Technical Report

Security hardening guide for NetApp SnapCenter

ONTAP TME Team, NetApp

January 2024 | TR-4957

Abstract

This technical report provides guidance and configuration settings for NetApp® SnapCenter® software to help organizations meet prescribed security objectives for information system confidentiality, integrity, and availability.

LIST OF TABLES

LIST OF FIGURES

Hardening the SnapCenter Server and plug-ins running on a Windows server

Introduction

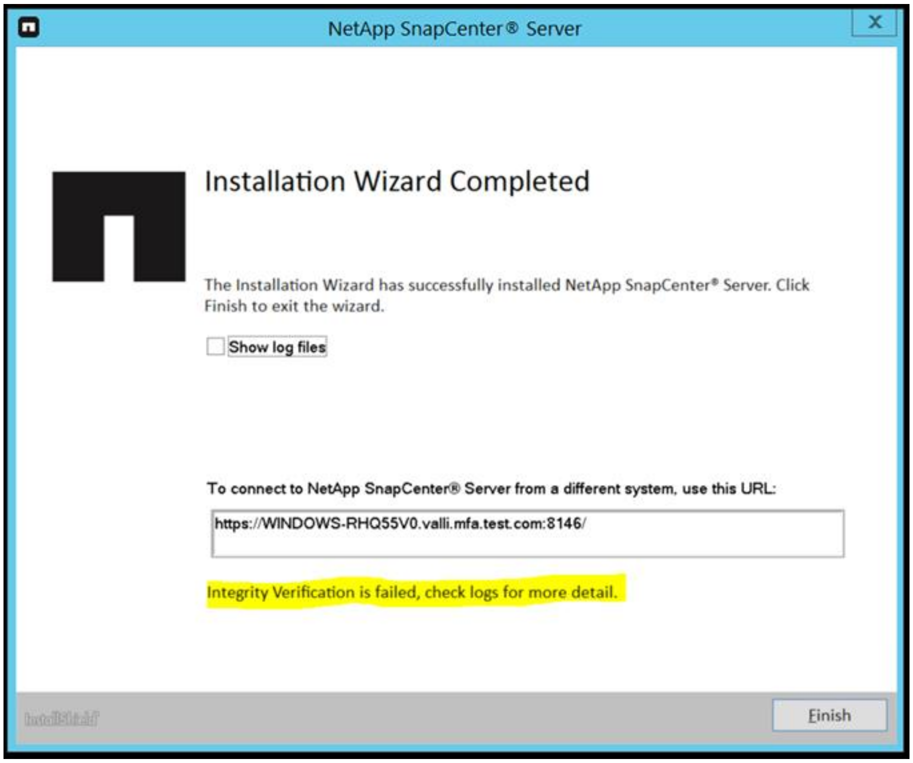
These guidelines and tools are provided to help you securely harden SnapCenter Server and plug-ins running on a Windows server with the goal of making them hack-proof. This involves eliminating or mitigating vulnerabilities. The term vulnerability refers to any software flaws and weaknesses that might occur in the implementation, configuration, design, or administration of a system. Hardening techniques typically involve locking down configurations so that you can achieve a balance between operational functionality and security. This guide helps operators and administrators with that task by using the confidentiality, integrity, and availability integral to the NetApp solution.

Installation and deployment

Integrity verification

At the end of SnapCenter Server installation, the integrity verifier performs two checks. The first check is a checksum validation of all files, including third-party and NetApp-owned files. Secondly, it performs digital signature validation for the NetApp binary files (executable and Dynamic Link Libraries (DLLs)). Any mismatches in the checksum and digital signature validation are reported at the end of the installer, as shown in the following screenshot.

Figure 1) Integrity verification.



NetApp SnapCenter® Server

Installation Wizard Completed

The Installation Wizard has successfully installed NetApp SnapCenter® Server. Click Finish to exit the wizard.

□ Show log files

To connect to NetApp SnapCenter® Server from a different system, use this URL:

https://WINDOWS-RHQ55V0.valli.mfa.test.com:8146/

Integrity Verification is failed, check logs for more detail.

Both checks are also performed when Windows Plug-ins are independently installed.

Integrity verification is performed only during fresh product installation or during product upgrades from previous releases.

Refer to the following logs for more information:

- SnapCenter log path: Temp directory `(%temp%)\IntegrityVerifier_<time_stamp>.log`
- Windows Plugin logs path: `C:\Windows\SnapCenter Plugin\<Job Name>\Integrity_Verifier.log`

If there is any discrepancy in the integrity verifier log with the error message FILE HASH NOT MATCHED or FILE HAS INVALID DIGITAL SIGNATURE, then the SnapCenter software must be reinstalled with a fresh download of the software package to avoid a file copy error. If the error persists for the same file, then contact technical support.

Note: You can exempt file not found and file busy error in case it appears.

Securing SnapCenter Server binaries

By default, SnapCenter Server creates a custom application pool during installation, and that local user account is named Internet Information Services (IIS) AppPool\\SnapCenter. To enhance the security and ease of managing SnapCenter file accessibility for other users, complete the following steps to change from the default user to the preferred domain or local workgroup user:

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.

Ports and protocols

The required ports and protocols enable communication between a SnapCenter Server and the plug-in hosts, storage systems, and other components.

- Make sure that connection and port requirements are met before installing 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:

Table 1) SnapCenter connections and ports requirements.

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 SnapCenter Server. Also used for communication from the plug-in hosts to the SnapCenter Server.
SnapCenter SMCore communication port	**8145** (HTTPS), bidirectional, customizable This port is used for communication between SnapCenter Server and the hosts where the SnapCenter plug-ins are installed.
MySQL port	**3306** (HTTPS), bidirectional This port is used for communication between SnapCenter and the MySQL repository database. You can create secure 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.
Linux or AIX plug-in hosts	**22** (SSH) This port is 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 storage VM (storage virtual machine, also known as SVM) management LIF and the SnapCenter Server.
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.
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), bidirectional **80** (HTTP), bidirectional The port is used by the Storage Abstraction Layer (SAL) for communication between the host running SnapCenter Server and the 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 the SVM.
SnapCenter Plug-in for SAP HANA Database	**3instance_number13** or **3instance_number15**, HTTP or HTTPS, bidirectional, and customizable

Type of port	Default port
vCode Spell Checkerports	For a multi-tenant 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.
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.

Authentication and login

Multifactor Authentication (MFA)

MFA was introduced in SnapCenter 4.7 to enhance the security layer. The MFA feature works with a standard Microsoft-based solution called Active Directory Federation Services (AD FS) identity manager. SnapCenter acts as the client for the AD FS manager, and the SnapCenter login page redirects to the AD FS login page. Also, AD FS is responsible for the SnapCenter user login, logout, and session timeout. Security Assertion Markup Language (SAML) 2.0 protocol is used to enable communication between the SnapCenter server and the AD FS identity manager.

To enable MFA functionality, you should perform some steps in the AD FS Server and SnapCenter Server. Before setting up the MFA, ensure the following:

- AD FS should be up and running in the respective domain.
- You should have any AD FS-supported MFA services such as Azure MFA, Cisco Duo, and so on.
- The SnapCenter and AD FS Server timestamp should be the same regardless of the time zone.
- You have procured and configured the authorized certificate authority (CA) certificate for SnapCenter Server.

A CA certificate is mandatory for the following reasons:

- The ADFS-F5 communications cannot break because the self-signed certificates are unique at the node level.
- During upgrade, repair, or disaster recovery (DR) in a standalone or high availability configuration, the self-signed certificate does not get recreated, thus avoiding MFA reconfiguration.
- Ensures IP-FQDN resolutions.

For more information on CA certificates, see Generating CA certificate CSR.

- SnapCenter supports SSO-based logins when other applications are configured in the same AD FS. In certain AD FS configurations, SnapCenter might require user authentication for security reasons depending on AD FS session persistence.
- Information regarding parameters 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.

How to enable SnapCenter MFA functionality

1. Connect to the AD FS host.
2. Download AD FS federation metadata file from `https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml`.
3. Copy the downloaded file to SnapCenter Server to enable the MFA feature.

4. Log into the SnapCenter Server as the SnapCenter Administrator user through PowerShell.
5. Using the PowerShell session, generate the SnapCenter MFA metadata file by using the `New-SmMultifactorAuthenticationMetadata -path` cmdlet. The path parameter specifies the path to save the MFA metadata file in the SnapCenter Server host.
6. Copy the generated file to the AD FS host to configure SnapCenter as the client entity.
7. Enable MFA for SnapCenter Server using the Set-SmMultiFactorAuthentication cmdlet. The path parameter specifies the location of the AD FS MFA metadata XML file, which was copied to SnapCenter Server in step 3.
8. (Optional) Check the MFA configuration status and settings by using the `Get-SmMultiFactorAuthentication` cmdlet.
9. Go to the Microsoft Management Console (MMC) and perform the following steps:

a. Click File > Add/Remove Snapin.

b. In the Add or Remove Snap-ins window, select Certificates and then click Add.

c. In the Certificates snap-in window, select the Computer account option, and then click Finish.

d. Click Console Root > Certificates – Local Computer > Personal > Certificates.

e. Right-click on the CA certificate bound to SnapCenter and then select All Tasks > Manage Private Keys.

f. On the permissions wizard, perform the following steps:

– Click Add.

– Click Locations and select the concerned host (top of hierarchy).

– Click OK in the Locations pop-up window.

– In the object name field, enter IIS_IUSRS and click Check Names and click OK. If the check is successful, click OK.

10. In the AD FS host, open AD FS management wizard and perform the following steps:

a. Right click on Relying Party Trusts > Add Relying Party Trust > Start.

b. Select the second option and browse the SnapCenter MFA Metadata file and click Next.

c. Specify a display name and click Next.

d. Choose and access control policy as required and click Next.

e. Set the settings in the next tab to default.

f. Click Finish.

SnapCenter is now reflected as a relying party with the provided display name.

11. Select the name and perform the following steps:

a. Click Edit Claim Issuance Policy.

b. Click Add Rule and click Next.

c. Specify a name for the claim rule.

d. Select Active Directory as the attribute store.

e. Select the attribute as User-Principal-Name and the outgoing claim type as Name-ID.

f. Click Finish.

12. Run the following PowerShell commands on the ADFS server.

```
Set-AdfsRelyingPartyTrust -TargetName ‘<Display name of relying party >’ -
SigningCertificateRevocationCheck None
Set-AdfsRelyingPartyTrust -TargetName ‘<Display name of relying party >’ -
EncryptionCertificateRevocationCheck None
```

13. Perform the following steps to confirm that the metadata was imported successfully.

   a. Right-click the relying party trust and select Properties.
   b. Ensure that the endpoints, identifiers, and signature fields are populated.

SnapCenter MFA functionality can also be enabled using REST APIs.

After enabling, updating, or disabling the MFA settings in SnapCenter, close all the browser tabs and reopen a browser to login again. This will clear the existing or active session cookies.

You should update the AD FS MFA metadata in SnapCenter whenever there is any modification in the AD FS server, such as an upgrade, CA certificate renewal, disaster recovery (DR), and so on.

How to update AD FS MFA metadata

1. Download the AD FS federation metadata file from `https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml`.
2. Copy the downloaded file to SnapCenter Server to update the MFA configuration.
3. Update the AD FS metadata in SnapCenter by running the following cmdlet:

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. After enabling, updating, or disabling the MFA settings in SnapCenter, close all the browser tabs and reopen a browser to log in again. This clears the existing or active session cookies.

Update SnapCenter MFA metadata

You should update the SnapCenter MFA metadata in AD FS whenever there is any modification to an AD FS server such as a repair, CA certificate renewal, DR, and so on.

In the AD FS host, open the AD FS management wizard and perform the following steps:

1. Click **Relying Party Trusts**.
2. Right-click on the relying party trust that was created for SnapCenter and click **Delete**.
3. The user-defined name of the relying party trust is displayed.
4. Enable Multifactor authentication (MFA).

See Enable Multifactor authentication for more information.

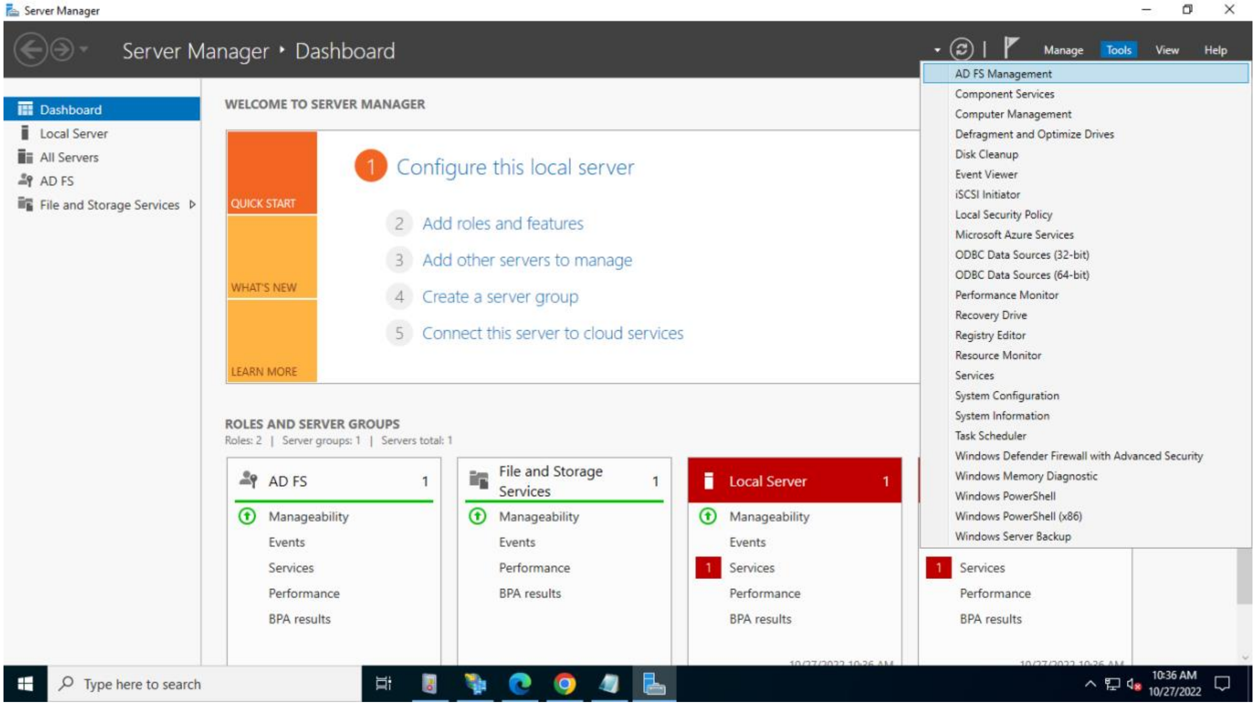
After enabling, updating, or disabling the MFA settings in SnapCenter, close all the browser tabs and reopen a browser to log in again. This clears the existing or active session cookies.

Manage multi-factor authentication (MFA) using Rest API, PowerShell, and SCCLI

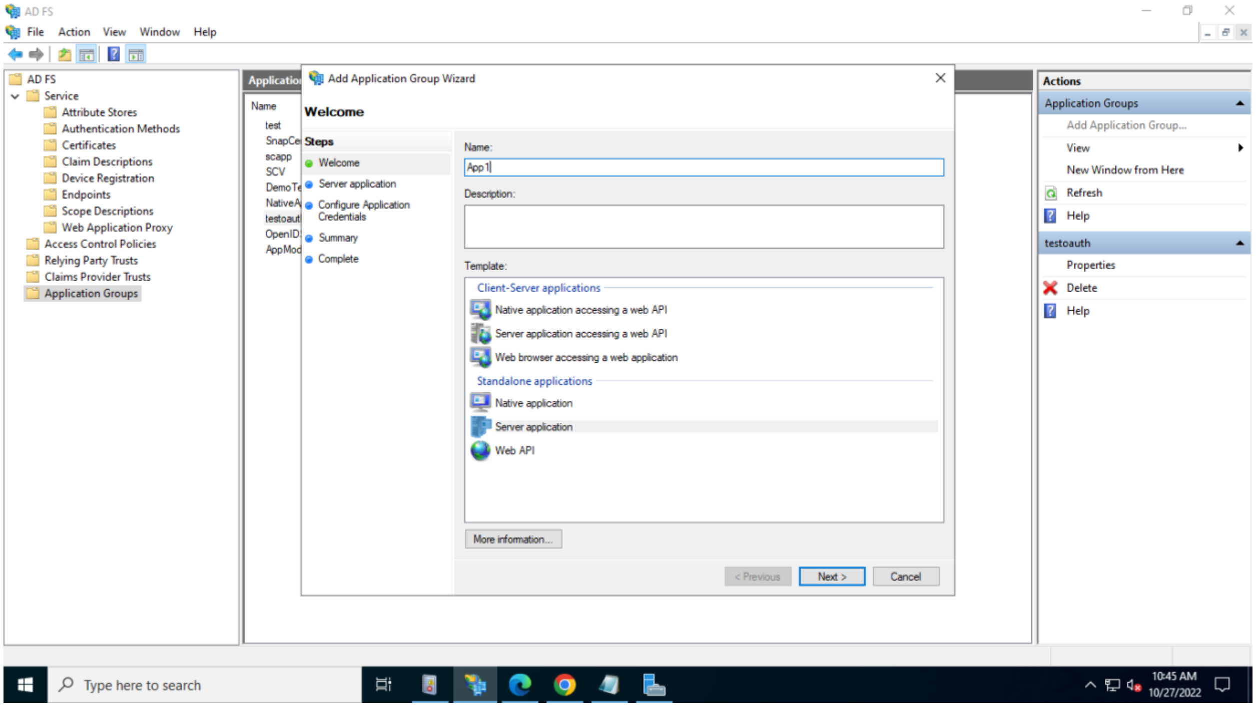
As mentioned in previous section MFA was introduced in SnapCenter 4.7 to enhance the security layer for the GUI Interface of SnapCenter. SnapCenter 4.9 extends the MFA feature to work with RestAPI, PowerShell, and SCCLI interfaces.

Setup Active Directory Federation Services (AD FS) as OAuth/OpenID Connect (OIDC)

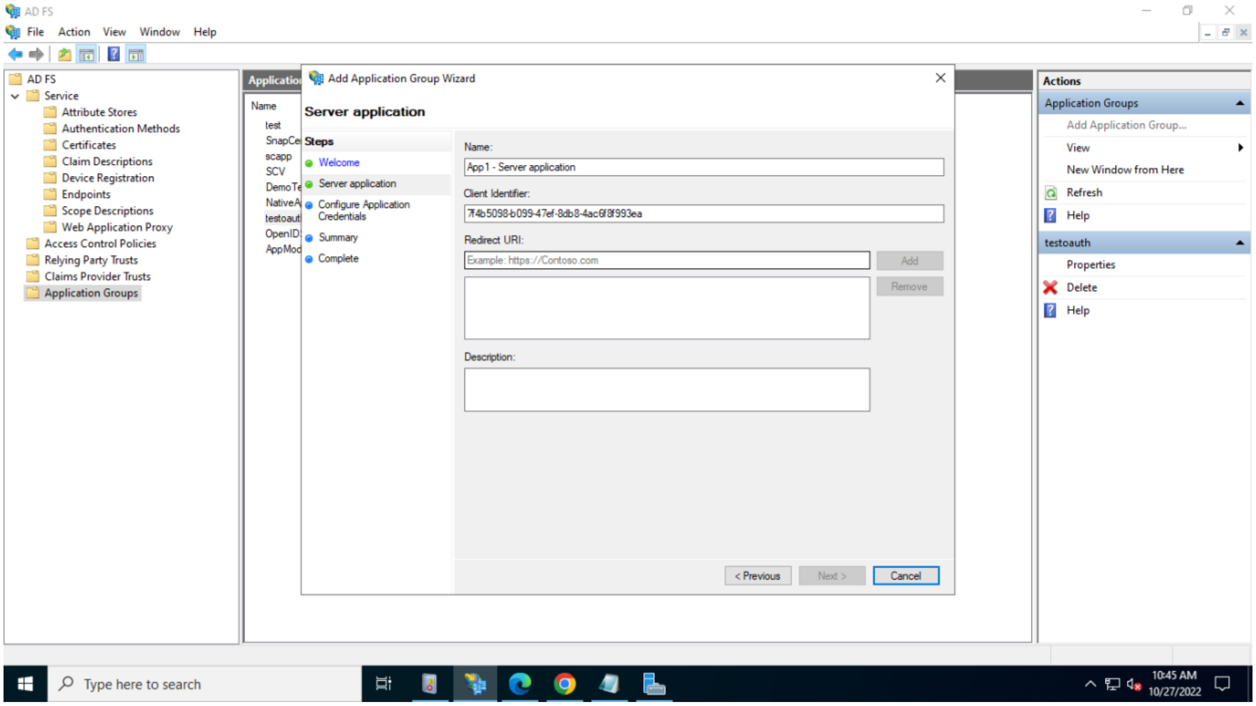
- Connect to the AD FS host, navigate to **Server Manager Dashboard->Tools->AD FS Management**.



- Navigate to **AD FS->Application Groups**. Right-click on **Application Groups** & click on **Add Application group** then enter **Application Name**. Select **Server Application** & click on **next**.



- Copy **Client Identifier**. This is your **Client ID**. Add **Callback URL** (SnapCenter Server URL) in **Redirect URL**. Click on **next**.



Add Application Group Wizard

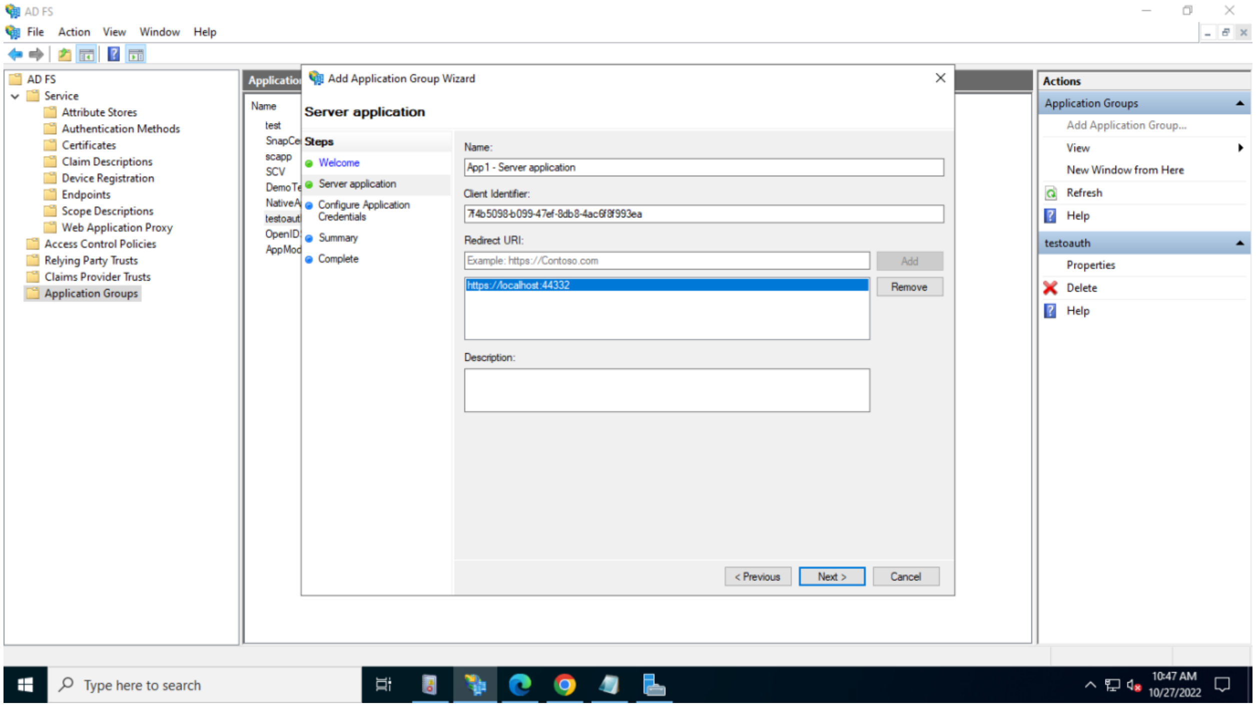
Server application

Name: App1 - Server application

Client Identifier: 7f4b5098-b099-47ef-8db8-4ac6f8f993ea

Redirect URI: Example: https://Contoso.com

Description:



Add Application Group Wizard

Server application

Name: App1 - Server application

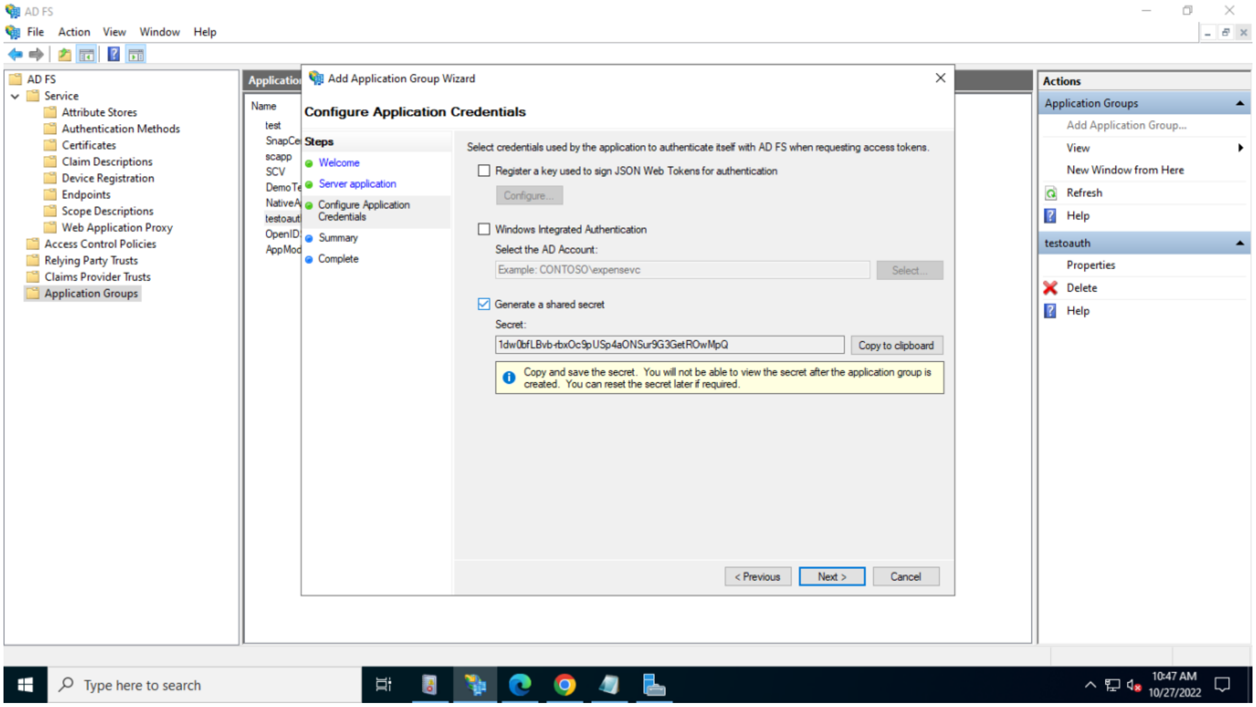
Client Identifier: 7f4b5098-b099-47ef-8db8-4ac6f8f993ea

Redirect URI: Example: https://Contoso.com

https://localhost:44332

Description:

- Click on **Generate shared secret**. Copy the **Secret value**. This is your **Client's Secret**. Click on **Next**.



Add Application Group Wizard

Configure Application Credentials

Steps
- Welcome
- Server application
- Configure Application Credentials
- Summary
- Complete

Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.

□ Register a key used to sign JSON Web Tokens for authentication

Configure...

□ Windows Integrated Authentication

Select the AD Account:

Example: CONTOSO\expensevc | Select...

☑ Generate a shared secret

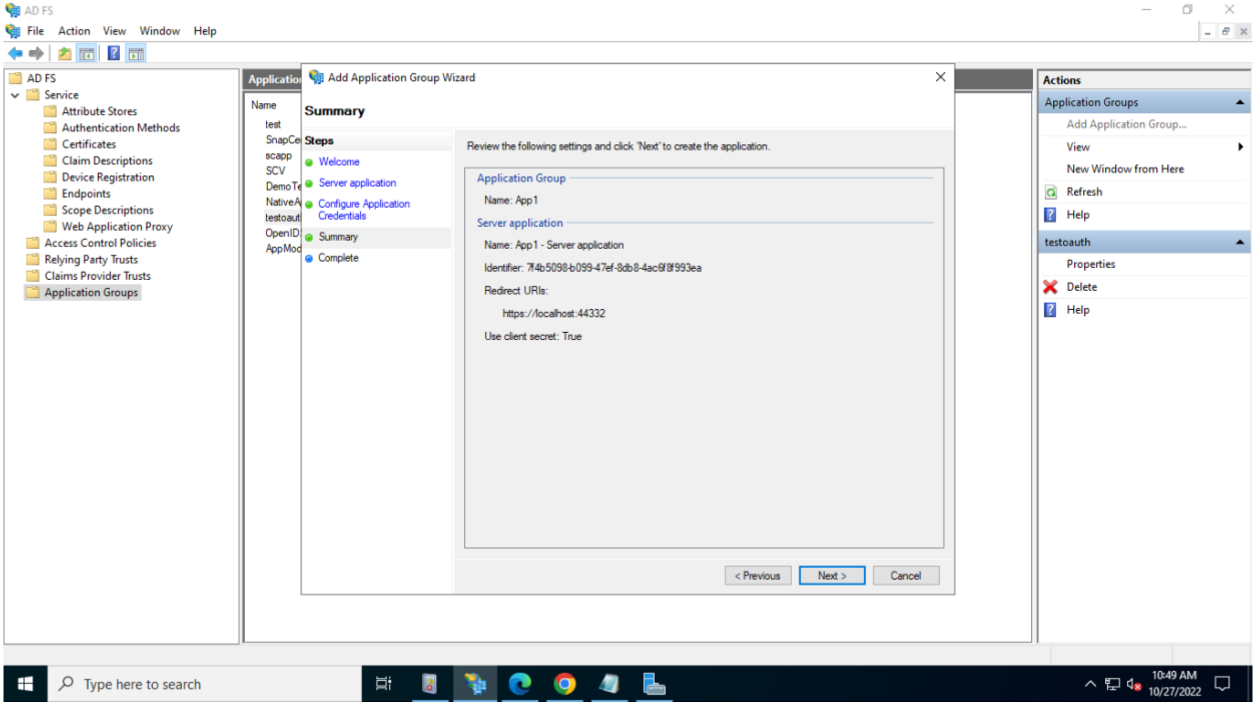
Secret:

1dw0bfLBvb-rbxOc9pUSp4aONSur9G3GetROwMpQ | Copy to clipboard

Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.

< Previous | Next > | Cancel

- On the **Summary** screen, click **Next.** On the **Complete** screen, click **Close**.



Add Application Group Wizard

Summary

Steps
- Welcome
- Server application
- Configure Application Credentials
- Summary
- Complete

Review the following settings and click 'Next' to create the application.

Application Group

Name: App1

Server application

Name: App1 - Server application

Identifier: 7f4b5098-b099-47ef-8db8-4ac6f8f993ea

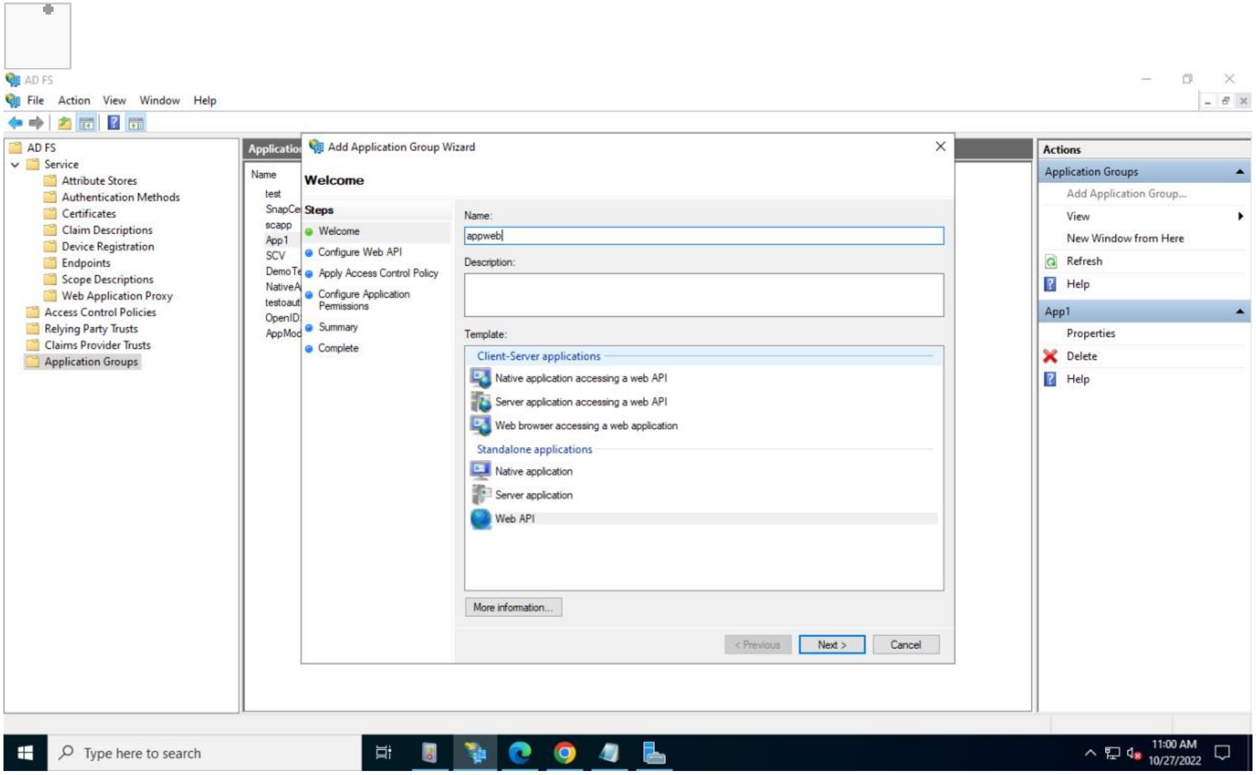
Redirect URIs:

https://localhost:44332

Use client secret: True

< Previous | Next > | Cancel

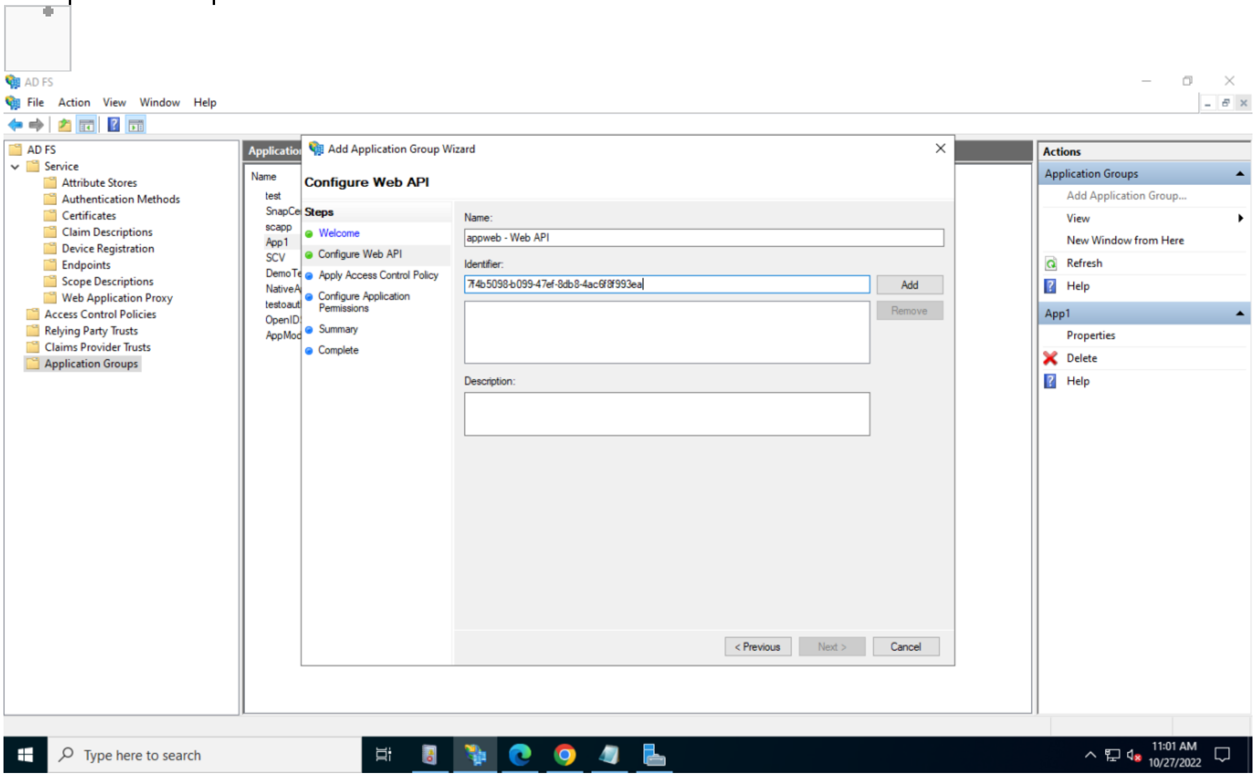
- Now, right-click on the newly added Application Group and select **Properties**.
- Click on **Add application** from **App Properties**.
- Click on the **Add application**. Then select **Web API** and click **Next**.



Name: appweb

Template: Web API

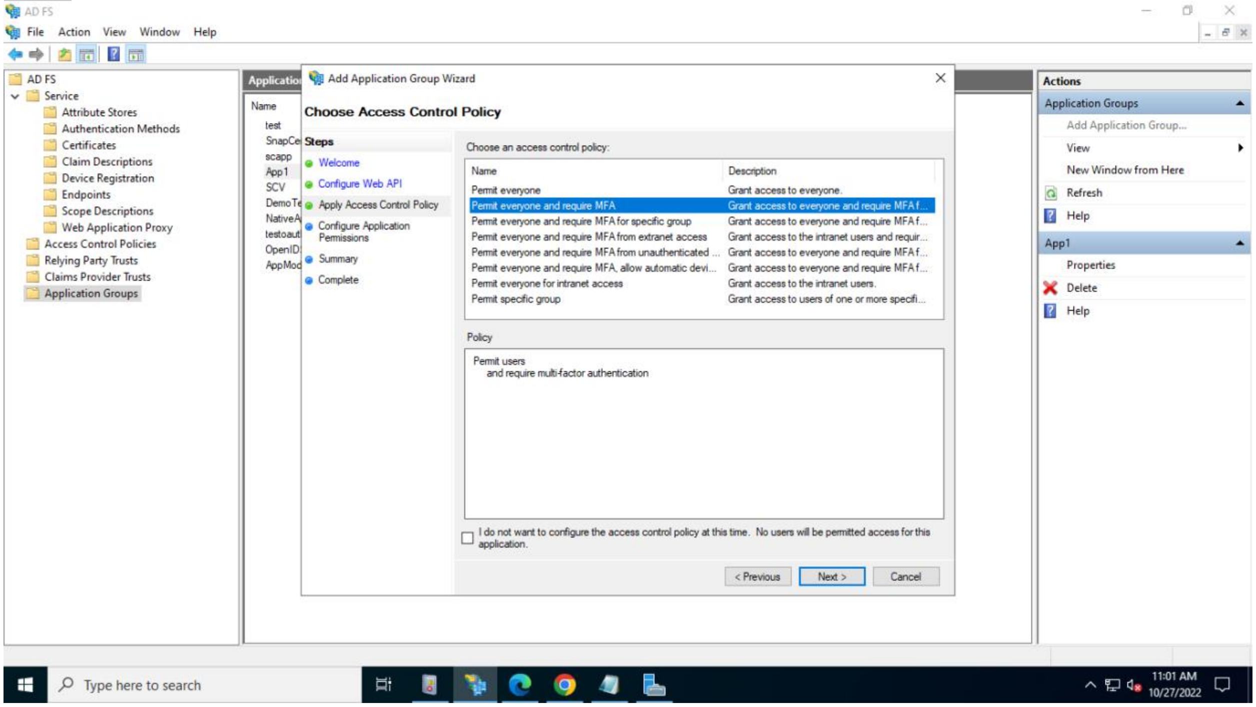
- On the **Configure Web API** screen, enter the **SnapCenter Server URL** and **Client Identifier** created in the previous step into the **Identifier** section. Click **Add**. Click **Next**.



Name: appweb - Web API

Identifier: 7f4b5098-b099-47ef-8db8-4ac6f8f993ea

- On the **Choose Access Control Policy** screen, select control policy based on your requirement (Ex: **Permit everyone and require MFA)** and click **Next**.



Add Application Group Wizard

Choose Access Control Policy

Steps
Welcome
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete

Choose an access control policy:

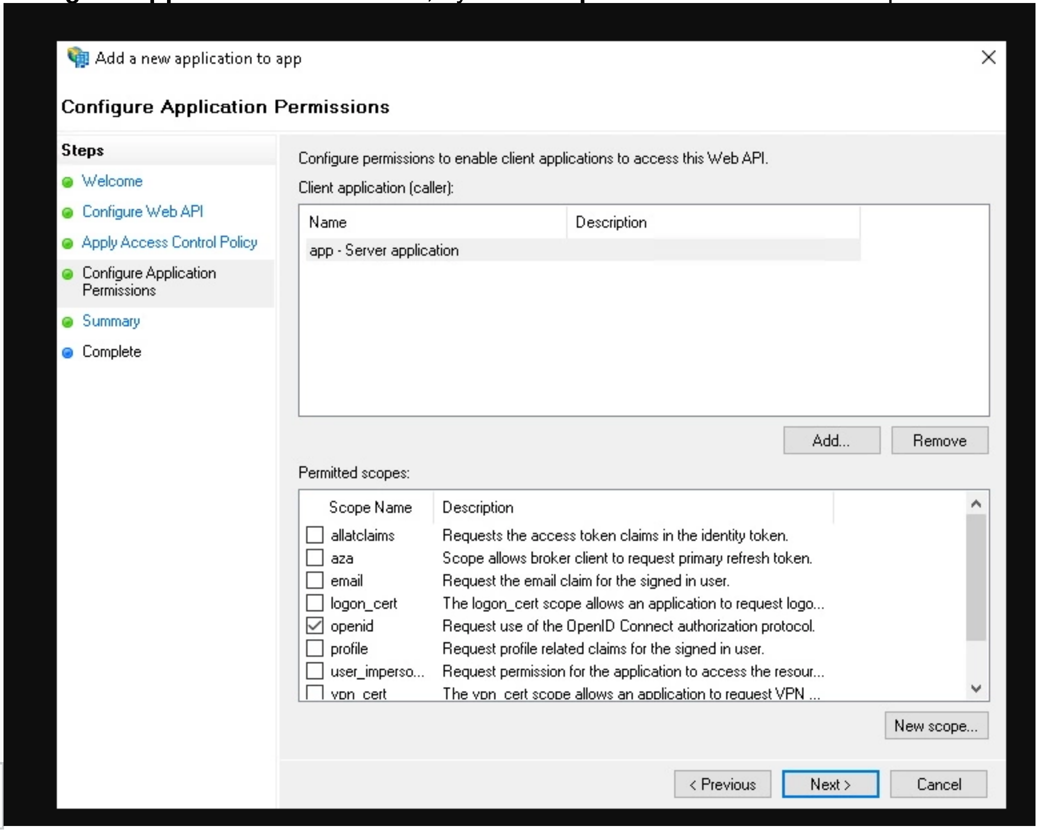
Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA f...
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA f...
Permit everyone and require MFA from extranet access	Grant access to the intranet users and requir...
Permit everyone and require MFA from unauthenticated ...	Grant access to everyone and require MFA f...
Permit everyone and require MFA, allow automatic devi...	Grant access to everyone and require MFA f...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more specifi...

Policy

Permit users
and require multi-factor authentication

□ I do not want to configure the access control policy at this time. No users will be permitted access for this application.

- On the **Configure Application Permission**, by default **openid** is selected as a scope & click on next.



Add a new application to app

Configure Application Permissions

Steps
Welcome
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete

Configure permissions to enable client applications to access this Web API.

Client application (caller):

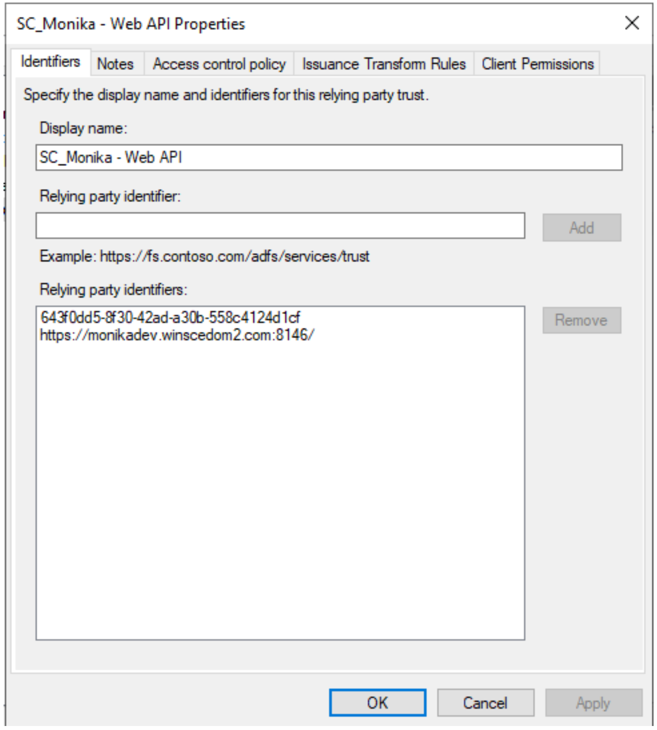
Name	Description
app - Server application	

Permitted scopes:

	Scope Name	Description
□	allatclaims	Requests the access token claims in the identity token.
□	aza	Scope allows broker client to request primary refresh token.
□	email	Request the email claim for the signed in user.
□	logon_cert	The logon_cert scope allows an application to request logo...
☑	openid	Request use of the OpenID Connect authorization protocol.
□	profile	Request profile related claims for the signed in user.
□	user_imperso...	Request permission for the application to access the resour...
□	vpn_cert	The vpn_cert scope allows an application to request VPN ...

- On the **Summary** screen, click **Next.** On the **Complete** screen, click **Close**.
- On the **Sample Application Properties** click **OK**.

- JWT token issued by an authorization server (AD FS) and intended to be consumed by the resource. The 'aud' or audience claim of this token must match the identifier of the resource or Web API.
- Edit the selected WebAPI and check that Callback URL (**SnapCenter Server URL)** and **Client Identifier** added correctly.



SC_Monika - Web API Properties

Specify the display name and identifiers for this relying party trust.

Display name:
SC_Monika - Web API

Relying party identifier:

Example: https://fs.contoso.com/adfs/services/trust

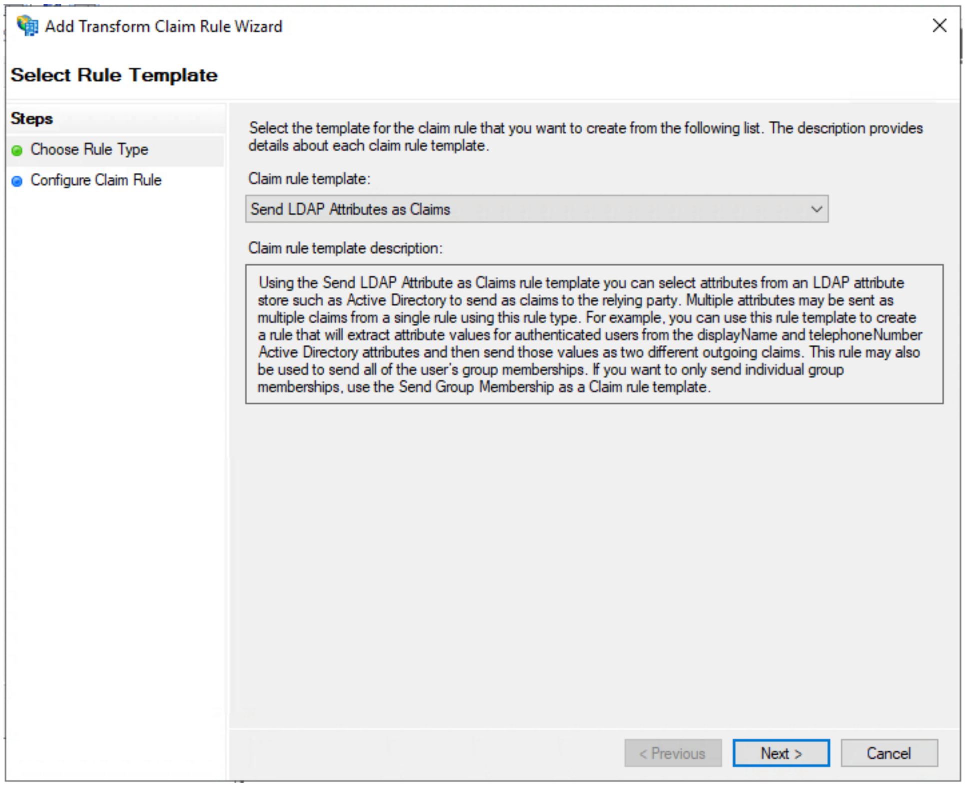
Relying party identifiers:
643f0dd5-8f30-42ad-a30b-558c4124d1cf
https://monikadev.winscedom2.com:8146/

Configure OpenID Connect (OIDC) to provide a username as claims.

OpenID Connect (OIDC) extends the OAuth 2.0 authorization protocol for use as an additional authentication protocol. You can use OIDC to enable single sign-on (SSO) between your OAuth-enabled applications by using a security token.

Open the "AD FS Management" tool located under the "Tools" menu at the top right of the Server Manager.

- Select the "Application Groups" folder item in the left sidebar.
- Now Select the **Web API** and click on **EDIT** button,
- Then go-to **Issuance Transform Rules** Tab
- Click on **Add Rule** button, Select the **Send LDAP Attributes as Claims** in the Claim rule template dropdown and click on **Next**.


Add Transform Claim Rule Wizard

Select Rule Template

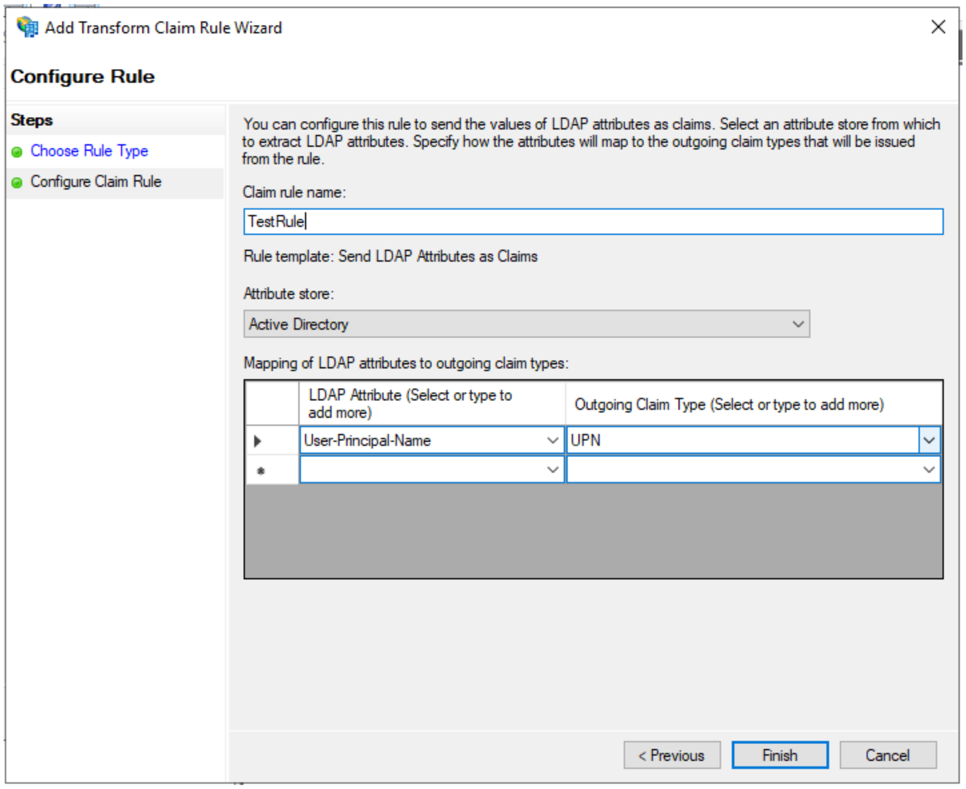
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Now Enter the **Claim rule** name, select **Active Directory** in the Attribute store dropdown, and then Select **User-Principal-Name** in the LDAP Attribute dropdown and **UPN** in the Outgoing Claim Type dropdown and then click on **Finish** button.


Add Transform Claim Rule Wizard

Configure Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: TestRule

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	UPN
*		

Automated creation of Application Group with PowerShell

Below are the high-level commands which are used to create the application group, web API and add the scope and claims.

- Create the new Application Group in AD FS.

'`ClientRoleIdentifier`' name of your application group, '`redirectURL`' valid URL for redirection after authorization

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier -
ApplicationGroupIdentifier $ClientRoleIdentifier
```

- Create the AD FS Server Application and generate the client secret.

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app" -
ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri
$redirectURL  -Identifier $identifier -GenerateClientSecret
```

- Create the AD FS Web API application and configure the policy name it should use.

```
 $identifier = (New-Guid).Guid
 Add-AdfsWebApiApplication -ApplicationGroupIdentifier
$ClientRoleIdentifier  -Name "App Web API" -Identifier $identifier -
AccessControlPolicyName "Permit everyone"
```

- Get the client id and client secret from this output because it is only shown once.

```
"client_id = $identifier"
"client_secret: "$($ADFSApp.ClientSecret)
```

- Grant the AD FS Application the allatclaims and openid permissions

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier -
 ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"
@RuleTemplate = "LdapClaims"
@RuleName = "AD User properties and Groups"
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
 , Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types =
 ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
 ";userPrincipalName;{0}", param = c.Value);
"@
```

- Write out the transform rules file

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force -
 Encoding ascii

$relativePath = Get-Item .\issueancetransformrules.tmp
```

- Name the Web API Application and define its Issuance Transform Rules using an external file.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API" -
 TargetIdentifier $identifier -Identifier $identifier,$redirectURL -
 IssuanceTransformRulesFile $relativePath
```

PowerShell Script file

Use the knowledge base article linked below to learn how to set up an Application Group in AD FS with a simple command in the command prompt or PowerShell.

Configure SnapCenter as an Application Group in ADFS

Update Access Token expiry time

- An access token can be used only for a specific combination of user, client, and resource. Access tokens cannot be revoked and are valid until their expiry.
- In Access Token by default expiry time is 60 minutes. This minimal Token lifetime is sufficient and scaled; We must provide sufficient value to avoid any ongoing business-critical jobs.
  To change the token lifetime for an application group WebApi, do the following.

```
Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName " <Web API> "
```

Note: The target name is the display name we have given for the Web API of that Application Group

Get the Bearer Token from AD FS

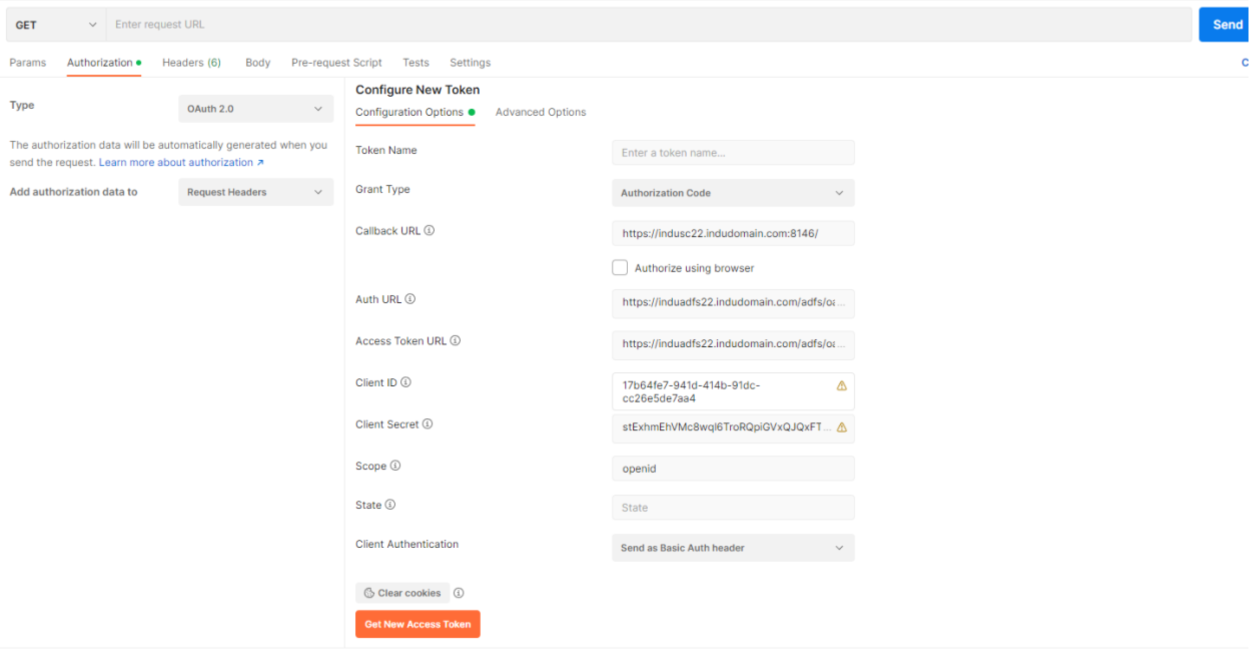
Need to fill in all the below-mentioned parameters in any REST client (like Postman) and it prompts you to fill in the concerned user credentials additionally it asks for second-factor authentication (something you have & something you are) to get the bearer token.
The validity of the bearer token is configurable from the ADFS server per application and the default validity period is 60Mins.

Field	Value
Grant type	Authorization Code
Callback URL	Enter your application's base URL if you don't have a callback URL
Auth URL	[adfs-domain-name]/adfs/oauth2/**authorize**
Access token URL	[adfs-domain-name]/adfs/oauth2/**token**
Client ID	Enter the ADFS Client ID
Client secret	Enter the ADFS Client secret
Scope	OpenID
Client Authentication	Send as Basic AUTH Header

Example: Fetch Access token through POSTMAN:

- Open the Postman Application.
- Go to the Authorization tab.

- From the dropdown select the type as OAuth 2.0 and click on Get access token.
- Add the following information from the table above.
- In the Advance Options tab, add the Resource field with the same value as the Callback URL which comes as an “aud” value in the JWT token.
- Postman starts the authentication flow and prompts you to use the access token.
- Select Add token to the header.
- Copy the only Access Token



Type: OAuth 2.0

The authorization data will be automatically generated when you send the request. Learn more about authorization ↗

Add authorization data to: Request Headers

Token Name:

Grant Type: Authorization Code

Callback URL ⓘ: https://indusc22.indudomain.com:8146/

□ Authorize using browser

Auth URL ⓘ: https://induadfs22.indudomain.com/adfs/oa...

Access Token URL ⓘ: https://induadfs22.indudomain.com/adfs/oa...

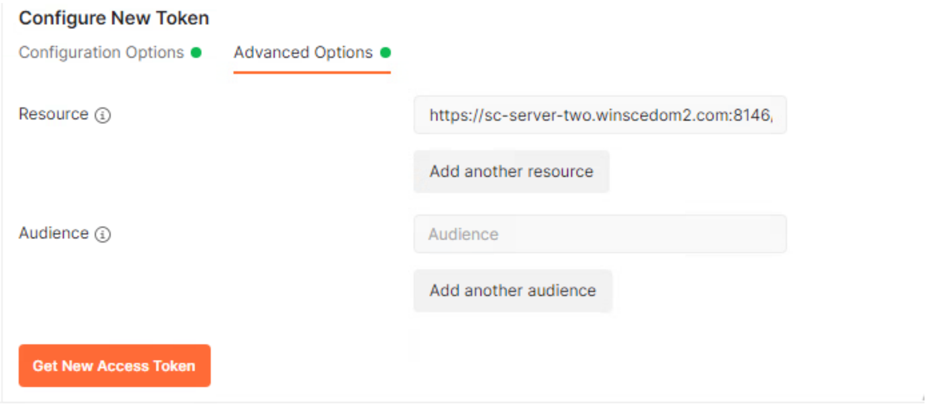
Client ID ⓘ: 17b64fe7-941d-414b-91dc-cc26e5de7aa4

Client Secret ⓘ: stExhmEhVMc8wql6TroRQpiGVxQJQxFT...

Scope ⓘ: openid

State ⓘ:

Client Authentication: Send as Basic Auth header



Resource ⓘ: https://sc-server-two.winscedom2.com:8146,

Audience ⓘ:

Configuration (SC Config & Host configuration)

SnapCenter MFA CLI Authentication

In PowerShell and SCCLI, Extended the existing cmdlet with one more field called "**AccessToken**" to use bearer token to authenticate the concerned user.

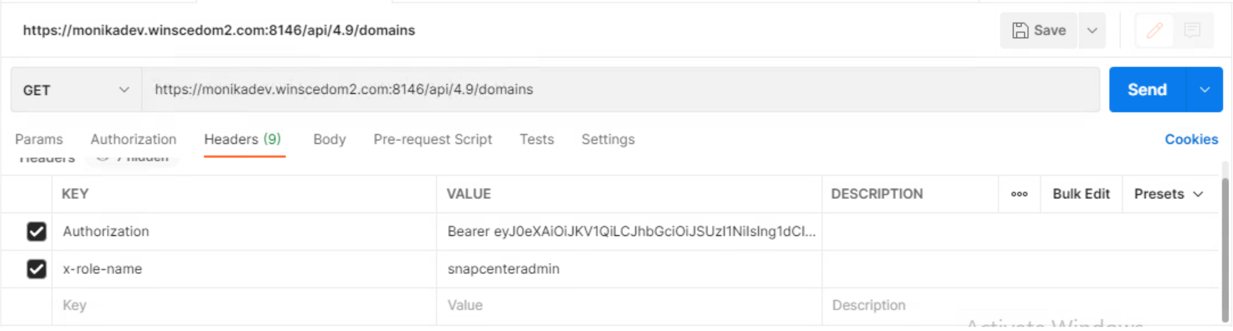
SYNTAX

```
  Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

Response: Execution of this cmdlet, create a session for the respective user to execute further SnapCenter cmdlets.

SnapCenter MFA RestAPI Authentication

Use bearer token in the format of ***Authorization, type=Bearer token*** in REST API client (like Postman or swagger) & mention user RoleName in the header to get the successful response from the SnapCenter as shown in the below images.



https://monikadev.winscedom2.com:8146/api/4.9/domains

GET https://monikadev.winscedom2.com:8146/api/4.9/domains

	KEY	VALUE	DESCRIPTION
☑	Authorization	Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI...	
☑	x-role-name	snapcenteradmin	
	Key	Value	Description

MFA Rest API Workflow

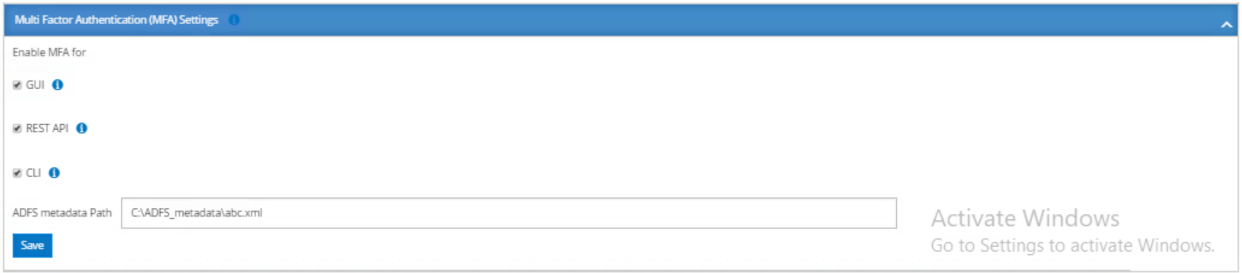
When MFA is configured with AD FS, users must authenticate by using an access (bearer) token when they access SnapCenter Application by any Rest API.
Below are the steps to get an access token and use it to authenticate subsequent requests (SnapCenter Rest API) to perform any operation.
To authenticate through AD FS MFA:

1. Need to use any Rest Client like Postman, Swagger UI or FireCamp
2. Configure the Postman to call AD FS endpoint to get the access token.
3. When a user hits the button to get an access token for an application, they are redirected to the AD FS SSO page where they must provide their AD credentials and authenticate with MFA.
    1. You are redirected to the AD FS SSO page.
    2. In the Username text box, type your username or email. Usernames must be formatted as user@domain or domain\user.
    3. In the Password text box, type your password.
    4. Click Log in.
    5. From the Sign-in Options section, select an authentication option and authenticate (Depending on customer configuration).
        1. Push — Approve the push notification that is sent to your phone.
        2. QR Code — Use the AUTH Point mobile app to scan the QR code, then type the verification code shown in the app.
        3. One-Timeime Password — Type the one-time password for your token.
4. After successful sign-in/approval. A popup will open that contains the Access, ID, and Refresh Token.
5. Need to copy this access token and will use it in the SnapCenter Rest API to perform the operation.
6. In Rest API, need to pass the access token and role name in the header section.
7. SC will validate this access token from ADFS. If it's a valid token, then SC will decode it and get the username.
8. Using the Username and Role Name, SC will authenticate the user for an API execution if it is valid then return the result else error message.

How to enable/disable SnapCenter MFA functionality for GUI, SCCLI, RestAPIs

GUI Interface

a. Log into the SnapCenter Server as the SnapCenter Administrator
b. Click Settings ->Global Settings->MultiFactorAuthentication(MFA) Settings
c. Selects the interfaces (GUI/RST API/CLI) that need to enable/disable for the MFA login.



Multi Factor Authentication (MFA) Settings

Enable MFA for

☑ GUI

☑ REST API

☑ CLI

ADFS metadata Path: C:\ADFS_metadata\abc.xml

PowerShell Interface

Run the following PowerShell/CLI commands for enabling MultiFactorAuthentication for GUI, Rest API, PowerShell, and sccli

This example syntax enables MFA for SnapCenter GUI, Rest API, PowerShell and SCCLIconfigured with specified AD FS   metadata file path.

```
C:\PS>Set-SmMultiFactorAuthentication -IsGuiMFAEnabled $true -
IsRestApiMFAEnabled    $true -IsCliMFAEnabled     $true -Path
C:\ADFS_metadata\FederationMetadata.xml
     IsGuiMFAEnabled = True
     ADFSConfigFilePath = C:\\ADFS_metadata\\FederationMetadata.xml
     SCConfigFilePath = c:\ProgramData\NetApp\SnapCenter\Package
Repository\SnapCenterMFAMetadata.xml
     IsRestApiMFAEnabled  = True
     IsCliMFAEnabled  = True
     ADFSHostName = adfs19.ad19domain.com

 - IsGuiMFAEnabled: To enable GUI MFA Login. Value-> $true/$false
 - IsRestApiMFAEnabled: To enable RestAPI MFA Login. Value-> $true/$false
 - IsCliMFAEnabled: To enable PowerShell and sccli MFA Login. Value->
$true/$false
 -Path - The path parameter specifies the location of the AD FS MFA metadata
XML file.
```

Check the MFA configuration status and settings by using the GetSmMultiFactorAuthentication cmdlet.

This example syntax gets the MFA configuration of the SnapCenter GUI, Rest API, PowerShell and SCCLI.

```
C:\PS>Get-SmMultiFactorAuthentication

    IsGuiMFAEnabled = true
```

```
     ADFSConfigFilePath = C:\\ADFS_metadata\\FederationMetadata.xml
     SCConfigFilePath = c:\ProgramData\NetApp\SnapCenter\Package
      Repository\SnapCenterMFAMetadata.xml
     IsRestApiMFAEnabled  = false
     IsCliMFAEnabled  = false
     ADFSHostName = adfs19.ad19domain.com
```

SCCLI Interface

```
# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -
IsRESTAPIMFAEnabled true -IsCliMFAEnabled true  -Path
"C:\ADFS_metadata\abc.xml"
  INFO: The command 'Set-SmMultiFactorAuthentication' executed successfully.
```

```
# sccli Get-SmMultiFactorAuthentication
 IsGuiMFAEnabled | IsRestApiMFAEnabled | IsCliMFAEnabled |
ADFSConfigFilePath    | SCConfigFilePath | ADFSHostName       |
false     | false      | true      | C:\ADFS_metadata\abc.xml |        | win-
adfs-sc49.winscedom2.com  |
```

REST APIs.

a. Run the following post API for enabling MultiFactorAuthentication for GUI, Rest API, PowerShell, and sccli

Parameter	Value
Requested URL	/api/4.9/settings/multifactorauthentication
HTTP method	Post

Request Body	{
	  "IsGuiMFAEnabled": false,
	  "IsRestApiMFAEnabled": true,
	  "IsCliMFAEnabled": false,
	  "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml"
	}

Response Body	{
	  "MFAConfiguration": {
	    "IsGuiMFAEnabled": false,
	    "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml",
	    "SCConfigFilePath": null,
	    "IsRestApiMFAEnabled": true,
	    "IsCliMFAEnabled": false,
	    "ADFSHostName": "win-adfs-sc49.winscedom2.com"
	  }
	}

b. Check the MFA configuration status and settings by using the below get API .

Parameter	Value
Requested URL	/api/4.9/settings/multifactorauthentication
HTTP method	Get

Response Body	{
	"MFAConfiguration": {
	"IsGuiMFAEnabled": false,
	"ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml",
	"SCConfigFilePath": null,
	"IsRestApiMFAEnabled": true,
	"IsCliMFAEnabled": false,
	"ADFSHostName": "win-adfs-sc49.winscedom2.com"
	}
	}

Certificate Based Authentication

Certificate-based authentication is a security feature that improves authentication using digital certificates. Certificate-based authentication provides stronger security than traditional username/password authentication. It relies on cryptographic keys and digital certificates, making it harder for unauthorized users to impersonate valid users. Certificate based authentication verifies the authenticity of respective users who try to access the SnapCenter plug-in host. User should export the SnapCenter server certificate without private key and import it in the plugin host trusted store. This feature works on top of the two-way SSL configured systems.

Export CA certificates from the SnapCenter Server:

You should export the CA certificates from the SnapCenter Server to the plug-in hosts using the Microsoft management console (MMC).

Prerequisite : Two-way SSL should be configured.

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** > **Personal** > **Certificates**.
5. Right-click on the procured CA certificate which is used for SnapCenter Server 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 **No**, do not export the private key, and then click **Next**.
Export File Format	Make no changes; click **Next**.
File Name	Click **Browse** and specify the file path to save the certificate, and then click **Next**.
Completing the Certificate Export Wizard	Review the summary, and then click **Finish** to start the export.

Note: SnapCenter HA configurations, are not supported.

Import CA Certificate to the Windows Host Plugins

Using exported SnapCenter server CA certificate you should import the concern certificate to the SnapCenter 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** > **Personal** > **Certificates**.
5. Right-click on the folder "**Personal**", and then select **All Tasks > Import** to start the import wizard.
6. Complete the wizard, as follows:

In this wizard window…	Do the following…
Store Location	Make no changes; click **Next**.
File to Import	Select the SnapCenter server certificate which ends .cer file format.
Certificate Store	Make no changes; click **Next**.
Completing the Certificate Import Wizard	Review the summary, and then click **Finish** to start the import.

PowerShell cmdlet to enable/disable Certificate based authentication

- To enable client certificate-based authentication:

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName <<hostname>>
```

- To disable client certificate-based authentication:

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName <<hostname>>
```

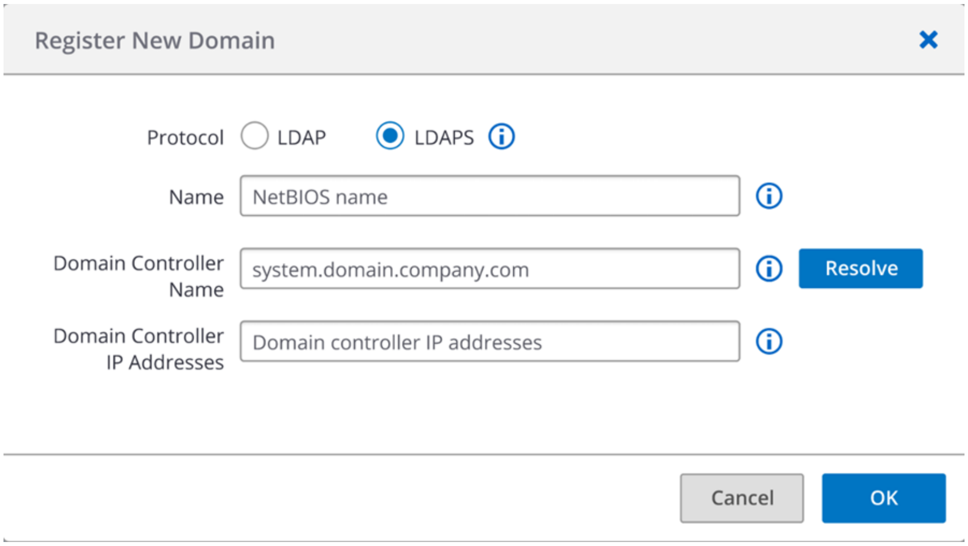
LDAPs

SnapCenter supports the LDAPS (LDAP over SSL) protocol to communicate with Windows Active Directory. An authorized CA certificate is used in the backend for secure communication.

Standalone Active Directory

- You need to explicitly select the LDAPS option to opt for a secure Active Directory connection.
- Replace the existing domain name (domain.com) user input field with the domain controller name (system.domain.company.com). This is a mandatory input to initiate communication with Active Directory.
- The domain controller name should get resolved either through DNS or an `etc/hosts` entry.
- Auto-resolved IP addresses are supported in the form of IPv4 and IPv6 (64 bit).
- Manual entry of IP addresses is not supported; they should resolve automatically. The domain controller IP address field is not editable.
- The provided domain controller name is validated against the following checks:
  - It can reach the Active Directory host or not.
  - It can detect it as the Active Directory host or non-Active Directory hosts operating on normal Windows servers.
  - It can communicate with LDAPS port or not.

Figure 2) New domain registration dialog box.



Register New Domain

Protocol ○ LDAP ● LDAPS

Name: NetBIOS name

Domain Controller Name: system.domain.company.com

Domain Controller IP Addresses: Domain controller IP addresses

High availability (HA) Active Directory

All the above-mentioned standalone steps are applicable.

- To support HA Active Directory, the user input Domain Controller Name receives input as a comma-separated value to store the multiple domain controller names as a single entry.
- Sample user input is dc01.domain.company.com,dc02.domain.company.com.
- An error is thrown for the end user if validation fails for any one of the nodes.

Custom port support

- The default LDAPS port is **636**.
- There is an option to extend the custom port support by manually adding a new key value pair in the SnapCenter Server `web.config` file.

  Note: web.config location (default path): `C:\Program Files\NetApp\SnapCenter WebApp\App_Data\Web.config`

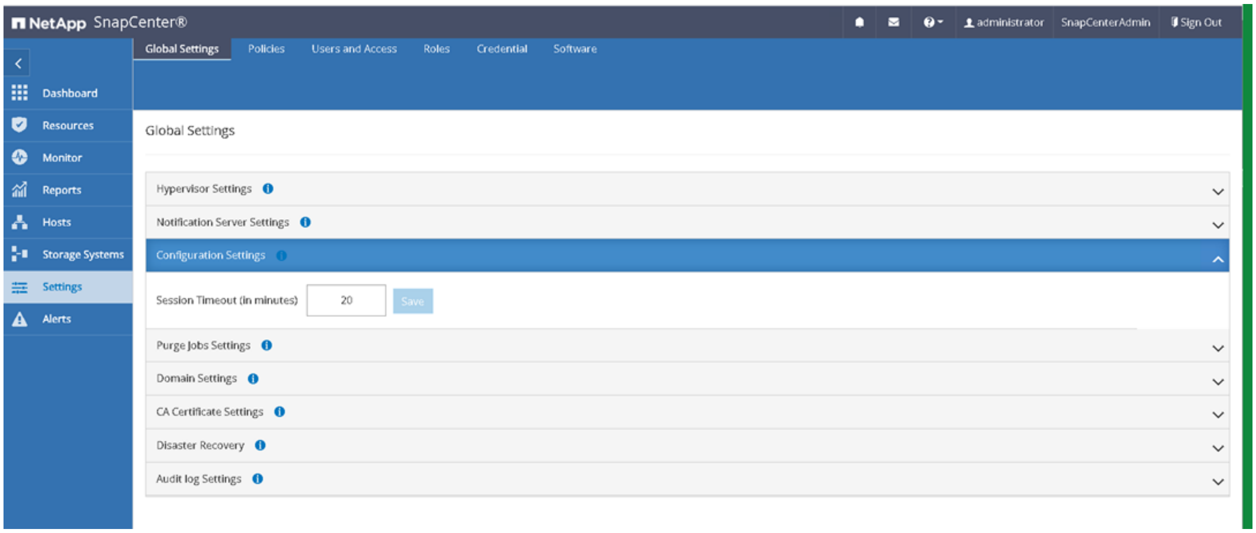
Note: key value pair: `<add key="LDAPSPort" value="3269" />` must be added in the Appsetting section.

- Updated values persist even after the SnapCenter Server is upgraded or repaired.
- LDAPS GC (Global Catalog) port is **3269**.
- The Active Directory GC Server has a copy of every object in the Active Directory tree, such as the parent domain and all sub-domain (child domains) objects.
- After configuring the custom port, you can proceed with the registration of the new domain.
- No service restart is needed after changing the default LDAPS communication port in the `web.config`.

Inactivity or timeout

The default session timeout is 20 minutes for an inactive webpage. This value is configurable.

Figure 3) SnapCenter default session timeout dialog box.



Session Timeout (in minutes) 20

Audit logs

Audit logs are generated for every SnapCenter server activity. Audit logs are secured in the default installed location `C:\Program Files\NetApp\SnapCenter WebApp\audit\`.

This section covers the configuration for audit logs from UI, its integrity check and transmission to a syslog server.

Securing audit logs

Audit logs are secured by generating digitally signed digests for every audit event to protect them from unauthorized modification. Generated digests are maintained in a separate audit checksum file, which undergoes periodic integrity checks to ensure integrity of the content.

Configuration

The configuration of audit log settings can be achieved from UI and PowerShell cmdlets. You can also enable or disable the audit integrity check schedule.

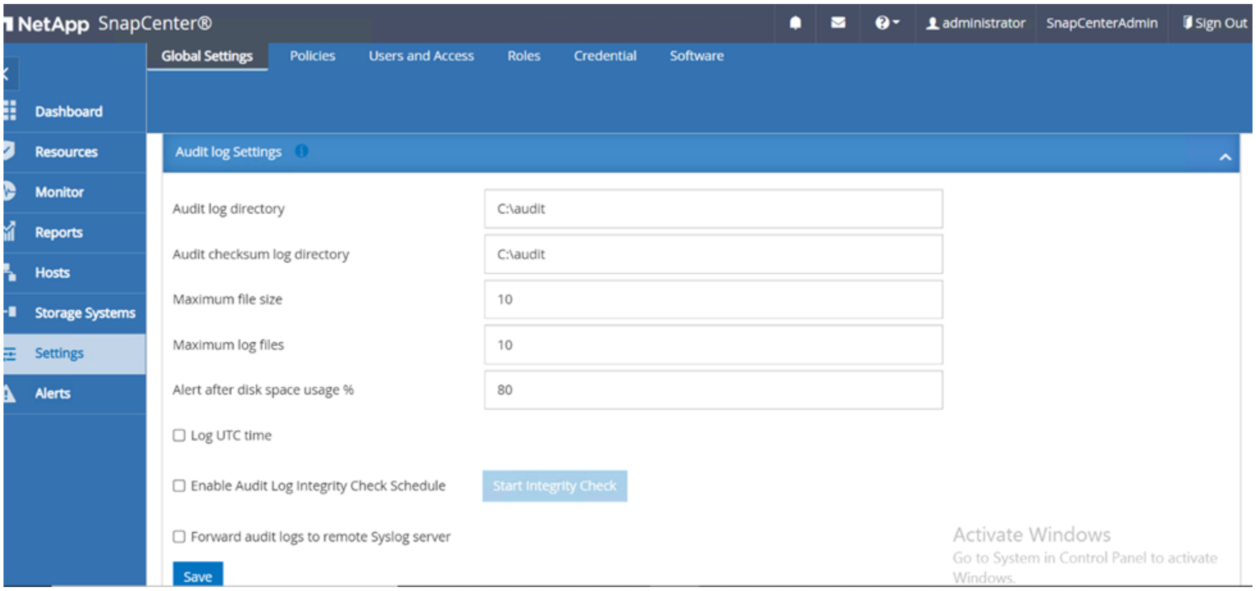
Audit log and audit checksum log directories can only be on a local drive on a SnapCenter Server. Any shared or network mounted drives are not supported.

SnapCenter alerts are raised to notify the admin when an audit integrity check is enabled and disabled.

UI

Audit settings can be configured through the UI: **SnapCenter** > **Global Settings** > **Audit Log Settings**.

Figure 4) Audit log settings.



Audit log Settings

Audit log directory: C:\audit

Audit checksum log directory: C:\audit

Maximum file size: 10

Maximum log files: 10

Alert after disk space usage %: 80

□ Log UTC time

□ Enable Audit Log Integrity Check Schedule

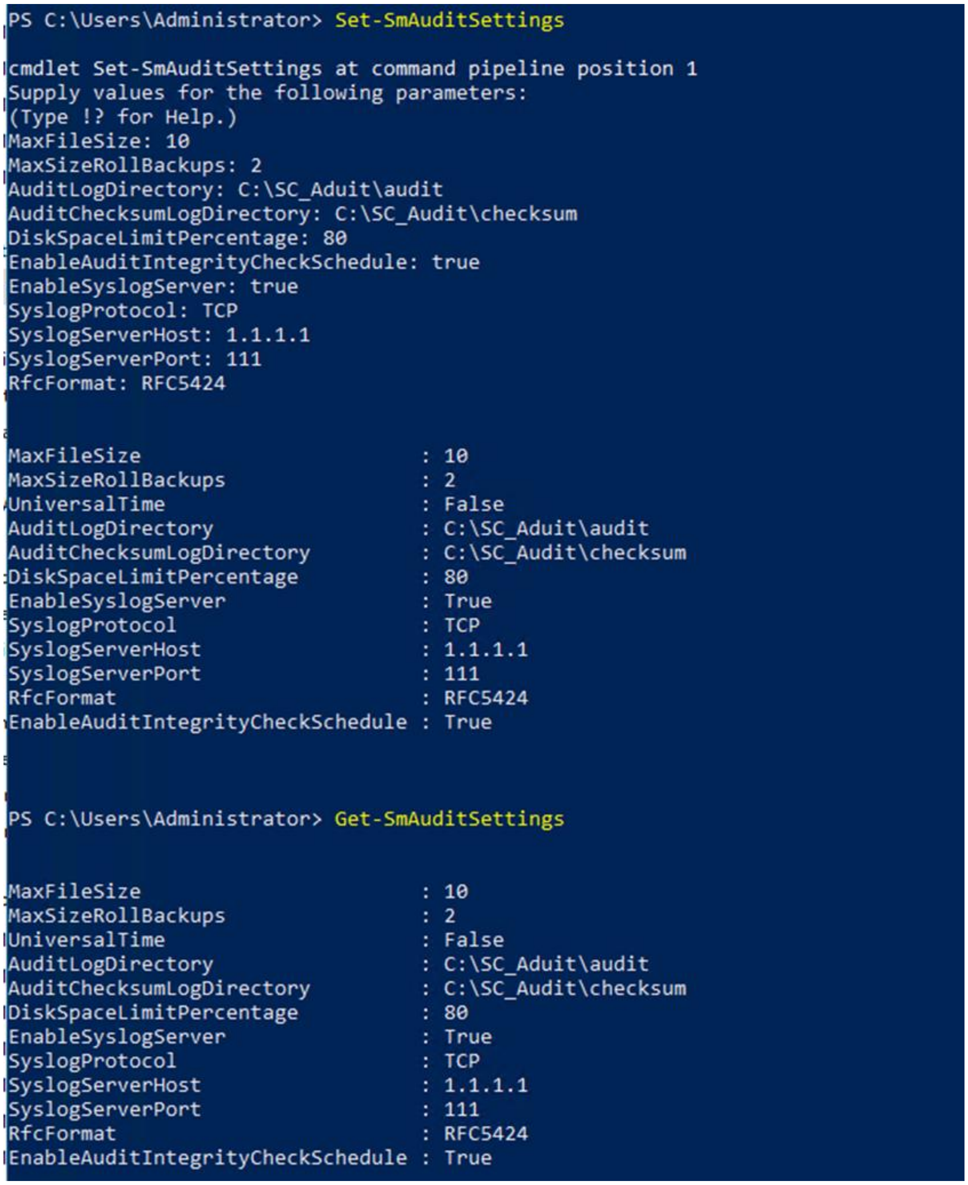
□ Forward audit logs to remote Syslog server

PowerShell cmdlets

Audit settings can be configured through the PS Cmdlets, `Get-SmAuditSettings` and `Set-SmAuditSettings`.

From UI and PS cmdlets, you can set and get audit log configurations.

```
MaxFileSize, MaxSizeRollBackups, UniversalTime, LogDirectory and DiskSpaceLimitPercentage
```



```
PS C:\Users\Administrator> Set-SmAuditSettings

cmdlet Set-SmAuditSettings at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
MaxFileSize: 10
MaxSizeRollBackups: 2
AuditLogDirectory: C:\SC_Aduit\audit
AuditChecksumLogDirectory: C:\SC_Audit\checksum
DiskSpaceLimitPercentage: 80
EnableAuditIntegrityCheckSchedule: true
EnableSyslogServer: true
SyslogProtocol: TCP
SyslogServerHost: 1.1.1.1
SyslogServerPort: 111
RfcFormat: RFC5424


MaxFileSize                       : 10
MaxSizeRollBackups                : 2
UniversalTime                     : False
AuditLogDirectory                 : C:\SC_Aduit\audit
AuditChecksumLogDirectory         : C:\SC_Audit\checksum
DiskSpaceLimitPercentage          : 80
EnableSyslogServer                : True
SyslogProtocol                    : TCP
SyslogServerHost                  : 1.1.1.1
SyslogServerPort                  : 111
RfcFormat                         : RFC5424
EnableAuditIntegrityCheckSchedule : True



PS C:\Users\Administrator> Get-SmAuditSettings


MaxFileSize                       : 10
MaxSizeRollBackups                : 2
UniversalTime                     : False
AuditLogDirectory                 : C:\SC_Aduit\audit
AuditChecksumLogDirectory         : C:\SC_Audit\checksum
DiskSpaceLimitPercentage          : 80
EnableSyslogServer                : True
SyslogProtocol                    : TCP
SyslogServerHost                  : 1.1.1.1
SyslogServerPort                  : 111
RfcFormat                         : RFC5424
EnableAuditIntegrityCheckSchedule : True
```

Note: These settings are saved as a JSON file –`\SnapCenter WebApp\Audit_LogSettings.json`.

Notifications

SnapCenter alerts can be raised to notify the administrator in the following cases:

- Audit integrity checks enabled alert
- Audit integrity checks disabled alert
- Low disk space alert
- Audit integrity check failure alert
- Audit failure alert

Email alerts

If there is an integrity verification failure, an email notification is sent to alert the SnapCenter administrator.

Transmission of audit logs

Audit logs can be securely transmitted to a syslog server to protect the confidentiality and integrity of the audit log file. By performing the following steps either in the SnapCenter UI or PowerShell, you can securely transmit the audit log.

Each audit record is transmitted to the syslog server on a real time basis to maintain a secondary copy for integrity verification purposes.

Configuration

The configuration of audit log settings can be achieved from the UI and PS cmdlets. A new field for a syslog server is added in the audit settings.

Table 2) Parameters to consider during the configuration of audit log settings.

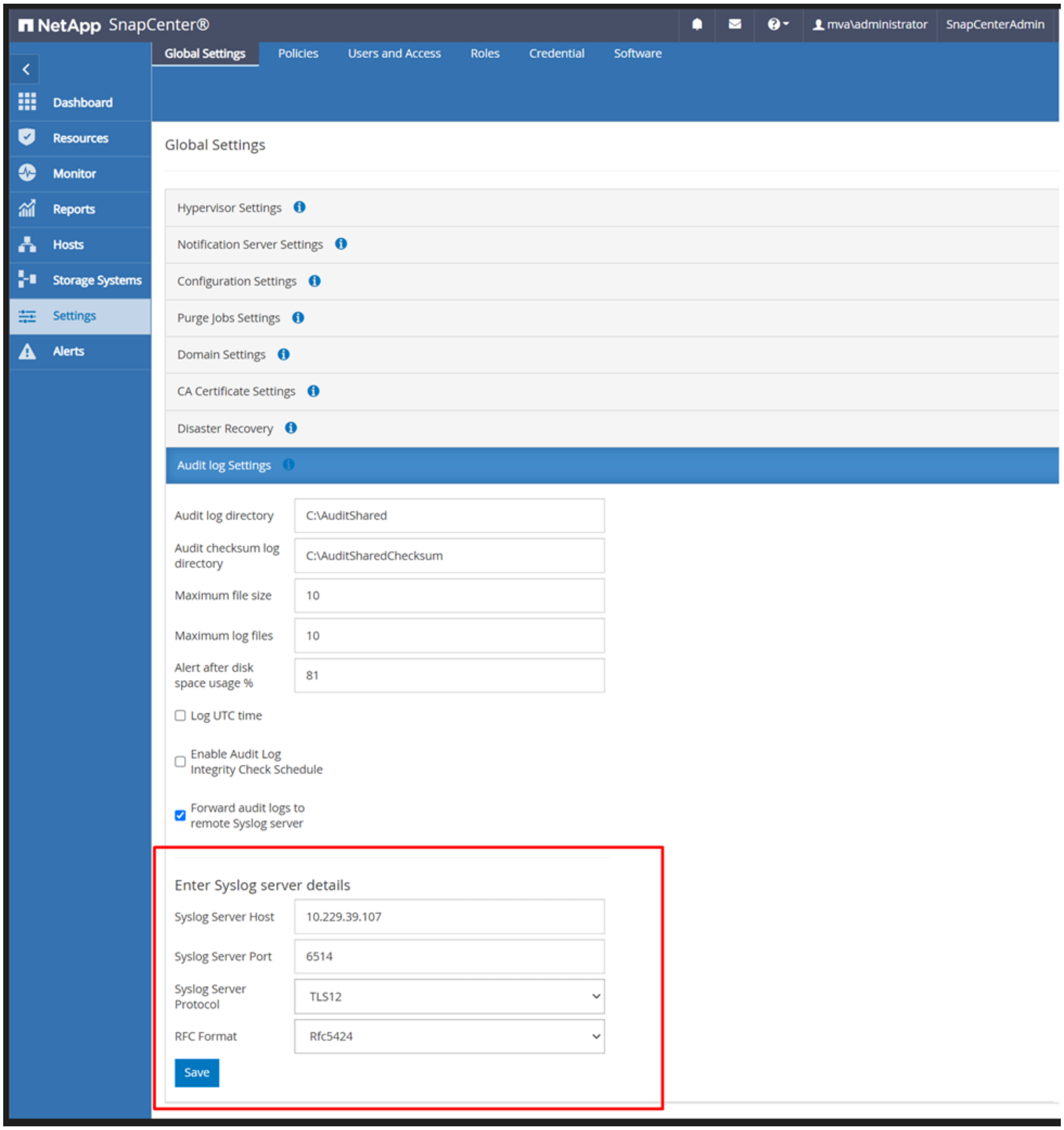
Parameter	Details
SyslogServerPort	Syslog server port (0 - 65535)
SyslogServerHost	Remote Syslog server IP
SyslogProtocol	Allowed protocols. Supported values: UDP or TCP or Transport Layer Security (TLS) 1.2 , TLS 1.3(UDP is supported only with RFC3164)
SyslogFormat	Rfc5424 or Rfc3164
EnableSyslogServer	PowerShell switch parameter to specify enable or disable forwarding logs to Syslog

Note: These settings are saved as a JSON file –`\SnapCenter WebApp\Audit_LogSettings.json`.

UI

Audit settings can be configured through the UI: **SnapCenter** > **Global Settings** > **Audit log Settings**.

Figure 5) Syslog server settings.



Audit log directory: C:\AuditShared

Audit checksum log directory: C:\AuditSharedChecksum

Maximum file size: 10

Maximum log files: 10

Alert after disk space usage %: 81

☐ Log UTC time

☐ Enable Audit Log Integrity Check Schedule

☑ Forward audit logs to remote Syslog server

Enter Syslog server details

Syslog Server Host: 10.229.39.107

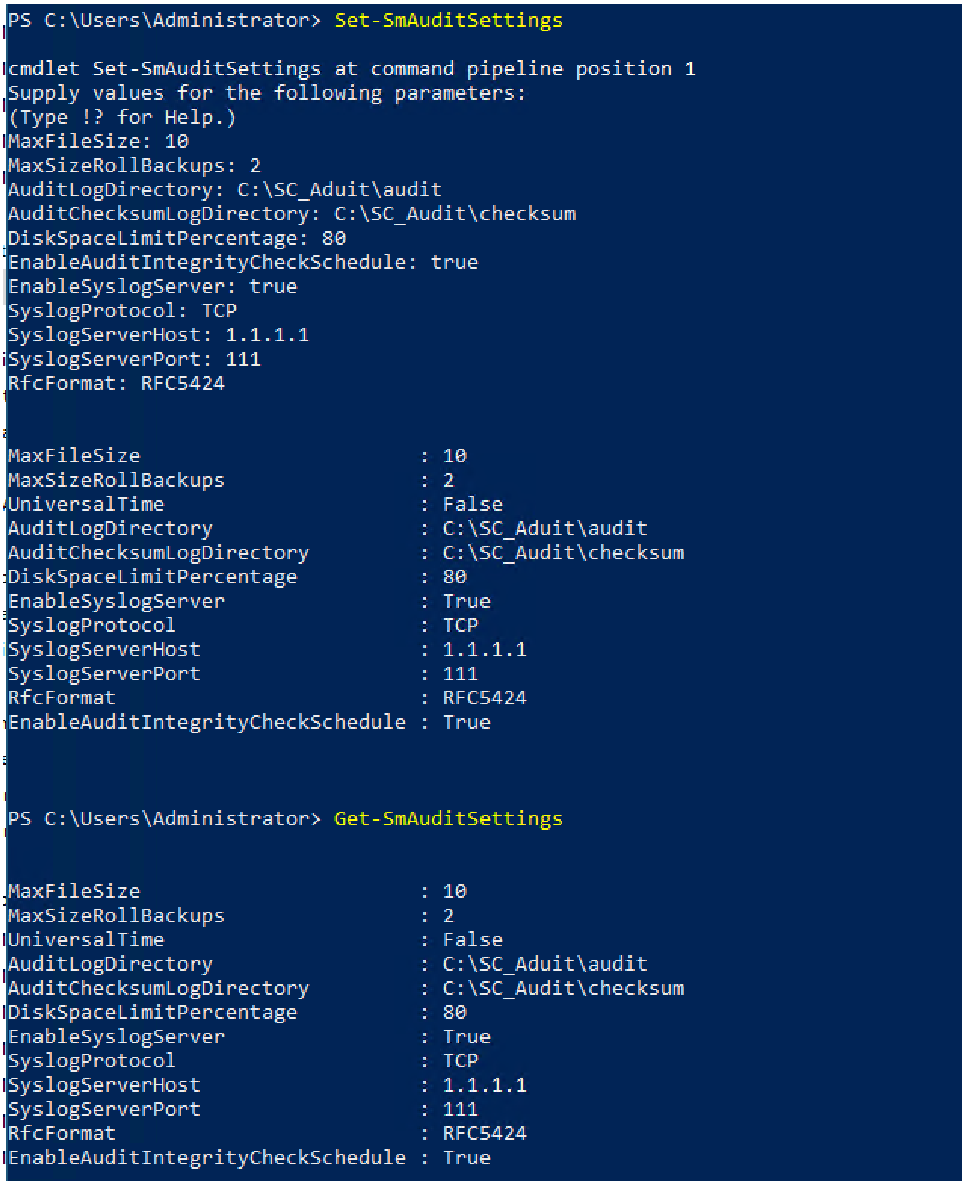
Syslog Server Port: 6514

Syslog Server Protocol: TLS12

RFC Format: Rfc5424

PowerShell cmdlets

Audit settings for the syslog server can be configured through PS cmdlets: `Set-SmAuditSettings`. Audit settings can be viewed through the PS Cmdlet: `Get-SmAuditSettings`.



```
PS C:\Users\Administrator> Set-SmAuditSettings

cmdlet Set-SmAuditSettings at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
MaxFileSize: 10
MaxSizeRollBackups: 2
AuditLogDirectory: C:\SC_Aduit\audit
AuditChecksumLogDirectory: C:\SC_Audit\checksum
DiskSpaceLimitPercentage: 80
EnableAuditIntegrityCheckSchedule: true
EnableSyslogServer: true
SyslogProtocol: TCP
SyslogServerHost: 1.1.1.1
SyslogServerPort: 111
RfcFormat: RFC5424


MaxFileSize                       : 10
MaxSizeRollBackups                : 2
UniversalTime                     : False
AuditLogDirectory                 : C:\SC_Aduit\audit
AuditChecksumLogDirectory         : C:\SC_Audit\checksum
DiskSpaceLimitPercentage          : 80
EnableSyslogServer                : True
SyslogProtocol                    : TCP
SyslogServerHost                  : 1.1.1.1
SyslogServerPort                  : 111
RfcFormat                         : RFC5424
EnableAuditIntegrityCheckSchedule : True



PS C:\Users\Administrator> Get-SmAuditSettings


MaxFileSize                       : 10
MaxSizeRollBackups                : 2
UniversalTime                     : False
AuditLogDirectory                 : C:\SC_Aduit\audit
AuditChecksumLogDirectory         : C:\SC_Audit\checksum
DiskSpaceLimitPercentage          : 80
EnableSyslogServer                : True
SyslogProtocol                    : TCP
SyslogServerHost                  : 1.1.1.1
SyslogServerPort                  : 111
RfcFormat                         : RFC5424
EnableAuditIntegrityCheckSchedule : True
```

Verified syslog servers

SnapCenter is verified with Syslog server Splunk and syslog watcher. SnapCenter supports syslog servers that use the following formats:

- BSD and RFC 5424 type
- Syslog-over-TCP-over-TLS and UDP
- TLS simple
- TLS over TCP (root certificate is required for TLS

Notifications

The following SnapCenter alerts are raised to notify the administrator in case of any failure in sending audit records to the syslog server.

- Syslog server enabled alert

- Syslog server disabled alert
- Audit logging to syslog server failure alert

Securing MySQL repository database

SnapCenter uses its own MySQL repository to store metadata. To secure and simplify the product installation, a MySQL password is auto generated with complex character sets.

Set a custom MySQL password

You do not need to reset a password and access the MySQL databases unless there is a compliance requirement. Any changes to the repository database should be done under the careful observation of technical support.

Complete the following steps to update the MySQL password, based on user-password policy recommendations.

1. Launch PowerShell as Administrator on the SnapCenter Server.
2. Type `Open-SmConnection`.
3. Enter the credentials for a user that has a SnapCenterAdmin role.
4. Type `Set-SmRepositoryPassword`.
5. Set the new password and retype the password to verify the passwords match.

Restricting the remote accessibility of the SnapCenter repository

This procedure tightens the security level of the SnapCenter repository by adding firewall rules to restrict the MySQL port inbound communications.

1. Enable the Windows firewall for the respective levels based on your system configuration: public, private, or domain.
2. Run the following PowerShell command to remove the stale firewall rules and avoid the firewall precedence problem during execution:

```
Remove-NetFirewallRule -DisplayName "Port 3306"
```

3. Determine the SnapCenter server configuration.
   – For standalone SnapCenter configurations, run the following PowerShell command:

```
New-NetFirewallRule -DisplayName "Port 3306" -Direction Inbound -LocalPort 3306 -Protocol TCP -
Action Block
```

   – For cluster SnapCenter configurations, run the following PowerShell command on each node:

```
Node1: New-NetFirewallRule -DisplayName "Port 3306" -Direction Inbound -LocalPort 3306 -Protocol
TCP -Action Allow -RemoteAddress <Node2_IP_address>
Node2: New-NetFirewallRule -DisplayName "Port 3306" -Direction Inbound -LocalPort 3306 -Protocol
TCP -Action Allow -RemoteAddress <Node1_IP_address>
```

Storage settings

This section describes the minimum permissions required to add ONTAP storage to SnapCenter and create a secure connection between the two. Once connected, SnapCenter then discovers a storage layout which hosts databases or application resources.

For SnapCenter and ONTAP communications with a CA certificate, complete the following steps:

4. Download a .pem file for a cluster or SVM from ONTAP and convert it to a .crt file (use OpenSSL).
5. Install CA certificates on the SnapCenter Server and plug-in machine or plug-in machines in the trusted root Certification Authority.

6. Enable the CA certificate on the SnapCenter server.
7. Add the following key in the `SMCoreServiceHost.exe.Config` file in the SnapCenter Server and plug-in machine:

```
<add key=”EnableSSLValicationWithPSTKCommand” value=”true” />
```

- Add the cluster or SVM details in the host file.
- Restart the SMCore service on the SnapCenter Server and plug-in machine.
- Add the cluster or SVM using a fully qualified domain name (FQDN).

Creating SVM roles with minimum privileges

There are several ONTAP CLI commands that 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\>
```

2. Repeat this command for each permission.
3. 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\>
```

4. Unlock the user.

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

ONTAP CLI commands for creating SVM roles and assigning permissions

Run the following ONTAP CLI commands to create SVM roles and assign permissions:

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

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot 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_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname “volume managed-feature” -access all`

Creating 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 administrator role to perform operations in SnapCenter. You can run several ONTAP CLI commands to create the ONTAP cluster role and assign minimum privileges.

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\>
```

2. Repeat this command for each permission.

3. 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\>
```

4. Unlock the user.

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

ONTAP CLI commands for creating cluster roles and assigning permissions

Run the following ONTAP CLI commands 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 -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all`
- `security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all`

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

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume 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`

Cipher configuration

By default, SnapCenter supports the TLS1.3, TLS1.2, TLS1.1, and TLS1.0 protocols. We have only extended support for TLS1.0 for the Windows Server 2012 OS.

Disable TLS 1.0

TLS 1.0 protocol can be disabled by running the following cmdlets in the SnapCenter Server and plug-in hosts. The parameter name is `DisableTLS1.0` to enable or disable the protocol scope.

```
Open-SmConnection -Credential <user_credentilas> -RoleName <only if user has multiple role>
Set-SmConfigSettings -Server -configSettings @{"DisableTLS1.0"="True";}
```

```
Set-SmConfigSettings -Agent -HostName <Plugin Host Name> -configSettings
@{"DisableTLS1.0"="True";}
```

Hardened cipher suites for Windows

Based on the operating system (OS) on which SnapCenter Server is running, Windows supports a certain set of SSL cipher suites to provide security across network communication.

Steps to configure SSL cipher suites for Windows Server 2008 and Windows Server 2012

1. At the command prompt, enter `gpedit.msc`, and press **Enter**. The Local Group Policy Editor is displayed.
2. Navigate to **Computer Configuration** > **Administrative Templates** > **Network** > **SSL Configuration Settings** and double-click **SSL Cipher Suite Order**.
3. In the SSL Cipher Suite Order window, click **Enabled**.
4. In the Options pane, replace the entire content of the SSL Cipher Suites text box with the following cipher list:

```
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
```

5. Restart the system.

Steps to configure SSL cipher suites for Windows Server 2016 and later

For the latest OS versions, you can directly control the cipher suites configuration through the SChannel registry key settings by means of disabling the non-recommended protocols, ciphers, hashes, and key exchanges and then enabling the recommended settings.

You can use either a manual registry key configuration or the IISCrypto tool 2.0 (or above) to select and deselect the required set of SChannel settings. The SChannel settings entry does not exist in the registry by default. You must create it forcefully to either disable or enable the required components.

Table 3) SChannel settings for Windows.

SChannel	Enable	Disable
Server protocols (client and server)	TLS 1.2, TLS 1.3	• Multi-Protocol Unified Hello • PCT 1.0 • SSL 2.0 • SSL 3.0 • TLS 1.0 • TLS 1.1
Ciphers	• AES 128 • AES 256	• NULL • DES 56 • RC2 40/128 • RC2 56/128 • RC2 128 • RC4 40/128 • RC4 56/128

SChannel	Enable	Disable
		- RC4 64/128 - RC4 128 - Triple DES 168
Hashes	- SHA 256 - SHA 384 - SHA 512	- MD5 - SHA
Key Exchanges	- Diffie-Hellam - ECDH	- PKCS

Restart the system after changing these settings.

Example 1: Configuring registry settings to enable TLS 1.2 protocol

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProv iders\SCHANNEL\Protocols\TLS
1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword: ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi ders\SCHANNEL\Protocols\TLS
1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword: ffffffff
```

Example 2: Using IISCrypto tool v2.0 or above

- IISCrypto tool v2.0 or above automatically updates the registry key settings based on the selection you choose in the tool.
- Restart the system to activate configured SChannel settings.

Certificates - one-way and mutual SSL

SnapCenter supports CA certificates for cross-communication between the server and plug-in hosts.

One-way SSL

This section of the document covers how to generate signed SSL certificates using Microsoft Certreq. It helps with the following:

- Generating a certificate signing request (CSR)
- Importing the certificate obtained from a CA using the generated CSR

The process outlined ensures that the certificate has a private key associated with it. The Microsoft Certreq tool is available by default on a Windows Server 2008 R2 system so a CSR can be generated.

Notes:

- The tool uses a configuration file to generate a certificate request.
- Make sure that you follow the complete procedure on the same server.

Create a configuration request.inf file

1. Create a configuration request.inf file by using the following content:

```
;----------------- request.inf -----------------
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=View_Server_FQDN, OU=Organizational_Unit_Name, O=Organization_Name, L=City_Name,
S=State_Name, C=Country_Name"
; replace the attributes appropriately in the above line, refer example in the next step.
KeySpec = 1
KeyLength = 2048  ; Can be 2048, 4096 or 8192 - Larger key sizes are more secure
HashAlgorithm = SHA256 ; Can be SHA256, SHA384, SHA512 - Higher values are more secure
KeyUsage = 0xA0 ; Digital Signature, Key Encipherment
```

```
MachineKeySet = TRUE  ; The key belongs to the local computer account
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
Exportable = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderType = 12
RequestType = PKCS10
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
[RequestAttributes]
; SAN= dns=FQDN_you_require&dns=other_FQDN_you_require
;-----------------------------------------------
```

2. Apply the following changes as applicable.
3. For example:

```
Subject = "CN=view.company.com , OU=IT, O=ABCCompany, L=Sunnyvale, S=California, C=US
```

4. If you are using a Subject Alternative Name (SAN), uncomment the line and update the SAN attribute with the FQDN.
5. For example:

```
SAN= dns= server1.domain.com&dns= server2.domain.com&dns= server3.domain.com&dns=
server4.domain.com&dns= server5.domain.com
```

6. Save and close the request.inf file.

Steps to generate a CSR using the configuration file

1. Open the Command Prompt by right-clicking **cmd.exe** and selecting **Run as administrator**.
2. Change the directory to the location where the request.inf file is saved.

For example:

```
cd C:\certificates
```

3. Run this command to generate a CSR file.

```
certreq.exe -new request.inf certreq.csr
```

4. Open the resulting `certreq.csr` CSR file in a text editor, copy the text of the file, or directly upload the CSR file and submit it to your CA to obtain a signed certificate from your CA.

   Note: The CA provides a signed certificate, a root CA certificate, and an intermediate CA certificate, if applicable. Different CAs have different lists of formats.

5. Save the certificate text to a new file or download the certificate named CER file `cert.cer` on the server where the certificate request was generated.
6. Save the root and intermediate CA certificates to files named `root.cer` and `intermediate.cer` on the server where the certificate request was generated. Different CAs might have a file format in either `.cer` or `.crt`.

Import the signed certificate

1. Open the command prompt by right-clicking on **cmd.exe** and selecting **Run as administrator**.
2. Change the directory to the location where the `cert.cer` file is saved.
3. For example:

```
cd C:\certificates
```

4. Run this command to import the signed certificate:

```
certreq.exe -accept -machine root.cer
certreq.exe -accept -machine intermediate.cer
certreq.exe -accept -machine cert.cer
```

5. After the import is completed, the certificate is imported into the local machine's personal certificate store.
6. Open the MMC as an administrator.
7. Click **File** > **Add or Remove Snap-ins** or press **CTRL**+**M**.
    a. In the available snap-ins, select the certificates and click **Add**. Make sure that you select the computer account.
    b. Click **Next** and then **Finish**.
8. Double-click the folder **Personal** > **Certificates** and select the recently imported SSL Certificate by its name.
9. Right-click the recently procured CA certificate, select **All Tasks** > **Export,** and continue the wizard by selecting the option **Export with Private Key**. Then proceed with the default option.
10. In the MMC wizard, right-click the **Trusted Root Certification Authorities** folder and select **All Tasks** > **Import**.
    a. The importing certificate should be bundled with the private key (supported formats are `*.pfx`, `* p12`, `*.p7b`). If the private key is not bundled with the certificate, then you cannot use it for the SnapCenter Server.
    b. Enter the password for the private key and proceed with the default option. Then click Finish.

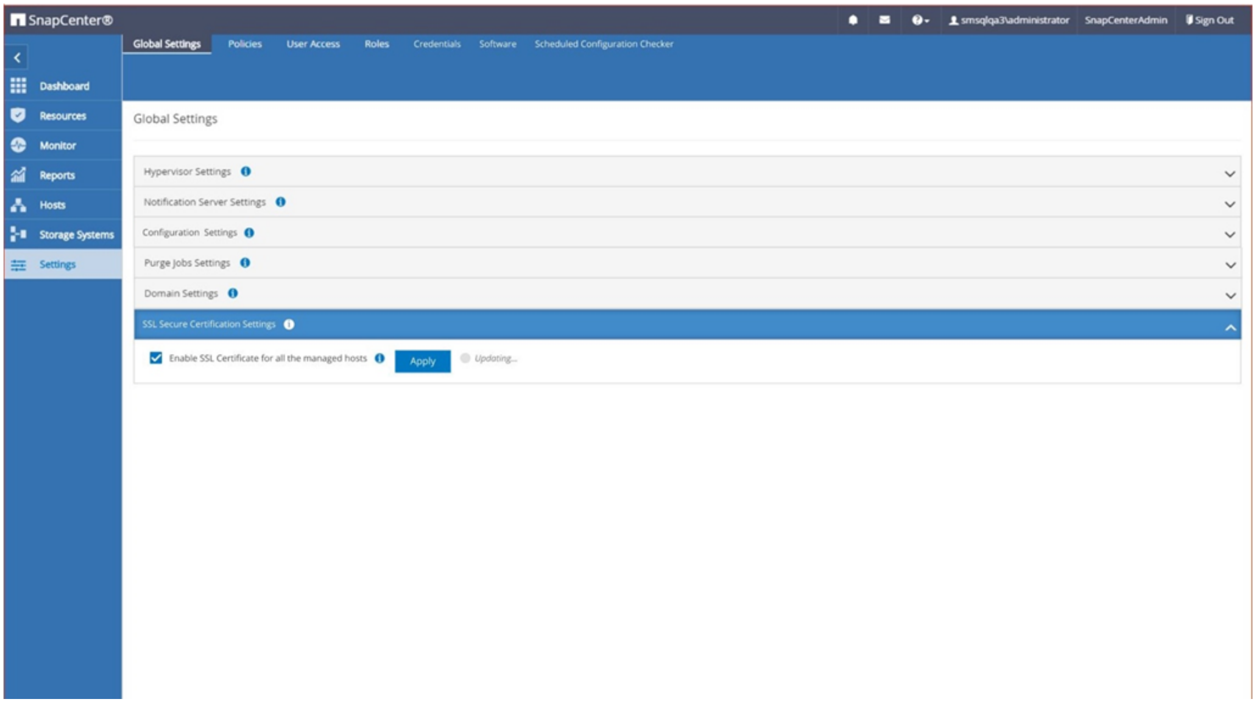
Repeat steps 8 and 9 for the root and intermediate CA certificates; the private key option is not available for these certificates.

Enable a CA certificate for the SnapCenter Server

The Certificate Authority is a trusted entity that issues Secure Sockets Layer (SSL) certificates. These digital certificates are data files used to cryptographically link an entity with a public key. SnapCenter has added support for server and plug-in cross-communication using authorized CA certificates. All HTTPS calls are validated based on secure SSL standards.

In the GUI, there is an option (check box) on the global settings page to enable the CA certificate feature at the SnapCenter level, and it shows the lock pad icon in the managed host page to represent the security level of each host.

Figure 6) SSL Secure certification settings.



Global Settings

- Hypervisor Settings
- Notification Server Settings
- Configuration Settings
- Purge Jobs Settings
- Domain Settings
- SSL Secure Certification Settings

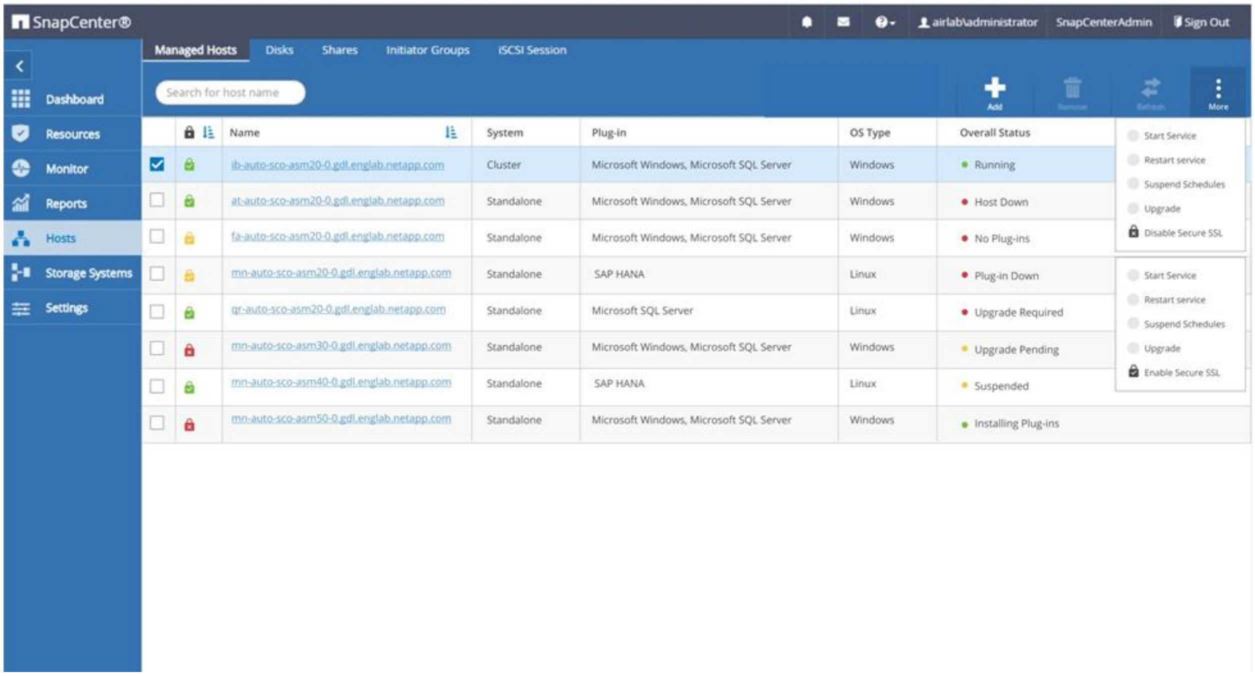
☑ Enable SSL Certificate for all the managed hosts [Apply] Updating...

Enable CA certificate for SnapCenter Plug-ins

The managed host page kebab menu contains an additional option to enable or disable the SSL secure validation for the plug-in host level.

You need to enable this option after configuring the CA certificates in the plug-in host.

Figure 7) Plug-in host security status



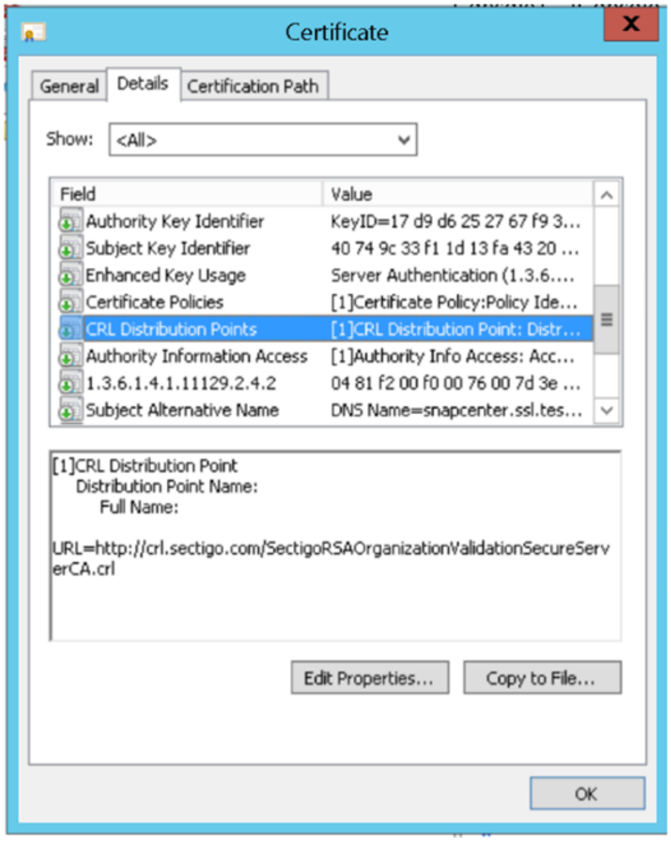
	🔒	Name	System	Plug-in	OS Type	Overall Status
☑	🔒	ib-auto-sco-asm20-0.gdl.englab.netapp.com	Cluster	Microsoft Windows, Microsoft SQL Server	Windows	● Running
□	🔒	at-auto-sco-asm20-0.gdl.englab.netapp.com	Standalone	Microsoft Windows, Microsoft SQL Server	Windows	● Host Down
□	🔒	fa-auto-sco-asm20-0.gdl.englab.netapp.com	Standalone	Microsoft Windows, Microsoft SQL Server	Windows	● No Plug-ins
□	🔒	mn-auto-sco-asm20-0.gdl.englab.netapp.com	Standalone	SAP HANA	Linux	● Plug-in Down
□	🔒	qr-auto-sco-asm20-0.gdl.englab.netapp.com	Standalone	Microsoft SQL Server	Linux	● Upgrade Required
□	🔒	mn-auto-sco-asm30-0.gdl.englab.netapp.com	Standalone	Microsoft Windows, Microsoft SQL Server	Windows	● Upgrade Pending
□	🔒	mn-auto-sco-asm40-0.gdl.englab.netapp.com	Standalone	SAP HANA	Linux	● Suspended
□	🔒	mn-auto-sco-asm50-0.gdl.englab.netapp.com	Standalone	Microsoft Windows, Microsoft SQL Server	Windows	● Installing Plug-ins

Certificate revocation list (CRL)

The following procedure describes how to update the CRL file for the SnapCenter CA certificate.

Mode: UI

1. Get the latest CRL file.
2. Open the MMC as an administrator.
3. Click **File** > **Add or Remove Snap-ins** or **Ctrl** + **M**.
4. In the available snap-ins, select **Certificates** and click **Add**. Also, make sure that you select **Computer Account**.
5. Select **Next** and then **Finish**.
6. In the folder Trusted Root Certification Authorities, double-click your server certificate.
7. In the Certificate dialog box, select the **Details** tab and select **CRL Distribution Points**.



Field	Value
Authority Key Identifier	KeyID=17 d9 d6 25 27 67 f9 3...
Subject Key Identifier	40 74 9c 33 f1 1d 13 fa 43 20 ...
Enhanced Key Usage	Server Authentication (1.3.6....
Certificate Policies	[1]Certificate Policy:Policy Ide...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
1.3.6.1.4.1.11129.2.4.2	04 81 f2 00 f0 00 76 00 7d 3e ...
Subject Alternative Name	DNS Name=snapcenter.ssl.tes...

```
[1]CRL Distribution Point
     Distribution Point Name:
          Full Name:

URL=http://crl.sectigo.com/SectigoRSAOrganizationValidationSecureServ
erCA.crl
```

8. Copy the URL and download the latest CRL file.

Configure a CA Certificate for the SnapCenter Server and Windows host

Mode: UI

1. In Certificates snap-in in the left pane of the MMC, expand the **Certificates (Local Computer)** node.
2. Expand the **Trusted Root Certification Authorities** node, right-click the **Certificates** subfolder, select **All Tasks**, and then select **Import**.
3. In the Certificate Import Wizard, on the Welcome page, select **Next**.
4. On the File to Import page, select **Browse**.

5. In the File Type field, select **Certificate Revocation List** (*.`crl`).
6. Browse to the location of the `.crl` file, select the file, and select **Open**.
7. On the File to Import page, select **Next**.
8. On the Certificate Store page, accept the default selection, and then select **Next**.
9. Upon completing the Certificate Import Wizard page, select **Finish.**
10. Select the **Trusted Root Certificate Authorities** node and then **refresh snap-in**.

A Certificate Revocation List folder that contains the new `.crl` file is created.

Configure CRL for SnapCenter custom plug-ins on a Windows host

SnapCenter custom plug-ins search for CRL files in a preconfigured directory. The default directory for CRL files for SnapCenter Custom Plug-ins is `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl`.

1. Modify and update the default directory in the `agent.properties` file against the key `CRL_PATH`.
2. Place more than one CRL file in this directory.

Incoming certificates are verified against each CRL.

Configure CRL for SnapCenter plug-in for VMware vSphere

The SnapCenter plug-in for VMware vSphere looks for the CRL files in a preconfigured directory. The default directory of the CRL files for the SnapCenter plug-in for VMware vSphere is `/opt/netapp/config/crl`. You can place more than one CRL file in this directory. The incoming certificates are verified against each CRL.

Two-way SSL (mutual authentication)

Along with the above one-way SSL steps, you can complete the following steps to enable mutual authentication between the SnapCenter Server and plug-in communication. This feature was introduced from SnapCenter 4.9 onwards.

Prerequisite*:*

- You should have generated the CA Certificate CSR file with the minimum supported key length of 3072.
- The CA certificate should support server authentication and client authentication.
- You should have a CA certificate with private key and thumbprint details.
- You should have enabled the one-way SSL configuration.
  For more details, see Configure CA certificate section.
- You must have enabled two-way SSL communication on all the plug-in hosts and the SnapCenter Server.

Note: Environment with some hosts or server not enabled for two-way SSL communication is not supported.

Steps

1. To bind the port, perform the following steps on SnapCenter Server host for SnapCenter IIS web server port 8146 (default) and once again for SMCore port 8145 (default) using PowerShell commands.

a. Remove the existing SnapCenter self-signed certificate port binding using the following PowerShell command.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>

For example,

> netsh http delete sslcert ipport=0.0.0.0:8145

> netsh http delete sslcert ipport=0.0.0.0:8146
```

b. Bind the newly procured CA certificate with the SnapCenter server and SMCore port

```
> $cert = “<CA_certificate thumbprint>”

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

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port> certhash=$cert
appid="$guid" clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

For example,

```
> $cert = “abc123abc123abc123abc123”

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

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert
appid="$guid" clientcertnegotiation=enable verifyclientcertrevocation=disable

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

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid" clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

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

2. To access permission to the CA certificate, add the SnapCenter’s default IIS web server user "**IIS AppPool\SnapCenter**" in the certificate permission list by performing the following steps to access the newly procured CA certificate.

    a. Go to the Microsoft management console (MMC), and then click **File** > **Add/Remove SnapIn**.

    b. In the Add or Remove Snap-ins window, select **Certificates** and then click **Add**.

    c. In the Certificates snap-in window, select the **Computer account** option, and then click **Finish**.

    d. Click **Console Root** > **Certificates – Local Computer** > **Personal** > **Certificates**.

    e. Select the SnapCenter certificate.

    f. Tto start the add user\permission wizard, right-click on the CA certificate and select **All Tasks** > **Manage private keys**.

    g. Click on **Add**, on Select users and groups wizard change the location to local computer name (top most in the hierarchy)

    h. Add the IIS AppPool\SnapCenter user, give full control permissions.

3. For **CA certificate IIS permission**, add the new DWORD registry keys entry in SnapCenter Server from the following path:

In the windows registry editor, traverse to the below mentioned path,

HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv ders\SCHANNEL

4. Create new DWORD registry key entry under the context of SCHANNEL registry configuration.

```
SendTrustedIssuerList = 0

ClientAuthTrustMode = 2
```

Configure SnapCenter Windows plug-in for Two-way SSL communication

You should configure SnapCenter Windows plug-in for two-way SSL communication using PowerShell commands.

Before you begin

Ensure that the CA certificate thumbprint is available.

Steps

1. To bind the port, perform the following actions on Windows plug-in host for SMCore port 8145 (default).
    a. Remove the existing SnapCenter self-signed certificate port binding using the following PowerShell command.

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

For example,

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

   b. Bind the newly procured CA certificate with the SMCore port.

```
> $cert = “<CA_certificate thumbprint>”

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

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
appid="$guid" clientcertnegotiation=enable verifyclientcertrevocation=disable

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

For example,

```
> $cert = “abc123abc123abc123abc123”

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

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid" clientcertnegotiation=enable verifyclientcertrevocation=disable

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

Enable two-way SSL communication

You can enable two-way SSL communication to secure the mutual communication between SnapCenter Server and the plug-ins using PowerShell commands.

Before you begin

Execute the commands for all the plug-ins and the SMCore agent first and then for server.

Steps

1. To enable the two-way SSL communication, run the following commands on the SnapCenter Server for the plug-ins, server, and for each of the agents for which the two-way SSL communication is required.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -
HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -
HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Perform the IIS SnapCenter Application pool recycle operation by using the following command. > Restart-WebAppPool -Name "SnapCenter"
3. For Windows plug-ins, restart the SMCore service by running the following PowerShell command:

```
> Restart-Service -Name SnapManagerCoreService
```

Disable two-way SSL Communication

You can disable the two-way SSL communication using PowerShell commands.

About this task

- Execute the commands for all the plug-ins and the SMCore agent first and then for server.
- When you disable the two-way SSL communication, the CA certificate and its configuration are not removed.
- To add a new host to SnapCenter Server, you must disable the two-way SSL for all plug-in hosts.
- NLB and F5 are not supported.

Steps

1. To disable the two-way SSL communication, run the following commands on SnapCenter Server for all the plug-in hosts and the SnapCenter host.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"} -
HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"} -
HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Perform the IIS SnapCenter Application pool recycle operation by using the following command.

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. For Windows plug-ins, restart the SMCore service by running the following PowerShell command:

```
> Restart-Service -Name SnapManagerCoreService
```

Service configuration

SnapCenter Server supports user accounts from local workgroups and domains for SnapCenter login and plug-in management. This section covers the updating of passwords for accounts and changing the ownership of services to service accounts, thereby decoupling services from user accounts.

SnapCenter service account password

If the password for the service account was changed on Active Directory, it is possible that the services do not update the password change until it is manually triggered, thereby causing the backups to fail.

Follow these steps on the host running SnapCenter plug-in for Windows:

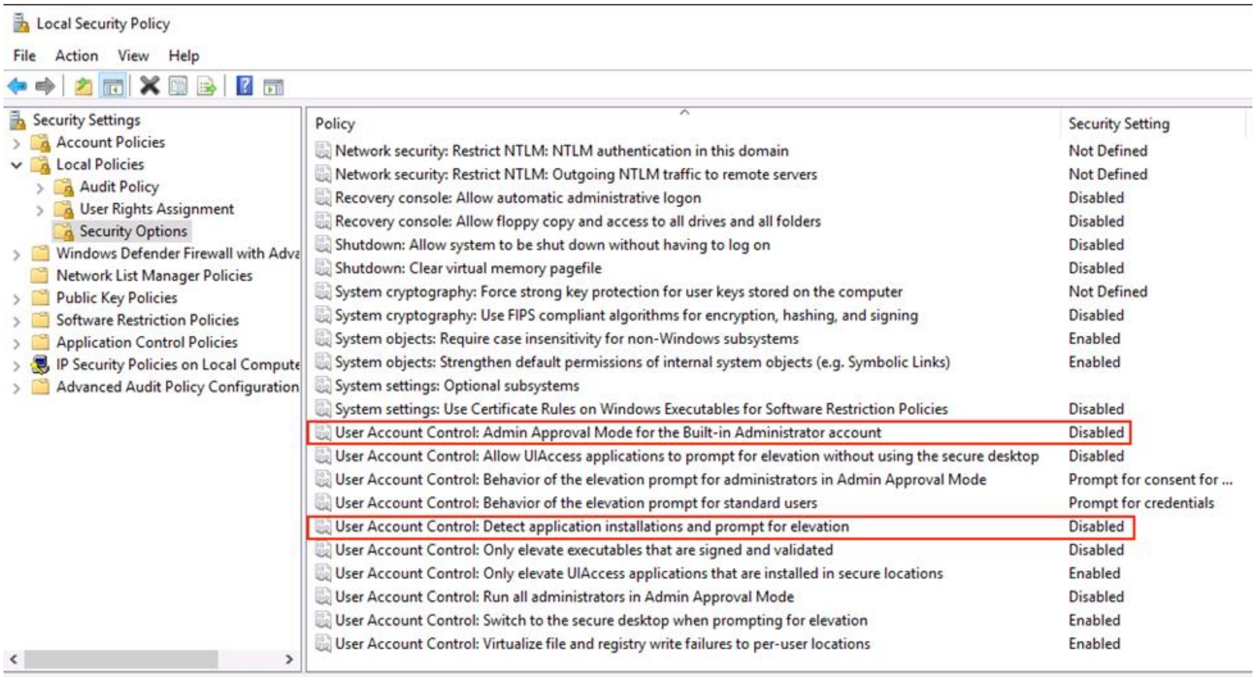
1. Suspend the plug-ins (whenever backups are not running).
2. Change the password for the SnapCenter service account in Active Directory.
3. Update the password for the credentials in the SnapCenter UI and on the SnapCenter plug-in for VMware configuration (and anywhere that domain account is being used).
4. Unsuspend the plug-ins on SnapCenter UI.
5. Restart the **Plug-in for Windows Service** and **SnapCenter SMCore service** on the affected hosts.
6. Run a test backup.

Permission setting for a SnapCenter plug-in host

Windows 2016 and 2019 have extra User Access Control (UAC) and remote Powershell Windows Management Instrumentation (WMI) security settings that keep the installer from running on a self-defined, local user.

To execute the installer, you can either use the host's local administrator account or you can disable UAC fully in the local security policy.

1. To open a remote session for the plug-in hosts, click **Start** and open **Local Security Policy** (`secpol.msc`).
2. Navigate to **Security Settings** > **Local Policies** > **Security Options**.
3. Set both of the following parameters to **Disabled**:
    a. User Account Control: Detect application installations and prompt for elevation.
    b. User Account Control: Run all administrators in Admin Approval Mode.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials
User Account Control: Detect application installations and prompt for elevation	Disabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Disabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

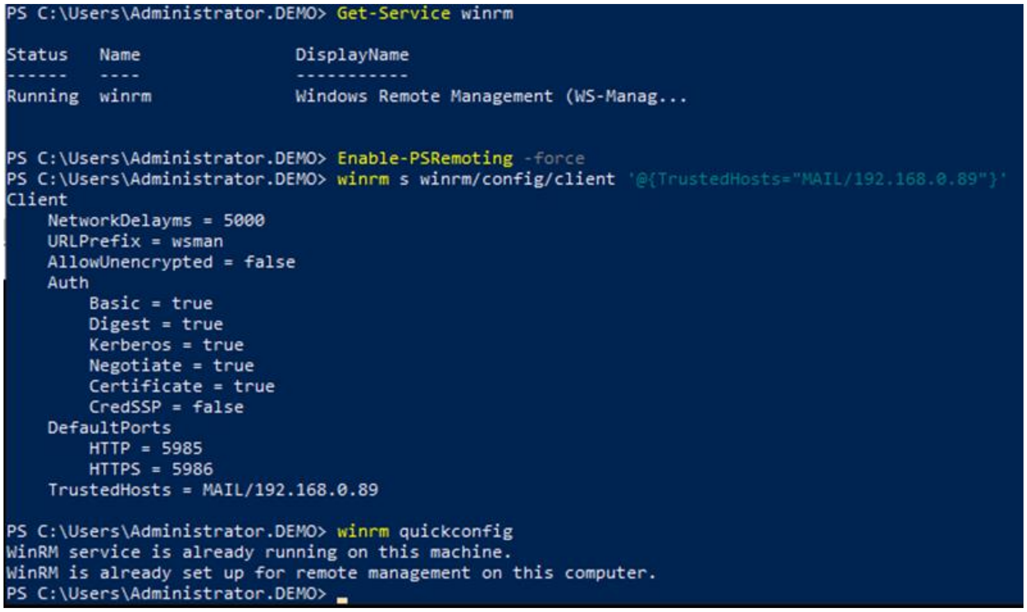
4. Open a PowerShell session and run the following commands:

```
Get-Service winrm
Enable-PSRemoting -force
winrm s winrm/config/client '@{TrustedHosts="SNAPCENTER_HOSTNAME/IP"}'
```

   – `SNAPCENTER_HOSTNAME` = Hostname of the SnapCenter Server
   – `IP` = IP address of the SnapCenter Server

```
winrm quickconfig
```

5. If needed, configure `winrm` based on the status of the last command.



```
PS C:\Users\Administrator.DEMO> Get-Service winrm

Status   Name               DisplayName
------   ----               -----------
Running  winrm              Windows Remote Management (WS-Manag...


PS C:\Users\Administrator.DEMO> Enable-PSRemoting -force
PS C:\Users\Administrator.DEMO> winrm s winrm/config/client '@{TrustedHosts="MAIL/192.168.0.89"}'
Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = true
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
        CredSSP = false
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    TrustedHosts = MAIL/192.168.0.89

PS C:\Users\Administrator.DEMO> winrm quickconfig
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.
PS C:\Users\Administrator.DEMO>
```

6. Reboot the server (to apply UAC changes).

7. Repeat on additional plug-in hosts as needed.

Group Managed Service Account (gMSA)

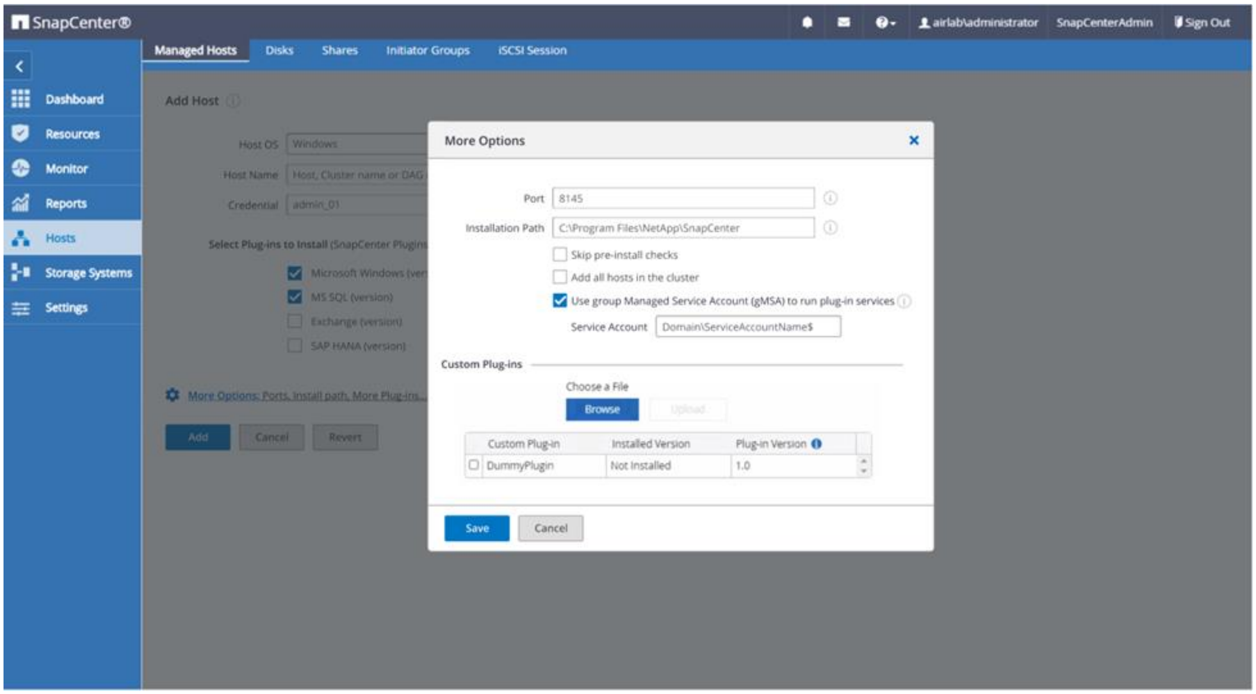
SnapCenter software supports running SnapCenter plug-in services using a gMSA that is not tied to any real user and provides automatic password management. A gMSA account is supported only for SnapCenter plug-in for Windows and SnapCenter plug-in for SQL Server services.

You can configure gMSA using the following options.

Add a host or a cluster

While registering the host, there is an option to specify a gMSA account to run plug-in services. To enable gMSA, go to **SnapCenter** > **Hosts** > **Add Host** > **More Options**.

Figure 8) gMSA dialog box.



Add Host

Host OS: Windows

Host Name: Host, Cluster name or DAG

Credential: admin_01

Select Plug-ins to Install (SnapCenter Plugins

☑ Microsoft Windows (ver

☑ MS SQL (version)

□ Exchange (version)

□ SAP HANA (version)

More Options

Port: 8145

Installation Path: C:\Program Files\NetApp\SnapCenter

□ Skip pre-install checks

□ Add all hosts in the cluster

☑ Use group Managed Service Account (gMSA) to run plug-in services

Service Account: Domain\ServiceAccountName$

Custom Plug-ins

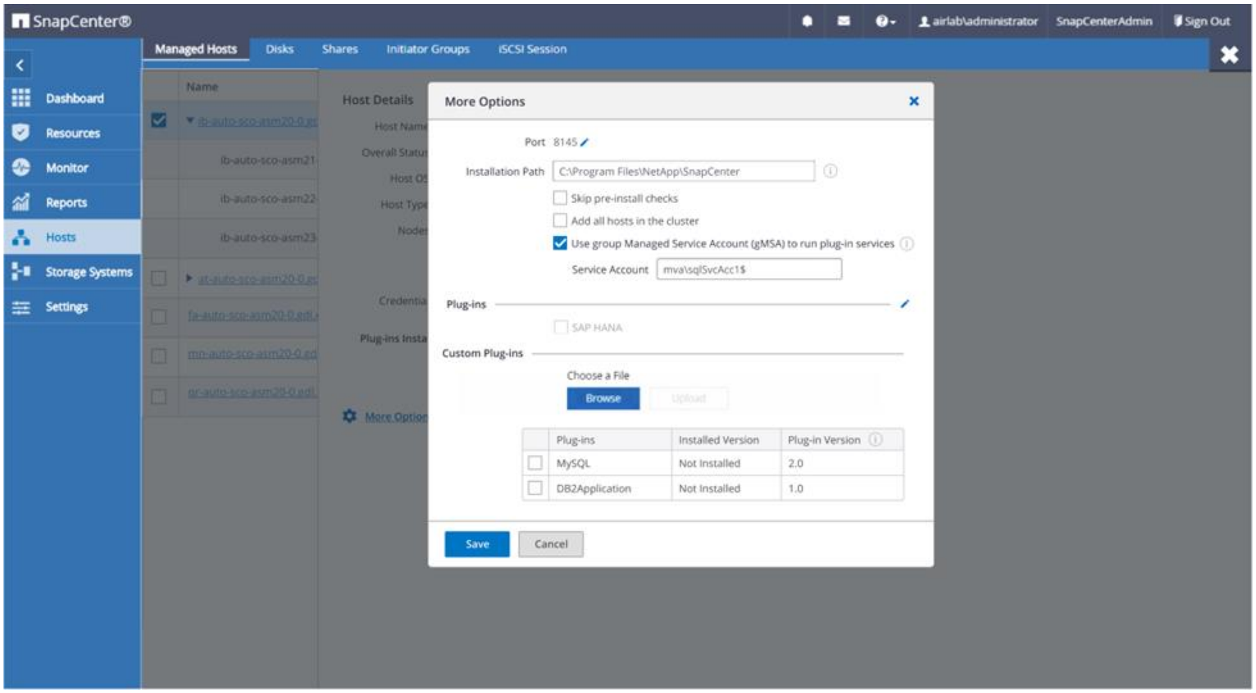
Choose a File

	Custom Plug-in	Installed Version	Plug-in Version
□	DummyPlugin	Not Installed	1.0

Modify a host or cluster

When plug-ins are already installed without specifying the gMSA, then, in the Modify Host UI, you can specify the gMSA account to use it as a plug-in service account.

To do so, navigate to **SnapCenter** > click the host name > **More options**.



More Options

Port 8145

Installation Path: C:\Program Files\NetApp\SnapCenter

☐ Skip pre-install checks

☐ Add all hosts in the cluster

☑ Use group Managed Service Account (gMSA) to run plug-in services

Service Account: mva\sqlSvcAcc1$

Plug-ins

☐ SAP HANA

Custom Plug-ins

Choose a File

	Plug-ins	Installed Version	Plug-in Version
☐	MySQL	Not Installed	2.0
☐	DB2Application	Not Installed	1.0

Using Powershell commandlets

To configure gMSA using commandlets, complete the following steps:

1. Run `Install-SmHostPackage`.

   For example:

```
Install-SmHostPackage -HostNames <hostname> -PluginCodes SCW,SCSQL -GMSAName <gMSA_Name>
```

2. Run `Set-SmHost`.

   For example:

```
Set-SmHost -HostName <hostname> -UseGMSA:$true -GMSAName <gMSA_Name>
```

Policy settings

Prescripts and postscripts

SnapCenter gives you the option to run prescripts or postscripts during operation workflows. For Windows plug-ins, you must save a scripts file in a predefined directory in the following location to run prescripts or postscripts during workflows:

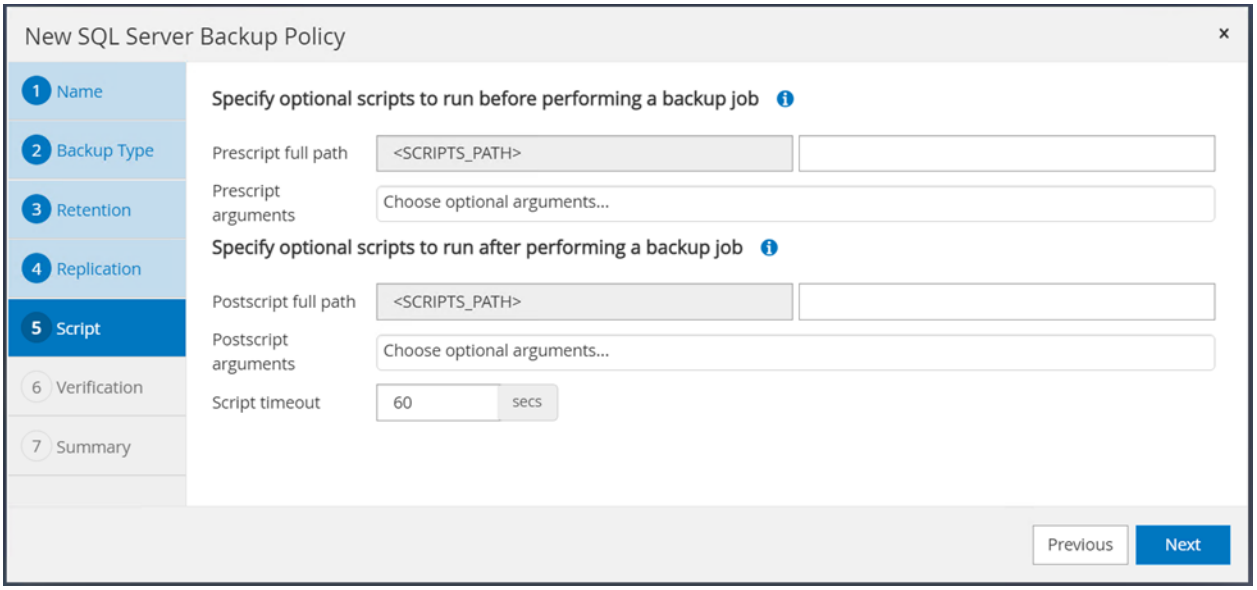
```
C:\Program Files\NetApp\SnapCenter\SMCore\Scripts\
```

Custom script directory

If you want to use a custom directory, then you need to configure from the `C:\Program Files\NetApp\SnapCenter\SMCore\SMCoreServiceHost.exe.Config` file. Change the value of the key `PredefinedWindowsScriptsDirectory`. The default key value is `PredefinedWindowsScriptsDirectory – C:\Program Files\NetApp\SnapCenter\SMCore\Scripts\`.

UI

The path provided in the textbox is appended to the script directory path. For example, if you enter a path as `MyScripts\TestScripts.cmd`, then SnapCenter searches for the script in location `C:\Program Files\NetApp\SnapCenter\SMCore\Scripts\MyScripts\TestScripts.cmd`.



Specify optional scripts to run before performing a backup job

Prescript full path: <SCRIPTS_PATH>

Prescript arguments: Choose optional arguments...

Specify optional scripts to run after performing a backup job

Postscript full path: <SCRIPTS_PATH>

Postscript arguments: Choose optional arguments...

Script timeout: 60 secs

Hardening the SnapCenter plug-in running on a Linux and AIX Server

This section describes the hardening steps necessary for the SnapCenter plug-in for Oracle on a Linux or AIX server and the SnapCenter plug-in for SAP HANA running on a Linux host.

Secure Shell (SSH) configuration

During the establishment of an SSH session, communication between the server and client is compliant with Federal Information Processing Standard (FIPS) 140-2 . All communication between endpoints happens through TLS 1.2 and TLS 1.3

The permitted ciphers are listed below. Cipher block chaining (CBC)-based ciphers are not vulnerable in combination with TLS 1.2 and TLS 1.3

- AES128-CTR
- AES192-CTR
- AES256-CTR
- AES128-CBC
- AES192-CBC
- AES256-CBC
- 3DES-CBC

Message authentication code-supported algorithms are as follows:

- For Linux, add MACs hmac-sha2-256 and MACs hmac-sha2-512 to `/etc/ssh/sshd_config`.
- For AIX, add MAC hmac-sha1 to `/etc/ssh/sshd_config`.

Key exchange algorithm used:

```
Diffie-hellman-group-exchange-sha256
```

Securing the operating system and configuring the firewall

Port security

Network ports that are not being used should be closed. Specifically, vulnerable ports, such as port 23 for Telnet connections, should be closed on all systems. The following required ports for the Linux system should be open:

- By default, SPL_PORT and SNAPCENTER_SERVER_PORT should be set to **8145** and **8146**, respectively. However, these port values can be configured using the configurable parameters defined in the file `/var/opt/snapcenter/spl/etc/spl.properties`.
- Enable port **22** (SSH) to install the plug-in. However, you can skip port **22** from the firewall list by installing it manually on the Linux host.
- Enable port **27216**. This default JDBC port is used by the plug-in for Oracle for connecting to the Oracle database.

Use the following command to find a listing of the listening ports:

```
netstat -tulpn
```

With this information, you can determine which listening ports are needed and which ones should be disabled.

To secure the remaining ports that are left open, restrict the port access to specific host IP addresses.

SELinux

Security enhanced Linux is a Kernel security mechanism supporting the access control security policy.

Run the following command to check the current SELinux mode:

```
sestatus
```

You must set SELinux to permissive so that the SnapCenter Plug-ins Package for Linux is able to perform the operation; otherwise, there is a chance of installation failure.

Root login security

Disabling or limiting root logins has multiple benefits. Forcing users to use the sudo command to execute administrative-level commands creates a level of auditing that does not exist if multiple users are logging in as root to perform the same tasks.

The most secure process is to disable all root access by installing the SnapCenter Plug-ins Package for Linux as a non-root user.

Firewall

Iptables is a user space application program that allows you to configure the firewall provided by the Linux Kernel. Firewall rules should not block ports mentioned in the Port security section and must be open to listen to the host IPs and the ports.

The following example shows how to configure SUSE Linux Enterprise Server:

1. Add the SnapCenter Plug-in Loader (SPL) port to iptables:
   – `/usr/sbin/iptables -A INPUT -p tcp -m tcp --dport 8145 -j ACCEPT`

- `/usr/sbin/iptables -A OUTPUT -p tcp -m tcp --dport 8145 -j ACCEPT`

2. Add the SPL port to firewall script by modifying the below parameters in the `/etc/sysconfig/SuSEfirewall2` file:
   - `FW_SERVICES_EXT_TCP="22 8145" <==== Add SSH and SPL ports`
   - `FW_SERVICES_EXT_UDP="22 8145"`
3. Depending on the SLES version, run the following commands:

   For SLES 11, run:

   a. `service SuSEfirewall2_setup stop`

   b. `service SuSEfirewall2_setup start`

   For SLES 12, run:

   a. `systemctl stop SuSEfirewall2`

   b. `systemctl start SuSEfirewall2`

If there are any company-wide policies to terminate the network connection after a certain time period (for example three hours), then it has to be turned off for SnapCenter applications; otherwise, operations start to fail.

Rate limiting provides a mechanism against DOS and DDoS attacks. You can rate limit per source an IP address for new connections through an OS network firewall which can prevent malicious attacks. In Red Hat Enterprise Linux (RHEL), you can configure a rate limiter through the `iptables` command. The following command is used to rate limit new connections with `n` request per second:

```
iptables -A INPUT -m conntrack --ctstate NEW -m hashlimit --hashlimit-above 10/sec --hashlimit-
burst 5 --hashlimit-mode srcip --hashlimit-name conn-rate-limit -j DROP
```

Authentication and login

Certificate Based Authentication

Certificate-based authentication is a security feature that improves authentication using digital certificates. Certificate-based authentication provides stronger security than traditional username/password authentication. It relies on cryptographic keys and digital certificates, making it harder for unauthorized users to impersonate valid users. Certificate based authentication verifies the authenticity of respective users who try to access the SnapCenter plug-in host. User should export the SnapCenter server certificate without private key and import it in the plugin host trusted store. This feature works on top of the two-way SSL configured systems.

Export CA certificates from the SnapCenter Server

You should export the CA certificates from the SnapCenter Server to the plug-in hosts using the Microsoft management console (MMC).

Prerequisite : Two-way SSL should be configured.

Steps

7. Go to the Microsoft management console (MMC), and then click **File** > **Add/Remove Snapin**.
8. In the Add or Remove Snap-ins window, select **Certificates** and then click **Add**.
9. In the Certificates snap-in window, select the **computer account** option, and then click **Finish**.
10. Click **Console Root** > **Certificates – Local Computer** > **Personal** > **Certificates**.

11. Right-click on the procured CA certificate which is used for SnapCenter Server and then select **All Tasks** > **Export** to start the export wizard.
12. Complete the wizard, as follows:

In this wizard window…	Do the following…
Export Private Key	Select the option **No**, do not export the private key, and then click **Next**.
Export File Format	Make no changes; click **Next**.
File Name	Click **Browse** and specify the file path to save the certificate, and then click **Next**.
Completing the Certificate Export Wizard	Review the summary, and then click **Finish** to start the export.

Note: SnapCenter HA configurations, are not supported.

Import CA Certificate to the Unix Host Plugins

- You can manage the password for SPL keystore, and the alias of the CA signed key pair in use.
- The password for SPL keystore and for all the associated alias password of the private key should be same.

Steps

1. You can retrieve SPL keystore default password from SPL property file. It is the value corresponding to the key `'SPL_KEYSTORE_PASS'`.
2. Change the keystore password:
```
$ keytool -storepasswd -keystore keystore.jks
```
3. Change the password for all aliases of private key entries in the keystore to the same password used for the keystore:
```
$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```
4. Update the same for the key `SPL_KEYSTORE_PASS` in spl.properties file.
5. Restart the service after changing the password.

Configure root or intermediate certificates to SPL trust-store.

You should configure the root or intermediate certificates to SPL trust-store. You should add the root CA certificate and then the intermediate CA certificates.

Steps

1. Navigate to the folder containing the SPL keystore: */var/opt/snapcenter/spl/etc*.
2. Locate the file 'keystore.jks'.
3. List the added certificates in the keystore:
```
$ keytool -list -v -keystore keystore.jks
```
4. Add a root or intermediate certificate:
```
$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file
/<CertificatePath> -keystore keystore.jks
```
5. Restart the service after configuring the root or intermediate certificates to SPL trust-store.

Configure CA signed key pair to SPL trust-store

Note: You should add the root CA certificate and then the intermediate CA certificates.

Steps

1. Navigate to the folder containing the SPL’s keystore /var/opt/snapcenter/spl/etc.
2. Locate the file 'keystore.jks'.
3. List the added certificates in the keystore:
   ```
   $ keytool -list -v -keystore keystore.jks
   ```
4. Add the CA certificate having both private and public key.
   ```
   $ keytool -importkeystore -srckeystore <CertificatePathToImport> -
   srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```
5. List the added certificates in the keystore.
   ```
   $ keytool -list -v -keystore keystore.jks
   ```
6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.
7. Change the added private key password for CA certificate to the keystore password.
   Default SPL keystore password is the value of the key SPL_KEYSTORE_PASS in spl.properties file.
   ```
   $ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
   keystore.jks
   ```
8. If the alias name in the CA certificate is long and contains space or special characters ("*",","), change the alias name to a simple name:
   ```
   $ keytool -changealias -alias "<OrignalAliasName>" -destalias
   "<NewAliasName>" -keystore keystore.jks
   ```
9. Configure the alias name from the keystore located in spl.properties file.
   Update this value against the key SPL_CERTIFICATE_ALIAS.
10. Restart the service after configuring the CA signed key pair to SPL trust-store.

Certificates - one-way and mutual SSL

Configuring a CA certificate for the SnapCenter Plug-in for SAP HANA Database and the SnapCenter Plug-in Loader service on a Linux host

Custom plug-ins use the file `keystore.jks`, which is located at `/opt/NetApp/snapcenter/scc/etc` both as its trust-store and key-store.

Manage password for a custom plug-in keystore and alias of the CA signed key pair that is in use.

You can retrieve a custom plug-in keystore default password from a custom plug-in agent property file. It is the value corresponding to the key KEYSTORE_PASS.

1. Change the keystore password.

```
keytool -storepasswd -keystore keystore.jks
```

2. Change the password for all aliases of private key entries in the keystore to the same password used for the keystore.

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

3. Update the same for the key KEYSTORE_PASS in `agent.properties` file.
4. Restart the service after changing the password.

Note: Passwords for custom plug-in keystores and for all the associated alias passwords of the private key should be the same.

Configure root or intermediate certificates to a custom plug-in trust-store

You should configure the root or intermediate certificates without a private key to a custom plug-in trust-store.

1. Navigate to the folder containing the custom plug-in keystore: `/opt/NetApp/snapcenter/scc/etc`.
2. Locate the file `keystore.jks`.
3. List the added certificates in the keystore.

```
keytool -list -v -keystore keystore.jks
```

4. Add a root or intermediate certificate.

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore
keystore.jks
```

5. Restart the service after configuring the root or intermediate certificates to the custom plug-in trust-store.

   Note: You should add the root CA certificate and then the intermediate CA certificates.

Configure CA-signed key pair to custom plug-in trust-store

You should configure the CA-signed key pair to the custom plug-in trust-store.

1. Navigate to the folder containing the custom plug-in keystore. `/opt/NetApp/snapcenter/scc/etc`.
2. Locate the file `keystore.jks`.
3. List the added certificates in the keystore.

```
keytool -list -v -keystore keystore.jks
```

4. Add the CA certificate having both a private and public key.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype
pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. List the added certificates in the keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.
7. Change the added private key password for the CA certificate to the keystore password.
8. The default custom plug-in keystore password is the value of the key KEYSTORE_PASS in the `agent.properties` file.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks
```

9. If the alias name in the CA certificate is long and contains a space or special characters ("*",","), change the alias name to a simple name.

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias" -keystore keystore.jks
```

10. Configure the alias name from the CA certificate in the `agent.properties` file.

11. Update this value against the key SCC_CERTIFICATE_ALIAS.
12. Restart the service after configuring the CA signed key pair to the custom plug-in trust-store.

Configure CRL for SnapCenter Custom Plug-ins

- SnapCenter Custom Plug-ins search for CRL files in a preconfigured directory.
- The default directory for the CRL files for SnapCenter Custom Plug-ins is `opt/NetApp/snapcenter/scc/etc/crl`.
- You can modify and update the default directory in the `agent.properties` file against the key CRL_PATH.
- You can place more than one CRL file in this directory. The incoming certificates are verified against each CRL.

Implementing a CA certificate with the SnapCenter Plug-in Loader service on a Linux host

The SnapCenter Plug-in Loader (SPL) service loads the plug-in package for Linux to interact with the SnapCenter Server. The SPL service is installed when you install the SnapCenter Plug-ins Package for Linux. SPL uses the file `keystore.jks`, which is located at `/var/opt/snapcenter/spl/etc` both as its trust-store and key-store.

Manage password for SPL keystore and alias of the CA signed key pair in use

You can retrieve the SPL keystore default password from the SPL property file. It is the value corresponding to the key SPL_KEYSTORE_PASS.

1. Change the keystore password:

```
keytool -storepasswd -keystore keystore.jks
```

2. Change the password for all aliases of private key entries in the keystore to the same password used for the keystore:

```
keytool -keypasswd -alias “<alias_name>” -keystore keystore.jks
```

3. Update the same for the key SPL_KEYSTORE_PASS in the `spl.properties` file.
4. Restart the service after changing the password.

Note: The password for the SPL keystore and for all the associated alias passwords of the private key should be same.

Configure root or intermediate certificates to SPL trust-store

You should configure the root or intermediate certificates without the private key to the SPL trust-store.

1. Navigate to the folder containing the SPL keystore `/var/opt/snapcenter/spl/etc`.
2. Locate the file `keystore.jks`.
3. List the added certificates in the keystore.

```
keytool -list -v -keystore keystore.jks
```

4. Add a root or intermediate certificate.

```
keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath>
-keystore keystore.jks
```

5. Restart the service after configuring the root or intermediate certificates to SPL trust-store.
6. You should add the root CA certificate and then the intermediate CA certificates.

Configure a CA signed key pair to the SPL trust-store

To configure a CA-signed key pair to the SPL trust-store, complete the following steps:

1. Navigate to the folder containing the SPL keystore `/var/opt/snapcenter/spl/etc`.
2. Locate the file `keystore.jks`.
3. List the added certificates in the keystore.

```
keytool -list -v -keystore keystore.jks
```

4. Add the CA certificate having both a private and a public key.

```
keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore
keystore.jks -deststoretype JKS
```

5. List the added certificates in the keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.
7. Change the added private key password for the CA certificate to the keystore password.

   The default SPL keystore password is the value of the key SPL_KEYSTORE_PASS in the `spl.properties` file.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks
```

8. If the alias name in the CA certificate is long and contains a space or special characters ("*",","), change the alias name to a simple name.

```
keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore
keystore.jks
```

9. Configure the alias name from the keystore located in the `spl.properties` file.

   Update this value against the key SPL_CERTIFICATE_ALIAS.
10. Restart the service after configuring the CA signed key pair to SPL trust-store.

Configure a certificate revocation list for SPL

You should configure a CRL for SPL.

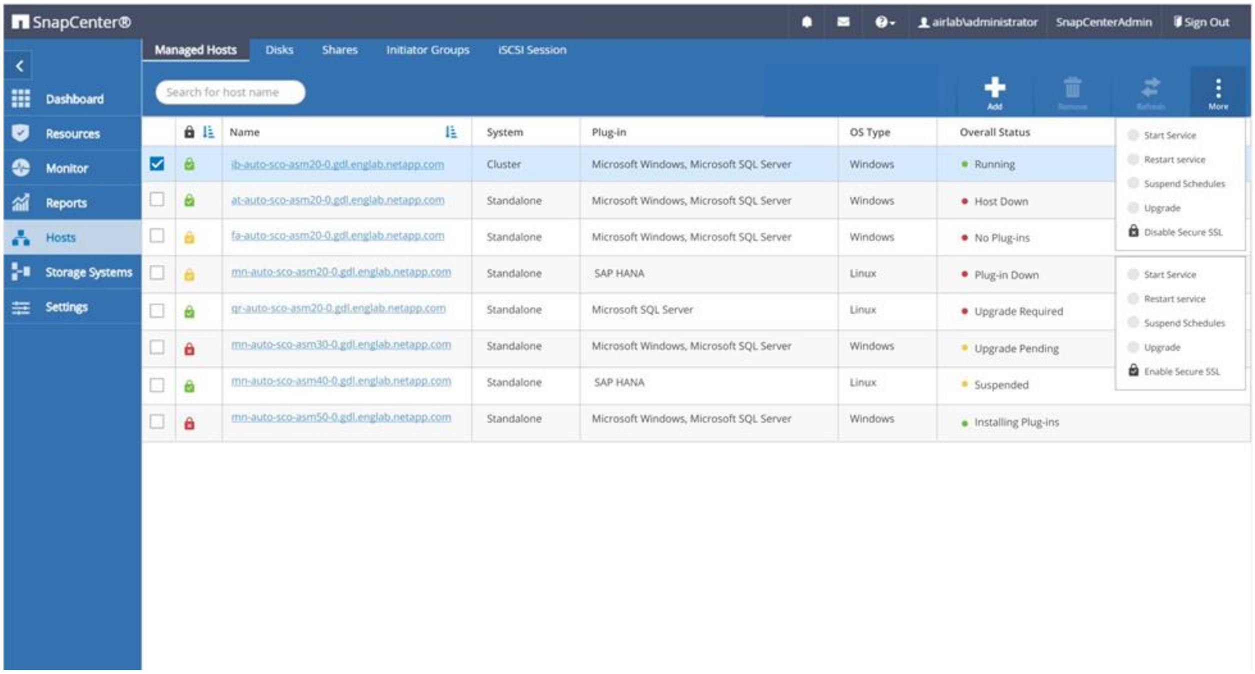
- SPL looks for CRL files in a preconfigured directory.
- The default directory for CRL files for SPL is `/var/opt/snapcenter/spl/etc/crl`.

1. Modify and update the default directory in the `spl.properties` file against the key `SPL_CRL_PATH`.
2. Place more than one CRL file in this directory.

Incoming certificates are verified against each CRL.

Enable a CA certificate for SnapCenter Plug-ins

You must enable the CA certificate feature at the SnapCenter level in the global settings page. After that, the managed host page menu in SnapCenter contains the additional option to enable or disable the SSL secure validation for the plug-in host level. You need to enable this option after configuring the CA certificates on the plug-in host. A green padlock indicates that a CA certificate is successfully validated.



		Name	System	Plug-in	OS Type	Overall Status
☑	🔒	ib-auto-sco-asm20-0.gdl.englab.netapp.com	Cluster	Microsoft Windows, Microsoft SQL Server	Windows	● Running
□	🔒	at-auto-sco-asm20-0.gdl.englab.netapp.com	Standalone	Microsoft Windows, Microsoft SQL Server	Windows	● Host Down
□	🔒	fa-auto-sco-asm20-0.gdl.englab.netapp.com	Standalone	Microsoft Windows, Microsoft SQL Server	Windows	● No Plug-ins
□	🔒	mn-auto-sco-asm20-0.gdl.englab.netapp.com	Standalone	SAP HANA	Linux	● Plug-in Down
□	🔒	qr-auto-sco-asm20-0.gdl.englab.netapp.com	Standalone	Microsoft SQL Server	Linux	● Upgrade Required
□	🔒	mn-auto-sco-asm30-0.gdl.englab.netapp.com	Standalone	Microsoft Windows, Microsoft SQL Server	Windows	● Upgrade Pending
□	🔒	mn-auto-sco-asm40-0.gdl.englab.netapp.com	Standalone	SAP HANA	Linux	● Suspended
□	🔒	mn-auto-sco-asm50-0.gdl.englab.netapp.com	Standalone	Microsoft Windows, Microsoft SQL Server	Windows	● Installing Plug-ins

Mutual SSL

No additional steps are required; the SSL configuration steps for one-way communication remain valid. Configure CA certificate using the SnapCenter Plug-in Loader (SPL) service on a Linux host).

Cipher configuration

Ciphers supported by SPL

SPL only supports AES128 and AES256 ciphers to communicate between the server and the Linux client.

```
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA256
AES256-GCM-SHA384
AES256-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA256
AES128-GCM-SHA256
AES128-SHA256
```

Remote Support Agent key

To set the minimum Remote Support Agent (RSA) public key length (in bits) allowed in the SSL/TLS certificate during SSL/TLS certificate validation on the Linux Plug-in host (SPL/SCC), you need to specify the value for the parameter `RSA_KEY_MINLENGTH`.

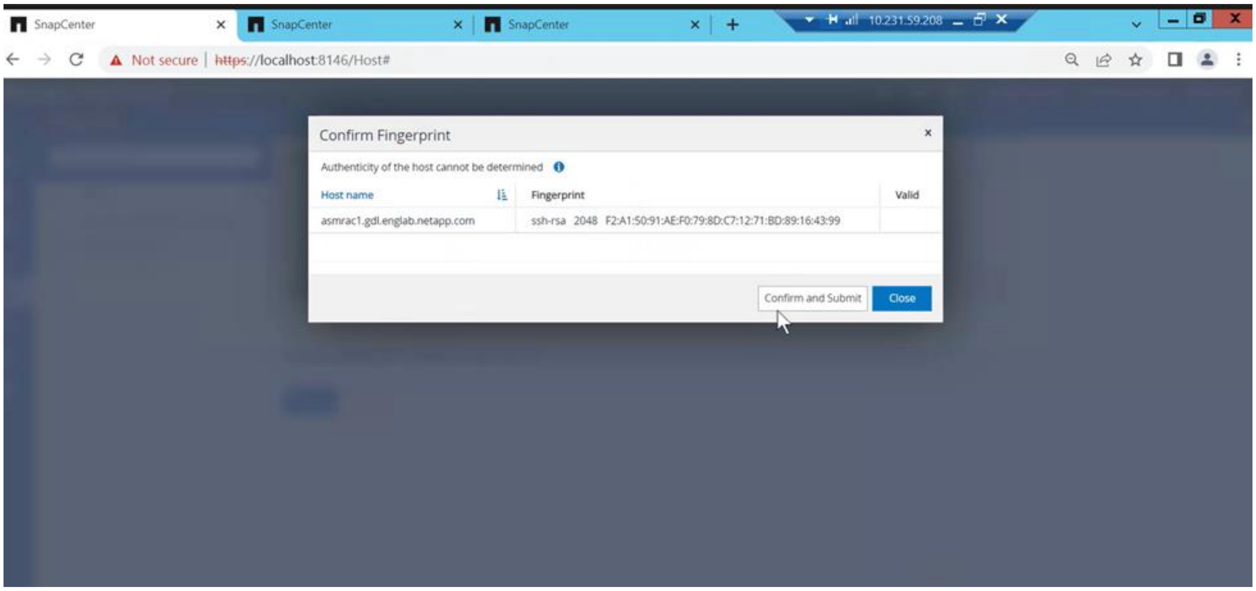
```
RSA_KEY_MINLENGTH=3072
```

For SPL, this parameter can be specified in the `spl.properties` file located at `/var/opt/snapcenter/spl/etc/spl.properties` and, for SCC, in `agent.properties` at `<user_install_path>/NetApp/snapcenter/scc/etc/agent.properties` for Linux.

Securing plug-in installation

Fingerprint validation in push installation

As part of the installation operation, before packages are being pushed to host, you should verify the fingerprint and click **Confirm fingerprint** as shown in the following screenshot by visually confirming against the host. In a cluster setup, the fingerprint of each of the nodes in the cluster should be verified. The minimum length of the fingerprint is 2048. Otherwise, installation does not proceed.



Confirm Fingerprint

Authenticity of the host cannot be determined

Host name	Fingerprint	Valid
asmrac1.gdl.englab.netapp.com	ssh-rsa 2048 F2:A1:50:91:AE:F0:79:8D:C7:12:71:BD:89:16:43:99	

Java Path availability

While installing the plug-in, the product automatically resolves the Java path that is set for the user who is trying to install the product.

Sudo configuration (for a non-root)

To install the SnapCenter for Linux plug-in for the non-root user, you need to add the content contained in the `oracle_checksum.txt` file located at `C:\ProgramData\NetApp\SnapCenter\Package Repository`, which contains the checksum and path-related information required to perform these operations.

Sample content for the sudoers file for the sudo version equal to or greater than 1.8.7

```
# ===== sudo user rules to be added on the Linux plug-in host if sudo package version is 1.8.7 or
later =====
# ===== Replace USER_HOME_DIRECTORY with the path of the home directory of the user who will
deploy the plug-in. =====
# ===== Replace LINUXUSER with the OS username identified for deploying the plug-in. =====
# ===== Replace /opt with the custom location where the plug-in will be installed. =====
Cmnd_Alias HPPLCMD = sha224:+GfDlO9XjgxmOqWhB2WRjwdqbu7ZskMYaFigdg==
/<USER_HOME_DIRECTORY>/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall, /opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:ir9Km4ctOavgJ60Fbbmmpx7a6dJ68FiQIXHdyw==
/<USER_HOME_DIRECTORY>/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:HQukzZNynG+nugzScFnHuccouOL75sZ1RRDaNg==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config_Check.sh
```

```
Cmnd_Alias SCCMD = sha224:GHupVXP5krvae06pNNxjvhZcM5VfRkOvc86Ibw==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR = sha224:Z/y0i1kAYtuWf/uOExqlnBOPVufF8samQPEE7g==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
<LINUXUSER> ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD, CONFIGCHECKCMD, SCCCMDEXECUTOR,
SCCMD
Defaults:<LINUXUSER> !visiblepw
Defaults:<LINUXUSER> !requiretty
```

Sample content for the sudoers file for the sudo version lesser than 1.8.7

```
# ===== sudo user rules to be added on the Linux plug-in host if sudo package version is below
1.8.7 =====
# ===== Replace USER_HOME_DIRECTORY with the path of the home directory of the user who will
deploy the plug-in. =====
# ===== Replace LINUXUSER with the OS username identified for deploying the plug-in. =====
# ===== Replace /opt with the custom location where the plug-in will be installed. =====
<LINUXUSER> ALL=(ALL) NOPASSWD:SETENV:
/<USER_HOME_DIRECTORY>/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall, /opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc, /<USER_HOME_DIRECTORY>/.sc_netapp/Linux_Prechecks.sh,
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config_Check.sh,
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
Defaults:<LINUXUSER> !visiblepw
Defaults:<LINUXUSER> !requiretty
```

Manual installation - signature verification steps

If you manually installed the SnapCenter Plug-in for Oracle, you need to validate the signature of the binary package by using the key `snapcenter_public_key.pub` (located at `C:\ProgramData\NetApp\SnapCenter\Package Repository`). To do so, run the following commands:

```
openssl dgst -sha256 -verify snapcenter_public_key.pub  -signature
snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin
```

Prerequisites

- OpenSSL: OpenSSL 1.0.2g

Checksum validation of the installed components

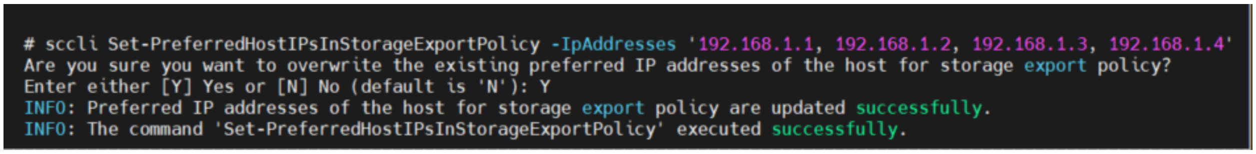
As part of the installation, the checksum validation for all the installed components is first validated against the manifest file of the product. If any checksum mismatch is detected, then installation is aborted, and packages are uninstalled. Secondly, the digital signature of all the NetApp owned jars is also validated, and, if any mismatch is detected, then the SPL service does not start, and installation is aborted.

Storage settings

Set the preferred IP addresses of the host for the storage export policy

Choose or control the IP addresses of the host to be added to the storage export policy for mount and clone operations by using the sccli command `Set-PreferredHostIPsInStorageExportPolicy`. By default, all the IP addresses of the host are added by SnapCenter to the storage export policy.

The following example shows how to set the IP address.



```
# sccli Set-PreferredHostIPsInStorageExportPolicy -IpAddresses '192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4'
Are you sure you want to overwrite the existing preferred IP addresses of the host for storage export policy?
Enter either [Y] Yes or [N] No (default is 'N'): Y
INFO: Preferred IP addresses of the host for storage export policy are updated successfully.
INFO: The command 'Set-PreferredHostIPsInStorageExportPolicy' executed successfully.
```

Securing the SnapCenter Plug-in for Oracle

All Oracle scripts (prescript or postscript) must be placed in the directory `/var/opt/snapcenter/spl/scripts/`. This directory is accessible only to the root user.

Oracle authentication

Database authentication

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

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 operating system OS authentication is disabled on the database host, you need 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 a catalog database, you need to add RMAN catalog authentication.

Securing SnapCenter Custom Plug-ins

Sudo configuration (for a non-root user)

For SnapCenter 4.8 and later releases, running the SnapCenter Custom Plug-in as a non-root user is supported.

To run the SnapCenter Custom Plugin as a non-root user, you need to complete the following steps before SnapCenter Custom Plug-in installation:

1. Create a non-root user on the Linux host.
2. Provide the correct sudo privileges for this non-root user by updating the sudoers file with the appropriate content (refer to the `oracle_checksum` file from the installed SnapCenter Server at `C:\ProgramData\NetApp\SnapCenter\Package Repository\oracle_checksum`).
3. Install the SnapCenter Custom Plug-in (SCC) from SnapCenter UI on this host or manually from this host using that configured non-root user.

Prescript or postscript

To enhance security during the prescript or postscript step in the clone or restore workflows of SnapCenter Custom Plug-ins, an `allowed_commands.config` file is shipped during the plug-in installation on the Linux or Windows host. Only the administrator on Windows or the root on Linux can write to the `allowed_commands.config` file.

If a command must be run during the pre or post step of the workflows on the host, it must be explicitly permitted by including it in the `allowed_commands.config` file. Only the administrator on Windows or the root on Linux can write to this file.

The path of `allowed_commands.config` on the host is as follows:

On Linux hosts

- Default: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`
- Custom path: `<Custome_Directory>/NetApp/snapcenter/scc/etc/allowed_commands.config`

On Windows hosts

- Default: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Custom path: `<Custome_Directory>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

To add a command to `allowed_commands.config`, open `allowed_commands.config` in an editor. Enter each command on its own line, exactly as you would enter the command at a command prompt. The case is significant.

For example:

```
command: mount
command: umount
command: "C:\Software\New command\commandLists\scripts\abc.bat"
command: "c:\a b\c.bat"
command: echo
```

Make sure to specify the fully qualified path name. Enclose the path name in quotation marks if it contains spaces.

For example:

```
command: "C:\Program Files\NetApp\SnapCreator commands\sdcli.exe"
command: myscript.bat
```

Note: For security reasons, you should not use a wildcard entry (*) to allow all commands.

Custom plug-ins

When any custom plug-in is imported on the host, SnapCenter checks if the SHA512 hash of the plug-in zip file is present in the `custom_plugin_checksum_list` file on the host.

The `custom_plugin_checksum_list` file is shipped as part of the custom plug-in installation on the host by SnapCenter. It contains the SHA512 hashes of the custom plug-ins created by NetApp. Only an administrator on Windows or root on Linux can write to the `custom_plugin_checksum_list` file.

The location of the checksum file on the Linux host is:

```
/var/opt/snapcenter/scc/custom_plugin_checksum_list.txt
```

Similarly, on a Windows host, the default location of the file is:

```
C:\Program Files\NetApp\SnapCenter Plug-in Creator\etc\custom_plugin_checksum_list.txt
```

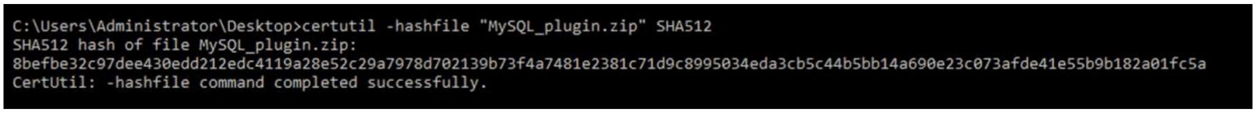
The default location is the same as above if a custom installation path is used at:

```
<custom path>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\custom_plugin_checksum_list.txt
```

To import any custom plug-in created by you, you need to add the SHA512 checksum of the plug-in zip file to `custom_plugin_checksum_list` on host. To do so, complete the following steps:

1. Generate the SHA512 hash of the plug-in zip file. Any online tool, like https://emn178.github.io/online-tools/sha512_file_hash.html or the SHA512 tool on Linux, can be used. You can also use the certutil

tool on Windows by using the command: `certutil –hashfile "<plugin_zipfile>"` SHA512 as shown below:



```
C:\Users\Administrator\Desktop>certutil -hashfile "MySQL_plugin.zip" SHA512
SHA512 hash of file MySQL_plugin.zip:
8befbe32c97dee430edd212edc4119a28e52c29a7978d702139b73f4a7481e2381c71d9c8995034eda3cb5c44b5bb14a690e23c073afde41e55b9b182a01fc5a
CertUtil: -hashfile command completed successfully.
```

2. Add the generated SHA512 hash in the `custom_plugin_checksum_list` file on the host on a separate line by contacting the host administrator (root on Linux). Comments can be added in the file starting with the # symbol for identifying the plug-in to which the hash belongs. On Windows, WordPad is recommended for editing this file.

   See the following sample entry in the checksum file:

```
#ORASCPM 0.1
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63d6e6777a2b2a1ec068bb0a93a
59a8ade71587182f8bccbe81f7e0ba6
```

3. Import the custom plug-in.

Auditing

If SPL or SCC is running as root, it is logged in an audit log located at `<user_install_dir>/Netapp/snapcenter/scc/logs/audit.log` like below:

```
06-12-2022 19:45:59: SPL process with pid 21234 is running as root
06-12-2022 19:45:59: SCC process with pid 21595 is running as root
```

You can monitor whether SCC/SPL is running as a privileged user (root) by using this audit file. Logging is only done whenever SPL/SCC run-as user is switched to root.

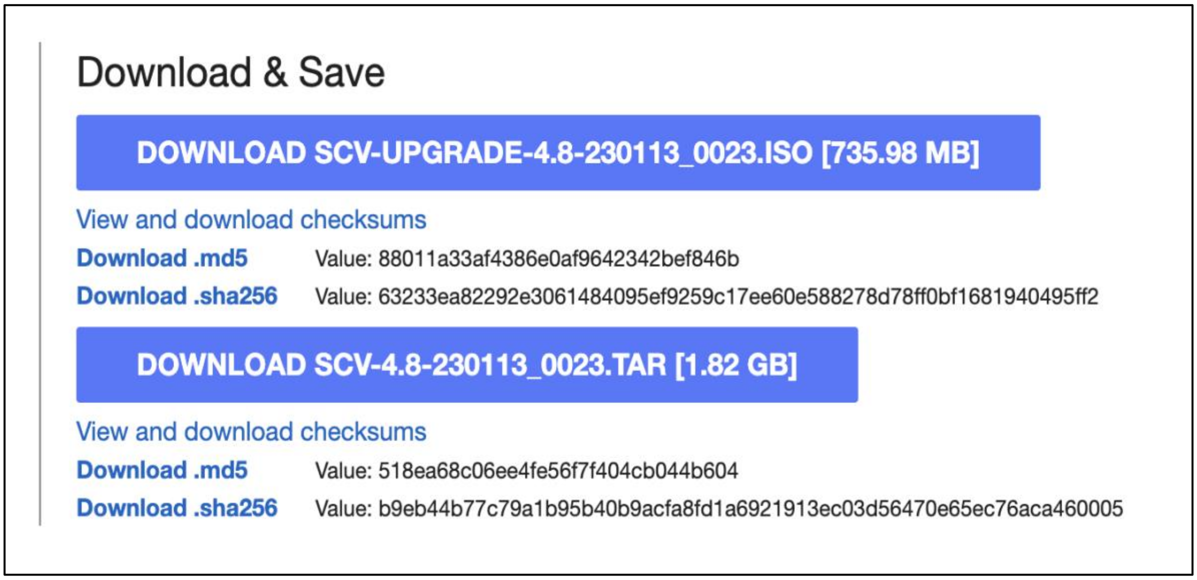
Hardening the SnapCenter plug-in for VMware vSphere

Integrity verification of SnapCenter plug-in for VMware vSphere

NetApp downloads

When downloading the product from the NetApp downloads page, NetApp recommends making a note of the MD5 and SHA256 checksums to ensure that the downloaded files have not been tampered with. You can use the standard checksum verification tools to verify checksums before deploying the product. This step helps to ensure the integrity and authenticity of the downloaded file and prevents the installation of a potentially malicious or corrupted software package.

The tar file contains the OVA (Open Virtual Appliance) and a certs folder, which includes certificates to validate the integrity and authenticity of the OVA and ISO.



Download & Save

DOWNLOAD SCV-UPGRADE-4.8-230113_0023.ISO [735.98 MB]

View and download checksums

Download .md5	Value: 88011a33af4386e0af9642342bef846b
Download .sha256	Value: 63233ea82292e3061484095ef9259c17ee60e588278d78ff0bf1681940495ff2

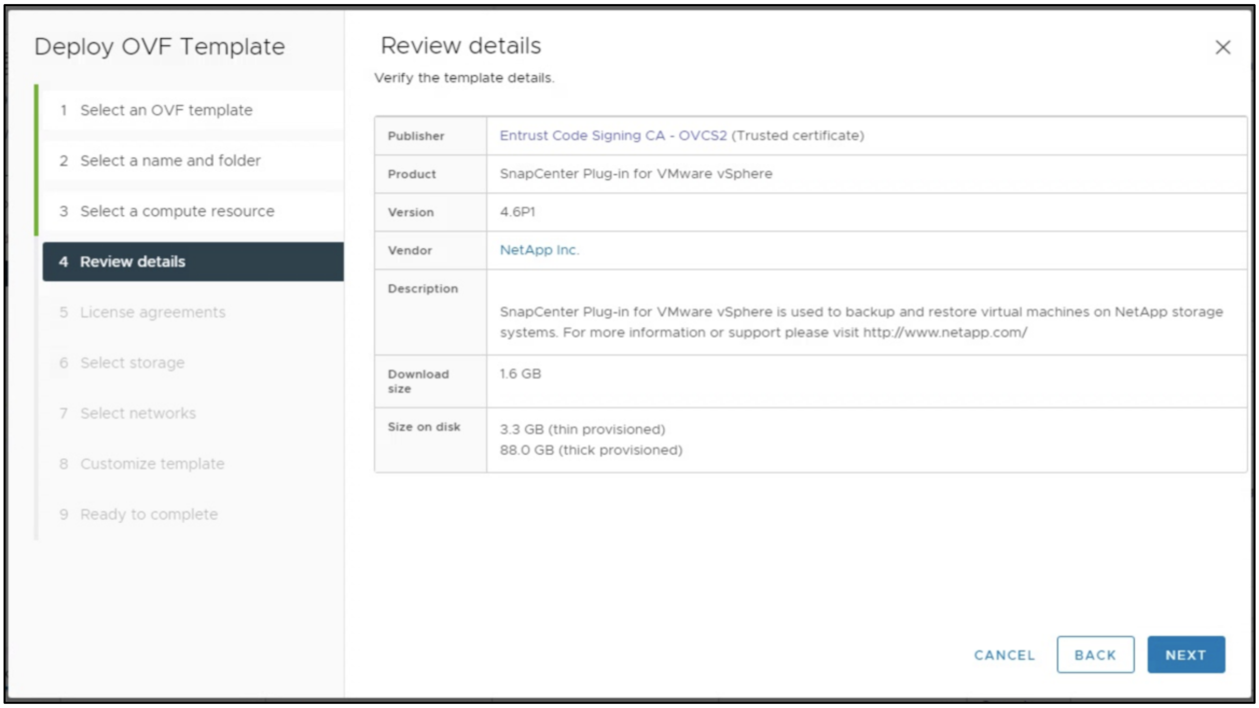
DOWNLOAD SCV-4.8-230113_0023.TAR [1.82 GB]

View and download checksums

Download .md5	Value: 518ea68c06ee4fe56f7f404cb044b604
Download .sha256	Value: b9eb44b77c79a1b95b40b9acfa8fd1a6921913ec03d56470e65ec76aca460005

Deploy OVA in VMware vCenter

The SnapCenter plug-in for VMware vSphere is shipped as an OVA file that can be deployed in vCenter. During the deployment process, vCenter validates the integrity of the OVA file to ensure that it has not been tampered with and is safe to install.

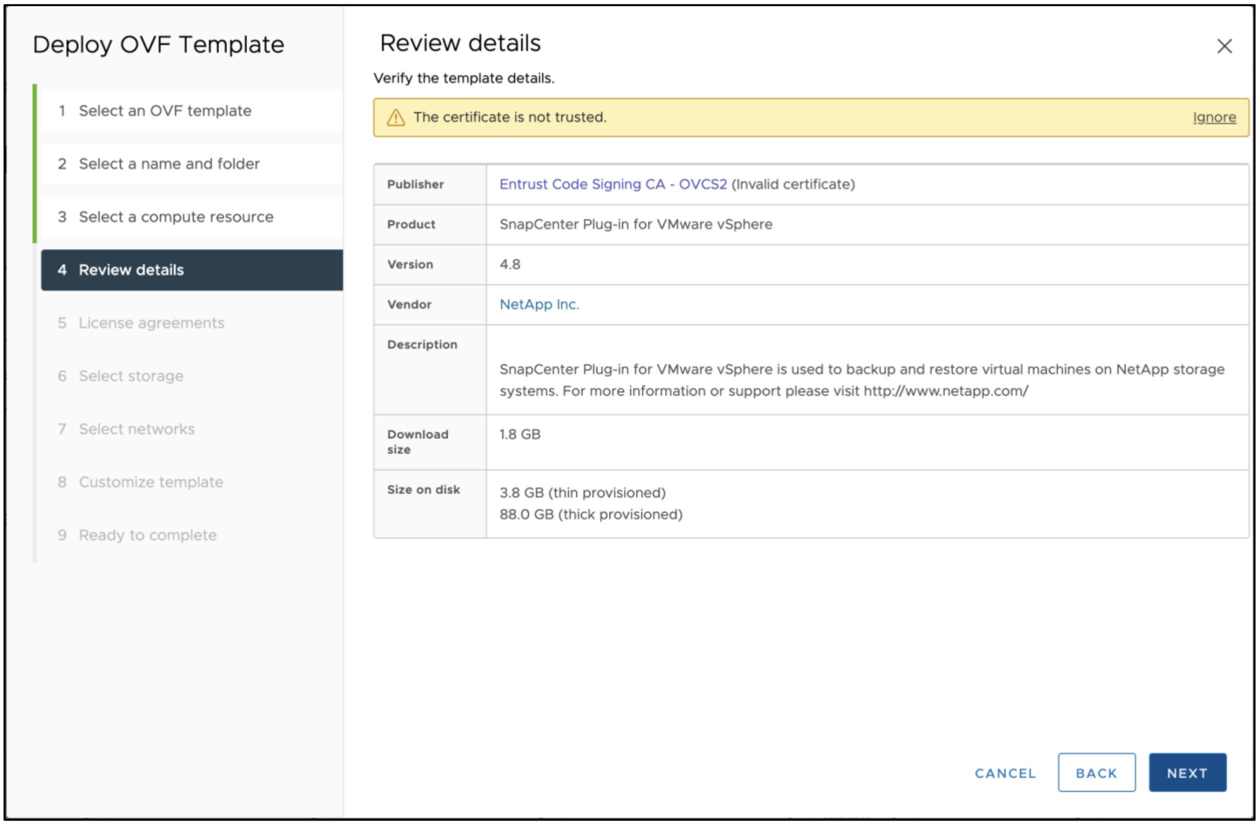


Review details

Verify the template details.

Publisher	Entrust Code Signing CA - OVCS2 (Trusted certificate)
Product	SnapCenter Plug-in for VMware vSphere
Version	4.6P1
Vendor	NetApp Inc.
Description	SnapCenter Plug-in for VMware vSphere is used to backup and restore virtual machines on NetApp storage systems. For more information or support please visit http://www.netapp.com/
Download size	1.6 GB
Size on disk	3.3 GB (thin provisioned) 88.0 GB (thick provisioned)

Due to a known issue, OVA integrity verification might not work properly in VC 7.0.3, which is shown in the following image.



Review details

Verify the template details.

⚠ The certificate is not trusted.

Publisher	Entrust Code Signing CA - OVCS2 (Invalid certificate)
Product	SnapCenter Plug-in for VMware vSphere
Version	4.8
Vendor	NetApp Inc.
Description	SnapCenter Plug-in for VMware vSphere is used to backup and restore virtual machines on NetApp storage systems. For more information or support please visit http://www.netapp.com/
Download size	1.8 GB
Size on disk	3.8 GB (thin provisioned) 88.0 GB (thick provisioned)

To enable OVA file integrity verification, you need to import certificates into vCenter (7.0U3E or above) by following the instructions provided in this link.

Securing SnapCenter plug-in for VMware vSphere appliance in vCenter

Manage appliance in vCenter

After deploying the appliance to vCenter, review the permissions assigned to it in vCenter. Check which users or groups have access to it and make any necessary changes to ensure proper access control.

Required RBAC privileges

You can find information on the required RBAC privileges for deploying, upgrading, and using the SnapCenter Plug-in for VMware vSphere in the NetApp Documentation page, which also provides guidance on assigning the necessary privileges to users or groups in vCenter.

For vCenter privileges, you can refer to the NetApp Documentation which provides you with the minimum requires privileges.

Enabling CA-signed certificate

The SnapCenter VMware plug-in employs Secure Socket Layer (SSL) encryption for secure communication with the client browser. Although this does enable encrypted data across the wire, creating a new self-signed certificate or using your own Certificate Authority (CA) infrastructure or a third-party CA ensures that the certificate is unique for your environment. For additional information, follow this link.

Software components

All NetApp and third-party components deployed and used in the appliance are checksum verified. Check the NetApp Documentation to know about secure development activities that are followed.

Table 4) Built-in users.

Users	Description
Maintenance console user	Performs maintenance console operations. To change credentials: 1. Access the maintenance console window. 2. Enter 2 for system configuration. 3. Enter 3 to change the maint user password. 4. Enter the new password.
Admin user	Use Management UI To change credentials: 1. Access maintenance console window 2. Enter 1 for application configuration. 3. Enter 4 to change the username or password. 4. Enter the new password.
vCenter user	Plug-in operations using the vSphere client and REST APIs Follow the vCenter documentation to change credentials.
MySQL user	Manage the MySQL instance in the appliance. To change credentials: 1. Access the maintenance console window 2. Enter 1 for application configuration. 3. Enter 5 to change the MySQL password. 4. Enter the new password.
Diag user	Performs remote diagnostics. You must set a password for the diag user when enabling remote diagnostics.

Ports and protocols

Table 5) Ports and protocols.

Type of port	Preconfigured port
VMware ESXi Server port	**443** (HTTPS), bidirectional The Guest File Restore feature uses this port.
SnapCenter Plug-in for VMware vSphere port	**8144** (HTTPS), bidirectional The port is used for communications from the VMware vSphere client and from the SnapCenter Server. **8080** bidirectional

Type of port	Preconfigured port
	This port is used to manage the virtual appliance. **Note:** You cannot modify the port configuration.
VMware vSphere vCenter Server port	You must use port **443** if you are protecting vVol VMs.
Storage cluster or storage VM port	**443** (HTTPS), bidirectional **80** (HTTP), bidirectional The port is used for communication between the virtual appliance and the storage VM or the cluster that contains the storage VM.

Audit logs

An audit log is a chronological record of system activity that provides a trail of events and actions taken on a system. It is used to monitor and review activity for security and compliance purposes. The audit log files are generated at `/var/log/netapp/audit`. NetApp recommends that you regularly review the audit log to track events, troubleshoot issues, and monitor user activities. Additional information can be found on NetApp Documentation page.

Securing MySQL repository database

Default configuration

The SnapCenter plug-in for VMware vSphere appliance comes with MySQL deployed, and the MySQL root user password is autogenerated, which is a complex password. The password should only be changed to inspect MySQL data. You can change the MYSQL password as follows:

1. Open a maintenance console window: Access the maintenance console.
2. From the Main Menu, enter option **1) Application Configuration**.
3. From the Application Configuration Menu, enter option **5) Change MySQL password**.
4. Review the guidelines and configure a new complex password.

Storage settings

Refer to the NetApp Documentation for required ONTAP privileges.

Authentication methods

The SnapCenter plug-in for VMware vSphere offers two authentication modes to manage storage: credentials-based and certificate-based.

Credentials-based authentication relies on a combination of username and password for authentication. However, for enhanced security and mutual authentication, NetApp recommends using certificate-based authentication. Depending on your requirements, you can follow the steps for either a CA-signed certificate or a self-signed certificate for authentication.

Transport Layer Security (TLS) configuration

By default, the SnapCenter plug-in for VMware vSphere appliance has TLS v1.0 and TLS v1.1 disabled to enhance security. This means that only TLS v1.2, TLS v1.3 are enabled and supported for communication.

Verify TLS settings

To disable or check the currently enabled TLS version in the SnapCenter plug-in for VMware vSphere appliance, you can refer to this knowledge base article.

Disable weak ciphers

SnapCenter is installed in a Windows Server where the ciphers are part of the Windows Configuration. By default, weak ciphers are enabled until the manual configurations are complete. Due to this scenario, SCV should use weak ciphers. You can disable weak ciphers by overriding the default value of the `disable.weakCiphers` property in the `scbr.override` file. Refer the NetApp documentation for instructions.

DOS attack

To protect a Debian system against DoS attacks, you can use the built-in firewall tool called iptables. With iptables, you can configure various rules to restrict and control incoming and outgoing network traffic.

One way to prevent DoS attacks using iptables is to limit the rate of traffic from specific IP addresses or networks. This technique is known as rate limiting, and it can be effective in mitigating attacks that involve flooding the network with traffic. By limiting the rate of traffic, you can minimize the impact of DoS attacks and ensure that legitimate traffic can still pass through.

```
iptables -A INPUT -m conntrack --ctstate NEW -m hashlimit --hashlimit-above 10/sec --hashlimit-burst 5 --hashlimit-mode srcip --hashlimit-name conn-rate-limit -j DROP
```

This command adds a new rule to the INPUT chain of the firewall, which limits the rate of incoming connections from each source IP address to no more than 10 connections per second with a burst of up to five connections. The rule only matches incoming traffic that is part of a new connection and drops the incoming packets that exceed the connection rate limit. This helps prevent DoS attacks by limiting the amount of traffic that can be generated from a single source IP address.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- SnapCenter Software Documentation Resources
  https://www.netapp.com/cyber-resilience/data-protection/snapcenter/documentation/
- Best practices for Microsoft SQL Server using NetApp SnapCenter
  https://www.netapp.com/pdf.html?item=/media/12400-tr4714.pdf
- Best practices for Oracle plugin with NetApp SnapCenter
  https://www.netapp.com/pdf.html?item=/media/12403-tr4700.pdf
- SnapCenter Plug-in VMware vSphere - Product security
  https://docs.netapp.com/us-en/netapp-solutions/virtualization/scvmware-security-secure-development-activities.html

Version history

Version	Date	Document version history
Version 1.0	March 2023	Initial document release.
Version 2.0	April 2023	Appended SCV content.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

Copyright Information

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.

Trademark Information