Install the SnapCenter Server using the install wizard

SnapCenter Software

NetApp
June 24, 2021

Table of Contents

Install the SnapCenter Server using the install wizard

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 cmdlet or SnapCenter CLI documentation 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

If you are using SnapCenter for the first time, the Storage Systems page is displayed, and the Get Started pane is expanded.

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 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.

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**.
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 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.