# NetApp

# Install the SnapCenter Server

SnapCenter software

NetApp
January 09, 2026

# Table of Contents

# Install the SnapCenter Server

## Install the SnapCenter Server on Windows host

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. You should be using PowerShell 7.4.2 or later.

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

**Before you begin**

- 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:\"`

## Features enabled on 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 maintaining the host system.

| Category | Feature |
|---|---|
| Web Server | • Internet Information Services<br>• World Wide Web Services<br>• Common HTTP Features<br>  ◦ Default Document<br>  ◦ Directory Browsing<br>  ◦ HTTP Errors<br>  ◦ HTTP Redirection<br>  ◦ Static Content<br>  ◦ WebDAV Publishing<br>• Health and Diagnostics<br>  ◦ Custom Logging<br>  ◦ HTTP Logging<br>  ◦ Logging Tools<br>  ◦ Request Monitor<br>  ◦ Tracing<br>• Performance Features<br>  ◦ Static Content Compression<br>• Security<br>  ◦ IP Security<br>  ◦ Basic Authentication<br>  ◦ Centralized SSL Certificate Support<br>  ◦ Client Certificate Mapping Authentication<br>  ◦ IIS Client Certificate Mapping Authentication<br>  ◦ IP and Domain Restrictions<br>  ◦ Request Filtering<br>  ◦ URL Authorization<br>  ◦ Windows Authentication<br>• Application Development Features<br>  ◦ .NET Extensibility 4.5<br>  ◦ Application Initialization<br>  ◦ ASP.NET Core Runtime 8.0.12 (and all subsequent 8.0.x patches) Hosting Bundle<br>  ◦ Server-Side Includes<br>  ◦ WebSocket Protocol<br>• Management Tools<br>  ◦ IIS Management Console |

| Category | Feature |
|---|---|
| IIS Management Scripts and Tools | • IIS Management Service<br>• Web Management Tools |
| .NET Framework 8.0.12 Features | • ASP.NET Core Runtime 8.0.12 (and all subsequent 8.0.x patches) Hosting Bundle<br>• Windows Communication Foundation (WCF) HTTP Activation45<br>  ◦ TCP Activation<br>  ◦ HTTP Activation<br><br>For .NET specific troubleshooting information, see SnapCenter upgrade or install fails for legacy systems that do not have internet connectivity. |
| Windows Process Activation Service | Process Model |
| Configuration APIs | All |

# Install the SnapCenter Server on Linux host

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

**Before you begin**

- If you want to install the SnapCenter Server using non-root user who does not have enough privileges to install SnapCenter, get the sudoers checksum file from the NetApp Support site. You should use appropriate checksum file based on the Linux Version.

- If the sudo package is not available in SUSE Linux, then install the sudo package to avoid authentication failure.

- For SUSE Linux, configure the hostname to avoid the installation failure.

- Check the secure Linux status by running the command `sestatus`. If the *SELinux status* is "enabled" and the *Current mode* is "enforcing", perform the following:

  ◦ Run the command: `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    The default value of *WEBAPP_EXTERNAL_PORT* is 8146

  ◦ If the firewall blocks the port, run `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    The default value of *WEBAPP_EXTERNAL_PORT* is 8146

  ◦ Run the following commands from the directory where you have read and write permission:

    ▪ `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

      If the command return "nothing to do", rerun the command after installing SnapCenter Server.

- If the command creates *my-nginx.pp*, run the command to make the policy package active: `sudo semodule -i my-nginx.pp`

  ○ The path used for MySQL PID directory is */var/opt/mysqld*. Run the following commands to set the permissions for MySQL installation.

    ▪ `mkdir /var/opt/mysqld`

    ▪ `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`

    ▪ `sudo restorecon -Rv /var/opt/mysqld`

  ○ The path used for MySQL Data directory is */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Run the following commands to set the permissions for MySQL data directory.

    ▪ `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

    ▪ `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`

    ▪ `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

### About this task

- When SnapCenter Server is installed on the Linux host, third-party services such as MySQL, RabbitMq, Errlang gets installed. You should not uninstall them.

- The SnapCenter Server installed on the Linux host does not support:

  ○ High availability

  ○ Windows plug-ins

  ○ Active Directory (Supports only the local users, both root and non-root user with creds)

  ○ Key based authentication to log into SnapCenter

- During the installation of .NET runtime, if the installation fails to resolve the dependencies of *libicu* library, then install *libicu* by running the command: `yum install -y libicu`

- If the installation of SnapCenter Server fails due to the non-availability of *Perl*, then install *Perl* by running the command: `yum install -y perl`

### Steps

1. Download the following from NetApp Support Site to */home directory*.

   ○ SnapCenter Server installation package - **snapcenter-linux-server-(el8/el9/sles15).bin**

   ○ Public key file - **snapcenter_public_key.pub**

   ○ Respective signature file - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**

2. Validate the signature file. `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`

3. For non-root user installation, add the visudo content specified in **snapcenter_server_checksum_(el8/el9/sles15).txt** available along with the .bin installer.

4. Assign the execute permission for the .bin installer. `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`

5. Perform one of the actions to install SnapCenter Server.

| If you want to perform… | Do this… |
| --- | --- |
| Interactive installation | `./snapcenter-linux-server-(el8/el9/sles15).bin`<br><br>You will be prompted to enter the following details:<br><br>• The webapp external port that is used to access SnapCenter Server outside the Linux host. The default value is 8146.<br>• The SnapCenter Server user who will install SnapCenter Server.<br>• The installation directory where packages will be installed. |

| If you want to perform… | Do this… |
| --- | --- |
| Non interactive installation | `sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>`<br><br>Example: sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log<br><br>Logs will be stored at */var/opt/snapcenter/logs*.<br><br>Parameters to be passed for installing SnapCenter Server:<br><br>• DWEBAPP_EXTERNAL_PORT: Webapp external port that is used to access SnapCenter Server outside the Linux host. The default value is 8146.<br><br>• DWEBAPP_INTERNAL_PORT: Webapp internal port that is used to access SnapCenter Server within the Linux host. The default value is 8147.<br><br>• DSMCORE_PORT: SMCore port on which the smcore services are running. The default value is 8145.<br><br>• DSCHEDULER_PORT: Scheduler port on which the scheduler services are running. The default value is 8154.<br><br>• DSNAPCENTER_SERVER_USER: SnapCenter Server user who will install SnapCenter Server. For *DSNAPCENTER_SERVER_USER*, the default is the user running the installer.<br><br>• DUSER_INSTALL_DIR: Installation directory where packages will be installed. For *DUSER_INSTALL_DIR*, the default installation directory is */opt*.<br><br>• DINSTALL_LOG_NAME: Log file name where installation logs will be stored. This is an optional parameter and if specified no logs will be displayed on the console.If you do not specify this parameter, logs will be displayed on the console and also stored in the default log file.<br><br>DSELINUX: If the *SELinux status* is "enabled", the *Current mode* is "enforcing", and you have |

**What's next?**

- If the *SELinux status* is "enabled" and the *Current mode* is "enforcing", the **nginx** service fails to start. You should run the the following commands:

  1. Go to home directory.

  2. Run the command: `journalctl -x|grep nginx`.

  3. If the Webapp internal port (8147) is not allowed to listen, run the following commands:

     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

     - `semodule -i my-nginx.pp`

  4. Run `setsebool -P httpd_can_network_connect on`

- executed the commands mentioned in Before you begin section, you should specify this parameter and assign the value as 1. The default value is 0.

- DUPGRADE: The default value is 0. Specify this parameter and it's value as any integer other than 0 to upgrade the SnapCenter Server.

## Features enabled on Linux host during installation

The SnapCenter Server installs below software packages which can help in troubleshooting and maintaining the host system.

- Rabbitmq
- Erlang

# Register SnapCenter

If you are new to NetApp products and do not have an existing NetApp account, you should register SnapCenter to enable support.

**Steps**

1. After installing SnapCenter, navigate to **Help > About**.

2. In the *About SnapCenter* dialog box, make a note of the SnapCenter Instance, a 20 digit number that starts with 971.

3. Click https://register.netapp.com.

4. Click **I am not a registered NetApp Customer**.

5. Specify your details to register yourself.

6. Leave the NetApp Reference SN field blank.

7. Select **SnapCenter** from the Product Line drop-down.

8. Select the billing provider.

9. Enter the 20-digit SnapCenter instance ID.

10. Click **Submit**.

# Log in to SnapCenter using RBAC authorization

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.

**Before you begin**

- 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.

- If SnapCenter Server is installed on Linux host, you should log in using the user account which was used to install the SnapCenter Server.

**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.

> (i) 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.

> (i) 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<br>• UserName@UPN suffix<br><br>  For example, username@netapp.com<br>• 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.

**Result**

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.

If you want to add the plug-in host in SnapCenter running on Linux host, you should get the checksum file from the location: */opt/NetApp/snapcenter/SnapManagerWeb/Repository*.

From 6.0 release, a shortcut for SnapCenter PowerShell is created on the desktop. You can directly access the SnapCenter PowerShell cmdlets by using the shortcut.

## Log in to SnapCenter using Multi-Factor Authentication (MFA)

SnapCenter Server supports MFA for domain account, which is part of the active directory.

**Before you begin**

You should have enabled MFA. For information on how to enable MFA, see Enable Multi-factor authentication

**About this task**

- Only FQDN is supported
- Workgroup and cross domain users cannot login using MFA

**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. In the AD FS login page, enter Username and Password.

   When the username or password invalid error message is displayed on the AD FS page, you should check for the following:

   - Whether the username or password is valid

     The user account should exist in the Active Directory (AD)

   - Whether you exceeded the maximum allowed attempts that was set in AD

   - Whether AD and AD FS is up and running

## 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.