GB NOTE: If you have the SnapCenter Server in the same drive where SnapCenter repository is installed, then it is recommended to have 10 GB.
Required software packages	• Microsoft .NET Framework 4.5.2 or later • Windows Management Framework (WMF) 4.0 or later • PowerShell 4.0 or later For the latest information about supported versions, see NetApp Interoperability Matrix Tool.

SAN host requirements

If your SnapCenter host is part of a FC/iSCSI environment, you might need to install additional software on the system to enable access to ONTAP storage.

SnapCenter does not include Host Utilities or a DSM. If your SnapCenter host is part of a SAN environment, you might need to install and configure the following software:

- Host Utilities

  The Host Utilities support FC and iSCSI, and it enables you to use MPIO on your Windows Servers. For information, see Host Utilities documentation.

- Microsoft DSM for Windows MPIO

  This software works with Windows MPIO drivers to manage multiple paths between NetApp and Windows host computers.

  A DSM is required for high availability configurations.

  If you were using ONTAP DSM, you should migrate to Microsoft DSM. For more information, see How to migrate from ONTAP DSM to Microsoft DSM.

Supported storage systems and applications

You should know the supported storage system, applications, and databases.

- SnapCenter supports ONTAP 8.3.0 and later to protect your data.
- SnapCenter supports Amazon FSx for NetApp ONTAP from SnapCenter Software 4.5 P1 patch release.

  If you are using Amazon FSx for NetApp ONTAP, ensure that the SnapCenter Server host plug-ins are upgraded to 4.5 P1 patch release to perform data protection operations.

For information about Amazon FSx for NetApp ONTAP, see Amazon FSx for NetApp ONTAP documentation.

- SnapCenter supports protection of different applications and databases.

  For detailed information about the supported applications and databases, see NetApp Interoperability Matrix Tool.

Supported browsers

SnapCenter Software can be used on multiple browsers.

- Chrome

  If you are using v66, you might fail to launch SnapCenter GUI.

- Internet Explorer

  SnapCenter UI does not load properly if you are using IE 10 or earlier versions. You should upgrade to IE 11.

  - Only default-level security is supported.

    Making changes to Internet Explorer security settings results in significant browser display issues.

  - Internet Explorer compatibility view must be disabled.
- Microsoft Edge

For the latest information about supported versions, see NetApp Interoperability Matrix Tool.

Connection and port requirements

You should ensure that the connections and ports requirements are met before installing the SnapCenter Server and application or database plug-ins.

- Applications cannot share a port.

  Each port must be dedicated to the appropriate application.

- For customizable ports, you can select a custom port during installation if you do not want to use the default port.

  You can change a plug-in port after installation by using the Modify Host wizard.

- For fixed ports, you should accept the default port number.
- Firewalls
  - Firewalls, proxies, or other network devices should not interfere with connections.
  - If you specify a custom port when you install SnapCenter, you should add a firewall rule on the plug-in host for that port for the SnapCenter Plug-in Loader.

The following table lists the different ports and their default values.

Type of port	Default port
SnapCenter port	8146 (HTTPS), bidirectional, customizable, as in the URL *https://server:8146* Used for communication between the SnapCenter client (the SnapCenter user) and the SnapCenter Server. Also used for communication from the plug-in hosts to the SnapCenter Server. To customize the port, see Install the SnapCenter Server using the install wizard.
SnapCenter SMCore communication port	8145 (HTTPS), bidirectional, customizable The port is used for communication between the SnapCenter Server and the hosts where the SnapCenter plug-ins are installed. To customize the port, see Install the SnapCenter Server using the install wizard.
MySQL port	3306 (HTTPS), bidirectional The port is used for communication between SnapCenter and MySQL repository database. You can create secured connections from the SnapCenter Server to the MySQL server. Learn more
Windows plug-in hosts	135, 445 (TCP) In addition to ports 135 and 445, the dynamic port range specified by Microsoft should also be open. Remote install operations use the Windows Management Instrumentation (WMI) service, which dynamically searches this port range. For information on the dynamic port range supported, see Service overview and network port requirements for Windows The ports are used for communication between the SnapCenter Server and the host on which the plug-in is being installed. To push plug-in package binaries to Windows plug-in hosts, the ports must be open only on the plug-in host, and they can be closed after installation.

Type of port	Default port
Linux or AIX plug-in hosts	22 (SSH) The ports are used for communication between the SnapCenter Server and the host where the plug-in is being installed. The ports are used by SnapCenter to copy plug-in package binaries to Linux or AIX plug-in hosts and should be open or excluded from the firewall or iptables.
SnapCenter Plug-ins Package for Windows, SnapCenter Plug-ins Package for Linux or SnapCenter Plug-ins Package for AIX	8145 (HTTPS), bidirectional, customizable The port is used for communication between SMCore and hosts where the plug-ins package is installed. The communication path also needs to be open between the SVM management LIF and the SnapCenter Server. To customize the port, see Add hosts and install SnapCenter Plug-in for Microsoft Windows or Add hosts and install SnapCenter Plug-ins package for Linux or AIX.
SnapCenter Plug-in for Oracle Database	27216, customizable The default JDBC port is used by the plug-in for Oracle for connecting to the Oracle database. To customize the port, see Add hosts and install SnapCenter Plug-ins package for Linux or AIX.
Custom plug-ins for SnapCenter	9090 (HTTPS), fixed This is an internal port that is used only on the custom plug-in host; no firewall exception is required. Communication between the SnapCenter Server and custom plug-ins is routed through port 8145.
ONTAP cluster or SVM communication port	443 (HTTPS), bidirectional80 (HTTP), bidirectional The port is used by the SAL (Storage Abstraction Layer) for communication between the host running SnapCenter Server and SVM. The port is currently also used by the SAL on SnapCenter for Windows Plug-in hosts for communication between the SnapCenter plug-in host and SVM.

Type of port	Default port
SnapCenter Plug-in for SAP HANA Database vCode Spell Checkerports	3instance_number13 or 3instance_number15, HTTP or HTTPS, bidirectional, and customizable For a multitenant database container (MDC) single tenant, the port number ends with 13; for non MDC, the port number ends with 15. For example, 32013 is the port number for instance 20 and 31015 is the port number for instance 10. To customize the port, see Add hosts and install plug-in packages on remote hosts.
Domain controller communication port	See the Microsoft documentation to identify the ports that should be opened in the firewall on a domain controller for authentication to work properly. It is necessary to open the Microsoft required ports on the domain controller so that the SnapCenter Server, Plug-in hosts, or other Windows client can authenticate the users.

To modify the port details, see Modify plug-in hosts.

SnapCenter licenses

SnapCenter requires several licenses to enable data protection of applications, databases, file systems, and virtual machines. The type of SnapCenter licenses you install depends on your storage environment and the features that you want to use.

License	Where required
SnapCenter Standard controller-based	Required for FAS and AFF SnapCenter Standard license is a controller-based license and is included as part of the premium bundle. If you have the SnapManager Suite license, you also get the SnapCenter Standard license entitlement. If you want to install SnapCenter on a trial basis with FAS or AFF storage, you can obtain a Premium Bundle evaluation license by contacting the sales representative. SnapCenter is also offered as part of data protection bundle. If you have purchased A400 or later, you should purchase the data protection bundle.

License	Where required
SnapCenter Standard capacity-based	Required with ONTAP Select and Cloud Volumes ONTAP If you are a Cloud Volumes ONTAP or ONTAP Select customer, you need to procure a per TB capacity-based license based on the data managed by SnapCenter. By default, SnapCenter ships a built-in 90-day 100 TB SnapCenter Standard capacity-based trial license. For other details, contact the sales representative.
SnapMirror or SnapVault	ONTAP Either SnapMirror or SnapVault license is required if replication is enabled in SnapCenter.
SnapRestore	Required to restore and verify backups. On primary storage systems • Required on SnapVault destination systems to perform remote verification and to restore from a backup. • Required on SnapMirror destination systems to perform remote verification.
FlexClone	Required to clone databases and verification operations. On primary and secondary storage systems • Required on SnapVault destination systems to create clones from secondary vault backup. • Required on SnapMirror destination systems to create clones from secondary SnapMirror backup.
Protocols	• iSCSI or FC license for LUNs • CIFS license for SMB shares • NFS license for NFS type VMDKs • iSCSI or FC license for VMFS type VMDKs Required on SnapMirror destination systems to serve data if a source volume is unavailable.

License	Where required
SnapCenter Standard licenses (optional)	Secondary destinations It is recommended, but not required, that you add SnapCenter Standard licenses to secondary destinations. If SnapCenter Standard licenses are not enabled on secondary destinations, you cannot use SnapCenter to backup resources on the secondary destination after performing a failover operation. However, a FlexClone license is required on secondary destinations to perform clone and verification operations.

SnapCenter Advanced and SnapCenter NAS File Services licenses are deprecated, and are no longer available.

You should install one or more SnapCenter licenses. For information on how to add licenses, see Add SnapCenter Standard controller-based licenses or Add SnapCenter Standard capacity-based licenses.

Single Mailbox Recovery (SMBR) licenses

If you are using SnapCenter Plug-in for Exchange to manage Microsoft Exchange Server databases and Single Mailbox Recovery (SMBR), you would need additional license for SMBR which needs to be purchased separately based on user mailbox.

NetApp® Single Mailbox Recovery has come to the end of availability (EOA) on May 12, 2023. For more information, refer CPC-00507. NetApp will continue to support customers that have purchased mailbox capacity, maintenance, and support through marketing part numbers introduced on June 24, 2020, for the duration of the support entitlement.

NetApp Single Mailbox Recovery is a partner product provided by Ontrack. Ontrack PowerControls offers capabilities that are similar to those of NetApp Single Mailbox Recovery. Customers can procure new Ontrack PowerControls software licenses and Ontrack PowerControls maintenance and support renewals from Ontrack (through licensingteam@ontrack.com) for granular mailbox recovery after the May 12, 2023, EOA date.

Authentication methods for your credentials

Credentials use different authentication methods depending upon the application or environment. Credentials authenticate users so they can perform SnapCenter operations. You should create one set of credentials for installing plug-ins and another set for data protection operations.

Windows authentication

The Windows authentication method authenticates against Active Directory. For Windows authentication, Active Directory is set up outside of SnapCenter. SnapCenter authenticates with no additional configuration. You need a Windows credential to perform tasks such as adding hosts, installing plug-in packages, and

scheduling jobs.

Untrusted domain authentication

SnapCenter allows the creation of Windows credentials using users and groups belonging to the untrusted domains. For the authentication to succeed, you should register the untrusted domains with SnapCenter.

Local workgroup authentication

SnapCenter allows the creation of Windows credentials with local workgroup users and groups. The Windows authentication for local workgroup users and groups does not happen at the time of Windows credential creation but is deferred until the host registration and other host operations are performed.

SQL Server authentication

The SQL authentication method authenticates against a SQL Server instance. This means that a SQL Server instance must be discovered in SnapCenter. Therefore, before adding a SQL credential, you must add a host, install plug-in packages, and refresh resources. You need SQL Server authentication for performing operations such as scheduling on SQL Server or discovering resources.

Linux authentication

The Linux authentication method authenticates against a Linux host. You need Linux authentication during the initial step of adding the Linux host and installing the SnapCenter Plug-ins Package for Linux remotely from the SnapCenter GUI.

AIX authentication

The AIX authentication method authenticates against an AIX host. You need AIX authentication during the initial step of adding the AIX host and installing the SnapCenter Plug-ins Package for AIX remotely from the SnapCenter GUI.

Oracle database authentication

The Oracle database authentication method authenticates against an Oracle database. You need an Oracle database authentication to perform operations on the Oracle database if the operating system (OS) authentication is disabled on the database host. Therefore, before adding a Oracle database credential, you should create an Oracle user in the Oracle database with sysdba privileges.

Oracle ASM authentication

The Oracle ASM authentication method authenticates against an Oracle Automatic Storage Management (ASM) instance. If you are required to access the Oracle ASM instance and if the operating system (OS) authentication is disabled on the database host, you need an Oracle ASM authentication. Therefore, before adding an Oracle ASM credential, you should create an Oracle user with sysasm privileges in the ASM instance.

RMAN catalog authentication

The RMAN catalog authentication method authenticates against the Oracle Recovery Manager (RMAN) catalog database. If you have configured an external catalog mechanism and registered your database to catalog database, you need to add RMAN catalog authentication.

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.

Install the SnapCenter Server

You can run the SnapCenter Server installer executable to install the SnapCenter Server.

You can optionally perform several installation and configuration procedures by using PowerShell cmdlets.

Silent installation of the SnapCenter Server from the command-line is not supported.

What you will need

- The SnapCenter Server host must be up to date with Windows updates with no pending system restarts.
- You should have ensured that MySQL Server is not installed on the host where you plan to install the SnapCenter Server.
- You should have enabled Windows installer debugging.

See the Microsoft web site for information about enabling Windows installer logging.

> You should not install the SnapCenter Server on a host that has Microsoft Exchange Server, Active Directory, or Domain Name Servers.

Steps

1. Download the SnapCenter Server installation package from NetApp Support Site.
2. Initiate the SnapCenter Server installation by double-clicking the downloaded .exe file.

   After you initiate the installation, all the prechecks are performed and if the minimum requirements are not met appropriate error or warning messages are displayed.

   You can ignore the warning messages and proceed with installation; however, errors should be fixed.
3. Review the pre-populated values required for the SnapCenter Server installation and modify if required.

   You do not have to specify the password for MySQL Server repository database. During SnapCenter Server installation the password is auto generated.

   > The special character “%” is not supported in the custom path for the repository database. If you include “%” in the path, installation fails.
4. Click **Install Now**.

   If you have specified any values that are invalid, appropriate error messages will be displayed. You should reenter the values, and then initiate the installation.

   > If you click the **Cancel** button, the step that is being executed will be completed, and then start the rollback operation. The SnapCenter Server will be completely removed from the host.

   However, if you click **Cancel** when "SnapCenter Server site restart" or "Waiting for SnapCenter Server to start" operations are being performed, installation will proceed without cancelling the operation.

   Log files are always listed (oldest first) in the %temp% folder of the admin user. If you want to redirect the log locations, initiate the SnapCenter Server installation from the command prompt by running:`C:\installer_location\installer_name.exe /log"C:\"`

Log in to SnapCenter

SnapCenter supports role-based access control (RBAC). SnapCenter admin assigns roles and resources through SnapCenter RBAC to either a user in workgroup or active directory, or to groups in active directory. The RBAC user can now log in to SnapCenter with the assigned roles.

What you will need

- You should enable Windows Process Activation Service (WAS) in Windows Server Manager.
- If you want to use Internet Explorer as the browser to log in to the SnapCenter Server, you should ensure

that the Protected Mode in Internet Explorer is disabled.

About this task

During installation, the SnapCenter Server Install wizard creates a shortcut and places it on the desktop and in the Start menu of the host where SnapCenter is installed. Additionally, at the end of the installation, the Install wizard displays the SnapCenter URL based on the information that you provided during installation, which you can copy if you want to log in from a remote system.

If you have multiple tabs open in your web browser, closing just the SnapCenter browser tab does not log you out of SnapCenter. To end your connection with SnapCenter, you must log out of SnapCenter either by clicking the **Sign out** button, or by closing the entire web browser.

Best Practice: For security reasons, it is recommended that you do not enable your browser to save your SnapCenter password.

The default GUI URL is a secure connection to the default port 8146 on the server where the SnapCenter Server is installed (*https://server:8146*). If you provided a different server port during the SnapCenter installation, that port is used instead.

For High Availability (HA) deployment, you must access SnapCenter using the virtual cluster IP *https://Virtual_Cluster_IP_or_FQDN:8146*. If you do not see the SnapCenter UI when you navigate to *https://Virtual_Cluster_IP_or_FQDN:8146* in Internet Explorer (IE), you must add the Virtual Cluster IP address or FQDN as a trusted site in IE on each plug-in host, or you must disable IE Enhanced Security on each plug-in host. For more information, see Unable to access cluster IP address from outside network.

In addition to using the SnapCenter GUI, you can use PowerShell cmdlets to create scripts to perform configuration, backup, and restore operations. Some cmdlets might have changed with each SnapCenter release. The SnapCenter Software Cmdlet Reference Guide has the details.

If you are logging in to SnapCenter for the first time, you must log in using the credentials that you provided during the install process.

Steps

1. Launch SnapCenter from the shortcut located on your local host desktop, or from the URL provided at the end of the installation, or from the URL provided by your SnapCenter administrator.
2. Enter user credentials.

To specify the following…	Use one of these formats…
Domain administrator	• NetBIOS\UserName • UserName@UPN suffix For example, username@netapp.com • Domain FQDN\UserName
Local administrator	UserName

3. If you are assigned more than one role, from the Role box, select the role that you want to use for this login

session.

Your current user and associated role are shown in the upper right of SnapCenter after you are logged in.

Results

The **Dashboard** page is displayed.

If the logging fails with the error that site cannot be reached, you should map the SSL certificate to SnapCenter. Learn more

After you finish

After logging to SnapCenter Server as an RBAC user for the first time, refresh the resources list.

If you have untrusted Active Directory domains that you want SnapCenter to support, you must register those domains with SnapCenter before configuring the roles for the users on untrusted domains. Learn more

Modify the SnapCenter default GUI session timeout

You can modify the SnapCenter GUI session timeout period to make it less than or greater than the default timeout period of 20 minutes.

As a security feature, after a default period of 15 minutes of inactivity, SnapCenter warns you that you will be logged out of the GUI session in 5 minutes. By default, SnapCenter logs you out of the GUI session after 20 minutes of inactivity, and you must log in again.

Steps

1. In the left navigation pane, click **Settings** > **Global Settings**.
2. In the Global Settings page, click **Configuration Settings**.
3. In the Session Timeout field, enter the new session timeout in minutes, and then click **Save**.

Secure the SnapCenter web server by disabling SSL 3.0

For security purposes, you should disable Secure Socket Layer (SSL) 3.0 protocol in Microsoft IIS if it is enabled on your SnapCenter web server.

There are flaws in the SSL 3.0 protocol that an attacker can use to cause connection failures, or to perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Steps

1. To launch Registry Editor on the SnapCenter web server host, click **Start** > **Run**, and then enter regedit.
2. In Registry Editor, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
   - If the Server key already exists:
     i. Select the Enabled DWORD, and then click **Edit** > **Modify**.
     ii. Change the value to 0, and then click **OK**.
   - If the Server key does not exist:

i. Click **Edit** > **New** > **Key**, and then name the key Server.

ii. With the new Server key selected, click **Edit** > **New** > **DWORD**.

iii. Name the new DWORD Enabled, and then enter 0 as the value.

3. Close Registry Editor.

Configure CA Certificate

Generate CA Certificate CSR file

You can generate a Certificate Signing Request (CSR) and import the certificate that can be obtained from a Certificate Authority (CA) using the generated CSR. The certificate will have a private key associated with it.

CSR is a block of encoded text that is given to an authorized certificate vendor to procure the signed CA certificate.

For information to generate a CSR, see How to generate CA Certificate CSR file.

If you own the CA certificate for your domain (*.domain.company.com) or your system (machine1.domain.company.com), you can skip generating the CA Certificate CSR file. You can deploy the existing CA certificate with SnapCenter.

For cluster configurations, the cluster name (virtual cluster FQDN), and the respective host names should be mentioned in the CA certificate. The certificate can be updated by filling the Subject Alternative Name (SAN) field before procuring the certificate. For a wild card certificate (*.domain.company.com), the certificate will contain all the hostnames of the domain implicitly.

Import CA certificates

You must import the CA certificates to the SnapCenter Server and the Windows host plug-ins using the Microsoft management console (MMC).

Steps

1. Go to the Microsoft management console (MMC), and then click **File** > **Add/Remove Snapin**.
2. In the **Add or Remove Snap-ins** window, select **Certificates** and then click **Add**.
3. In the **Certificates snap-in** window, select the **Computer account** option, and then click **Finish**.
4. Click **Console Root** > **Certificates – Local Computer** > **Trusted Root Certification Authorities** > **Certificates**.
5. Right-click on the folder “Trusted Root Certification Authorities”, and then select **All Tasks** > **Import** to start the import wizard.
6. Complete the wizard, as follows:

In this wizard window…	Do the following…
Import Private Key	Select the option **Yes**, import the private key, and then click **Next**.

In this wizard window…	Do the following…
Import File Format	Make no changes; click **Next**.
Security	Specify the new password to be used for the exported certificate, and then click **Next**.
Completing the Certificate Import Wizard	Review the summary, and then click **Finish** to start the import.

Importing certificate should be bundled with the private key (supported formats are: *.pfx, *.p12, *.p7b).

7. Repeat Step 5 for the “Personal” folder.

Get the CA certificate thumbprint

A certificate thumbprint is a hexadecimal string that identifies a certificate. A thumbprint is calculated from the content of the certificate using a thumbprint algorithm.

Steps

1. Perform the following on the GUI:
   a. Double-click the certificate.
   b. In the Certificate dialog box, click the **Details** tab.
   c. Scroll through the list of fields and click **Thumbprint**.
   d. Copy the hexadecimal characters from the box.
   e. Remove the spaces between the hexadecimal numbers.

      For example, if the thumbprint is: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", after removing the spaces, it will be: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Perform the following from PowerShell:
   a. Run the following command to list the thumbprint of the installed certificate and identify the recently installed certificate by the subject name.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copy the thumbprint.

Configure CA certificate with Windows host plug-in services

You should configure the CA certificate with Windows host plug-in services to activate the installed digital certificate.

Perform the following steps on the SnapCenter Server and all the plug-in hosts where CA certificates are already deployed.

Steps

1. Remove the existing certificate binding with SMCore default port 8145, by running the following command:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   For example:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

2. Bind the newly installed certificate with the Windows host plug-in services, by running the following commands:

   ```
   > $cert = "<certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
   appid="$guid"
   ```

   For example:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
   appid="$guid"
   ```

Configure CA certificate with SnapCenter site

You should configure the CA certificate with SnapCenter site on Windows host.

Steps

1. Open IIS Manager on the Windows Server where SnapCenter is installed.
2. In the left navigation pane, click **Connections**.
3. Expand the name of the server and **Sites**.
4. Select the SnapCenter website on which you want to install the SSL Certificate.
5. Navigate to **Actions** > **Edit Site**, click **Bindings**.
6. In the Bindings page, select **binding for https**.
7. Click **Edit**.
8. From the SSL certificate drop-down list, select the recently imported SSL Certificate.
9. Click **OK**.

> If the recently deployed CA certificate is not listed in the drop-down menu, check if the CA certificate is associated with the private key.

Ensure that the certificate is added using the following path: **Console Root > Certificates – Local Computer > Trusted Root Certification Authorities > Certificates**.

Enable CA certificates for SnapCenter

You should configure the CA certificates and enable the CA certificate validation for the SnapCenter Server.

What you will need

- You can enable or disable the CA certificates using the Set-SmCertificateSettings cmdlet.
- You can display the certificate status for the SnapCenter Server using the Get-SmCertificateSettings 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.

Steps

1. In the Settings page, navigate to **Settings** > **Global Settings** > **CA Certificate Settings**.
2. Select **Enable Certificate Validation**.
3. Click **Apply**.

After you finish

The Managed Hosts tab host displays a padlock and the color of the padlock indicates the status of the connection between SnapCenter Server and the plug-in host.

- indicates that there is no CA certificate enabled or assigned to the plug-in host.
- indicates that the CA certificate is successfully validated.
- indicates that the CA certificate could not be validated.
- indicates that the connection information could not be retrieved.

When the status is yellow or green, the data protection operations completes successfully.

Register untrusted Active Directory domains

You should register the Active Directory with SnapCenter Server to manage hosts, users, and groups from multiple untrusted Active Directory domains.

What you will need

- The fully qualified domain name (FQDN) should be reachable from SnapCenter Server.
- If the FQDN is not resolvable, the domain controller IP addresses that are provided should be resolvable from SnapCenter Server.
- You should have enabled bidirectional communication between the plug-in hosts and the SnapCenter Server.

- DNS resolution should be set up from the SnapCenter Server to the plug-in hosts and vice-versa.

About this task

You can register an untrusted domain with the FQDN. If the FQDN is not resolvable from the SnapCenter Server, you can register with an IP address.

You can use either the SnapCenter user interface or PowerShell cmdlets to register an untrusted domain.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Global Settings**..
3. In the Global Settings page, click **Domain Settings**.
4. Click + to register a new domain.
5. In the Register New Domain page, specify the information that is required for registering the untrusted domain:

For this field…	Do this…
Domain Name	Specify the NetBIOS name for the domain.
Domain FQDN	Specify the FQDN and click **Resolve**.
Domain controller IP addresses	If the domain FQDN is not resolvable from the SnapCenter Server, specify one or more domain controller IP addresses. For more information, see Add domain controller IP for untrusted domain from GUI.

6. Click **OK**.

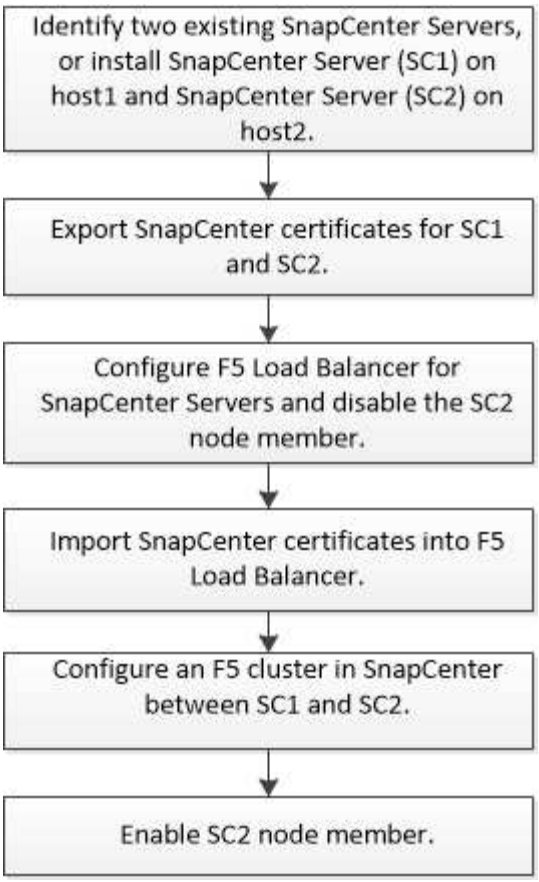
Configure High Availability

Configure SnapCenter Servers for High Availability using F5

To support High Availability (HA) in SnapCenter, 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.

If you have upgraded from SnapCenter 4.2.x and were previously using Network Load Balancing (NLB), you can continue to use that configuration or switch to F5.

The workflow image lists the steps to configure SnapCenter Servers for high availability using F5 load balancer. For detailed instruction, see 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, see SnapCenter Software Cmdlet Reference Guide.

Additional F5 configuration 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 node that is partially resolved by the NLB or F5 node and if the SnapCenter node is not able to reach out to this node, then the SnapCenter host page switches between hosts down and running state frequently. To resolve this issue, you should ensure that both the SnapCenter nodes are able to resolve the host in NLB or F5 node.

Configure Microsoft Network Load Balancer manually

You can configure Microsoft Network Load Balancing (NLB) to set up SnapCenter High Availability. From SnapCenter 4.2, you should manually configure NLB outside of SnapCenter installation for high availability.

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

SnapCenter 4.1.1 or earlier supported configuration of Network Load Balancing (NLB) while installing SnapCenter.

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.

Export SnapCenter certificates

Steps

1. Go to the Microsoft management console (MMC), and then click **File** > **Add/Remove Snap-in**.
2. In the Add or Remove Snap-ins window, select **Certificates** and then click **Add**.
3. In the Certificates snap-in window, select the **My user account** option, and then click **Finish**.
4. Click **Console Root** > **Certificates - Current User** > **Trusted Root Certification Authorities** > **Certificates**.
5. Right-click the certificate that has the SnapCenter Friendly Name, and then select **All Tasks** > **Export** to start the export wizard.
6. Complete the wizard, as follows:

In this wizard window…	Do the following…
Export Private Key	Select the option **Yes, export the private key**, and then click **Next**.
Export File Format	Make no changes; click **Next**.
Security	Specify the new password to be used for the exported certificate, and then click **Next**.
File to Export	Specify a file name for the exported certificate (you must use .pfx), and then click **Next**.
Completing the Certificate Export Wizard	Review the summary, and then click **Finish** to start the export.

Results

Certificates are exported in .pfx format.

Configure role-based access control (RBAC)

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.

What you will need

- 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.

  The user names and group names should not include /\[ ];|=,+*?< >' characters.

- 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 Snapshot copies, 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.

For this field…	Do this…
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.

Create a role

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

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

Steps

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

From SnapCenter 4.5, you cannot have a role name that include /\[ ];|=,+*?< >' characters. If you want to use a role that you created in an earlier release of SnapCenter with these special characters, you can disable the validation of the role name by changing the value of 'DisableSQLInjectionValidation' parameter to true.

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 ONTAP RBAC role using security login commands

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

What you will need

- Before you create an ONTAP RBAC role for storage systems running clustered ONTAP, you must identify the following:
  - The task (or tasks) that you want to perform
  - The privileges required to perform these tasks
- Configuring an RBAC role requires that you perform the following actions:
  - 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.
  - Vary 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 configuring these roles on storage systems, you can use the RBAC User Creator for Data 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 Data 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 Data 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.

For consistency, the SnapCenter documentation refers to the roles as using privileges. The OnCommand System Manager GUI uses the term “attribute” instead of “privilege.” When setting up ONTAP RBAC roles, both these terms mean the same thing.

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 -role SVM_SVM_Role_Name -cmddirname "snapmirror list-destinations" -vserver SVM_Name -access all`
- `security login role create -role SVM_SVM_Role_Name -cmddirname "event generate-autosupport-log" -vserver SVM_Name -access all`
- `security login role create -vserver SVM_Name -role SVM_SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_Name -role SVM_SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_SVM_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_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_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 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 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 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_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_SVM_Role_Name -cmddirname "volume clone split status" -access all`

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 -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 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 "security login" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror list-destinations" -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 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 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

Configure IIS Application Pools to enable Active Directory read permissions

You can configure Internet Information Services (IIS) on your Windows Server to create a custom Application Pool account when you need to enable Active Directory read permissions for SnapCenter.

Steps

1. Open IIS Manager on the Windows Server where SnapCenter is installed.
2. In the left navigation pane, click **Application Pools**.
3. Select SnapCenter in the Application Pools list, and then click **Advanced Settings** in the Actions pane.
4. Select Identity, and then click **…** to edit the SnapCenter application pool identity.
5. In the Custom Account field, enter a domain user or domain admin account name with Active Directory read permission.
6. Click OK.

   The custom account replaces the built-in ApplicationPoolIdentity account for the SnapCenter application pool.

Add storage systems

You should set up the storage system that gives SnapCenter access to ONTAP storage 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 in SnapCenter 4.5 P1 or add FSx SVM in SnapCenter.

What you will need

- 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 Snapshot copies 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.

   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**.

Results

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
enable -noteto enable
```

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

Add SnapCenter Standard controller-based licenses

A SnapCenter Standard controller-based license is required if you are using FAS or AFF 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
- Enabled by adding it directly to the FAS or AFF storage controller by using either the ONTAP System Manager or the storage cluster command line

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

- Locked to the controller's serial number

For information on the licenses required, see SnapCenter licenses.

Prerequisites to add controller-based license

Before you add a controller-based license, you should verify if the SnapManager Suite license is installed, identify the licenses installed on the controller, retrieve the serial number of the controller, and retrieve the serial number of the controller-based license.

Verify if the SnapManager Suite license is installed

You can use the SnapCenter GUI to view whether a SnapManager Suite license is installed on FAS or AFF primary storage systems, and to identify which storage systems might require SnapManager Suite licenses. SnapManager Suite licenses apply only to FAS and AFF SVMs or clusters on primary storage systems.

If you already have a SnapManager Suite license on your controller, SnapCenter Standard controller-based license entitlement is provided automatically. 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, click **Storage Systems**.
2. On 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 click 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 or AFF primary storage system.
   - indicates that a SnapManager Suite license is not installed on a FAS or AFF primary storage system.
   - Not applicable indicates that a SnapManager Suite license is not applicable because the storage controller is on Cloud Volumes ONTAP, ONTAP Select, or Secondary storage platforms.

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 or AFF system.

The SnapCenter Standard controller-based license is displayed as SnapManagerSuite license on the controller.

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 determine whether the SnapManagerSuite license is installed.

```
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.

Retrieve the controller serial number

You need to have the controller serial number to retrieve the serial number of your controller-based license. You can retrieve the controller serial number using the ONTAP command line. You should be a cluster administrator on the FAS or AFF system.

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.

```
cluster1::> system show -instance

Node: fas8080-41-42-01
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.

Retrieve the serial number of the controller-based license

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

What you will need

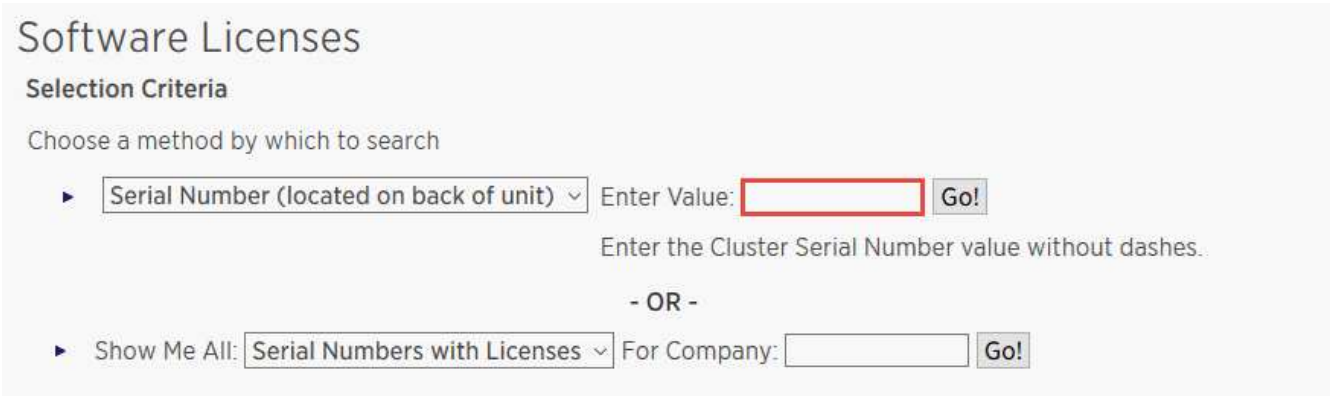
- You should have a valid NetApp Support Site login credentials.

  If you do not enter valid credentials, no information is returned for your search.

- You should have the controller serial number.

Steps

1. Log in to the NetApp Support Site at mysupport.netapp.com.
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 click **Go!**.



   A list of licenses for the specified controller is displayed.

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

Add controller-based license

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

What you will need

- You should be a cluster administrator on the FAS or AFF 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 or AFF 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
   ```

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 GUI.

Removing a trial license manually is only required if you are using a SnapCenter Standard controller-based license. If you procured a SnapCenter Standard capacity-based license and add it in the SnapCenter GUI, the trial license gets overwritten automatically.

Steps

1. On the SnapCenter Server, open a PowerShell window to reset the MySQL password.
   a. Run the Open-SmConnection cmdlet to initiate a connection session 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';
   ```

Add SnapCenter Standard capacity-based licenses

You use a SnapCenter Standard capacity license to protect data on ONTAP Select and Cloud Volumes ONTAP platforms.

The license has the following characteristics:

- Composed of a nine-digit serial number with the format 51xxxxxxx

  You use the license serial number and valid NetApp Support Site login credentials to enable the license using the SnapCenter GUI.
- Available as a separate, perpetual license, with the cost based on either the used storage capacity or the size of the data you want protected, whichever is lower, and the data is managed by SnapCenter
- Available per terabyte

  For example, you can obtain a capacity-based license for 1 TB, 2 TBs, 4 TBs, and so on.
- Available as a 90-day trial license with 100 TB capacity entitlement

For information on the licenses required, see SnapCenter licenses.

Prerequisites to add capacity-based license

Before you add a capacity-based license, you should calculate the capacity requirements, retrieve the serial number of the capacity-based license, and optionally generate a license file.

Calculate capacity requirements

Before you obtain a SnapCenter capacity-based license, you should calculate the amount of capacity on a host that is to be managed by SnapCenter.

You should be a cluster administrator on the Cloud Volumes ONTAP or ONTAP Select system.

About this task

SnapCenter calculates the actual capacity used. If the size of the file system or database is 1 TB, but only 500 GB of space is used, SnapCenter calculates 500 GB of used capacity. The volume capacity is calculated after dedupe and compression, and it is based on the entire volume's used capacity.

Steps

1. Log in to the NetApp controller using the ONTAP command line.
2. To view the volume capacity used, enter the command.

```
select::> vol show -fields used -volume Engineering,Marketing
vserver volume       used
------- ------       ------
VS1     Engineering  2.13TB
VS1     Marketing    2.62TB

2   entries were displayed.
```

   The combined used capacity for the two volumes is less than 5 TB; therefore, if you want to protect all 5 TB of data, the minimum SnapCenter capacity-based license requirement is 5 TB.

   However, if you want to protect only 2 TB of the 5 TB of total used capacity, you can acquire a 2 TB capacity-based license.

Retrieve the serial number of capacity-based license

Your SnapCenter capacity-based license serial number is available in your order confirmation or in your documentation package; however, if you do not have this serial number, you can retrieve it from the NetApp Support Site.

You should have valid NetApp Support Site login credentials.

Steps

1. Log in to the NetApp Support Site at mysupport.netapp.com.
2. Navigate to **Systems** > **Software Licenses**.
3. In the Selection Criteria area, choose **SC_STANDARD** from the Show Me All: Serial Numbers and

Licenses drop-down menu.

4. Type your company name, and then click **Go!**.

   The nine-digit SnapCenter license serial number, with the format 51xxxxxxx, is displayed.

5. Record the serial number.

Generate a NetApp license file

If you prefer not to enter your NetApp Support Site credentials and the SnapCenter license serial number in the SnapCenter GUI, or if you do not have internet access to the NetApp Support Site from SnapCenter, you can generate a NetApp license file (NLF), and then download and store the file in a location accessible from the SnapCenter host.

What you will need

- You should be using SnapCenter with either ONTAP Select or Cloud Volumes ONTAP.
- You should have a valid NetApp Support Site login credentials.
- You should have your nine-digit serial number of the license in the format 51xxxxxxx.

Steps

1. Navigate to the NetApp License File Generator.
2. Enter the required information.
3. In the Product Line field, select **SnapCenter Standard (capacity-based)** from the pull-down menu.
4. In the Product Serial Number field, enter the SnapCenter license serial number
5. Read and accept the NetApp Data Privacy Policy, and then click **Submit**.
6. Save the license file, and then record the file location.

Add capacity-based license

If you are using SnapCenter with ONTAP Select or Cloud Volumes ONTAP platforms, you should install one or more SnapCenter capacity-based licenses.

What you will need

- You should log in as the SnapCenter Admin user.
- You should have a valid NetApp Support Site login credentials.

- You should have your nine-digit serial number of the license in the format 51xxxxxxx.

  If you are using a NetApp license file (NLF) to add your license, you should know the location of the license file.

About this task

You can perform the following tasks on the Settings page:

- Add a license.
- View license details to quickly locate information about each license.
- Modify a license when you want to replace the existing license, for example, to update the license capacity or to change the threshold notification settings.
- Delete a license when you want to replace an existing license or when the license is no longer required.

> The trial license (serial number ending with 50) cannot be deleted using the SnapCenter GUI. The trial license automatically gets overwritten when you add a procured SnapCenter Standard capacity-based licensed.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Software**.
3. In the License section of the Software page, click **Add** (+).
4. In the Add SnapCenter License wizard, select one of the following methods to obtain the license you want to add:

For this field…	Do this…
Enter your NetApp Support Site (NSS) login credentials to import licenses	a. Enter your NSS user name. b. Enter your NSS password. c. Enter the serial number of the controller-based license.
NetApp License File	a. Browse to the location of the license file, and then select it. b. Click **Open**.

5. In the Notifications page, enter the capacity threshold at which SnapCenter sends email, EMS, and AutoSupport notifications.

   The default threshold is 90 percent.

6. To configure the SMTP server for email notifications, click **Settings** > **Global Settings** > **Notification Server Settings**, and then enter the following details:

For this field…	Do this…
Email preference	Choose either **Always** or **Never**.
Provide email settings	If you select **Always**, specify the following: • Sender email address • Receiver email address • Optional: Edit the default Subject line The default subject reads as follows: "SnapCenter License Capacity Notification".

7. If you want to have Event Management System (EMS) messages sent to the storage system syslog or have AutoSupport messages sent to the storage system for failed operations, select the appropriate check boxes.

Best Practice: Enabling AutoSupport is recommended to help troubleshoot issues you might experience.

8. Click **Next**.
9. Review the summary, and then click **Finish**.

How SnapCenter calculates capacity usage

SnapCenter automatically calculates capacity usage once a day at midnight on the ONTAP Select and Cloud Volumes ONTAP storage it manages. To ensure you have configured SnapCenter correctly, you should be aware of how SnapCenter calculates capacity.

When you are using a Standard Capacity license, SnapCenter calculates the unused capacity by deducting the used capacity on all volumes from the total licensed capacity. If used capacity exceeds the licensed capacity, an overuse warning is displayed on the SnapCenter Dashboard. If you configured capacity thresholds and notifications in SnapCenter, an email is sent when the used capacity reaches the threshold you specify.

Provision your storage system

Provision storage on Windows hosts

Configure LUN storage

You can use SnapCenter to configure an FC-connected or iSCSI-connected LUN. You can also use SnapCenter to connect an existing LUN to a Windows host.

LUNs are the basic unit of storage in a SAN configuration. The Windows host sees LUNs on your system as virtual disks. For more information, see ONTAP 9 SAN Configuration Guide.

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.

Disconnect an iSCSI session

Occasionally, you might require to disconnect an iSCSI session from a target with which you have multiple sessions.

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. From the list of iSCSI sessions, select the session that you want to disconnect and click **Disconnect Session**.
6. In the Disconnect Session dialog box, click **OK**.

   SnapCenter disconnects the iSCSI session.

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.

In this field…	Do this…
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 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.

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.

What you will need

- 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. On 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. On 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.
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. On 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.

Property	Description
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.
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. On 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. On 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 autocomplete the field.

10. On 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 copy before resizing a LUN.
- If you need to restore a LUN from a Snapshot copy made before the LUN was resized, SnapCenter automatically resizes the LUN to the size of the Snapshot copy.

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

What you will need

- 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. On 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. On 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. On 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. On 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. On 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 automatically complete the field.

10. On 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.

What you will need

- 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.

What you will need

- 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 that are provided by SnapCenter Plug-in for Microsoft Windows. 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.

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 the Snapshot copies.

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

For the latest information about supported versions, see NetApp Interoperability Matrix Tool.

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.

Related information

Refer to Broadcom Technical Documentation and search for documentation on clustering virtual machines across physical hosts and creating shared FC RDM LUNs for Microsoft clusters.

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 web.config file.

   The following example shows the value of the MySQLProtocol key updated in the web.config file.

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

7. Update the web.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 web.config file for both the HA nodes.

   The following example shows the value of MySQLProtocol key updated in the web.config file.

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

8. Update the web.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.

Features enabled on your Windows host during installation

The SnapCenter Server installer enables the Windows features and roles on your Windows host during installation. These might be of interest for troubleshooting and host system maintenance purposes.

Category	Feature
Web Server	• Internet Information Services • World Wide Web Services • Common HTTP Features ◦ Default Document ◦ Directory Browsing ◦ HTTP Errors ◦ HTTP Redirection ◦ Static Content ◦ WebDAV Publishing • Health and Diagnostics ◦ Custom Logging ◦ HTTP Logging ◦ Logging Tools ◦ Request Monitor ◦ Tracing • Performance Features ◦ Static Content Compression • Security ◦ IP Security ◦ Basic Authentication ◦ Centralized SSL Certificate Support ◦ Client Certificate Mapping Authentication ◦ IIS Client Certificate Mapping Authentication ◦ IP and Domain Restrictions ◦ Request Filtering ◦ URL Authorization ◦ Windows Authentication • Application Development Features ◦ .NET Extensibility 4.5 ◦ Application Initialization ◦ ASP.NET 4.5 ◦ Server-Side Includes ◦ WebSocket Protocol • Management Tools ◦ IIS Management Console

Category	Feature
IIS Management Scripts and Tools	• IIS Management Service • Web Management Tools
.NET Framework 4.5.2 Features	• .NET Framework 4.5.2 • ASP.NET 4.5.2 • Windows Communication Foundation (WCF) HTTP Activation45 ◦ TCP Activation ◦ HTTP Activation ◦ Message Queuing (MSMQ) activation
Message Queuing	• Message Queuing Services Ensure that no other applications uses the MSMQ service that SnapCenter creates and manages. • MSMQ Server
Windows Process Activation Service	• Process Model
Configuration APIs	All

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.