



SnapCenter® Software 4.2

Installation and Setup Guide

October 2019 | 215-14397_2019-10_en-us
doccomments@netapp.com

Updated for 4.2.1

Contents

Deciding whether to read the SnapCenter installation and setup information	7
Preparing for the SnapCenter Server installation	8
Host requirements	8
Domain and workgroup requirements	8
Space and sizing requirements	9
SAN host requirements	9
Supported storage systems and applications	10
Supported browsers	10
Connection and port requirements	10
Licensing requirements	12
SnapCenter repository	12
SVM connections and credentials	13
Authentication methods for your credentials	14
Network Load Balancing and Application Request Routing requirements	15
High availability for the SnapCenter MySQL repository	15
Installing the SnapCenter Server	17
Installing the SnapCenter Server using the Install wizard	18
Logging in to SnapCenter	19
Modifying the SnapCenter default GUI session timeout	21
Configuring role-based access control (RBAC)	21
Adding a user or group and assigning role and assets	21
Assigning users access to assets	23
Configuring IIS Application Pools to enable Active Directory read permissions	24
Adding storage systems	25
Securing the SnapCenter web server by disabling SSL 3.0	27
Adding SnapCenter licenses	29
SnapCenter Standard controller-based licenses	30
Viewing SnapManager Suite storage controller license installation status using the SnapCenter GUI	30
Viewing licenses installed on the controller using the ONTAP command line	31
Locating the controller serial number	32
Retrieving SnapCenter controller-based licenses from the NetApp Support Site	33
Adding a SnapCenter Standard controller-based license using the ONTAP command line	34
Removing the trial license	34
SnapCenter Standard capacity-based licenses	35
How SnapCenter calculates capacity usage	35

Calculating capacity requirements for a SnapCenter capacity-based license	36
Retrieving SnapCenter capacity-based license serial numbers from the NetApp Support Site	36
Generating a NetApp license file	37
Adding SnapCenter capacity-based licenses using the SnapCenter GUI	38
Installing SnapCenter Plug-in for Microsoft Exchange Server	40
Prerequisites to adding hosts and installing SnapCenter Plug-in for Microsoft Exchange Server	40
Exchange Server privileges required	41
Setting up credentials for the Plug-in for Windows	42
Adding hosts and installing Plug-in for Exchange	43
Installing Plug-in for Exchange from the SnapCenter Server host using PowerShell cmdlets	45
Installing the SnapCenter Plug-in for Exchange silently from the command line	46
Configuring SnapManager 7.x for Exchange and SnapCenter to coexist	47
Installing SnapCenter Plug-in for Microsoft SQL Server	50
Storage types supported by SnapCenter Plug-ins for Microsoft Windows and for Microsoft SQL Server	50
Prerequisites to adding hosts and installing SnapCenter Plug-in for Microsoft SQL Server	52
Host requirements to install SnapCenter Plug-ins Package for Windows	53
Setting up credentials for the SnapCenter Plug-ins Package for Windows	53
Configuring credentials for an individual SQL Server resource	55
Adding hosts and installing the SnapCenter Plug-ins Package for Windows	57
Installing SnapCenter Plug-in for Microsoft Windows on multiple remote hosts by using cmdlets	60
Installing SnapCenter Plug-in for Microsoft SQL Server independently	60
Preparation to install the SnapCenter Plug-in for Microsoft SQL Server	61
Installing the SnapCenter Plug-in for Microsoft SQL Server silently from the command line	61
Importing archived backups from SnapManager for Microsoft SQL Server to SnapCenter	63
Limitations related to the import feature	63
Importing archived backups	63
Viewing the imported backups in SnapCenter Server	64
Installing SnapCenter Plug-in for Microsoft Windows	65
Storage types supported by SnapCenter Plug-ins for Microsoft Windows and for Microsoft SQL Server	65
Installation requirements for SnapCenter Plug-in for Microsoft Windows	66
Adding storage systems	67
Setting up your credentials for the Plug-in for Windows	69
Adding hosts and installing SnapCenter Plug-in for Microsoft Windows	70
Installing SnapCenter Plug-in for Microsoft Windows on multiple remote hosts using PowerShell cmdlets	73

Installing the SnapCenter Plug-in for Microsoft Windows silently from the command line	74
Installing SnapCenter Plug-in for Oracle Database	76
Storage types supported by SnapCenter Plug-in for Oracle Database	76
Prerequisites for adding hosts and installing SnapCenter Plug-in for Oracle Database	77
Configuring sudo privileges for non-root users	77
Host requirements for installing the SnapCenter Plug-ins Package for Linux	79
Setting up your credentials for the SnapCenter Plug-ins Package for Linux	80
Configuring credentials for an Oracle database	81
Adding hosts and installing the SnapCenter Plug-ins Package for Linux	82
Installing SnapCenter Plug-ins Package for Linux on multiple remote hosts using cmdlets	85
Installing SnapCenter Plug-ins Package for Linux using the command-line interface	86
Installing the SnapCenter Plug-ins Package for Linux interactively	86
Installing SnapCenter Plug-ins Package for Linux on cluster host	86
Installing the SnapCenter Plug-ins Package for Linux in silent mode or console mode	87
Importing data from SnapManager for Oracle and SnapManager for SAP to SnapCenter	88
Configurations supported for importing data	89
Preparing to import data	91
Importing data	92
Canceling an import operation	94
Troubleshooting an import operation	94
Configuring the SnapCenter Plug-in Loader service for Linux	94
Installing SnapCenter Plug-in for SAP HANA Database	96
Storage types supported by SnapCenter Plug-in for SAP HANA Database	96
Prerequisites for adding hosts and installing SnapCenter Plug-in for SAP HANA Database	96
Host requirements to install SnapCenter Plug-ins Package for Windows	98
Host requirements for installing the SnapCenter Plug-ins Package for Linux	99
Setting up credentials for the SnapCenter Plug-in for SAP HANA Database	100
Adding hosts and installing plug-in packages on remote hosts	102
Installing SnapCenter Plug-in Packages for Linux or Windows on multiple remote hosts by using cmdlets	104
Installing SnapCenter Plug-in for SAP HANA Database independently on the Linux host	104
Preparation for installing the SnapCenter Plug-in for SAP HANA Database on the Linux host	105
Installing the SnapCenter Plug-in for SAP HANA Database on Linux hosts by using the command-line interface	105

Adding databases to SnapCenter Plug-in for SAP HANA Database	106
Installing SnapCenter Custom Plug-ins	109
Storage types supported by SnapCenter Custom Plug-ins	109
Prerequisites for adding hosts and installing SnapCenter Custom Plug-ins	109
Host requirements to install SnapCenter Plug-ins Package for Windows ...	111
Host requirements for installing the SnapCenter Plug-ins Package for	
Linux	112
Setting up credentials for SnapCenter Custom Plug-ins	113
Adding hosts and installing plug-in packages on remote hosts	115
Installing SnapCenter Plug-in Packages for Linux or Windows on multiple	
remote hosts by using cmdlets	118
Adding resources to SnapCenter Custom Plug-ins	119
Installing SnapCenter Plug-in for VMware vSphere	122
Managing SnapCenter plug-ins	123
Monitoring SnapCenter plug-in package installation status	123
Managing Configuration Checker	123
Viewing Configuration Checker alerts	124
Running Configuration Checker on the plug-in hosts	124
Managing the Configuration Checker Schedules	125
Identifying available resources	125
Modifying plug-in hosts	125
Adding an ONTAP RBAC role using security login commands	126
ONTAP CLI commands for creating SVM roles	128
Upgrading SnapCenter Server and plug-ins	132
Configuring SnapCenter to check for available updates	132
Backing up the SnapCenter repository	133
Upgrading the SnapCenter Server	133
Upgrading your plug-in packages	135
Uninstalling SnapCenter plug-ins and plug-in packages	137
Removing a host from SnapCenter Server	137
Prerequisites for removing a host	137
Removing a host	138
Uninstalling plug-ins from a host using the SnapCenter GUI	138
Uninstalling Windows plug-ins using the PowerShell cmdlet on the	
SnapCenter Server host	139
Uninstalling plug-ins locally on a host	140
Uninstalling SnapCenter Plug-ins Package for Linux using the	
command-line interface	140
Uninstalling the SnapCenter Server	141
Minimum ONTAP privileges required	142
Features enabled on your Windows host during installation	146
Copyright	148
Trademark	149
How to send comments about documentation and receive update	
 notifications	150

Deciding whether to read the SnapCenter installation and setup information

This information describes how to install or upgrade SnapCenter Server and the required plug-ins, how to add licenses, and how to configure your environment. This information also describes how to import data from previous versions of SnapDrive and SnapManager to your SnapCenter environment.

Before you install any SnapCenter component, you should read the SnapCenter Software Release Notes.

If this information is not suitable for your situation, you should see the following documentation instead:

- Streamlined SnapCenter installation and setup
[*Getting Started*](#)
- SnapCenter architecture, features, and benefits
[*Concepts*](#)
- Deploying the NetApp Data Broker virtual appliance and enabling the SnapCenter Plug-in for VMware vSphere
[*Deployment Guide for SnapCenter Plug-in for VMware vSphere*](#)

After installation, you can use the following information to accomplish your data protection goals:

- SnapCenter concepts, including architecture, features, and benefits
[*Concepts*](#)
- SnapCenter Data Protection Guides for specific types of resources, such as Microsoft SQL Server, Oracle, Windows file systems, and custom plug-ins in the SnapCenter Documentation Center
- SnapCenter administration, including dashboards, reporting capabilities, and REST APIs, and managing licenses, storage connections, and the SnapCenter Server repository
[*Performing administrative tasks*](#)
- SnapCenter PowerShell cmdlets or Linux commands
[*SnapCenter Software 4.2 Windows Cmdlet Reference Guide*](#)
[*SnapCenter Software 4.2 Linux Command Reference Guide*](#)

Preparing for the SnapCenter Server installation

You should be aware of the requirements and prerequisites before installing SnapCenter Server.

- Host requirements
- Supported storage systems and applications
- Supported browsers
- Connection and port requirements
- SnapCenter licensing
- Repository setup
- SVM connections and credentials

The Interoperability Matrix Tool (IMT) contains the latest information about requirements.

[*NetApp Interoperability Matrix Tool*](#)

Host requirements

Before you begin the SnapCenter installation, you should be familiar with the host requirements, domain requirements, sizing requirements, and operating system requirements.

Domain and workgroup requirements

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

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

- If you are using an Active Directory domain: You must use a Domain user with local administrator rights. The Domain user must be a member of the local Administrator group on the Windows host.
- If you are using workgroups: You must use a local account that has local administrator rights.

The *Administration Guide* contains more information about registering untrusted Active Directory domains.

[*Performing administrative tasks*](#)

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

<https://technet.microsoft.com/en-us/library/cc770299.aspx>.

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

Space and sizing requirements

Before you install the SnapCenter Server, you should be familiar with the space and sizing requirements.

Note: Before installing the SnapCenter Server and the plug-ins, you should apply the available system and security updates.

SnapCenter Server requirements

Item	Requirements
Operating Systems	Microsoft Windows For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool
Minimum CPU count	4 cores
Minimum RAM	8 GB Note: The MySQL Server buffer pool uses 20 percent of the total RAM.
Minimum hard drive space for the SnapCenter Server software and logs	4 GB
Minimum hard drive space for the SnapCenter repository	6 GB
Required software packages	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.5.2 or later • Windows Management Framework (WMF) 4.0 or later • PowerShell 4.0 or later <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>

SAN host requirements

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

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

- **Host Utilities**
The Host Utilities support FC and iSCSI, and it enables you to use MPIO on your Windows Servers.
- **ONTAP DSM for Windows MPIO**
This software works with Windows MPIO drivers to manage multiple paths between NetApp and Windows host computers.
A DSM is required for high availability configurations.

For more information, see the Host Utilities and ONTAP DSM for Windows MPIO product documentation and the Interoperability Matrix Tool on the NetApp Support Site.

[NetApp Documentation](#)

[NetApp Interoperability Matrix Tool](#)

Supported storage systems and applications

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

- SnapCenter supports ONTAP 8.3.0 and later to protect your data.
- SnapCenter supports protection of different applications and databases.
For detailed information about the supported applications and databases, see the Interoperability Matrix Tool (IMT).

[NetApp Interoperability Matrix Tool](#)

Related information

[NetApp Documentation: Virtual Storage Console for VMware vSphere](#)

Supported browsers

SnapCenter Software can be used on multiple browsers.

- Chrome
If you are using v66, you might fail to launch SnapCenter GUI. For information about the issue and the solution, see NetApp knowledgebase.
[NetApp Knowledgebase Answer 1078814: SnapCenter will not open in Chrome](#)
- Internet Explorer
 - Only default-level security is supported.
Making changes to Internet Explorer security settings results in significant browser display issues.
 - Internet Explorer compatibility view must be disabled.
- Microsoft Edge

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

[NetApp Interoperability Matrix Tool](#)

Connection and port requirements

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

- Applications cannot share a port.
All ports 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.

SnapCenter uses the following default ports:

Type of port	Default port
SnapCenter port	8146 (HTTPS), bidirectional, customizable, as in the URL <code>https://server:8146</code> Used for communication between the SnapCenter client (the SnapCenter user) and the SnapCenter Server. Also used for communication from the plug-in hosts to the SnapCenter Server.
SnapCenter SMCORE communication port	8145 (HTTPS), bidirectional, customizable The port is used for communication between the SnapCenter Server and the hosts where the SnapCenter plug-ins are installed.
MySQL port	3306 (HTTPS), bidirectional The port is used for communication between SnapCenter and MySQL repository database. You can create secured connections from the SnapCenter Server to the MySQL server. Details are in the <i>Administration Guide</i> . Performing administrative tasks
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 Microsoft Support Article 832017: Service overview and network port requirements for Windows The ports are used for communication between the SnapCenter Server and the host where 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 plug-in hosts	22 (SSH) The ports are used for communication between the SnapCenter Server and the host where the plug-in is being installed. The ports are used by SnapCenter to copy plug-in package binaries to Linux plug-in hosts and should be open or excluded from the firewall or iptables.
SnapCenter Plug-ins Package for Windows	8145 (HTTPS), bidirectional, customizable The port is used for communication between SMCORE and hosts where the SnapCenter plug-ins package for Windows is installed. The communication path also needs to be open between the SVM management LIF and the SnapCenter Server.
SnapCenter Plug-ins Package for Linux	8145 (HTTPS), bidirectional, customizable The port is used for communication between SMCORE and hosts where the SnapCenter plug-ins package for Linux is installed. The communication path needs also to be open between the SVM management LIF and the SnapCenter Server.

Type of port	Default port
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 SAL (Storage Abstraction Layer) for communication between the host running SnapCenter Server and SVM. The port is currently also used by the SAL on SnapCenter for Windows Plug-in hosts for communication between the SnapCenter plug-in host and SVM.
SnapCenter Plug-in for SAP HANA Database ports	<i>3instance_number</i> 13 or <i>3instance_number</i> 15, HTTP or HTTPS, bidirectional, and customizable For a multitenant database container (MDC) single tenant, the port number ends with 13; for non MDC, the port number ends with 15. For example, 32013 is the port number for instance 20 and 31015 is the port number for instance 10.

Licensing requirements

Several licenses are required for data protection operations. The Release Notes contain details about the licenses required for your environment.

[SnapCenter Software Release Notes](#)

Related tasks

[Adding SnapCenter licenses](#) on page 29

SnapCenter repository

The SnapCenter repository, sometimes referred to as the *NSM database*, stores information and metadata for every SnapCenter operation.

The MySQL Server repository database is installed by default when you install the SnapCenter Server. If MySQL Server is already installed and you are doing a fresh installation of SnapCenter Server, you should uninstall the MySQL Server.

SnapCenter supports MySQL Server 5.7.25 or later as the SnapCenter repository database. If you were using an earlier version of MySQL Server with an earlier version of SnapCenter, during SnapCenter upgrade, the MySQL Server is upgraded to 5.7.25.

The SnapCenter repository stores the following information and metadata:

- Backup, clone, restore, and verification metadata
- Reporting, job, and event information
- Host and plug-in information
- Role, user, and permission details
- Storage system connection information

SnapCenter can back up its own repository by using the SnapCenter repository management features. The *Administration Guide* or the *Windows Cmdlet Reference Guide* contain details.

The NetApp Interoperability Matrix Tool (IMT) contains the latest information about the MySQL supported versions.

[NetApp Interoperability Matrix Tool](#)

Related information

[Performing administrative tasks](#)

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

[NetApp Knowledgebase Answer 1087640: SnapCenter Server query is timed out](#)

SVM connections and credentials

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

- SVM connections

SVM connections give the SnapCenter Server and the SnapCenter plug-ins access to ONTAP storage. Setting up these connections also involves configuring AutoSupport and Event Management System (EMS) features.
- Credentials
 - Domain administrator or any member of the administrator group

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

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

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

```
UserName
```
 - Credentials for individual resource groups

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

Related tasks

[Adding storage systems](#) on page 25

You should set up the storage system that gives SnapCenter access to ONTAP storage to perform data protection and provisioning operations. You can either add a stand alone SVM or a cluster comprising of multiple SVMs.

Authentication methods for your credentials

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

Windows authentication

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

Untrusted domain authentication

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

Local workgroup authentication

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

SQL Server authentication

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

Linux authentication

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

Oracle database authentication

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

Oracle ASM authentication

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

RMAN catalog authentication

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

Network Load Balancing and Application Request Routing requirements

You should manually configure NLB and ARR outside of SnapCenter installation for high availability (HA) from SnapCenter 4.2 .

How to configure NLB and ARR with SnapCenter has information about how to configure Network Load Balancing (NLB) and Application Request Routing (ARR) with SnapCenter.

[NetApp Knowledgebase Answer 1087382: How to configure NLB and ARR with SnapCenter](#)

Note: SnapCenter 4.1.1 or earlier supported configuration of Network Load Balancing (NLB) and Application Request Routing (ARR) while installing SnapCenter.

Related information

[Performing administrative tasks](#)

High availability for the SnapCenter MySQL repository

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

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

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

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

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

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

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

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

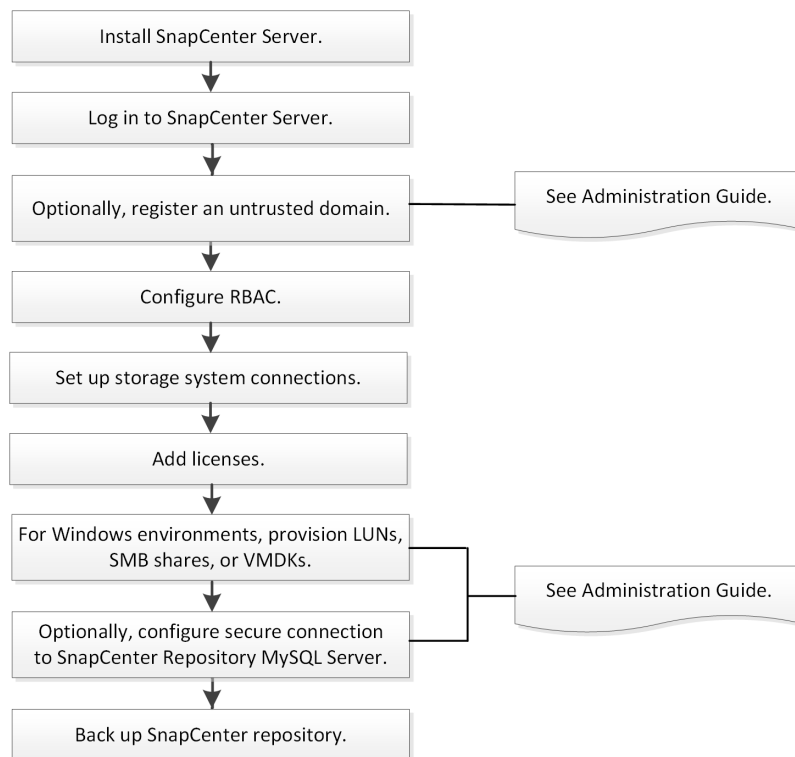
- When failover is initiated, jobs that are running might fail.
If failover happens because MySQL Server or SnapCenter Server is down, then any jobs that are running might fail. After failing over to the second node, all subsequent jobs run successfully.

The *How to configure NLB and ARR with SnapCenter* article contains information about configuring high availability.

[*NetApp Knowledgebase Answer 1087382: How to configure NLB and ARR with SnapCenter*](#)

Installing the SnapCenter Server

To install the SnapCenter Server, you must install SnapCenter, log in, and perform configuration tasks.



You can optionally create secured connections from the SnapCenter Server to the MySQL server. See the *Administration Guide*.

Performing administrative tasks

You can optionally perform several installation and configuration procedures by using PowerShell cmdlets. For details, use the SnapCenter cmdlet help or see the cmdlet reference information.

SnapCenter Software 4.2 Windows Cmdlet Reference Guide

Steps

1. [Installing the SnapCenter Server using the Install wizard](#) on page 18
You can run the SnapCenter Server installer executable to install the SnapCenter Server.
2. [Logging in to SnapCenter](#) on page 19
SnapCenter supports role-based access control (RBAC). SnapCenter admin assigns roles and resources through SnapCenter RBAC to either a user in workgroup or active directory, or to groups in active directory. The RBAC user can now log in to SnapCenter with the assigned roles.
3. [Modifying the SnapCenter default GUI session timeout](#) on page 21
You can modify the SnapCenter GUI session timeout period to make it less than or greater than the default timeout period of 20 minutes.
4. [Configuring role-based access control \(RBAC\)](#) on page 21
After you install SnapCenter Server and log in, you should add users or groups to roles and then assign users access to assets.

5. [Adding storage systems](#) on page 25

You should set up the storage system that gives SnapCenter access to ONTAP storage to perform data protection and provisioning operations. You can either add a stand alone SVM or a cluster comprising of multiple SVMs.

6. [Securing the SnapCenter web server by disabling SSL 3.0](#) on page 27

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

Related information

[Performing administrative tasks](#)

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

Installing the SnapCenter Server using the Install wizard

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

Before you begin

- The SnapCenter Server host must be up to date with Windows updates with no pending system restarts.
- You should have ensured that MySQL Server is not installed on the host where you plan to install the SnapCenter Server.
- You should have enabled Windows installer debugging.
See the Microsoft web site for information about enabling Windows Installer logging.
[Microsoft Support Article 223300: How to enable Windows Installer logging](#)
- You should not install the SnapCenter Server on a host that has Microsoft Exchange Server.

About this task

- Provisioning in Windows environments
For Windows environments, you should provision LUNs, SMB shares, or VMDKs. You can provision after you install the SnapCenter Server by using the SnapCenter Plug-in for Microsoft Windows, as documented in the administration documentation.
[Performing administrative tasks](#)
- Installing from the CLI
Installing SnapCenter Server silently from the command-line is not supported.

Steps

1. Download the SnapCenter Server installation package from NetApp Support Site.
[NetApp Downloads: SnapCenter Software](#)
2. Initiate the SnapCenter Server installation by double-clicking the downloaded .exe file.
After you initiate the installation, all the prechecks are performed and if the minimum requirements are not met appropriate error or warning messages are displayed.
You can ignore the warning messages and proceed with installation; however, errors should be fixed.
3. Review the pre-populated values required for the SnapCenter Server installation and modify if required.

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

Note: The special character “%” is not supported in the custom path for the repository database. If you include “%” in the path, installation fails.

4. Click **Install Now**.

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

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

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

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

```
C:\installer_location\installer_name.exe /log"C:\\"
```

Related information

[NetApp Knowledgebase Answer 1086822: SnapCenter installation fails to create a database with the error: Invalid username/password](#)

[NetApp Knowledgebase Answer 1086821: Unable to access cluster IP address from outside the network](#)

Logging in to SnapCenter

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

Before you begin

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

About this task

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

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

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

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

For Network Load Balance (NLB) deployment, you must access SnapCenter using the NLB cluster IP (https://NLB_Cluster_IP:8146). If you do not see the SnapCenter UI when you navigate to https://NLB_Cluster_IP:8146 in Internet Explorer (IE), you must add the NLB IP address as a trusted site in IE on each plug-in host, or you must disable IE Enhanced Security on each plug-in host.

[NetApp KB Article 2025082: SnapCenter in an HA configuration with Application Request Routing enabled.](#)

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

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

Steps

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

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

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

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

Result

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

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

After logging to SnapCenter Server for the first time, the SnapCenter Server Configuration Checker schedule is created. The default values are Weekly and Every Sunday at 11:59 pm. To modify the schedule or run the SnapCenter Server schedule, click **Settings > Scheduled Configuration Checker**.

After you finish

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

*Performing administrative tasks***Related tasks***Viewing Configuration Checker alerts* on page 124*Running Configuration Checker on the plug-in hosts* on page 124*Managing the Configuration Checker Schedules* on page 125**Related information***SnapCenter Software 4.2 Windows Cmdlet Reference Guide**SnapCenter Software 4.2 Linux Command Reference Guide*

Modifying the SnapCenter default GUI session timeout

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

About this task

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

Steps

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

Configuring role-based access control (RBAC)

After you install SnapCenter Server and log in, you should add users or groups to roles and then assign users access to assets.

See the administration documentation for more information on RBAC.

Performing administrative tasks

Adding a user or group and assigning role and assets

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

Before you begin

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

Note: The group names should not include /[] :;|=,*?<>' characters.

About this task

- SnapCenter includes several predefined roles.

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


- After you assign a role to a user or group that contains the appropriate permissions, you must assign the user access to SnapCenter assets, such as hosts and storage connections. This enables users to perform the actions for which they have permissions on the assets that are assigned to them.
- You should assign a role to the user or group at some point to take advantage of RBAC permissions and efficiencies.
- You can assign assets like host, resource groups, policy, storage connection, plug-in, and credential to the user while creating the user or group.
- When a new node is added to a Windows cluster or a DAG (Exchange Server Database Availability Group) asset and if this new node is assigned to a user, you must reassign the asset to the user or group to include the new node to the user or group.
You should reassign the RBAC user or group to the cluster or DAG to include the new node to the RBAC user or group. For example, you have a two-node cluster and you have assigned an RBAC user or group to the cluster. When you add another node to the cluster, you should reassign the RBAC user or group to the cluster to include the new node for the RBAC user or group.
- If you are planning to replicate Snapshot copies, you must assign the storage connection for both the source and destination volume to the user performing the operation.
You should add assets before assigning access to the users.

Attention: If you are using the NetApp Data Broker, SnapCenter Plug-in for VMware vSphere functions, to protect VMs, VMDKs, or datastores, you use the VMware vSphere GUI to add a vCenter user to a SnapCenter Plug-in for VMware vSphere role. The vCenter documentation contains information about adding a user to a role in vCenter

The SnapCenter concepts documentation contains more information about SnapCenter role-based access control (RBAC).

Concepts

Steps

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

For this field...	Do this...
Access Type	<p>Select either Domain or workgroup</p> <p>For Domain authentication type, you should specify the domain name of the user or group to which you want to add the user to a role.</p> <p>By default, it is pre-populated with the logged in domain name.</p> <p>Note: You must register the untrusted domain in the Settings > Global Settings > Domain Settings page.</p>
Type	<p>Select either User or Group</p> <p>Note: SnapCenter supports only security group and not the distribution group.</p>

For this field...	Do this...
User Name	<p>a. Type the partial user name, and then click Add.</p> <p>Note: The user name is case-sensitive.</p> <p>b. Select the user name from the search list.</p> <p>Note: When you add users from a different domain or an untrusted domain, you should type the user name fully because there is no search list for cross domain users.</p> <p>Repeat this step to add additional users or groups to the selected role.</p>
Roles	Select the role to which you want to add the user.

4. Click **Assign**, and then in the **Assign Assets** page:
 - a. Select the type of asset from the **Asset** drop-down list.
 - b. In the Asset table, select the asset.
The assets are listed only if the user has added the assets to SnapCenter.
 - c. Repeat this procedure for all of the required assets.
 - d. Click **Save**.
5. Click **Submit**.

Related tasks

[Adding an ONTAP RBAC role using security login commands](#) on page 126

Related information

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

Assigning users access to assets

Setting up role-based access control (RBAC) for users is a two-step process. After you add a user or group to a role that contains the appropriate permissions, you must assign the user access to SnapCenter assets, such as hosts and storage connections. This enables users to perform the actions for which they have permissions on the assets that are assigned to them.

About this task

You can assign access to users or groups even if the user or group is not part of a role. This helps you add users or groups; however, you must add the user or group to a role at some point to take advantage of RBAC permissions and efficiencies.

You can also assign credential maintenance to a user.

When you add a new node to a Windows cluster or DAG (Exchange Server Database Availability Group), you should reassign the RBAC user or group to the cluster or DAG to include the new node to the RBAC user or group. For example, you have a two-node cluster and you have assigned an RBAC user or group to the cluster. When you add another node to the cluster, you should reassign the RBAC user or group to the cluster to include the new node for the RBAC user or group.

If you are planning to replicate Snapshot copies, you must assign the storage connection for both the source and destination volume to the user performing the operation. You should add assets before assigning access to the users.

NEED REPLACEMENT TEXT FOR: If you are protecting CMs, VMDKs, or datastores, you must use NDAS.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **User Access**.
3. In the **User Access** page, select the type of asset from the **Asset** drop-down list.
4. In the **Asset** table, select the asset, and then click **Assign**.
5. Select **Domain or Workgroup** as the Authentication type.

For Domain authentication type, you should specify the domain name of the user or group to assign users access to assets.

Note: You must register the untrusted domain in the **Settings > Global Settings > Domain Settings** page.

6. Select either User or Group.
7. Enter the user or group name, and then click **Add**.
If you are not sure about the name, use a more advanced search by clicking the **Search users or group** heading, typing a partial name, and then clicking **Search**.
8. Repeat this procedure until each user or group has access to all of the required assets.
9. Click **OK** to save your changes.

Related tasks

[Adding resources to SnapCenter Custom Plug-ins](#) on page 119

[Adding databases to SnapCenter Plug-in for SAP HANA Database](#) on page 106

Configuring IIS Application Pools to enable Active Directory read permissions

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

Steps

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

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

Adding storage systems

You should set up the storage system that gives SnapCenter access to ONTAP storage to perform data protection and provisioning operations. You can either add a stand alone SVM or a cluster comprising of multiple SVMs.

Before you begin

- You should have the required permissions in the Infrastructure Admin role to create storage connections.
- You should ensure that the plug-in installations are not in progress.
Host plug-in installations must not be in progress while adding a storage system connection because the host cache might not be updated and databases status might be displayed in the SnapCenter GUI as “Not available for backup” or “Not on NetApp storage”.
- Storage system names should be unique.
SnapCenter does not support multiple storage systems with the same name on different clusters. Each storage system that is supported by SnapCenter should have a unique name and a unique data LIF IP address.

About this task

- When you configure storage systems, you can also enable Event Management System (EMS) & AutoSupport features. The AutoSupport tool collects data about the health of your system and automatically sends the data to NetApp technical support, enabling them to troubleshoot your system.
If you enable these features, SnapCenter sends AutoSupport information to the storage system and EMS messages to the storage system syslog when a resource is protected, a restore operation finishes successfully, or an operation fails.
The administrative documentation contains details about managing EMS data collection.
[Performing administrative tasks](#)
- If you are planning to replicate Snapshot copies to a SnapMirror destination or SnapVault destination, you must set up storage system connections for the destination SVM or Cluster as well as the source SVM or Cluster.

Note: If you change the storage system password, scheduled jobs, on demand backup, and restore operations might fail. After you change the storage system password, you should remove and add the storage system.

Steps

1. In the left navigation pane, click **Storage Systems**.
2. In the **Storage Systems** page, click **New**.
3. In the **Add Storage System** page, provide the following information:

For this field...	Do this...
Storage System	<p>Enter the storage system name or IP address.</p> <p>Note: Storage system names, not including the domain name, must have 15 or fewer characters, and the names must be resolvable. To create storage system connections with names that have more than 15 characters, you can use the <code>Add-SmStorageConnection</code> PowerShell cmdlet.</p> <p>SnapCenter does not support multiple SVMs with the same name on different clusters. Each SVM that is supported by SnapCenter must have a unique name.</p> <p>Note: After adding the storage connection to SnapCenter, you should not rename the SVM or the Cluster using ONTAP.</p> <p>Note: If SVM is added with a short name or FQDN then it has to be resolvable from both the SnapCenter and the plug-in host.</p>
User name/ Password	<p>Enter the credentials that are used to access the storage system.</p> <ul style="list-style-type: none"> You should use <code>vsadmin</code> as the user name to add a SVM. You should use <code>admin</code> as the user name to add a cluster.
Event Management System (EMS) & AutoSupport Settings	<p>If you want to send EMS messages to the storage system syslog or if you want to have AutoSupport messages sent to the storage system for applied protection, completed restore operations, or failed operations, select the appropriate checkbox.</p> <p>When you select the Send AutoSupport Notification for failed operations to storage system checkbox, the Log SnapCenter Server events to syslog checkbox is also selected because EMS messaging is required to enable AutoSupport notifications.</p>

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

If the SVM is the secondary storage system in a backup relationship, select the **Secondary** checkbox. When the **Secondary** option is selected, SnapCenter does not perform a license check immediately.
 - b. In **Protocol**, select the protocol that was configured during SVM or Cluster setup, typically HTTPS.
 - c. Enter the port that the storage system accepts.

The default port 443 typically works. See the connection and ports requirements information.
 - d. Enter the time in seconds that should elapse before communication attempts are halted.

The default value is 60 seconds.
 - e. If the SVM has multiple management interfaces, select the **Preferred IP** checkbox, and then enter the preferred IP address for SVM connections.
 - f. Click **Save**.
5. Click **Submit**.

Result

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

- Select **ONTAP SVMs** if you want to view all the SVMs that were added.
- Select **ONTAP Clusters** if you want to view all the clusters that were added.
When you click on the cluster name, all the SVMs that are part of the cluster are displayed in the Storage Virtual Machines section.
If a new SVM is added to the ONTAP cluster using ONTAP GUI, click **Rediscover** to view the newly added SVM.

After you finish

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

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

.

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

For information on managing storage systems, see the *Administration Guide*.

[Performing administrative tasks](#)

Related tasks

[Adding SnapCenter licenses](#) on page 29

Related references

[Connection and port requirements](#) on page 10

Securing the SnapCenter web server by disabling SSL 3.0

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

About this task

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

Steps

1. To launch **Registry Editor** on the SnapCenter web server host, click **Start > Run**, and then enter regedit.
2. In **Registry Editor**, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\
 - If the Server key already exists:
 - a. Select the Enabled DWORD, and then click **Edit > Modify**.
 - b. Change the value to 0, and then click **OK**.

- If the `Server` key does not exist:
 - a. Click **Edit > New > Key**, and then name the key `Server`.
 - b. With the new `Server` key selected, click **Edit > New > DWORD**.
 - c. Name the new DWORD `Enabled`, and then enter 0 as the value.
3. Close **Registry Editor**.

Adding SnapCenter licenses

The SnapCenter Standard license enables the protection of applications, databases, files systems, and virtual machines. Before you add a storage system to SnapCenter, you must install one or more SnapCenter licenses.

About this task

You must install a SnapCenter license if you are using any SnapCenter plug-ins, including the following:

- SnapCenter Plug-in for Microsoft Exchange Server
- SnapCenter Plug-in for Microsoft SQL Server
- SnapCenter Plug-in for Microsoft Windows
- SnapCenter Plug-in for Oracle Database
- SnapCenter Plug-in for UNIX
- SnapCenter Plug-in for SAP HANA Database
- SnapCenter Custom Plug-ins

The type of SnapCenter licenses you install depends on your storage environment and the features that you want to use.

To enable protection of applications, databases, file systems, and virtual machines, you must have either a Standard controller-based license installed on your FAS or AFF storage system, or a Standard capacity-based license installed on your ONTAP Select and Cloud Volumes ONTAP platforms.

A SnapCenter Standard controller-based or Standard capacity license enables you add an SVM to a SnapCenter instance to provide support for all data protection operations provided by SnapCenter plug-ins on ONTAP storage.

Best Practice: It is recommended, but not required, that you also add SnapCenter Standard licenses to secondary destinations. If SnapCenter Standard licenses are not enabled on secondary systems, you cannot use SnapCenter after performing a failover operation. However, FlexClone license on secondary is required to perform clone and verification operations.

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

You can view information about your currently installed capacity-based licenses on the Dashboard Licensed Capacity tile. See the administrative documentation for details.

Related concepts

[SnapCenter Standard controller-based licenses](#) on page 30

[SnapCenter Standard capacity-based licenses](#) on page 35

Related information

[Performing administrative tasks](#)

SnapCenter Standard controller-based licenses

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

The controller-based license has the following characteristics:

- SnapCenter Standard entitlement included with purchase of Premium or Flash Bundle (not with the base pack)
- Unlimited storage usage
- Enabled by adding it directly to the FAS or AFF storage controller by using either the ONTAP System Manager or the storage cluster command line

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

- Is locked to the controller's serial number

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

Viewing SnapManager Suite storage controller license installation status using the SnapCenter GUI



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

Steps

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

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

The Controller License column displays the following statuses:

	Indicates that a SnapManager Suite license is installed on a FAS or AFF primary storage system.
	Indicates that a SnapManager Suite license is not installed on a FAS or AFF primary storage system.

Not applicable	<p>Indicates that a SnapManager Suite license is not applicable for this controller. This message is displayed for the following platforms:</p> <ul style="list-style-type: none"> • Cloud Volumes ONTAP • ONTAP Select • Secondary storage • MetroCluster
----------------	--

Viewing licenses installed on the controller using the ONTAP command line

You can use the ONTAP command line to view all the licenses installed on your controller to determine whether you have the SnapManagerSuite license already installed.

Before you begin

You must be a cluster administrator on the FAS or AFF system.

About this task

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

Steps

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

Example

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

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

Serial Number: 1-81-00000000000000000000000000xx
Owner: cluster1-01
Package      Type      Description      Expiration
-----
NFS          license   NFS License      -
CIFS         license   CIFS License      -
iSCSI        license   iSCSI License      -
FCP          license   FCP License      -
SnapRestore  license   SnapRestore License -
SnapMirror   license   SnapMirror License -
FlexClone    license   FlexClone License -
SnapVault    license   SnapVault License -
SnapManagerSuite license   SnapManagerSuite License -
```

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

After you finish

If no SnapManagerSuite license is displayed, you must obtain your controller serial number, and then retrieve your license from the NetApp Support Site.

Locating the controller serial number

You must know your controller serial number before you can retrieve your SnapCenter controller-based license. You can locate the controller serial number using the ONTAP command line.

Before you begin

You must be a cluster administrator on the FAS or AFF system.

Steps

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

Example

```
cluster1::> system show -instance

                                Node: fas8080-41-42-01
                                Owner:
                                Location: RTP 1.5
                                Model: FAS8080
                                Serial Number: 123451234511
                                Asset Tag: -
                                Uptime: 143 days 23:46
                                NVRAM System ID: xxxxxxxxxx
                                System ID: xxxxxxxxxx
                                Vendor: NetApp
                                Health: true
                                Eligibility: true
                                Differentiated Services: false
                                All-Flash Optimized: false

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

2 entries were displayed.
```

3. Record the serial numbers.

Retrieving SnapCenter controller-based licenses from the NetApp Support Site

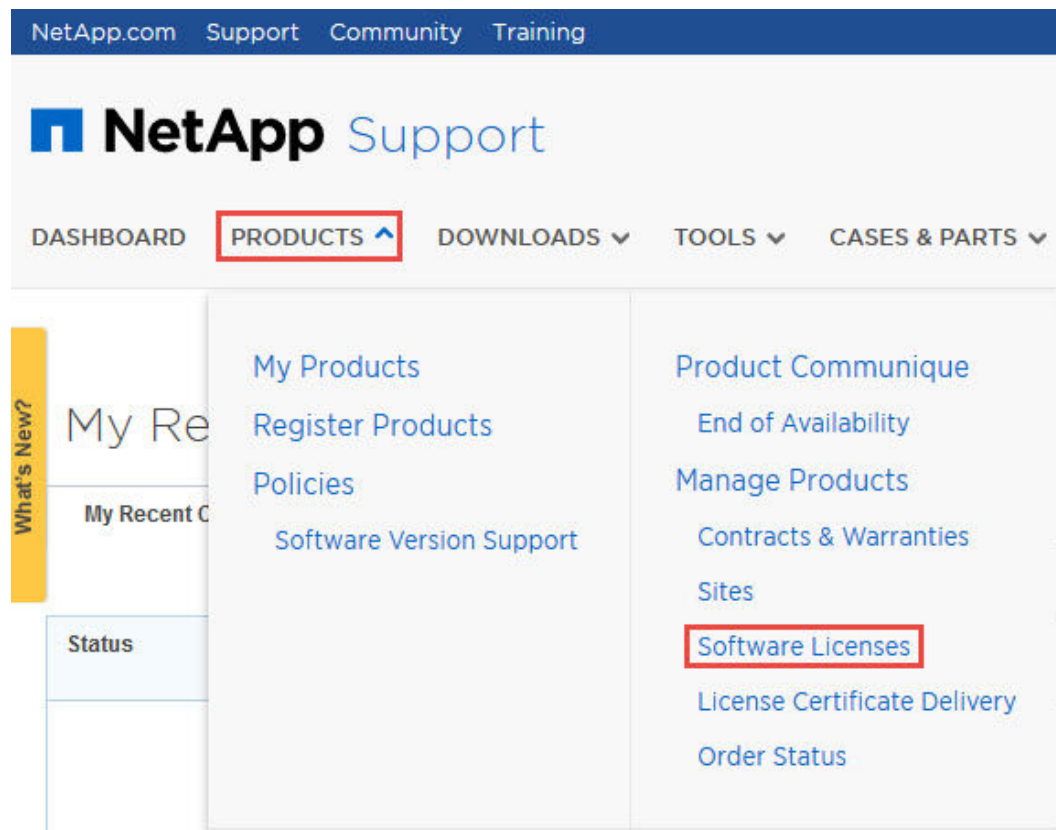
If you are using FAS or AFF storage, you can retrieve the SnapCenter controller-based license from the NetApp Support Site before you can install it using the ONTAP command line.

Before you begin

- You must have valid NetApp Support Site login credentials.
If you do not enter valid credentials, no information is returned for your search.
- You must have the controller serial number.

Steps

1. Log in to the the NetApp Support Site at mysupport.netapp.com.
2. Navigate to **Products > Manage Products > Software Licenses**.



3. In the **Selection Criteria** area, ensure **Serial Number (located on back of unit)** is selected, enter the controller serial number, and then click **Go!**.

Software Licenses

Selection Criteria

Choose a method by which to search

► Enter Value:
 Enter the Cluster Serial Number value without dashes.

- OR -

► Show Me All: For Company:

A list of licenses for the specified controller is displayed.

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

Adding a SnapCenter Standard controller-based license using the ONTAP command line

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

Before you begin

- You must be a cluster administrator on the FAS or AFF system.
- You must have the SnapCenter Standard or SnapManagerSuite license.
- If you want to install SnapCenter on a trial basis with FAS or AFF storage, you can obtain a Premium Bundle evaluation license to install on your controller.
- If you want to install SnapCenter on a trial basis, you should contact your sales representative to obtain a Premium Bundle evaluation license to install on your controller.

About this task

This command is available at the admin privilege level.

Steps

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

```
system license add -license-code license_key
```
3. Verify that the SnapManagerSuite license is installed:

```
license show
```

Removing the trial license

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

Before you begin

A SnapCenter Standard controller-based license must be added before you can remove the trial license. Instructions are in the “Adding a SnapCenter controller-based license using the ONTAP command line” section.

About this task

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

Steps

1. On the SnapCenter Server, open a command prompt.

2. Connect to MySQL:

```
mysql -u root -p
```

MySQL prompts you for the password.

3. Enter the MySQL credentials used at the time of installing SnapCenter.

4. Remove the trial license from the database:

```
use nsm;
```

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

Related tasks

[Adding a SnapCenter Standard controller-based license using the ONTAP command line](#) on page 34

SnapCenter Standard capacity-based licenses

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

The license has the following characteristics:

- Composed of a nine-digit serial number with the format 51xxxxxxx
You use the license serial number and valid NetApp Support Site login credentials to enable the license using the SnapCenter GUI.
- Available as a separate, perpetual license, with the cost based on either the used storage capacity or the size of the data you want protected, whichever is lower, and the data is managed by SnapCenter
- Available per terabyte
For example, you can obtain a capacity-based license for 1 TB, 2 TBs, 4 TBs, and so on.
- Available as a 90-day trial license with 100 TB capacity entitlement

How SnapCenter calculates capacity usage

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

If you are using ONTAP Select or Cloud Volumes ONTAP as your storage platform, you must have a SnapCenter Standard capacity-based license installed to enable SnapCenter features such backup and restore. When you are using a Standard Capacity license, SnapCenter calculates the unused capacity by deducting the used capacity on all volumes from the total licensed capacity. If used capacity exceeds the licensed capacity, an overuse warning is displayed on the SnapCenter Dashboard. If you configured capacity thresholds and notifications in SnapCenter, an email is sent when the used capacity reaches the threshold you specify.

Calculating capacity requirements for a SnapCenter capacity-based license

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

Before you begin

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

About this task

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

Steps

1. Log in to the NetApp controller using the ONTAP command line.
2. To view the volume capacity used, enter the `vol show -field used -volume <volume1>, <volume2>` command.

Example

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

2      entries were displayed.
```

The combined used capacity for the two volumes is less than 5 TB; therefore, if you want to protect all 5 TB of data, the minimum SnapCenter capacity-based license requirement is 5 TB. However, if you want to protect only 2 TB of the 5 TB of total used capacity, you can acquire a 2 TB capacity-based license.

Retrieving SnapCenter capacity-based license serial numbers from the NetApp Support Site

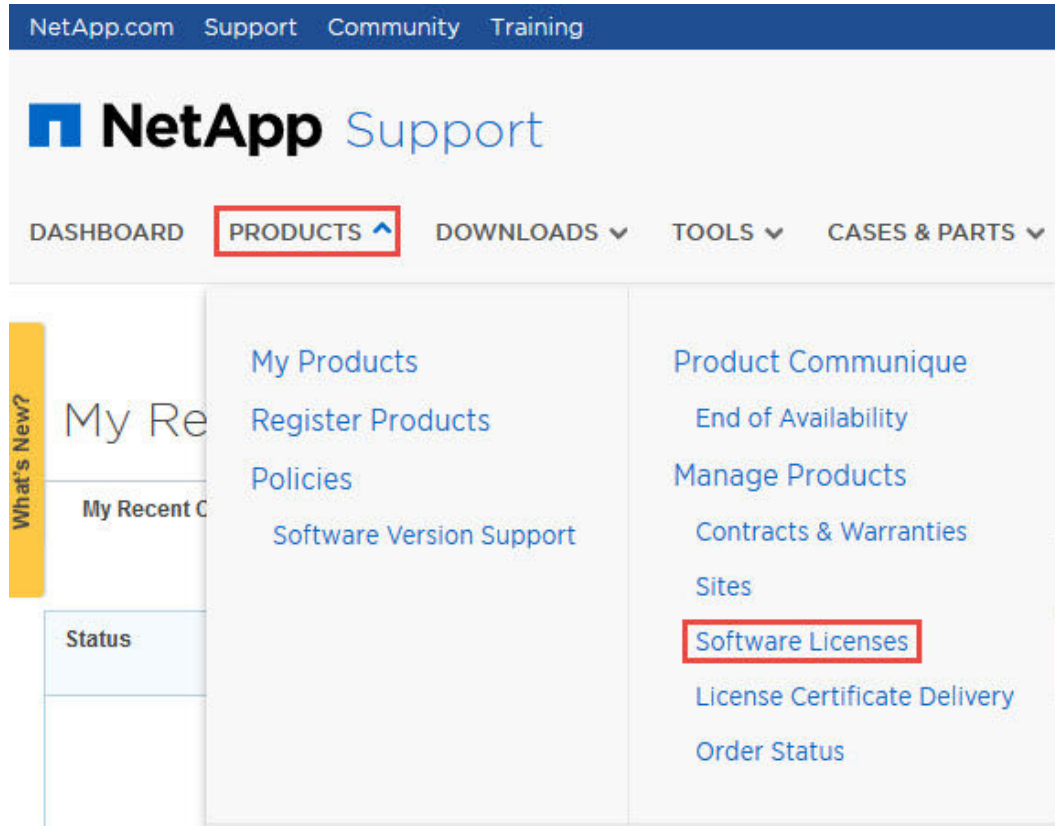
Your SnapCenter capacity-based license serial number is available in your order confirmation or in your documentation package; however, if you do not have this serial number, you can retrieve it from the NetApp Support Site.

Before you begin

You must have valid NetApp Support Site login credentials. If you do not enter valid credentials, no information is returned for your search.

Steps

1. Log in to the the NetApp Support Site at mysupport.netapp.com.
2. Navigate to **Products > Manage Products > Software Licenses**.



3. In the **Selection Criteria** area, choose **SC_STANDARD** from the **Show Me All: Serial Numbers and Licenses** drop-down menu.

Software Licenses

Selection Criteria

Choose a method by which to search

☐ Serial Number (located on back of unit) Enter Value:

Enter the Cluster Serial Number value without dashes.

- OR -

☐ Show Me All: **Serial Numbers with Licenses** For Company:

4. Type your company name, and then click **Go!**.
The nine-digit SnapCenter license serial number, with the format 51xxxxxxx, is displayed.
5. Record the SnapCenter license serial number.

Generating a NetApp license file

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

Before you begin

- You must be using SnapCenter with either ONTAP Select or Cloud Volumes ONTAP.
- You must have valid NetApp Support Site login credentials.

- You must have your nine-digit SnapCenter license serial number in the format 51xxxxxxx.

Steps

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

Adding SnapCenter capacity-based licenses using the SnapCenter GUI

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

Before you begin

- You must log in as the SnapCenter Admin user.
- If you want to log in to the NetApp Support Site using SnapCenter to obtain your licenses, you must have the license serial numbers and valid NetApp Support Site credentials.
- If you are using a NetApp license file (NLF) to add your license, you must know the location of the license file.


About this task

Tasks you can perform on the Settings page:

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

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

Steps

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

For this field...	Do this...
Enter your NetApp Support Site (NSS) login credentials to import licenses	<ol style="list-style-type: none"> Enter your NSS user name. Enter your NSS password. Enter your SnapCenter license serial number. <p>Note: This is not your storage controller serial number. If you are using a storage controller-based capacity license, you must enter it on the storage controller. You do not use the SnapCenter GUI to enter controller-based licenses.</p>
NetApp License File	<ol style="list-style-type: none"> Browse to the location of the license file, and then select it. Click Open.

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

The default threshold is 90 percent.

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

For this field...	Do this...
Email preference	Choose either Always or Never .
Provide email settings	<p>If you select Always, specify the following:</p> <ul style="list-style-type: none"> Sender email address Receiver email address Optional: Edit the default Subject line The default subject reads as follows: "SnapCenter License Capacity Notification"

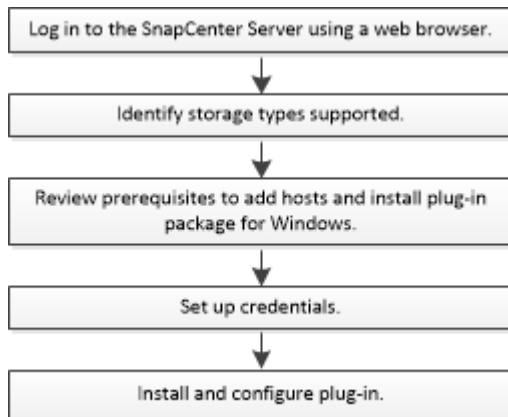
7. If you want to have Event Management System (EMS) messages sent to the storage system syslog or have AutoSupport messages sent to the storage system for failed operations, select the appropriate check boxes.

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

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

Installing SnapCenter Plug-in for Microsoft Exchange Server

You should install and set up SnapCenter Plug-in for Microsoft Exchange Server if you want to protect Exchange databases.



Related tasks

[Setting up credentials for the Plug-in for Windows](#) on page 42

[Adding hosts and installing Plug-in for Exchange](#) on page 43

[Installing Plug-in for Exchange from the SnapCenter Server host using PowerShell cmdlets](#) on page 45

Prerequisites to adding hosts and installing SnapCenter Plug-in for Microsoft Exchange Server

Before you add a host and install the plug-in packages, you must complete all the requirements.

- If you are using iSCSI, the iSCSI service must be running.
- You must have a domain user with local administrator privileges with local login permissions on the remote host.
- You must be using Microsoft Exchange Server 2013 or 2016 for standalone and Database Availability Group configurations.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in or if the user belongs to a local workgroup user, you must disable UAC on the host.
- If you manage cluster nodes in SnapCenter, you must have a user with administrative privileges to all the nodes in the cluster.
- You must have a user with administrative permissions on the Exchange Server.
- If SnapManager for Microsoft Exchange Server and SnapDrive for Windows are already installed, you must unregister the VSS Hardware Provider used by SnapDrive for Windows before you and install Plug-in for Exchange on the same Exchange Server to ensure successful data protection using SnapCenter.

- If SnapManager for Microsoft Exchange Server and Plug-in for Exchange are installed on the same server, you must suspend or delete from the Windows scheduler all schedules created by SnapManager for Microsoft Exchange Server.

[NetApp Interoperability Matrix Tool](#)

Related tasks

[Configuring SnapManager 7.x for Exchange and SnapCenter to coexist](#) on page 47

[Adding SnapCenter licenses](#) on page 29

Exchange Server privileges required

To enable SnapCenter to add Exchange Server or DAG, and to install SnapCenter Plug-in for Microsoft Exchange Server on a host or DAG, you must configure SnapCenter with credentials for a user with a minimum set of privileges and permissions.

You must have a domain user with local administrator privileges, and with local login permissions on the remote Exchange host, as well as administrative permissions on all the nodes in the DAG. The domain user requires the following minimum permissions:

- Add-MailboxDatabaseCopy
- Dismount-Database
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:\$true
- Mount-Database
- New-MailboxDatabase
- New-PublicFolderDatabase
- Remove-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Remove-PublicFolderDatabase
- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:\$true
- Set-MailboxDatabaseCopy

- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

Setting up credentials for the Plug-in for Windows

SnapCenter uses credentials to authenticate users for SnapCenter operations. You should create credentials for installing the plug-in package and additional credentials for performing data protection operations on databases.

About this task

You must set up credentials for installing plug-ins on Windows hosts. Although you can create credentials for Windows after deploying hosts and installing plug-ins, the best practice is to create credentials after you add SVMs, before you deploy hosts and install plug-ins.

Set up the credentials with administrator privileges, including administrator rights on the remote host.

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

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Credential**.
3. Click **New**.
The Credential window is displayed.
4. In the **Credential** page, do the following:

For this field...	Do this...
Credential name	Enter a name for the credential.
Username	<p>Enter the user name used for authentication.</p> <ul style="list-style-type: none"> • Domain administrator or any member of the administrator group Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the <i>Username</i> field are: <code>NetBIOS\UserName</code> <code>Domain FQDN\UserName</code> • Local administrator (for workgroups only) For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the <i>Username</i> field is: <code>UserName</code>

For this field...	Do this...
Password	Enter the password used for authentication.
Authentication	Select Windows as the authentication mode.

5. Click **OK**.

Adding hosts and installing Plug-in for Exchange

You can use the SnapCenter Add Host page to add Windows hosts. The Plug-in for Exchange is automatically installed on the specified host. This is the recommended method for installing plug-ins. You can add a host and install a plug-in either for an individual host or a cluster.

Before you begin

- You must be a user that is assigned to a role that has the plug-in install and uninstall permissions, such as the SnapCenter Admin.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in, or if the user belongs to a local workgroup user, you must disable UAC on the host.
- The message queueing service must be running.

About this task

You can add a host and install plug-in packages either for an individual host or a cluster. If you are installing plug-ins on a cluster (Exchange DAG), they are installed on all of the nodes of the cluster even if some of nodes do not have databases on NetApp LUNs.

Plug-in for Exchange depends on SnapCenter Plug-ins Package for Windows, and the versions must be the same. During the Plug-in for Exchange installation, SnapCenter Plug-ins Package for Windows is selected by default and is installed along with the VSS Hardware Provider.

If SnapManager for Microsoft Exchange Server and SnapDrive for Windows are already installed, and you want to install Plug-in for Exchange on the same Exchange Server, you must unregister the VSS Hardware Provider used by SnapDrive for Windows because it is incompatible with the VSS Hardware Provider installed with Plug-in for Exchange and SnapCenter Plug-ins Package for Windows.

The administration documentation contains information about managing hosts.

Performing administrative tasks

Steps

1. In the left navigation pane, click **Hosts**.
2. Verify that **Managed Hosts** is selected at the top.
3. Click **Add**.
4. On the **Hosts** page, do the following:

For this field...	Do this...
Host Type	<p>Select Windows as the host type.</p> <p>SnapCenter Server adds the host and then installs on the host the Plug-in for Windows and the Plug-in for Exchange if they are not already installed.</p> <p>Plug-in for Windows and Plug-in for Exchange must be the same version. If a different version of Plug-in for Windows was previously installed, SnapCenter updates the version as part of the installation.</p>
Host name	<p>Enter the fully qualified domain name (FQDN) or the IP address of the host.</p> <p>SnapCenter depends on the proper configuration of the DNS. Therefore, the best practice is to enter the fully qualified domain name (FQDN).</p> <p>An IP address is supported for untrusted domain hosts only if it resolves to the FQDN.</p> <p>You can enter IP addresses or the FQDN of one of the following:</p> <ul style="list-style-type: none"> • Stand-alone host • Exchange DAG <p>If you are adding a host using SnapCenter and it is part of a subdomain, you must provide the FQDN.</p>
Credentials	<p>Select the credential name that you created, or create the new credentials.</p> <p>The credential must have administrative rights on the remote host. For details, see information about creating a credential.</p> <p>You can view details about the credentials by positioning your cursor over the credential name that you specified.</p> <p>Note: Credentials authentication mode is determined by the host type that you specify in the Add Host wizard.</p>

5. In the **Select Plug-ins to Install** section, select the plug-ins to install.

When you select Plug-in for Exchange, SnapCenter Plug-in for Microsoft SQL Server is deselected automatically. Microsoft recommends that SQL Server and Exchange server not be installed on the same system due to the amount of memory used and other resource usage required by Exchange.

6. (Optional) Click **More Options**.

For this field...	Do this...
Port	<p>Either retain the default port number or specify the port number. The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port.</p> <p>Note: If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.</p>
Installation Path	<p>The default path is C:\Program Files\NetApp\SnapCenter. You can optionally customize the path.</p>

For this field...	Do this...
Add all hosts in the DAG	Select this check box when you add a DAG..
Skip preinstall checks	Select this check box if you already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.

7. Click **Submit.**

If you have not selected the Skip prechecks check box, the host is validated to determine whether it meets the requirements to install the plug-in. If the minimum requirements are not met, the appropriate error or warning messages are displayed.

If the error is related to disk space or RAM, you can update the `web.config` file located at `C:\Program Files\NetApp\SnapCenter WebApp` to modify the default values. If the error is related to other parameters, you must fix the issue.

Note: In an NLB setup, if you are updating `web.config` file, you must update the file on both nodes.

8. Monitor the installation progress.

Result

The configuration checker operation is triggered automatically and provides alerts for recommendations, corrective actions, and notifications to resolve the issues.

Related tasks

[Configuring SnapManager 7.x for Exchange and SnapCenter to coexist](#) on page 47

[Viewing Configuration Checker alerts](#) on page 124

[Running Configuration Checker on the plug-in hosts](#) on page 124

[Managing the Configuration Checker Schedules](#) on page 125

Related information

[NetApp Knowledgebase Answer 1087846: Validation of adding a host fails](#)

Installing Plug-in for Exchange from the SnapCenter Server host using PowerShell cmdlets

You should install the Plug-in for Exchange from the SnapCenter GUI. If you do not want to use the GUI, you can use PowerShell cmdlets on the SnapCenter Server host or on a remote host.

Before you begin

- SnapCenter Server must have been installed and configured.
- You must be a local administrator on the host or a user with administrative privileges.
- You must be a user that is assigned to a role that has the plug-in, install, and uninstall permissions, such as the SnapCenter Admin.
- You must have reviewed the installation requirements and types of supported configurations before installing the Plug-in for Exchange.
- The host on which you want the Plug-in for Exchange installed must be a Windows host.

Steps

1. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
2. Add the host on which you want to install the Plug-in for Exchange using the `Add-SmHost` cmdlet with the required parameters.

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

The host can be a standalone host or a DAG. If you specify a DAG, the `-IsDAG` parameter is required.

3. Install the Plug-in for Exchange using the `Install-SmHostPackage` cmdlet with the required parameters.

This command installs the Plug-in for Exchange on the specified host, and then registers the plug-in with SnapCenter.

Related tasks

[Setting up credentials for the Plug-in for Windows](#) on page 42

Related references

[Prerequisites to adding hosts and installing SnapCenter Plug-in for Microsoft Exchange Server](#) on page 40

Installing the SnapCenter Plug-in for Exchange silently from the command line

You should install Plug-in for Exchange from within the SnapCenter user interface. However, if you cannot for some reason, you can run the Plug-in for Exchange installation program unattended in silent mode from the Windows command line.

Before you begin

- You must have backed up your Microsoft Exchange Server resources.
- SnapCenter plug-in packages must be installed.

Steps

1. Download the SnapCenter Plug-in for Microsoft Windows from `C:\ProgramData\NetApp\SnapCenter\Package Repository`.

This path is accessible from the host where the SnapCenter Server is installed.

2. Copy the installation file to the host on which you want to install the plug-in.
3. From a Windows command prompt on the local host, navigate to the directory to which you saved the plug-in installation files.
4. Enter the following command to install replacing the variables with your data:

```
"snapcenter_windows_host_plugin.exe"/silent /
debuglog"<Debug_Log_Path>" /log"<Log_Path>" BI_SNAPCENTER_PORT=<Num>
```

```
SUITE_INSTALLDIR="<Install_Directory_Path>" BI_SERVICEACCOUNT=<domain
\administrator> BI_SERVICEPWD=<password> ISFeatureInstall=SCW,SCE
```

For example,

```
"C:\ProgramData\NetApp\SnapCenter\Package Repository
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
\HPPW_SCSQL_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW,SCE
```

Enter the following values for the variables:

Variable	Value
<i>/</i> <i>debuglog</i> " <i><Debug_Log_Path></i>	Specify the name and location of the suite installer log file, as in the following example: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
<i>BI_SNAPCENTER_PORT</i>	Specify the port on which SnapCenter communicates with SMCORE.
<i>SUITE_INSTALLDIR</i>	Specify host plug-in package installation directory.
<i>BI_SERVICEACCOUNT</i>	Specify SnapCenter Plug-in for Microsoft Windows web service account.
<i>BI_SERVICEPWD</i>	Specify the password for SnapCenter Plug-in for Microsoft Windows web service account.
<i>ISFeatureInstall</i>	Specify the solution to be deployed by SnapCenter on remote host.

Configuring SnapManager 7.x for Exchange and SnapCenter to coexist

To enable SnapCenter Plug-in for Microsoft Exchange Server to coexist with SnapManager for Microsoft Exchange Server, you need to install SnapCenter Plug-in for Microsoft Exchange Server on the same Exchange Server on which SnapManager for Microsoft Exchange Server is installed, disable SnapManager for Exchange schedules, and configure new schedules and backups using SnapCenter Plug-in for Microsoft Exchange Server.

Before you begin

- SnapManager for Microsoft Exchange Server and SnapDrive for Windows are already installed, and SnapManager for Microsoft Exchange Server backups exist on the system and in the SnapInfo directory.
- You have deleted or reclaimed backups taken by SnapManager for Microsoft Exchange Server that you no longer require.
- You have suspended or deleted from the Windows scheduler all schedules created by SnapManager for Microsoft Exchange Server.

About this task

- SnapCenter Plug-in for Microsoft Exchange Server and SnapManager for Microsoft Exchange Server can coexist on the same Exchange Server, but you cannot upgrade existing SnapManager for Microsoft Exchange Server installations to SnapCenter. SnapCenter does not provide an option for the upgrade.
- SnapCenter does not support restoring Exchange databases from SnapManager for Microsoft Exchange Server backup.

If you do not uninstall SnapManager for Microsoft Exchange Server after the SnapCenter Plug-in for Microsoft Exchange Server installation and later want to restore a SnapManager for Microsoft Exchange Server backup, you must perform additional steps.

Steps

1. Using PowerShell on all DAG nodes, determine whether the SnapDrive for Windows VSS Hardware Provider is registered:

```
vssadmin list providers
```

Example

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
Version: 7. 1. 4. 6845
```

2. From the SnapDrive directory, unregister the VSS Hardware Provider from SnapDrive for Windows:
3. Verify that the VSS Hardware Provider was removed:
4. Add the Exchange host to SnapCenter, and then install the SnapCenter Plug-in for Microsoft Windows and the SnapCenter Plug-in for Microsoft Exchange Server.
5. From the SnapCenter Plug-in for Microsoft Windows directory on all DAG nodes, verify that the VSS Hardware Provider is registered:

```
vssadmin list providers
```

Example

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
Version: 7. 0. 0. 5561
```

6. Stop the SnapManager for Microsoft Exchange Server backup schedules.
 7. Using the SnapCenter GUI, create on-demand backups, configure scheduled backups, and configure retention settings.
 8. Uninstall SnapManager for Microsoft Exchange Server.
- If you do not uninstall SnapManager for Microsoft Exchange Server now and later want to restore a SnapManager for Microsoft Exchange Server backup:

- a. Unregister SnapCenter Plug-in for Microsoft Exchange Server from all DAG nodes:

```
navssprv.exe -r service -u
```



```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for  
Microsoft Windows>navssprv.exe -r service -u
```

- b. From the C:\Program Files\NetApp\SnapDrive\ directory, register SnapDrive for Windows on all DAG nodes:

```
navssprv.exe -r service -a hostname\username -p password
```

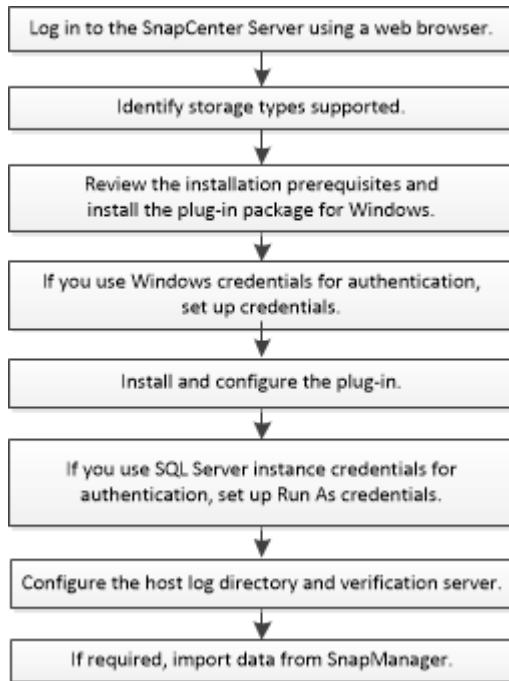
Related tasks

[Adding hosts and installing Plug-in for Exchange](#) on page 43

Installing SnapCenter Plug-in for Microsoft SQL Server

You should install and set up the SnapCenter Plug-in for Microsoft SQL Server if you want to protect SQL Server databases.

About this task



Storage types supported by SnapCenter Plug-ins for Microsoft Windows and for Microsoft SQL Server

SnapCenter supports a wide range of storage types on both physical machines and virtual machines. You must verify whether support is available for your storage type before installing the package for your host.

SnapCenter provisioning and data protection support is available on Windows Server. For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT).

[*NetApp Interoperability Matrix Tool*](#)

Machine	Storage type	Provision using	Support notes
Physical server	FC-connected LUNs	SnapCenter graphical user interface (GUI) or PowerShell cmdlets	
	iSCSI-connected LUNs	SnapCenter GUI or PowerShell cmdlets	
	SMB3 (CIFS) shares residing on a storage virtual machine (SVM)	SnapCenter GUI or PowerShell cmdlets	Support for provisioning only. You cannot use SnapCenter to back up any data or shares using the SMB protocol.
VMware VM	RDM LUNs connected by an FC or iSCSI HBA	PowerShell cmdlets	
	iSCSI LUNs connected directly to the guest system by the iSCSI initiator	SnapCenter GUI or PowerShell cmdlets	
	Virtual Machine File Systems (VMFS) on VMFS or NFS datastores	VMware vSphere or VSC cloning utility	
	A guest system connected to SMB3 shares residing on an SVM	SnapCenter GUI or PowerShell cmdlets	Support for provisioning only. You cannot use SnapCenter to back up any data or shares using the SMB protocol.
Hyper-V VM	Virtual FC (vFC) LUNs connected by a virtual Fibre Channel Switch	SnapCenter GUI or PowerShell cmdlets	You must use Hyper-V Manager to provision Virtual FC (vFC) LUNs connected by a virtual Fibre Channel Switch.
	iSCSI LUNs connected directly to the guest system by the iSCSI initiator	SnapCenter GUI or PowerShell cmdlets	
	A guest system connected to SMB3 shares residing on an SVM	SnapCenter GUI or PowerShell cmdlets	Support for provisioning only. You cannot use SnapCenter to back up any data or shares using the SMB protocol.
	Note: Hyper-V pass through disks and backing up databases on VHD(x) that are provisioned on NetApp storage are not supported.		

Prerequisites to adding hosts and installing SnapCenter Plug-in for Microsoft SQL Server

Before you add a host and install the plug-ins packages, you must complete all the requirements.

- If you are using iSCSI, the iSCSI service must be running.
- You must have a user with local administrator privileges with local login permissions on the remote host.
- If you manage cluster nodes in SnapCenter, you must have a user with administrative privileges to all the nodes in the cluster.
- You must have a user with sysadmin permissions on the SQL Server.
SnapCenter Plug-in for Microsoft SQL Server uses Microsoft VDI Framework, which requires sysadmin access.

[Microsoft Support Article 2926557: SQL Server VDI backup and restore operations require Sysadmin privileges](#)

- When installing a plug-in on a Windows host, if you specify a credential that is not built-in or if the user belongs to a local workgroup user, you must disable UAC on the host.
- If SnapManager for Microsoft SQL Server is installed, you must have stopped or disabled the service and schedules.
If you plan to import backup or clone jobs into SnapCenter, do not uninstall SnapManager for Microsoft SQL Server.
- Data protection using SnapCenter requires a two-way trust relationship between the SnapCenter Server domain and the plug-in domain using the Microsoft Active Directory Domains and Trusts snap-in.
Although domain trusts, multidomain forests, and cross-domain trusts are supported, cross-forest domains are not.
<https://technet.microsoft.com/en-us/library/cc770299.aspx>
- The host must be resolvable to the fully qualified domain name (FQDN) from the server. If the hosts file is modified to make it resolvable and if both the short name and the FQDN are specified in the hosts file, create a entry in the SnapCenter hosts file in the following format:
`<ip_address> <host_fqdn> <host_name>`

Related tasks

[Adding SnapCenter licenses](#) on page 29

Host requirements to install SnapCenter Plug-ins Package for Windows

Before you install the SnapCenter Plug-ins Package for Windows, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating Systems	<p>Microsoft Windows</p> <p>Note: You must enable the Cluster Shared Volumes (CSV) feature in Windows Server 2008 R2 SP1 if you want to create CSV-type disks.</p> <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	<p>2 GB</p> <p>Note: You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.</p>
Required software packages	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.5.2 or later • Windows Management Framework (WMF) 4.0 or later • PowerShell 4.0 or later <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>

Setting up credentials for the SnapCenter Plug-ins Package for Windows

SnapCenter uses credentials to authenticate users for SnapCenter operations. You should create credentials for installing SnapCenter plug-ins and additional credentials for performing data protection operations on databases or Windows file systems.

About this task

- You must set up Windows credentials before installing plug-ins.
- You must set up the credentials with administrator privileges, including administrator rights on the remote host.

- SQL authentication on Windows hosts

You must set up SQL credentials after installing plug-ins.

If you are deploying SnapCenter Plug-in for Microsoft SQL Server, you must set up SQL credentials after installing plug-ins. Set up a credential for a user with SQL Server sysadmin permissions.

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

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Credential**.
3. Click **New**.
4. In the **Credential** page, specify the information required for configuring credentials:

For this field...	Do this...
Credential name	Enter a name for the credential.
User name/Password	<p>Enter the user name and password that are to be used for authentication.</p> <ul style="list-style-type: none"> • Domain administrator Specify the domain administrator on the system on which you are installing the SnapCenter plug-in. Valid formats for the <i>Username</i> field are: <i>NetBIOS\UserName</i> <i>Domain FQDN\UserName</i> • Local administrator (for workgroups only) For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the <i>Username</i> field is: <i>UserName</i> <p>Do not use double quotes (") in passwords.</p>
Authentication Mode	<p>Select the authentication mode that you want to use.</p> <p>If you select the SQL authentication mode, you must also specify the SQL server instance and the host where the SQL instance is located.</p>

5. Click **OK**.

After you finish

After you finish setting up the credentials, you might want to assign credential maintenance to a user or group of users on the My SnapCenter Assets page.

Configuring credentials for an individual SQL Server resource

You can configure credentials to perform data protection jobs on individual SQL Server resources for each user. While you can configure the credentials globally, you might want to do this only for a particular resource.

About this task

- If you are using Windows credentials for authentication, you must set up your credential before installing plug-ins.
However, if you are using an SQL Server instance for authentication, you must add the credential after installing plug-ins.
- If you have enabled SQL authentication while setting up the credentials, the discovered instance or database is shown with a red color lock icon.
If the lock icon appears, you must specify the instance or database credentials to successfully add the instance or database to a resource group.
- You must assign the credential to a role-based access control (RBAC) user without sysadmin access when the following conditions are met:
 - The credential is assigned to an SQL instance.
 - The SQL instance or host is assigned to an RBAC user.



The user must have both the resource group and backup privileges.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Credential**.
3. To add a new credential, click **New**.
4. In the **Credential** page, configure the credentials:

For this field...	Do this...
Credential name	Enter a name for the credentials.

For this field...	Do this...
Username	<p>Enter the user name used for SQL Server authentication.</p> <ul style="list-style-type: none"> Domain administrator or any member of the administrator group Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the <i>Username</i> field are: <code>NetBIOS\UserName</code> <code>Domain FQDN\UserName</code> Local administrator (for workgroups only) For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the <i>Username</i> field is: <code>UserName</code>
Password	Enter the password used for authentication.
Authentication mode	<p>Select the SQL Server authentication mode.</p> <p>You can also choose Windows authentication if the Windows user has sysadmin privileges on the SQL server.</p>
Host	Select the host.
SQL Server Instance	Select the SQL Server Instance.

5. Click **OK** to add the credential.
6. In the left navigation pane, click **Resources**.
7. In the **Resources** page, select **Instance** from the **View** list.
 - a. Click , and then select the host name to filter the instances.
 - b. Click  to close the filter pane.

Note: The credential option does not apply to databases and availability groups.
8. In the **Instance Protect** page, protect the instance, and if required, click **Configure Credentials**.
If the user who is logged in to the SnapCenter Server does not have access to SnapCenter Plug-in for Microsoft SQL Server, then the user has to configure the credentials.
9. Click **Refresh Resources**.

Adding hosts and installing the SnapCenter Plug-ins Package for Windows

You must use the SnapCenter Add Host page to add hosts, and then install the plug-ins packages. The plug-ins are automatically installed on the remote hosts.

Before you begin

- You must be a user that is assigned to a role that has the plug-in install and uninstall permissions, such as the SnapCenter Admin role.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in, you should disable UAC on the host.
- You should ensure that the message queueing service is in running state.

About this task

You can add a host and install the plug-in packages either for an individual host or for a cluster. If you are installing the plug-ins on a cluster or WSFC, the plug-ins are installed on all of the nodes of the cluster.

For information on managing hosts, see the administration documentation.

Performing administrative tasks

Steps

1. In the left navigation pane, click **Hosts**.
2. Verify that the **Managed Hosts** tab is selected at the top.
3. Click **Add**.
4. On the **Hosts** page:

For this field...	Do this...
Host Type	<p>Select Windows as the host type.</p> <p>The SnapCenter Server adds the host, and then installs the Plug-in for Windows if the plug-in is not already installed on the host.</p> <p>If you select the Microsoft SQL Server option on the Plug-ins page, the SnapCenter Server installs the Plug-in for SQL Server.</p>
Host name	<p>Enter the fully qualified domain name (FQDN) or the IP address of the host.</p> <p>IP address is supported for untrusted domain hosts only if it resolves to the FQDN.</p> <p>SnapCenter depends on the proper configuration of the DNS. Therefore, the best practice is to enter the FQDN.</p> <p>You can enter the IP addresses or FQDN of one of the following:</p> <ul style="list-style-type: none"> • Stand-alone host • Windows Server Failover Clustering (WSFC) <p>If you are adding a host by using SnapCenter and the host is part of a subdomain, you must provide the FQDN.</p>

For this field...	Do this...
Credentials	<p>Select the credential name that you created or create new credentials.</p> <p>The credential must have administrative rights on the remote host. For details, see the information about creating credentials.</p> <p>You can view details about the credentials by positioning your cursor over the credential name that you specified.</p> <p>Note: The credentials authentication mode is determined by the host type that you specify in the Add Host wizard.</p>

5. In the **Select Plug-ins to Install** section, select the plug-ins to install.

6. (Optional) Click **More Options**.

For this field...	Do this...
Port	<p>Either retain the default port number or specify the port number. The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port.</p> <p>Note: If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.</p>
Installation Path	The default path is C:\Program Files\NetApp\SnapCenter. You can optionally customize the path.
Add all hosts in the cluster	Select this check box to add all of the cluster nodes in a WSFC or a SQL Availability Group.
Skip preinstall checks	Select this check box if you already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.

7. Click **Submit**.

8. For SQL Plug-in, select the host to configure the log directory.

9. Click **Configure log directory** and on the **Configure host log directory** page, click **Browse** and complete the following steps:

Only NetApp LUNs (drives) are listed for selection. SnapCenter backs up and replicates the host log directory as part of the backup operation.

- a. Select the drive letter or mount point on the host where the host log will be stored.
- b. Choose a subdirectory, if required.
- c. Click **Save**.

10. Click **Submit.**

If you have not selected the Skip prechecks check box, the host is validated to verify whether it meets the requirements for installing the plug-in. The disk space, RAM, PowerShell version, .NET version, location (for Windows plug-ins), and Java version (for Linux plug-ins) are validated against the minimum requirements. If the minimum requirements are not met, appropriate error or warning messages are displayed.

If the error is related to disk space or RAM, you can update the `web.config` file located at `C:\Program Files\NetApp\SnapCenter WebApp` to modify the default values. If the error is related to other parameters, you must fix the issue.

Note: In an NLB setup, if you are updating `web.config` file, you must update the file on both nodes.

11. Monitor the installation progress.

Result

The configuration checker operation is triggered automatically and provides alerts for recommendations, corrective actions, and notifications to resolve the issues.

Related tasks

[Setting up credentials for the SnapCenter Plug-ins Package for Windows](#) on page 53

[Viewing Configuration Checker alerts](#) on page 124

[Running Configuration Checker on the plug-in hosts](#) on page 124

[Managing the Configuration Checker Schedules](#) on page 125

Related references

[Prerequisites to adding hosts and installing SnapCenter Plug-in for Microsoft SQL Server](#) on page 52

[Host requirements to install SnapCenter Plug-ins Package for Windows](#) on page 53

Related information

[NetApp Knowledgebase Answer 1086819: Unable to install plug-in or the installed plug-in is not discovered](#)

[NetApp Knowledgebase Answer 1087846: Validation of adding a host fails](#)

Installing SnapCenter Plug-in for Microsoft Windows on multiple remote hosts by using cmdlets

You can install the SnapCenter Plug-ins Package for Windows on multiple hosts simultaneously by using the `Install-SmHostPackage` PowerShell cmdlet.

Before you begin

You must have logged in to SnapCenter as a domain user with local administrator rights on each host on which you want to install the plug-in package.

Steps

1. Launch PowerShell.
2. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
3. Install the SnapCenter Plug-in for Microsoft Windows on multiple remote hosts using the `Install-SmHostPackage` cmdlet and the required parameters.

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

You can use the `-skipprecheck` option when you have already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.

4. Enter your credentials for remote installation.

Related tasks

[Setting up credentials for the SnapCenter Plug-ins Package for Windows](#) on page 53

[Setting up credentials for the SnapCenter Plug-ins Package for Windows](#) on page 53

Related references

[Prerequisites to adding hosts and installing SnapCenter Plug-in for Microsoft SQL Server](#) on page 52

[Installation requirements for SnapCenter Plug-in for Microsoft Windows](#) on page 66

Installing SnapCenter Plug-in for Microsoft SQL Server independently

You can install the SnapCenter Plug-in for Microsoft SQL Server locally if you are unable to install the plug-in from the SnapCenter user interface.

Preparation to install the SnapCenter Plug-in for Microsoft SQL Server

The SnapCenter Plug-in for Microsoft SQL Server installer consists of third-party and NetApp packages. You can also upgrade, repair, or remove the packages using the installer.

Third-party packages

Following are the third-party packages:

- **Microsoft Visual C++ 2012 Redistributable Package (x86)**
This installs runtime components that are required to run C++ applications built with Visual Studio 2012.
- **Microsoft SQL Server 2016 CLR Types (x64)**
This is part of the Microsoft SQL Server Feature Pack but also is a stand-alone software that can be installed separately. The SQL Server System CLR Types package contains the components implementing the new geometry, geography, and hierarchy ID types in SQL Server 2016. You can install this component separately from the server to allow client applications to use these types outside of the server.
- **Microsoft SQL Server 2016 Management Objects (x64)**
This is a collection of objects that are designed for programming all aspects of managing Microsoft SQL Server. This object model works with SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, and SQL Server 2016. It is included in all SQL Server editions, including the Express Edition and requires Microsoft SQL Server System CLR Types.

The SnapCenter Plug-in for Microsoft SQL Server requires all these packages to perform backup, restore, and recovery operations for SQL databases running on NetApp storage systems.

Prerequisites

The following must have already been installed:

- SnapCenter Plug-in for Microsoft Windows on the same host where SnapCenter Plug-in for Microsoft SQL Server is installed
SnapCenter Server must be installed on a separate host.
- Windows PowerShell v4.0 or later for Windows Server 2008 R2 SP1
- Microsoft .Net Framework v4.5.2 or later
- The latest Microsoft Windows updates

Installing the SnapCenter Plug-in for Microsoft SQL Server silently from the command line

You should install SnapCenter Plug-in for Microsoft SQL Server from within the SnapCenter user interface. However, if you cannot for some reason, you can run the SnapCenter Plug-in for Microsoft SQL Server installation program unattended in silent mode from the Windows command line.

Before you begin

- You must have backed up your SQL databases.
- SnapCenter plug-in packages must be installed.

Steps

1. Download the SnapCenter Plug-in for Microsoft Windows from C:\ProgramData\NetApp\SnapCenter\Package Repository.
This path is accessible from the host where the SnapCenter Server is installed.
2. Copy the installation file to the host on which you want to install the plug-in.
3. From a Windows command prompt on the local host, navigate to the directory to which you saved the plug-in installation files.
4. Enter the following command to install replacing the variables with your data:

```
"snapcenter_windows_host_plugin.exe" /silent /
debuglog"<Debug_Log_Path>" /log"<Log_Path>" BI_SNAPCENTER_PORT=<Num>
SUITE_INSTALLDIR=<Install_Directory_Path>" BI_SERVICEACCOUNT=<domain
\administrator> BI_SERVICEPWD=<password> ISFeatureInstall=SCW,SCSQL
```

For example,

```
"C:\ProgramData\NetApp\SnapCenter\Package Repository
\snapcenter_windows_host_plugin.exe" /silent /debuglog"C:
\HPPW_SCSQL_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW,SCSQL
```

Enter the following values for the variables:

Variable	Value
/ debuglog"<Debug_Log_Path>	Specify the name and location of the suite installer log file, as in the following example: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
BI_SNAPCENTER_PORT	Specify the port on which SnapCenter communicates with SMCORE.
SUITE_INSTALLDIR	Specify host plug-in package installation directory.
BI_SERVICEACCOUNT	Specify SnapCenter Plug-in for Microsoft Windows web service account.
BI_SERVICEPWD	Specify the password for SnapCenter Plug-in for Microsoft Windows web service account.
ISFeatureInstall	Specify the solution to be deployed by SnapCenter on remote host.

Related tasks

[Setting up credentials for the SnapCenter Plug-ins Package for Windows](#) on page 53

[Configuring credentials for an individual SQL Server resource](#) on page 55

Related references

[Prerequisites to adding hosts and installing SnapCenter Plug-in for Microsoft SQL Server](#) on page 52

Importing archived backups from SnapManager for Microsoft SQL Server to SnapCenter

Importing data from SnapManager for Microsoft SQL Server to SnapCenter enables you to continue to use your data from previous versions. You can import only those backups that were archived using SnapVault technology from SnapManager for Microsoft SQL Server to SnapCenter.

SnapCenter does not support Data ONTAP operating in 7-Mode. You can use the 7-Mode Transition Tool to migrate data and configurations that are stored on a system running Data ONTAP operating in 7-Mode to an ONTAP system.

Related information

[NetApp Documentation: 7-Mode Transition Tool](#)

Limitations related to the import feature

Understanding limitations before you import archived backups from SnapManager for Microsoft SQL Server to SnapCenter will help you complete the import successfully. These backups must have been archived with SnapVault technology.

- You cannot manage clones created using SnapManager for Microsoft SQL Server in SnapCenter. You must manage the clones in SnapManager for Microsoft SQL Server.
- You cannot import backups from the SnapCenter graphical user interface (GUI).

Importing archived backups

You can import only those backups that were archived using SnapVault technology from SnapManager for Microsoft SQL Server to SnapCenter from the command-line interface.

Before you begin

- Both the SnapCenter Plug-in for Microsoft SQL Server and SnapManager for Microsoft SQL Server 7.x must be installed on the same host.
 - For cluster support, both the plug-in and 7.x product must have been installed on each node in the cluster.
 - You must have added the host or cluster to SnapCenter and discovered the resources available for backup on the host or cluster.
 - You must have backed up the SnapManager for Microsoft SQL Server SnapInfo folder.
- If the import operation fails, you can retrieve the backup metadata from the SnapInfo directory.

Best Practice: It is a best practice to configure the log backup folder for the SnapCenter Plug-in for Microsoft SQL Server.

For information on SnapCenter installation and configuration tasks, see the SnapCenter installation information. For information on SnapManager for Microsoft SQL Server installation and configuration tasks, see the SnapManager installation information.

About this task

After the archived backups have been imported to SnapCenter from SnapManager for Microsoft SQL Server, you can perform restore and clone operations on these backups from SnapCenter. Simultaneously, you can also continue to perform backup, restore, and clone operations using SnapManager for Microsoft SQL Server.

Steps

1. Perform the following steps to create schedules similar to SnapManager for Microsoft SQL Server schedules manually in SnapCenter:
 - a. Retrieve the schedule information from SnapManager for Microsoft SQL Server by using the `Get-SmSchedule` cmdlet.
 - b. Save the schedule information.
You can use this schedule information while creating policies in SnapCenter.
 - c. Disable SnapManager for Microsoft SQL Server schedules by using the `Get-SmSchedule -Hostname <hostname> -PluginCode SMSQL -DisableCurrentGenSchedule` cmdlet.
2. Import archived backups by using the `Invoke-SmBackupMigration` cmdlet.

Related information

[*Protecting Microsoft SQL Server databases*](#)

[*SnapManager 7.2 for Microsoft SQL Server Installation and Setup Guide For Clustered Data ONTAP*](#)

Viewing the imported backups in SnapCenter Server

After you have imported your SnapManager for Microsoft SQL Server archived backups, you can view these backups in SnapCenter from the **Topology** page.

Steps

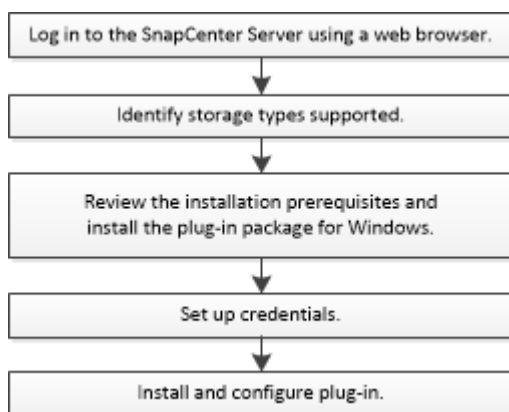
1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. Create a resource group with all the databases.
3. Select the resource group.
4. Protect the resource group.
5. In the **Topology** page, **Manage Copies** view, click backups from Vault copies.
The details of the backups are displayed.

Related information

[*Protecting Microsoft SQL Server databases*](#)

Installing SnapCenter Plug-in for Microsoft Windows

You must install and set up SnapCenter Plug-in for Microsoft Windows if you want to protect Windows files that are not database files.



Storage types supported by SnapCenter Plug-ins for Microsoft Windows and for Microsoft SQL Server

SnapCenter supports a wide range of storage types on both physical machines and virtual machines. You must verify whether support is available for your storage type before installing the package for your host.

SnapCenter provisioning and data protection support is available on Windows Server. For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT).

[NetApp Interoperability Matrix Tool](#)

Machine	Storage type	Provision using	Support notes
Physical server	FC-connected LUNs	SnapCenter graphical user interface (GUI) or PowerShell cmdlets	
	iSCSI-connected LUNs	SnapCenter GUI or PowerShell cmdlets	
	SMB3 (CIFS) shares residing on a storage virtual machine (SVM)	SnapCenter GUI or PowerShell cmdlets	Support for provisioning only. You cannot use SnapCenter to back up any data or shares using the SMB protocol.

Machine	Storage type	Provision using	Support notes
VMware VM	RDM LUNs connected by an FC or iSCSI HBA	PowerShell cmdlets	
	iSCSI LUNs connected directly to the guest system by the iSCSI initiator	SnapCenter GUI or PowerShell cmdlets	
	Virtual Machine File Systems (VMFS) on VMFS or NFS datastores	VMware vSphere or VSC cloning utility	
	A guest system connected to SMB3 shares residing on an SVM	SnapCenter GUI or PowerShell cmdlets	Support for provisioning only. You cannot use SnapCenter to back up any data or shares using the SMB protocol.
Hyper-V VM	Virtual FC (vFC) LUNs connected by a virtual Fibre Channel Switch	SnapCenter GUI or PowerShell cmdlets	You must use Hyper-V Manager to provision Virtual FC (vFC) LUNs connected by a virtual Fibre Channel Switch.
	iSCSI LUNs connected directly to the guest system by the iSCSI initiator	SnapCenter GUI or PowerShell cmdlets	
	A guest system connected to SMB3 shares residing on an SVM	SnapCenter GUI or PowerShell cmdlets	Support for provisioning only. You cannot use SnapCenter to back up any data or shares using the SMB protocol.
	Note: Hyper-V pass through disks and backing up databases on VHD(x) that are provisioned on NetApp storage are not supported.		

Installation requirements for SnapCenter Plug-in for Microsoft Windows

You should be aware of certain installation requirements before you install the Plug-in for Windows.

Before you begin to use the Plug-in for Windows, the SnapCenter administrator must install and configure SnapCenter Server and perform prerequisite tasks.

- You must have SnapCenter admin privileges to install the Plug-in for Windows. The SnapCenter admin role must have admin privileges.
- You must have installed and configured the SnapCenter Server.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in or if the user belongs to a local workgroup user, you must disable UAC on the host.
- You must set up SnapMirror and SnapVault if you want backup replication.

For details, see SnapCenter installation information.

Related tasks

[Adding SnapCenter licenses](#) on page 29

Related references

[Host requirements](#) on page 8

Adding storage systems

You should set up the storage system that gives SnapCenter access to ONTAP storage to perform data protection and provisioning operations. You can either add a stand alone SVM or a cluster comprising of multiple SVMs.

Before you begin

- You should have the required permissions in the Infrastructure Admin role to create storage connections.
- You should ensure that the plug-in installations are not in progress.
Host plug-in installations must not be in progress while adding a storage system connection because the host cache might not be updated and databases status might be displayed in the SnapCenter GUI as “Not available for backup” or “Not on NetApp storage”.
- Storage system names should be unique.
SnapCenter does not support multiple storage systems with the same name on different clusters. Each storage system that is supported by SnapCenter should have a unique name and a unique data LIF IP address.

About this task

- When you configure storage systems, you can also enable Event Management System (EMS) & AutoSupport features. The AutoSupport tool collects data about the health of your system and automatically sends the data to NetApp technical support, enabling them to troubleshoot your system.
If you enable these features, SnapCenter sends AutoSupport information to the storage system and EMS messages to the storage system syslog when a resource is protected, a restore operation finishes successfully, or an operation fails.
The administrative documentation contains details about managing EMS data collection.
[Performing administrative tasks](#)
- If you are planning to replicate Snapshot copies to a SnapMirror destination or SnapVault destination, you must set up storage system connections for the destination SVM or Cluster as well as the source SVM or Cluster.

Note: If you change the storage system password, scheduled jobs, on demand backup, and restore operations might fail. After you change the storage system password, you should remove and add the storage system.

Steps

1. In the left navigation pane, click **Storage Systems**.
2. In the **Storage Systems** page, click **New**.
3. In the **Add Storage System** page, provide the following information:

For this field...	Do this...
Storage System	<p>Enter the storage system name or IP address.</p> <p>Note: Storage system names, not including the domain name, must have 15 or fewer characters, and the names must be resolvable. To create storage system connections with names that have more than 15 characters, you can use the <code>Add-SmStorageConnection</code> PowerShell cmdlet.</p> <p>SnapCenter does not support multiple SVMs with the same name on different clusters. Each SVM that is supported by SnapCenter must have a unique name.</p> <p>Note: After adding the storage connection to SnapCenter, you should not rename the SVM or the Cluster using ONTAP.</p> <p>Note: If SVM is added with a short name or FQDN then it has to be resolvable from both the SnapCenter and the plug-in host.</p>
User name/ Password	<p>Enter the credentials that are used to access the storage system.</p> <ul style="list-style-type: none"> You should use <code>vsadmin</code> as the user name to add a SVM. You should use <code>admin</code> as the user name to add a cluster.
Event Management System (EMS) & AutoSupport Settings	<p>If you want to send EMS messages to the storage system syslog or if you want to have AutoSupport messages sent to the storage system for applied protection, completed restore operations, or failed operations, select the appropriate checkbox.</p> <p>When you select the Send AutoSupport Notification for failed operations to storage system checkbox, the Log SnapCenter Server events to syslog checkbox is also selected because EMS messaging is required to enable AutoSupport notifications.</p>

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

If the SVM is the secondary storage system in a backup relationship, select the **Secondary** checkbox. When the **Secondary** option is selected, SnapCenter does not perform a license check immediately.
 - b. In **Protocol**, select the protocol that was configured during SVM or Cluster setup, typically HTTPS.
 - c. Enter the port that the storage system accepts.

The default port 443 typically works. See the connection and ports requirements information.
 - d. Enter the time in seconds that should elapse before communication attempts are halted.

The default value is 60 seconds.
 - e. If the SVM has multiple management interfaces, select the **Preferred IP** checkbox, and then enter the preferred IP address for SVM connections.
 - f. Click **Save**.
5. Click **Submit**.

Result

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

- Select **ONTAP SVMs** if you want to view all the SVMs that were added.
- Select **ONTAP Clusters** if you want to view all the clusters that were added.
When you click on the cluster name, all the SVMs that are part of the cluster are displayed in the Storage Virtual Machines section.
If a new SVM is added to the ONTAP cluster using ONTAP GUI, click **Rediscover** to view the newly added SVM.

After you finish

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

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

.

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

For information on managing storage systems, see the *Administration Guide*.

[Performing administrative tasks](#)

Related tasks

[Adding SnapCenter licenses](#) on page 29

Related references

[Connection and port requirements](#) on page 10

Setting up your credentials for the Plug-in for Windows

SnapCenter uses credentials to authenticate users for SnapCenter operations. You should create credentials for installing SnapCenter plug-ins, and additional credentials for performing data protection operations on Windows file systems.

About this task

You must set up Windows credentials before installing plug-ins.

You must set up the credentials with administrator privileges, including administrator rights, on the remote host.

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

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Credential**.
3. Click **New**.
4. In the **Credential** page, do the following:

For this field...	Do this...
Credential name	Enter a name for the credentials.
User name/Password	<p>Enter the user name and password used for authentication.</p> <ul style="list-style-type: none"> Domain administrator or any member of the administrator group Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the <i>Username</i> field are as follows: <i>NetBIOS\UserName</i> <i>Domain FQDN\UserName</i> <i>UserName@upn</i> Local administrator (for workgroups only) For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the <i>Username</i> field is as follows: <i>UserName</i> <p>Do not use double quotes (") in passwords.</p>
Password	Enter the password used for authentication.
Authentication Mode	<p>Select the authentication mode that you want to use.</p> <p>If you select the SQL authentication mode, you must also specify the SQL server instance and the host where the SQL instance is located.</p>

5. Click **OK**.

After you finish

After you finish setting up credentials, you might want to assign credential maintenance to a user or group of users on the My SnapCenter Assets page.

Adding hosts and installing SnapCenter Plug-in for Microsoft Windows

You can use the SnapCenter Add Host page to add Windows hosts. The SnapCenter Plug-in for Microsoft Windows is automatically installed on the specified host. This is the recommended method for installing plug-ins. You can add a host and install a plug-in either for an individual host or a cluster.

Before you begin

- You must be a user that is assigned to a role that has the plug-in install and uninstall permissions, such as the SnapCenter Admin role.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in or if the user belongs to a local workgroup user, you must disable UAC on the host.

- The SnapCenter user should be added to the “Log on as a service” role of the Windows Server.
- You should ensure that the message queueing service is in running state.

About this task

- Windows plug-ins
 - Microsoft Windows
 - Microsoft SQL Server
 - SAP HANA
 - Custom plug-ins
- Installing plug-ins on a cluster
If you install plug-ins on a cluster (WSFC, Oracle RAC, or Exchange DAG), they are installed on all of the nodes of the cluster.
- E-series storage
You cannot install the Plug-in for Windows on a Windows host connected to E-series storage.

The administration documentation has more information on managing hosts..

Performing administrative tasks

Steps

1. In the left navigation pane, click **Hosts**.
2. Ensure that **Managed Hosts** is selected at the top.
3. Click **Add**.
4. On the **Hosts** page, do the following:

For this field...	Do this...
Host Type	<p>Select the Windows type of host.</p> <p>SnapCenter Server adds the host and then installs the Plug-in for Windows if it is not already installed on the host.</p> <p>If you also select the Microsoft SQL Server option on the Plug-ins page, SnapCenter Server also installs the Plug-in for SQL Server.</p>
Host name	<p>Enter the fully qualified domain name (FQDN) or the IP address of the host.</p> <p>SnapCenter depends on the proper configuration of the DNS. Therefore, the best practice is to enter the fully qualified domain name (FQDN).</p> <p>You can enter the IP addresses or FQDN of one of the following:</p> <ul style="list-style-type: none"> • Stand-alone host • Windows Server Failover Clustering (WSFC) <p>If you are adding a host using SnapCenter and it is part of a subdomain, you must provide the FQDN.</p>

For this field...	Do this...
Credentials	<p>Select the credential name that you created or create the new credentials.</p> <p>The credential must have administrative rights on the remote host. For details, see information about creating a credential.</p> <p>Details about credentials, including the user name, domain, and host type, are displayed by placing your cursor over the credential name you provided.</p> <p>Note: credentials authentication mode is determined by the host type that you specify in the Add Host wizard.</p>

5. In the **Select Plug-ins to Install** section, select the plug-ins to install.

For new deployments, no plug-in packages are listed.

6. (Optional) Click **More Options**.

For this field...	Do this...
Port	<p>Either retain the default port number or specify the port number. The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port.</p> <p>Note: If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.</p>
Installation Path	<p>The default path is C:\Program Files\NetApp\SnapCenter. You can optionally customize the path.</p> <p>For SnapCenter Plug-ins Package for Windows, the default path is C:\Program Files\NetApp\SnapCenter. However, if you want, you can customize the default path.</p>
Add all hosts in the cluster	Select this check box to add all of the cluster nodes in a WSFC or a SQL Availability Group.
Skip preinstall checks	Select this check box if you already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.

7. Click **Submit**.

If you have not selected the **Skip prechecks** checkbox, the host is validated to see whether it meets the requirements to install the plug-in. The disk space, RAM, PowerShell version, .NET version, and location are validated against the minimum requirements. If the minimum requirements are not met, appropriate error or warning messages are displayed.

If the error is related to disk space or RAM, you can update the `web.config` file located at C:\Program Files\NetApp\SnapCenter\WebApp to modify the default values. If the error is related to other parameters, you must fix the issue.

Note: In an NLB setup, if you are updating `web.config` file, you must update the file on both nodes.

8. Monitor the installation progress.

Result

The configuration checker operation is triggered automatically and provides alerts for recommendations, corrective actions, and notifications to resolve the issues.

Related tasks

[Adding a user or group and assigning role and assets](#) on page 21

[Viewing Configuration Checker alerts](#) on page 124

[Running Configuration Checker on the plug-in hosts](#) on page 124

[Managing the Configuration Checker Schedules](#) on page 125

Related information

[NetApp Knowledgebase Answer 1086819: Unable to install plug-in or the installed plug-in is not discovered](#)

[NetApp Knowledgebase Answer 1087846: Validation of adding a host fails](#)

Installing SnapCenter Plug-in for Microsoft Windows on multiple remote hosts using PowerShell cmdlets

If you want to install SnapCenter Plug-in for Microsoft Windows on multiple hosts at one time, you can do so by using the `Install-SmHostPackage` PowerShell cmdlet.

Before you begin

You must have logged in to SnapCenter as a domain user with local administrator rights on each host on which you want to install plug-ins.

Steps

1. Launch PowerShell.
2. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
3. Add the standalone host or the cluster to SnapCenter using the `Add-SmHost` cmdlet and the required parameters.

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

4. Install the plug-in on multiple hosts using the `Install-SmHostPackage` cmdlet and the required parameters.

You can use the `-skipprecheck` option when you have installed the plug-ins manually and do not want to validate whether the host meets the requirements to install the plug-in.

Related tasks

[Setting up your credentials for the Plug-in for Windows](#) on page 69

Related references

[Installation requirements for SnapCenter Plug-in for Microsoft Windows](#) on page 66

Installing the SnapCenter Plug-in for Microsoft Windows silently from the command line

You can install the SnapCenter Plug-in for Microsoft Windows locally on a Windows host if you are unable to install the plug-in remotely from the SnapCenter GUI. You can run the SnapCenter Plug-in for Microsoft Windows installation program unattended, in silent mode, from the Windows command line.

Before you begin

- If installed, you must have stopped the Windows Host utilities and provisioning and protection capabilities of the OnCommand Unified Manager Core Package.
- You must have installed Microsoft .Net 4.5.2 or later.
- You must have installed PowerShell 4.0 or later.
- You must have turned on Windows message queuing.
- You must be a local administrator on the host.

Steps

1. Download the SnapCenter Plug-in for Microsoft Windows from your install location. For example, the default installation path is `C:\ProgramData\NetApp\SnapCenter\Package Repository`.

This path is accessible from the host where the SnapCenter Server is installed.
2. Copy the installation file to the host on which you want to install the plug-in.
3. From the command prompt, navigate to the directory where you downloaded the installation file.
4. Enter the following command, replacing variables with your data:

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog" /log"
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT=
BI_SERVICEPWD= ISFeatureInstall=SCW
```

For example,

```
"C:\ProgramData\NetApp\SnapCenter\Package Repository
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
\HPPW_SCW_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW
```

Enter the values for the following variables:

Variable	Value
<code>/ debuglog" <Debug_Log_Path></code>	Specify the name and location of the suite installer log file, as in the following example: <code>Setup.exe /debuglog"C:\PathToLog\setupexe.log"</code> .
<code>BI_SNAPCENTER_PORT</code>	Specify the port on which SnapCenter communicates with SMCORE.
<code>SUITE_INSTALLDIR</code>	Specify host plug-in package installation directory.
<code>BI_SERVICEACCOUNT</code>	Specify SnapCenter Plug-in for Microsoft Windows web service account.
<code>BI_SERVICEPWD</code>	Specify the password for SnapCenter Plug-in for Microsoft Windows web service account.

Variable	Value
<i>ISFeatureInstall</i>	Specify the solution to be deployed by SnapCenter on remote host.

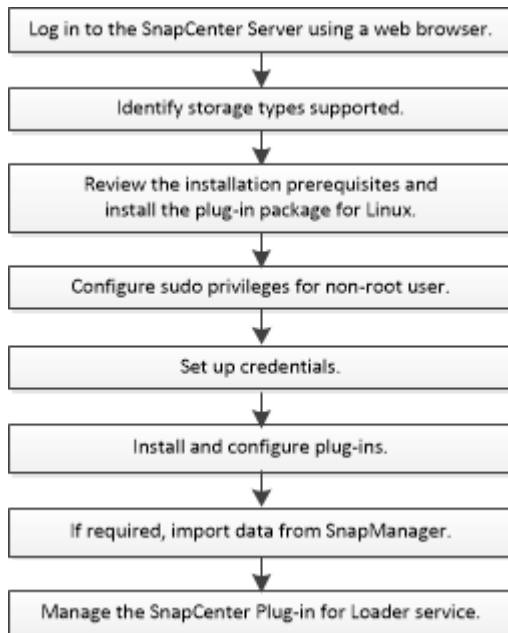
The `debuglog` parameter includes the path of the log file for SnapCenter. Writing to this log file is the preferred method of obtaining troubleshooting information, because the file contains the results of checks that the installation performs for plug-in prerequisites.

If necessary, you can find additional troubleshooting information in the log file for the SnapCenter for Windows package. Log files for the package are listed (oldest first) in the `%Temp%` folder, for example, `C:\temp\`.

Installing SnapCenter Plug-in for Oracle Database

You should install and set up the SnapCenter Plug-in for Oracle Database if you want to protect Oracle databases.

About this task



Storage types supported by SnapCenter Plug-in for Oracle Database

SnapCenter supports a wide range of storage types on both physical and virtual machines. You must verify the support for your storage type before installing the SnapCenter Plug-ins Package for Linux.

Storage provisioning using SnapCenter is not supported for SnapCenter Plug-ins Package for Linux.

Machine	Storage type
Physical server	FC-connected LUNs
	iSCSI-connected LUNs
	NFS-connected volumes
VMware ESX	RDM LUNs connected by an FC or iSCSI ESXi HBA
	iSCSI LUNs connected directly to the guest system by the iSCSI initiator
	VMDKs on VMFS or NFS datastores
	NFS volumes connected directly to the guest system

The storage configurations not supported by SnapCenter Plug-in for Oracle Database are:

- ASM on VMDK

- ASM on RDM LUN
- RAC on VMDK
- RAC on RDM LUN

Prerequisites for adding hosts and installing SnapCenter Plug-in for Oracle Database

Before you add a host and install the plug-ins packages, you must complete all the requirements.

- If you are using iSCSI, the iSCSI service must be running.
- You must have enabled the password-based SSH connection for the root or non-root user. From SnapCenter 2.0, SnapCenter Plug-in for Oracle Database can be installed by a non-root user. However, you must configure the sudo privileges for the non-root user to install and start the plug-in process.
- You must have installed Java 1.8, 64-bit, on your Linux host. The Interoperability Matrix Tool (IMT) contains the latest information about requirements.
[Java Downloads for All Operating Systems](#)
[NetApp Interoperability Matrix Tool](#)
- For Oracle databases that are running on a Linux host, you must install both SnapCenter Plug-in for Oracle Database and SnapCenter Plug-in for UNIX.
Note: You can use the Plug-in for Oracle Database to manage Oracle databases for SAP as well. However, SAP BR*Tools integration is not supported.
- If you are using Oracle database 11.2.0.3 or later, you must install the 13366202 Oracle patch.
- You should always have read/write permission for the “/tmp” folder on the plug-in host.

Related tasks

[Adding SnapCenter licenses](#) on page 29

Configuring sudo privileges for non-root users

SnapCenter 2.0 and later releases enable a non-root user to install the SnapCenter Plug-ins Package for Linux and to start the plug-in process. You must configure sudo privileges for the non-root user to provide access to several paths.

Before you begin

- You should be using Sudo 1.8.7 or later.
- You should ensure that the non-root user is part of the Oracle installation group.
- You should edit the `/etc/ssh/sshd_config` file to configure the message authentication code algorithms: MACs `hmac-sha2-256` and MACs `hmac-sha2-512`. Restart the `sshd` service after updating the configuration file.
Example:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
```

```
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

About this task

You should configure sudo privileges for the non-root user to provide access to the following paths:

- `/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin`
- `/custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/custom_location/NetApp/snapcenter/spl/bin/spl`

Steps

1. Log in to the Linux host on which you want to install the SnapCenter Plug-ins Package for Linux.
2. Add the following lines to the `/etc/sudoers` file by using the `visudo` Linux utility.

Example

```
Cmnd_Alias SCCMD = sha224:checksum_value== /tmp/sc-plugin
-installer/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /tmp/netapp/Linux_Prechecks.sh
non_root_user ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
env_keep=JAVA_HOME
Defaults:non_root_user !visiblepw
Defaults:non_root_user !requiretty
```

`non_root_user` is the name of the non-root user that you created.

You can obtain the checksum value from the `oracle_checksum.txt` file, which is located at `C:\ProgramData\NetApp\SnapCenter\Package Repository`. If you have specified a custom location, the location will be `custom_path\NetApp\SnapCenter\Package Repository`.

Important: The example should be used only as a reference for creating your own data.

Host requirements for installing the SnapCenter Plug-ins Package for Linux

Before you install the SnapCenter Plug-ins Package for Linux, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating systems	<ul style="list-style-type: none"> Red Hat Enterprise Linux Oracle Linux <p>Note: If you are using Oracle database on LVM in Oracle Linux or Red Hat Enterprise Linux 6.6 or 7.0 operating systems, you must install the latest version of Logical Volume Manager (LVM).</p> SUSE Linux Enterprise Server (SLES) <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	2 GB <p>Note: You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.</p>
Required software packages	Java 1.8 (64-bit) Oracle Java and OpenJDK flavors If you have upgraded JAVA to the latest version, you must ensure that the JAVA_HOME option located at <code>/var/opt/snapcenter/spl/etc/spl.properties</code> is set to the correct JAVA version and the correct path. For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool

Setting up your credentials for the SnapCenter Plug-ins Package for Linux

SnapCenter uses credentials to authenticate users for SnapCenter operations. You should create credentials for installing the plug-in package and additional credentials for performing data protection operations on databases.

About this task

You must set up credentials for installing plug-ins on Linux hosts. You must set up the credentials for the root user or for a non-root user who has sudo privileges to install and start the plug-in process.

Best Practice: Although you are allowed to create credentials for Linux after deploying hosts and installing plug-ins, the best practice is to create credentials after you add SVMs, before you deploy hosts and install plug-ins.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Credential**.
3. Click **New**.

4. In the **Credential** page, enter the credential information:

For this field...	Do this...
Credential name	Enter a name for the credentials.

For this field...	Do this...
User name/Password	<p>Enter the user name and password that are to be used for authentication.</p> <ul style="list-style-type: none"> Domain administrator Specify the domain administrator on the system on which you are installing the SnapCenter plug-in. Valid formats for the <i>Username</i> field are: <code>NetBIOS\UserName</code> <code>Domain FQDN\UserName</code> Local administrator (for workgroups only) For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the <i>Username</i> field is: <code>UserName</code>
Authentication Mode	Select the authentication mode that you want to use.
Use sudo privileges	Select the Use sudo privileges check box if you are creating credentials for a non-root user.

5. Click **OK**.

After you finish

After you finish setting up the credentials, you might want to assign credential maintenance to a user or group of users on the My SnapCenter Assets page.

Configuring credentials for an Oracle database

You must configure credentials that are used to perform data protection operations on Oracle databases.

Before you begin

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






About this task

If you have enabled Oracle database authentication, a red lock icon is shown in the resources view. You must configure database credentials to be able to protect the database or add it to the resource group to perform data protection operations.

Note: If you specify incorrect details while creating a credential, an error message is displayed. You must click **Cancel**, and then retry.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.

2. In the **Resources** page, select **Database** from the **View** list.
3. Click , and then select the host name and the database type to filter the resources.
You can then click  to close the filter pane.
4. Select the database, and then click **Database Settings > Configure Database**.
5. In the **Configure database settings** section, from the **Use existing Credential** drop-down list, select the credential that should be used to perform data protection jobs on the Oracle database.
You can also create a credential by clicking .
Note: The database port number is automatically populated.
6. In the **Configure ASM settings** section, from the **Use existing Credential** drop-down list, select the credential that should be used to perform data protection jobs on the ASM instance.
You can also create a credential by clicking .
Note: The ASM instance port number is automatically populated.
7. In the **Configure RMAN catalog settings** section, from the **Use existing credential** drop-down list, select the credential that should be used to perform data protection jobs on the Oracle Recovery Manager (RMAN) catalog database.
You can also create a credential by clicking .
In the **TNSName** field, enter the Transparent Network Substrate (TNS) file name that will be used by the SnapCenter Server to communicate with the database.
8. In the **Preferred RAC Nodes** field, specify the Real Application Cluster (RAC) nodes preferred for backup.
The preferred nodes might be one or all cluster nodes where the RAC database instances are present. The backup operation is triggered only on these preferred nodes in the order of preference.
In RAC One Node, only one node is listed in the preferred nodes, and this preferred node is the node where the database is currently hosted.
After failover or relocation of RAC One Node database, refreshing of resources in the SnapCenter Resources page will remove the host from the **Preferred RAC Nodes** list where the database was earlier hosted. The RAC node where the database is relocated will be listed in **RAC Nodes** and will need to be manually configured as the preferred RAC node.
9. Click **OK**.

Adding hosts and installing the SnapCenter Plug-ins Package for Linux

You must use the SnapCenter Add Host page to add hosts, and then install the SnapCenter Plug-ins Package for Linux. The plug-ins are automatically installed on the remote hosts.

Before you begin

- You must be a user that is assigned to a role that has the plug-in install and uninstall permissions, such as the SnapCenter Admin role.

- You should ensure that the message queueing service is running.

About this task

You can add a host and install plug-in packages either for an individual host or for a cluster. If you are installing the plug-in on a cluster (Oracle RAC), the plug-in is installed on all of the nodes of the cluster. For Oracle RAC One Node, you should install the plug-in on both active and passive nodes.

The administration documentation contains information about managing hosts.

Performing administrative tasks

Steps

1. In the left navigation pane, click **Hosts**.
2. Verify that the **Managed Hosts** tab is selected at the top.
3. Click **Add**.
4. On the **Hosts** page, perform the following actions:

For this field...	Do this...
Host Type	<p>Select Linux as the host type.</p> <p>The SnapCenter Server adds the host, and then installs the Plug-in for Oracle Database and the Plug-in for UNIX if the plug-ins are not already installed on the host.</p>
Host name	<p>Enter the fully qualified domain name (FQDN) or the IP address of the host.</p> <p>SnapCenter depends on the proper configuration of the DNS. Therefore, the best practice is to enter the FQDN.</p> <p>You can enter the IP addresses or FQDN of one of the following:</p> <ul style="list-style-type: none"> • Stand-alone host • Any node in the Oracle Real Application Clusters (RAC) environment <p>Node VIP or scan IP is not supported</p> <p>If you are adding a host by using SnapCenter and the host is part of a subdomain, you must provide the FQDN.</p>
Credentials	<p>Either select the credential name that you created, or create new credentials.</p> <p>The credential must have administrative rights on the remote host. For details, see the information about creating credentials.</p> <p>You can view details about the credentials by positioning the cursor over the credential name that you specified.</p> <p>Note: The credentials authentication mode is determined by the host type that you specify in the Add Host wizard.</p>

5. In the **Select Plug-ins to Install** section, select the plug-ins to install.
6. (Optional) Click **More Options**.

For this field...	Do this...
Port	<p>Either retain the default port number or specify the port number. The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port.</p> <p>Note: If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.</p>
Installation Path	The default path is <code>/opt/NetApp/snapcenter</code> . You can optionally customize the path.
Add all hosts in the Oracle RAC	Select this checkbox to add all of the cluster nodes in an Oracle RAC.
Skip preinstall checks	Select this checkbox if you already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.

7. Click **Submit**.

If you have not selected the Skip prechecks checkbox, the host is validated to verify whether the host meets the requirements for installing the plug-in. If the minimum requirements are not met, appropriate error or warning messages are displayed.

If the error is related to disk space or RAM, you can update the `web.config` file located at `C:\Program Files\NetApp\SnapCenter WebApp` to modify the default values. If the error is related to other parameters, you must fix the issue.

Note: In an NLB setup, if you are updating `web.config` file, you must update the file on both nodes.

8. Verify the fingerprint, and then click **Confirm and Submit**.

In a cluster setup, you should verify the fingerprint of each of the nodes in the cluster.

Note: SnapCenter does not support ECDSA algorithm.

Note: Fingerprint verification is mandatory even if the same host was added earlier to SnapCenter and the fingerprint was confirmed.

9. Monitor the installation progress.

The installation-specific log files are located at `/custom_location/snapcenter/logs`.

Result

The configuration checker operation is triggered automatically and provides alerts for recommendations, corrective actions, and notifications to resolve the issues.

After you finish

After installing the plug-in, all of the databases on that host are automatically discovered and displayed in the Resources page. If nothing is displayed, click **Refresh Resources**.

Related tasks

[Configuring sudo privileges for non-root users](#) on page 77

[Setting up your credentials for the SnapCenter Plug-ins Package for Linux](#) on page 80

[Viewing Configuration Checker alerts](#) on page 124

[Running Configuration Checker on the plug-in hosts](#) on page 124

[Managing the Configuration Checker Schedules](#) on page 125

Related references

[Prerequisites for adding hosts and installing SnapCenter Plug-in for Oracle Database](#) on page 77

[Host requirements for installing the SnapCenter Plug-ins Package for Linux](#) on page 79

Related information

[NetApp Knowledgebase Answer 1086824: SnapCenter Plug-ins Package for Linux installation fails](#)

[NetApp Knowledgebase Answer 1086819: Unable to install plug-in or the installed plug-in is not discovered](#)

[NetApp Knowledgebase Answer 1087846: Validation of adding a host fails](#)

Installing SnapCenter Plug-ins Package for Linux on multiple remote hosts using cmdlets

If you want to install SnapCenter Plug-ins Package for Linux on multiple hosts at one time, you can do so by using the `Install-SmHostPackage` PowerShell cmdlet.

Before you begin

You must be logged in to SnapCenter as a domain user with local administrator rights on each host on which you want to install the plug-in package.

Steps

1. Launch PowerShell.
2. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
3. Install the SnapCenter Plug-ins Package for Linux using the `Install-SmHostPackage` cmdlet and the required parameters.

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

You use the `-skipprecheck` option when you have already installed the plug-ins manually and do not want to validate whether the host meets the requirements to install the plug-in.

4. Enter your credentials for remote installation.

Related tasks

[Setting up your credentials for the SnapCenter Plug-ins Package for Linux](#) on page 80

[Configuring credentials for an Oracle database](#) on page 81

Related references

[Prerequisites for adding hosts and installing SnapCenter Plug-in for Oracle Database](#) on page 77

Related information

[NetApp Knowledgebase Answer 1086818: SnapCenter Server is unable to communicate with the plug-in host](#)

Installing SnapCenter Plug-ins Package for Linux using the command-line interface

You can install SnapCenter Plug-ins Package for Linux locally on the Linux host if you cannot install the plug-in from the SnapCenter user interface. You can use the command-line interface to install the plug-in.

The SnapCenter Plug-ins Package for Linux must be installed on each Linux host where the Oracle database resides.

Installing the SnapCenter Plug-ins Package for Linux interactively

You should install the SnapCenter Plug-ins Package for Linux by using the SnapCenter user interface (UI). If you cannot use the SnapCenter UI for some reason, you can use the installation wizard to install the SnapCenter Plug-ins Package for Linux interactively on a Linux host.

Before you begin

- You must have reviewed the prerequisites for installing the SnapCenter Plug-ins Package for Linux.
- You must have set the `DISPLAY` environment variable to specify the IP address and port number of the Linux host where you want to launch the wizard.

Steps

1. Download the SnapCenter Plug-ins Package for Linux installer from your installation location.
The default installation path is `C:\ProgramData\NetApp\SnapCenter\Package Repository`. This path is accessible from the host where the SnapCenter Server is installed.
2. Copy the installation file to the host on which you want to install the plug-in.
3. From the command prompt, navigate to the directory where you downloaded the installation file.
4. Run the executable file:

```
./SnapCenter_linux_host_plugin.bin -i swing
```
5. Follow the on-screen prompts in the wizard to install the SnapCenter Plug-ins Package for Linux.
6. Click **Finish** to complete the installation.

Installing SnapCenter Plug-ins Package for Linux on cluster host

You should install SnapCenter Plug-ins Package for Linux on both the nodes of the cluster host.

About this task

Each of the nodes of the cluster host has two IPs. One of the IPs will be the public IP of the respective nodes and the second IP will be the cluster IP that is shared between both the nodes.

Steps

1. Install SnapCenter Plug-ins Package for Linux on both the nodes of the cluster host.

See *Installing the SnapCenter Plug-ins Package for Linux interactively*.

2. Validate that the correct values for `SNAPCENTER_SERVER_HOST` and `SPL_ENABLED_PLUGINS` parameters are specified in the `spl.properties` file located at `/var/opt/snapcenter/spl/etc/`.
 - `SNAPCENTER_SERVER_HOST=server_IPaddress`
 - `SPL_ENABLED_PLUGINS=SCO,SCU`
3. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
4. In each of the nodes, set the preferred IPs of the node using the `Set-PreferredHostIPsInStorageExportPolicy` sccli command and the required parameters.

The information regarding the parameters that can be used with the command and their descriptions can be obtained by running `help command_name`. Alternatively, you can also refer to the *Command Reference Guide*.

[SnapCenter Software 4.2 Linux Command Reference Guide](#)

5. In the SnapCenter Server host, add an entry for the cluster IP and corresponding DNS name in `C:\Windows\System32\drivers\etc\hosts`.
6. Add the node to the SnapCenter Server using the `Add-SmHost` cmdlet by specifying the cluster IP for the host name.

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

After you finish

Discover the Oracle database on node 1 (assuming the cluster IP is hosted on node 1) and create a backup of the database. If a fail over happens, you can use the backup created on node 1 to restore the database on node 2. You can also use the backup created on node 1 to create a clone on node 2.

Note: There will be stale volumes, directories, and lock file if the fail over happens while any other SnapCenter operations are running.

Related tasks

[Installing the SnapCenter Plug-ins Package for Linux interactively](#) on page 86

Installing the SnapCenter Plug-ins Package for Linux in silent mode or console mode

You should install the SnapCenter Plug-ins Package for Linux by using the SnapCenter user interface (UI). If you cannot use the SnapCenter UI for some reason, you can install the SnapCenter Plug-ins Package for Linux either in console mode or in silent mode by using the command-line interface (CLI).

Before you begin

- You should have reviewed the prerequisites for installing the SnapCenter Plug-ins Package for Linux.
- You should ensure that the `DISPLAY` environment variable is not set.

If the `DISPLAY` environment variable is set, you should run `unset DISPLAY`, and then try to manually install the plug-in.

About this task

For console mode installation, you must provide the required installation information while installing the SnapCenter Plug-ins Package for Linux. For silent mode installation, you do not have to provide installation information while installing the SnapCenter Plug-ins Package for Linux.

Steps

1. Download the SnapCenter Plug-ins Package for Linux from `C:\ProgramData\NetApp\SnapCenter\Package Repository`.
This path is accessible from the host where the SnapCenter Server is installed.
2. From the command prompt, navigate to the directory where you downloaded the installation file.
3. Install the SnapCenter Plug-ins Package for Linux in console mode or in silent mode:

- Console mode installation:

- a. Run the executable file:

```
./SnapCenter_linux_host_plugin.bin -i console
```

- b. Follow the on-screen prompts to complete the installation.

- Silent mode installation:

```
./SnapCenter_linux_host_plugin.bin -i silent -DPORT -DSERVER_IP -  
DSERVER_PORT -DUSER_INSTALL_DIR=/opt/custom_path
```

Importing data from SnapManager for Oracle and SnapManager for SAP to SnapCenter

Importing data from SnapManager for Oracle and SnapManager for SAP to SnapCenter enables you to continue to use your data from previous versions.

You can import data from SnapManager for Oracle and SnapManager for SAP to SnapCenter by running the import tool from the command-line interface (Linux host CLI).

The import tool creates policies and resource groups in SnapCenter. The policies and resource groups created in SnapCenter correspond to the profiles and operations performed using those profiles in SnapManager for Oracle and SnapManager for SAP. The SnapCenter import tool interacts with the SnapManager for Oracle and SnapManager for SAP repository databases and the database that you want to import.

- Retrieves all the profiles, schedules, and operations performed using the profiles.
- Creates a SnapCenter backup policy for each unique operation and each schedule attached to a profile.
- Creates a resource group for each target database.

You can run the import tool by executing the `sc-migrate` script located at `/opt/NetApp/snapcenter/spl/bin`. When you install the SnapCenter Plug-ins Package for Linux on the database host that you want to import, the `sc-migrate` script is copied to `/opt/NetApp/snapcenter/spl/bin`.

Note: Importing data is not supported from SnapCenter graphical user interface (GUI).

SnapCenter does not support Data ONTAP operating in 7-Mode. You can use the 7-Mode Transition Tool to migrate data and configurations that are stored on a system running Data ONTAP operating in 7-Mode to an ONTAP system.

Related information

[NetApp Documentation: 7-Mode Transition Tool](#)

Configurations supported for importing data

Before you import data from SnapManager 3.4.x for Oracle and SnapManager 3.4.x for SAP to SnapCenter, you should be aware of the configurations that are supported with the SnapCenter Plug-in for Oracle Database.

The configurations that are supported with the SnapCenter Plug-in for Oracle Database are listed in the NetApp Interoperability Matrix Tool.

Related information

[NetApp Interoperability Matrix Tool](#)

What gets imported to SnapCenter

You can import profiles, schedules, and operations performed using the profiles.

From SnapManager for Oracle and SnapManager for SAP	To SnapCenter
Profiles without any operations and schedules	A policy is created with default backup type as Online and backup scope as Full.
Profiles with one or more operations	Multiple policies are created based on a unique combination of a profile and operations performed using that profile. The policies created in SnapCenter contain the archive log pruning and retention details retrieved from the profile and corresponding operations.
Profiles with Oracle Recovery Manager (RMAN) configuration	Policies are created with the Catalog backup with Oracle Recovery Manager option enabled. If external RMAN cataloging was used in SnapManager, you must configure the RMAN catalog settings in SnapCenter. You can either select the existing credential or create a new credential. If RMAN was configured through control file in SnapManager, then you do not have to configure RMAN in SnapCenter.
Schedule attached to a profile	A policy is created just for the schedule.
Database	A resource group is created for each database that is imported. In a Real Application Clusters (RAC) setup, the node on which you run the import tool becomes the preferred node after importing and the resource group is created for that node.

Note: When a profile is imported, a verification policy is created along with the backup policy.

When SnapManager for Oracle and SnapManager for SAP profiles, schedules, and any operations performed using the profiles are imported to SnapCenter, the different parameters values are also imported.

SnapManager for Oracle and SnapManager for SAP parameter and values	SnapCenter parameter and values	Notes
Backup Scope <ul style="list-style-type: none"> Full Data Log 	Backup Scope <ul style="list-style-type: none"> Full Data Log 	
Backup Mode <ul style="list-style-type: none"> Auto Online Offline 	Backup Type <ul style="list-style-type: none"> Online Offline Shutdown 	If the backup mode is Auto, then the import tool checks the database state when the operation was performed, and appropriately sets the backup type as either Online or Offline Shutdown.
Retention <ul style="list-style-type: none"> Days Counts 	Retention <ul style="list-style-type: none"> Days 	SnapManager for Oracle and SnapManager for SAP uses both Days and Counts to set the retention. In SnapCenter, there is either Days <i>OR</i> Counts. So, the retention is set with respect to days as the days get preference over counts in SnapManager for Oracle and SnapManager for SAP.
Pruning for Schedules <ul style="list-style-type: none"> All system change number (SCN) Date Logs created before specified hours, days, weeks, and months 	Pruning for Schedules <ul style="list-style-type: none"> All Logs created before specified hours and days 	SnapCenter does not support pruning based on SCN, Date, weeks, and months.
Notification <ul style="list-style-type: none"> Emails sent only for successful operations Emails sent only for failed operations Emails sent for both success and failed operations 	Notification <ul style="list-style-type: none"> Always On failure Always 	The email notifications are imported. However, you must manually update the SMTP server using the SnapCenter GUI. The subject of the email is left blank for you to configure.

What does not get imported to SnapCenter

The import tool does not import everything to SnapCenter.

You cannot import the following to SnapCenter:

- Backup metadata
- Partial backups
- Raw device mapping (RDM) and Virtual Storage Console (VSC) related backups
- Roles or any credentials available in the SnapManager for Oracle and SnapManager for SAP repository
- Data related to verification, restore, and clone operations
- Pruning for operations
- Replication details specified in the SnapManager for Oracle and SnapManager for SAP profile
After importing, you must manually edit the corresponding policy created in SnapCenter to include the replication details.
- Cataloged backup information

Preparing to import data

Before you import data to SnapCenter, you must perform certain tasks to complete the import operation successfully.

Steps

1. Identify the database that you want to import.
2. Using SnapCenter, add the database host and install SnapCenter Plug-ins Package for Linux.
3. Using SnapCenter, set up the connections for the storage virtual machines (SVMs) used by the databases on the host.
4. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
5. On the **Resources** page, ensure that the database to be imported is discovered and displayed.

When you want to run the import tool, the database must be accessible or else the resource group creation fails.

If the database has credentials configured, you must create a corresponding credential in SnapCenter, assign the credential to the database, and then re-run discovery of the database. If the database is residing on Automatic Storage Management (ASM), you must create credentials for the ASM instance, and assign the credential to the database.

6. Ensure that the user running the import tool has sufficient privileges to run SnapManager for Oracle or SnapManager for SAP CLI commands (such as the command to suspend schedules) from SnapManager for Oracle or SnapManager for SAP host.
7. Run the following commands on the SnapManager for Oracle or SnapManager for SAP host to suspend the schedules:

If you want to...	Then run the following commands...
Suspend the schedules on the SnapManager for Oracle host	<ul style="list-style-type: none"> <code>smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database</code> <code>smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database</code> <code>smo credential set -profile -name profile_name</code> You must run the <code>smo credential set</code> command for each profile on the host.
Suspend the schedules on the SnapManager for SAP host	<ul style="list-style-type: none"> <code>smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database</code> <code>smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database</code> <code>smsap credential set -profile -name profile_name</code> You must run the <code>smsap credential set</code> command for each profile on the host.

8. Ensure that fully qualified domain name (FQDN) of the database host is displayed when you run `hostname -f`.

If FQDN is not displayed, you must modify `/etc/hosts` to specify the FQDN of the host.

Related information

[Protecting Oracle databases](#)

[SnapCenter Software 4.2 Linux Command Reference Guide](#)

Importing data

You can import data by running the import tool from the database host. Before you start importing data, you must complete the pre-requisites.

About this task

The SnapCenter backup policies that are created after importing have different naming formats:

- Policies created for the profiles without any operations and schedules have the `SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED` format.
When no operation is performed using a profile, the corresponding policy is created with default backup type as online and backup scope as full.
- Policies created for the profiles with one or more operations have the `SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED` format.
- Policies created for the schedules attached to the profiles have the `SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED` format.

Steps

1. Log in to the database host that you want to import.
2. Run the import tool by executing the `sc-migrate` script located at `/opt/NetApp/snapcenter/spl/bin`.
3. Enter the SnapCenter Server user name and password.
After validating the credentials, a connection is established with SnapCenter.
4. Enter the SnapManager for Oracle or SnapManager for SAP repository database details.
The repository database lists the databases that are available on the host.
5. Enter the target database details.
If you want to import all the databases on the host, enter `all`.
6. If you want to generate a system log or send ASUP messages for failed operations, you must enable them either by running the `Add-SmStorageConnection` or `Set-SmStorageConnection` command.

Result

The SnapCenter backup policies are created for profiles, schedules, and operations performed using the profiles. Resource groups are also created for each target database.

After importing the data successfully, the schedules associated with the imported database are suspended in SnapManager for Oracle and SnapManager for SAP.

Note: After importing, you must manage the imported database or file system using SnapCenter.

Related tasks

[Preparing to import data](#) on page 91

Related references

[Configurations supported for importing data](#) on page 89

Canceling an import operation

If you want to cancel an import operation, either while running the import tool or after importing, you must manually delete the SnapCenter policies, credentials, and resource groups that were created as part of import operation.

Troubleshooting an import operation

The logs for every execution of the import tool are stored in the `/var/opt/snapcenter/spl/logs` directory with the name `spl_migration_timestamp.log`. You can refer to this log to review import errors and troubleshoot them.

Configuring the SnapCenter Plug-in Loader service for Linux

The SnapCenter Plug-in Loader service loads the plug-in package for Linux to interact with the SnapCenter Server. The SnapCenter Plug-in Loader service is installed when you install the SnapCenter Plug-ins Package for Linux.

About this task

After installing the SnapCenter Plug-ins Package for Linux, the SnapCenter Plug-in Loader service starts automatically. If the SnapCenter Plug-in Loader service fails to start automatically, you should:

- Ensure that the directory where the plug-in is operating is not deleted
- Increase the memory space allotted to the Java Virtual Machine

You can also manually start and stop the service, and find the status of the service. When you restart the Linux host, the SnapCenter Plug-in Loader service is started automatically.

The `spl.properties` file, which is located at `/custom_location/NetApp/snapcenter/spl/etc/`, contains the following parameters. Default values are assigned to these parameters.

Parameter name	Description
LOG_LEVEL	Displays the log levels that are supported. The possible values are INFO, DEBUG, TRACE, ERROR, FATAL, and WARN.
SPL_PROTOCOL	Displays the protocol that is supported by SnapCenter Plug-in Loader. Only the HTTPS protocol is supported. You can add the value if the default value is missing.
SNAPCENTER_SERVER_PROTOCOL	Displays the protocol that is supported by SnapCenter Server. Only the HTTPS protocol is supported. You can add the value if the default value is missing.
SPL_KEYSTORE_PASS	Displays the password of the keystore file. You can change this value only if you change the password or create a new keystore file.

Parameter name	Description
SPL_PORT	Displays the port number on which the SnapCenter Plug-in Loader service is running. You can add the value if the default value is missing. Note: You should not change the value after installing the plug-ins for Linux.
SNAPCENTER_SERVER_HOST	Displays the IP address or host name of the SnapCenter Server.
SPL_KEYSTORE_PATH	Displays the absolute path of the keystore file.
SNAPCENTER_SERVER_PORT	Displays the port number on which the SnapCenter Server is running.
SPL_LOGS_MAX_COUNT	Displays the number of SnapCenter Plug-in Loader log files that are retained in the <code>/custom_location/snapcenter/spl/logs</code> folder. The default value is set to 5000. If the count is more than the specified value, then the last 5000 modified files are retained. The check for the number of files is done automatically every 24 hours from when SnapCenter Plug-in Loader service is started. Note: If you manually delete the <code>spl.properties</code> file, then the number of files to be retained is set to 9999.

If any of these parameters are not assigned to the default value or if you want to assign or change the value, then you can modify the `spl.properties` file. You can also verify the `spl.properties` file and edit the file to troubleshoot any issues related to the values that are assigned to the parameters. After you modify the `spl.properties` file, you must restart the SnapCenter Plug-in Loader service.

Step

1. Start or stop the SnapCenter Plug-in Loader service, or find the status of the SnapCenter Plug-in Loader service, as required:
 - Start the SnapCenter Plug-in Loader service:

```
/custom_location/NetApp/snapcenter/spl/bin/spl start
```

 You must start the service as a root user.
 - Stop the SnapCenter Plug-in Loader service:

```
/custom_location/NetApp/snapcenter/spl/bin/spl stop
```

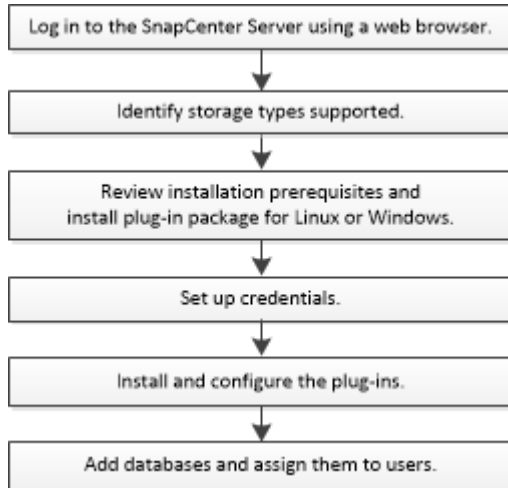
Note: You can use the `-force` option with the `stop` command to stop the SnapCenter Plug-in Loader service forcefully. However, you should use caution before doing so because it also terminates the existing operations.
 - Find the status of the SnapCenter Plug-in Loader service:

```
/custom_location/NetApp/snapcenter/spl/bin/spl status
```

Installing SnapCenter Plug-in for SAP HANA Database

You should install and set up the SnapCenter Plug-in for SAP HANA Database if you want to protect SAP HANA databases.

About this task



Storage types supported by SnapCenter Plug-in for SAP HANA Database

SnapCenter supports a wide range of storage types on both physical machines and virtual machines (VMs). You must verify the support for your storage type before installing SnapCenter Plug-in for SAP HANA Database.

Machine	Storage type
Physical and virtual servers	FC-connected LUNs
	NFS-connected volumes

Prerequisites for adding hosts and installing SnapCenter Plug-in for SAP HANA Database

Before you add a host and install the plug-in packages, you must complete all the requirements. SnapCenter Plug-in for SAP HANA Database is available in both Windows and Linux environments.

- You must have installed Java 1.8 64-bit on your Linux or Windows host.
- You must have installed SAP HANA database interactive terminal (HSBSQL client) on the host. For Windows, the HDBSQL client must be running using the “SYSTEM” Windows user.

- For Windows, plug-in Creator Service should be running using the “LocalSystem” windows user, which is the default behavior when Plug-in for SAP HANA Database is installed as domain administrator.
- For Windows, user store keys should be created as SYSTEM user. For example, `hdbuserstore -u SYSTEM -i set`
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in or if the user belongs to a local workgroup user, you must disable UAC on the host.
- For Linux host, user store keys are accessed as OS database user.
- SnapCenter Server should have access to the 8145 or custom port of Plug-in for SAP HANA host.

General

If you are using iSCSI, the iSCSI service must be running.

Windows hosts

- You must have a domain user with local administrator privileges with local login permissions on the remote host.
- If you manage cluster nodes in SnapCenter, you must have a user with administrative privileges to all the nodes in the cluster.
- Data protection using SnapCenter requires a two-way trust relationship between the SnapCenter Server domain and the plug-in domain using the Microsoft Active Directory Domains and Trusts snap-in.
Although domain trusts, multidomain forests, and cross-domain trusts are supported, cross-forest domains are not.
<https://technet.microsoft.com/en-us/library/cc770299.aspx>

Linux hosts

- You must have enabled the password-based SSH connection for the root or non-root user.
- You must have installed Java 1.8 64-bit on your Linux host.
If you are using Windows 2016 for the SnapCenter Server host, you must install Java 1.8, 64-bit. The Interoperability Matrix Tool (IMT) contains the latest information about requirements.
[Java Downloads for All Operating Systems](#)
[NetApp Interoperability Matrix Tool](#)
- You should always have read/write permission for the “/tmp” folder on the plug-in host.

Related tasks

[Adding SnapCenter licenses](#) on page 29

Host requirements to install SnapCenter Plug-ins Package for Windows

Before you install the SnapCenter Plug-ins Package for Windows, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating Systems	<p>Microsoft Windows</p> <p>Note: You must enable the Cluster Shared Volumes (CSV) feature in Windows Server 2008 R2 SP1 if you want to create CSV-type disks.</p> <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	<p>2 GB</p> <p>Note: You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.</p>
Required software packages	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.5.2 or later • Windows Management Framework (WMF) 4.0 or later • PowerShell 4.0 or later <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>

Host requirements for installing the SnapCenter Plug-ins Package for Linux

Before you install the SnapCenter Plug-ins Package for Linux, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating systems	<ul style="list-style-type: none"> Red Hat Enterprise Linux Oracle Linux <p>Note: If you are using Oracle database on LVM in Oracle Linux or Red Hat Enterprise Linux 6.6 or 7.0 operating systems, you must install the latest version of Logical Volume Manager (LVM).</p> SUSE Linux Enterprise Server (SLES) <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	2 GB <p>Note: You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.</p>
Required software packages	Java 1.8 (64-bit) Oracle Java and OpenJDK flavors If you have upgraded JAVA to the latest version, you must ensure that the JAVA_HOME option located at <code>/var/opt/snapcenter/spl/etc/spl.properties</code> is set to the correct JAVA version and the correct path. For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool

Setting up credentials for the SnapCenter Plug-in for SAP HANA Database

SnapCenter uses credentials to authenticate users for SnapCenter operations. You should create credentials for installing SnapCenter plug-ins and additional credentials for performing data protection operations on databases or Windows file systems.

About this task

- Linux hosts

You must set up credentials for installing plug-ins on Linux hosts.

You must set up the credentials for the root user or for a non-root user who has sudo privileges to install and start the plug-in process.

Best Practice: Although you are allowed to create credentials for Linux after deploying hosts and installing plug-ins, the best practice is to create credentials after you add SVMs, before you deploy hosts and install plug-ins.

- Windows hosts

You must set up Windows credentials before installing plug-ins.

You must set up the credentials with administrator privileges, including administrator rights on the remote host.

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

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Credential**.
3. Click **New**.

Credential [X]

Provide information for the Credential you want to add

Credential Name:

Username: ⓘ

Password:

Authentication:

☐ Use sudo privileges ⓘ

Cancel OK

4. In the **Credential** page, specify the information required for configuring credentials:

For this field...	Do this...
Credential name	Enter a name for the credentials.
User name	<p>Enter the user name and password that are to be used for authentication.</p> <ul style="list-style-type: none"> Domain administrator or any member of the administrator group Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the <i>Username</i> field are: <code>NetBIOS\UserName</code> <code>Domain FQDN\UserName</code> Local administrator (for workgroups only) For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the <i>Username</i> field is: <code>UserName</code> <p>Do not use double quotes (") in passwords for Windows SVMs.</p>
Password	Enter the password used for authentication.
Authentication Mode	<p>Select the authentication mode that you want to use.</p> <p>If you select the SQL authentication mode, you must also specify the SQL server instance and the host where the SQL instance is located.</p>
Use sudo privileges	<p>Select the Use sudo privileges check box if you are creating credentials for a non-root user.</p> <p>Note: Applicable to Linux users only.</p>

5. Click **OK**.

After you finish

After you finish setting up the credentials, you might want to assign credential maintenance to a user or group of users on the My SnapCenter Assets page.

Adding hosts and installing plug-in packages on remote hosts

You must use the SnapCenter Add Host page to add hosts, and then install the plug-ins packages. The plug-ins are automatically installed on the remote hosts. You can add a host and install plug-in packages either for an individual host or for a cluster.

Before you begin

- You must be a user that is assigned to a role that has the plug-in install and uninstall permissions, such as the SnapCenter Admin role.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in, or if the user belongs to a local workgroup user, you must disable UAC on the host.
- You should ensure that the message queueing service is running.
- The administration documentation contains information about managing hosts.

[Performing administrative tasks](#)

Steps

1. In the left navigation pane, click **Hosts**.
2. Verify that the **Managed Hosts** tab is selected at the top.
3. Click **Add**.
4. On the **Hosts** page, perform the following actions:

For this field...	Do this...
Host Type	Select the type of host: <ul style="list-style-type: none"> • Windows • Linux <p>Note: The Plug-in for SAP HANA is installed on the HDBSQL client host, and this host can be on either a Windows system or a Linux system.</p>
Host name	Enter the communication host name. You must configure the HDBSQL client and HDBUserStore on this host.
Credentials	Either select the credential name that you created or create new credentials. The credential must have administrative rights on the remote host. For details, see the information about creating credentials. You can view details about the credentials by positioning your cursor over the credential name that you provided. <p>Note: The credentials authentication mode is determined by the host type that you specify in the Add Host wizard.</p>

5. In the **Select Plug-ins to Install** section, select the plug-ins to install.

6. (Optional) Click **More Options**.

For this field...	Do this...
Port	<p>Either retain the default port number or specify the port number. The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port.</p> <p>Note: If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.</p>
Installation Path	<p>The Plug-in for SAP HANA is installed on the HDBSQL client host, and this host can be on either a Windows system or a Linux system.</p> <ul style="list-style-type: none"> For the SnapCenter Plug-ins Package for Windows, the default path is <code>C:\Program Files\NetApp\SnapCenter</code>. Optionally, you can customize the path. For the SnapCenter Plug-ins Package for Linux, the default path is <code>/opt/NetApp/snapcenter</code>. Optionally, you can customize the path.
Skip preinstall checks	<p>Select this check box if you already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.</p>

7. Click **Submit**.

If you have not selected the Skip prechecks checkbox, the host is validated to verify whether the host meets the requirements for installing the plug-in. The disk space, RAM, PowerShell version, .NET version, location (for Windows plug-ins), and Java version (for Linux plug-ins) are validated against the minimum requirements. If the minimum requirements are not met, appropriate error or warning messages are displayed.

If the error is related to disk space or RAM, you can update the `web.config` file located at `C:\Program Files\NetApp\SnapCenter WebApp` to modify the default values. If the error is related to other parameters, you must fix the issue.

Note: In an NLB setup, if you are updating `web.config` file, you must update the file on both nodes.

8. If host type is Linux, verify the fingerprint, and then click **Confirm and Submit**.

In a cluster setup, you should verify the fingerprint of each of the nodes in the cluster.

Note: Fingerprint verification is mandatory even if the same host was added earlier to SnapCenter and the fingerprint was confirmed.

9. Monitor the installation progress.

The installation-specific log files are located at `/custom_location/snapcenter/logs`.

Result

The configuration checker operation is triggered automatically and provides alerts for recommendations, corrective actions, and notifications to resolve the issues.

Related tasks

[Viewing Configuration Checker alerts](#) on page 124

[Running Configuration Checker on the plug-in hosts](#) on page 124

[Managing the Configuration Checker Schedules](#) on page 125

Related references

[Prerequisites for adding hosts and installing SnapCenter Plug-in for SAP HANA Database](#) on page 96

[Host requirements to install SnapCenter Plug-ins Package for Windows](#) on page 53

[Host requirements for installing the SnapCenter Plug-ins Package for Linux](#) on page 79

Related information

[NetApp Knowledgebase Answer 1087846: Validation of adding a host fails](#)

Installing SnapCenter Plug-in Packages for Linux or Windows on multiple remote hosts by using cmdlets

You can install the SnapCenter Plug-in Packages for Linux or Windows on multiple hosts simultaneously by using the `Install-SmHostPackage` PowerShell cmdlet.

Before you begin

You must have logged in to SnapCenter as a domain user with local administrator rights on each host on which you want to install the plug-in package.

Steps

1. Launch PowerShell.
2. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
3. Install the plug-in on multiple hosts using the `Install-SmHostPackage` cmdlet and the required parameters.

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

You can use the `-skipprecheck` option when you have installed the plug-ins manually and do not want to validate whether the host meets the requirements to install the plug-in.

4. Enter your credentials for remote installation.

Installing SnapCenter Plug-in for SAP HANA Database independently on the Linux host

You can install the SnapCenter Plug-in for SAP HANA Database directly on the Linux host if your environment does not allow remote installation of the plug-in from the SnapCenter Server. You can use an interactive wizard or the command-line interface to install the plug-in.

The Plug-in for SAP HANA Database must be installed on each of the Linux host where the HDBSQL client resides.

Preparation for installing the SnapCenter Plug-in for SAP HANA Database on the Linux host

The Linux host on which you are installing the SnapCenter Plug-in for SAP HANA Database must meet the dependent software, database, and operating system requirements.

The Interoperability Matrix Tool (IMT) contains the latest information about the supported configurations.

The SnapCenter Plug-in for SAP HANA Database is part of SnapCenter Plug-ins Package for Linux. Before you install SnapCenter Plug-ins Package for Linux, you must have already installed SnapCenter 4.0 on a Windows host.

Installing the SnapCenter Plug-in for SAP HANA Database on Linux hosts by using the command-line interface

You should install the SnapCenter Plug-in for SAP HANA Database by using the SnapCenter user interface (UI). If your environment does not allow remote installation of the plug-in from the SnapCenter UI, you can install the Plug-in for SAP HANA Database either in console mode or in silent mode by using the command-line interface (CLI).

Steps

1. Copy the SnapCenter Plug-ins Package for Linux installation file (snapcenter_linux_host_plugin.bin) from C:\ProgramData\NetApp\SnapCenter\Package Repository to the host where you want to install the Plug-in for SAP HANA Database.

You can access this path from the host where the SnapCenter Server is installed.

2. From the command prompt, navigate to the directory where you copied the installation file.
3. Install the plug-in:

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -  
DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT specifies the SMCore HTTPS communication port.
- -DSERVER_IP specifies the SnapCenter Server IP address.
- -DSERVER_HTTPS_PORT specifies the SnapCenter Server HTTPS port.
- -DUSER_INSTALL_DIR specifies the directory where you want to install the SnapCenter Plug-ins Package for Linux.
- DINSTALL_LOG_NAME specifies the name of the log file.

Example

```
tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent -  
DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146 -  
DUSER_INSTALL_DIR=/opt -  
DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log -  
DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Edit the /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties file, and then add the PLUGINS_ENABLED = hana:3.0 parameter.

5. Add the host to the SnapCenter Server using the `Add-Smhost` cmdlet and the required parameters.

Note: You can add a host only from the command-line interface.

The information regarding the parameters that can be used with the command and their descriptions can be obtained by running `help command_name`. Alternatively, you can also refer to the *Command Reference Guide*.

[SnapCenter Software 4.2 Linux Command Reference Guide](#)

Related tasks

[Setting up credentials for the SnapCenter Plug-in for SAP HANA Database](#) on page 100

Related references

[Prerequisites for adding hosts and installing SnapCenter Plug-in for SAP HANA Database](#) on page 96

Adding databases to SnapCenter Plug-in for SAP HANA Database

You must add the databases that you want to back up or clone.

Before you begin

You must have completed tasks such as installing the SnapCenter Server, adding hosts, creating storage system connections, and adding credentials.

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click **Resources**.
2. In the **Resources** page, click **Add SAP HANA Database**.
3. In the **Provide Resource Details** page, perform the following actions:

For this field...	Do this...
Resource Type	Enter the resource type. Resource types are Single Container, Multitenant Database Containers (MDC) – Single Tenant, and Non-data Volumes.
SAP HANA System Name	Enter the descriptive SAP HANA system name.
SID	Enter the system ID (SID). The installed SAP HANA system is identified by a single SID.
Tenant Database	Enter the name of the tenant database for SAP HANA databases. This option is available only if you selected the Multitenant Database Containers (MDC) – Single Tenant resource type.
HDBSQL Client Host	Select the communication host.
HDB Secure User Store Keys	Enter the key to connect to the SAP HANA system. The key contains the login information to connect to the database.

For this field...	Do this...
HDBSQL OS User	Enter the user name for whom the HDB Secure User Store Key is configured. For Windows, it is mandatory for the HDBSQL OS User to be the SYSTEM user. Therefore, you must configure the HDB Secure User Store Key for the SYSTEM user.
Resource Name	Enter the resource name. This option is available only if you selected the Non-data Volumes.

Provide Resource Details

☒ Single Container
 Resource Type ☐ Multitenant Database Container (MDC) - Single Tenant
☐ Non-data Volumes

HANA System Name


SID

HDBSQL Client Host

HDB Secure User Store Keys

HDBSQL OS User

4. In the **Provide Storage Footprint** page, select a storage system and choose one or more volumes, LUNs, and qtrees, and then click **Save**.

Optional: You can click the  icon to add more volumes, LUNs, and qtrees from other storage systems.

Note: SnapCenter Plug-in for SAP HANA Database does not support automatic discovery of the resources and storage details for physical and virtual environments. You must provide the storage information for physical and virtual environments while adding the databases.

5. In the **Resource Settings** page, perform the following actions:

For this field...	Do this...
Prefix	Enter the prefix of the File-Based backup name. If the prefix is not provided, the default value is used.
Location	Enter the path on the SAP HANA node to save the File-Based backup. If the path is not provided, SAP HANA uses the default path configured on the system, for example, <i>HANA shared path/ <SID>/HDBINSTANCE_ID/backup/data</i> .

6. Review the summary, and then click **Finish**.

The databases are displayed along with information such as the SID, Tenant Database for MDC, communication host, associated resource groups and policies, and overall status.

After you finish

If you want to provide users access to resources, you must assign the resources to the users. This enables users to perform the actions for which they have permissions on the assets that are assigned to them.

After adding the databases, you can modify the SAP HANA database details.

You cannot modify the following if the SAP HANA database has backups associated with it:

- Multitenant database containers (MDC): SID, Tenant Database, or HDBSQL Client Host
- Single Container: SID or HDBSQL Client Host
- NonDataVolume: Resource name, Associated SID, or Plug-in Host

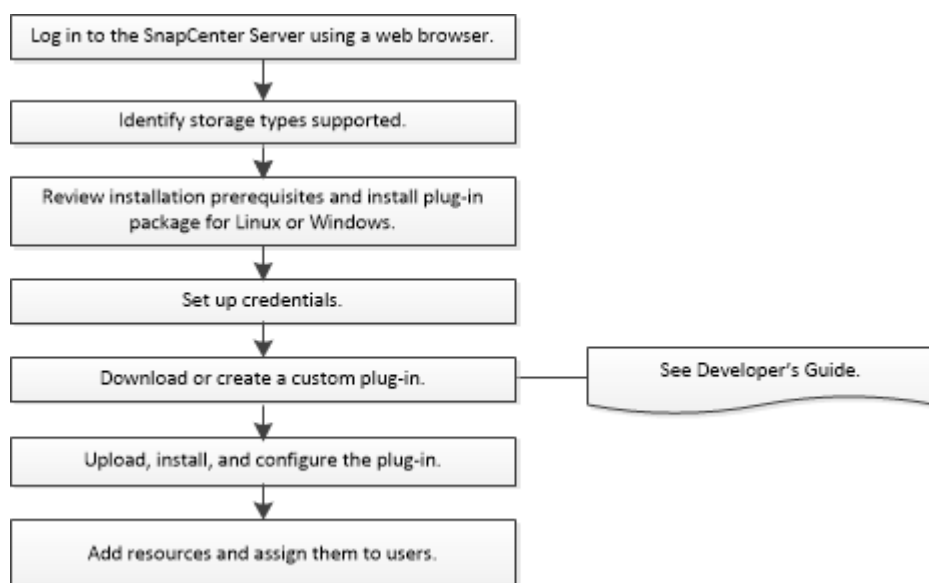
Related tasks

[Assigning users access to assets](#) on page 23

Installing SnapCenter Custom Plug-ins

You should install and set up SnapCenter Custom Plug-ins if you want to protect custom plug-in resources.

About this task



Storage types supported by SnapCenter Custom Plug-ins

SnapCenter supports a wide range of storage types on both physical and virtual machines. You must verify the support for your storage type before installing SnapCenter Custom Plug-ins.

Provisioning using SnapCenter is supported on Windows using SnapCenter Plug-in for Microsoft Windows. Provisioning is not supported for SnapCenter Plug-ins Package for Linux.

Machine	Storage type
Physical and virtual servers (VMDKs and RDM LUNs are not supported.)	FC-connected LUNs
	iSCSI-connected LUNs
	NFS-connected volumes

Prerequisites for adding hosts and installing SnapCenter Custom Plug-ins

Before you add a host and install the plug-ins packages, you must complete all the requirements. The Custom Plug-ins can be used in both Windows and Linux environments.

- You must have created a custom plug-in. For details, see the developer information.
[Developer Guide for Creating Custom Plug-ins](#)

- If you want to manage MySQL or DB2 applications, you must have downloaded the MySQL and DB2 Custom Plug-ins that are provided by NetApp.
- You must have installed Java 1.8, 64-bit on your Linux or Windows host.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in, or if the user belongs to a local workgroup user, you must disable UAC on the host.
- The Custom Plug-ins must be available on the client host from where the add host operation is performed.

General

If you are using iSCSI, the iSCSI service must be running.

Windows hosts

- You must have a domain user with local administrator privileges with local login permissions on the remote host.
- If you manage cluster nodes in SnapCenter, you must have a user with administrative privileges to all the nodes in the cluster.
- Data protection using SnapCenter requires a two-way trust relationship between the SnapCenter Server domain and the plug-in domain using the Microsoft Active Directory Domains and Trusts snap-in.

Although domain trusts, multidomain forests, and cross-domain trusts are supported, cross-forest domains are not.

<https://technet.microsoft.com/en-us/library/cc770299.aspx>

Linux hosts

- You must have enabled the password-based SSH connection for the root or non-root user.
- You must have installed Java 1.8 64-bit, on your Linux host.
If you are using Windows 2016 for the SnapCenter Server host, you must install Java 1.8, 64-bit. The Interoperability Matrix Tool (IMT) contains the latest information about requirements.
[Java Downloads for All Operating Systems](#)
[NetApp Interoperability Matrix Tool](#)
- You must configure sudo privileges for the non-root user to provide access to several paths. Add the following lines to the /etc/sudoers file by using the visudo Linux utility. For example,

```
Cmdnd_Alias SCCMD = /opt/NetApp/snapcenter/scc/bin/scc <non_root_user>
ALL=(ALL) NOPASSWD:SETENV: SCCMD
```

non_root_user is the name of the non-root user that you created.

- You should always have read/write permission for the “/tmp” folder on the plug-in host.

Related tasks

[Adding SnapCenter licenses](#) on page 29

Host requirements to install SnapCenter Plug-ins Package for Windows

Before you install the SnapCenter Plug-ins Package for Windows, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating Systems	<p>Microsoft Windows</p> <p>Note: You must enable the Cluster Shared Volumes (CSV) feature in Windows Server 2008 R2 SP1 if you want to create CSV-type disks.</p> <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	<p>2 GB</p> <p>Note: You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.</p>
Required software packages	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.5.2 or later • Windows Management Framework (WMF) 4.0 or later • PowerShell 4.0 or later <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>

Host requirements for installing the SnapCenter Plug-ins Package for Linux

Before you install the SnapCenter Plug-ins Package for Linux, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating systems	<ul style="list-style-type: none"> Red Hat Enterprise Linux Oracle Linux <p>Note: If you are using Oracle database on LVM in Oracle Linux or Red Hat Enterprise Linux 6.6 or 7.0 operating systems, you must install the latest version of Logical Volume Manager (LVM).</p> SUSE Linux Enterprise Server (SLES) <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool</p>
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	2 GB <p>Note: You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.</p>
Required software packages	Java 1.8 (64-bit) Oracle Java and OpenJDK flavors If you have upgraded JAVA to the latest version, you must ensure that the JAVA_HOME option located at <code>/var/opt/snapcenter/spl/etc/spl.properties</code> is set to the correct JAVA version and the correct path. For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT). NetApp Interoperability Matrix Tool

Setting up credentials for SnapCenter Custom Plug-ins

SnapCenter uses credentials to authenticate users for SnapCenter operations. You should create credentials for installing SnapCenter plug-ins and additional credentials for performing data protection operations on databases or Windows file systems.

About this task

- Linux hosts

You must set up credentials for installing plug-ins on Linux hosts.

You must set up the credentials for the root user or for a non-root user who has sudo privileges to install and start the plug-in process.

Best Practice: Although you are allowed to create credentials for Linux after deploying hosts and installing plug-ins, the best practice is to create credentials after you add SVMs, before you deploy hosts and install plug-ins.

- Windows hosts

You must set up Windows credentials before installing plug-ins.

You must set up the credentials with administrator privileges, including administrator rights on the remote host.

- Custom Plug-ins applications

The plug-in uses the credentials that are selected or created while adding a resource. If a resource does not require credentials during data protection operations, you can set the credentials as **None**.

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

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Credential**.
3. Click **New**.

Credential

Provide information for the Credential you want to add

Credential Name

Name

Username

Username

Password

Password

Authentication

Linux

☐ Use sudo privileges

Cancel

OK

4. In the **Credential** page, specify the information required for configuring credentials:

For this field...	Do this...
Credential name	Enter a name for the credentials.
User name	<div>Enter the user name and password that are to be used for authentication.</div> <div><ul style="list-style-type: none">Domain administrator or any member of the administrator group Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the <i>Username</i> field are: <i>NetBIOS\UserName</i> <i>Domain FQDN\UserName</i>Local administrator (for workgroups only) For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the <i>Username</i> field is: <i>UserName</i></div>
Password	Enter the password used for authentication.
Authentication Mode	<div>Select the authentication mode that you want to use.</div> <div>If you select the SQL authentication mode, you must also specify the SQL server instance and the host where the SQL instance is located.</div>

For this field...	Do this...
Use sudo privileges	Select the Use sudo privileges check box if you are creating credentials for a non-root user. Note: Applicable to Linux users only.

5. Click **OK**.

After you finish

After you finish setting up the credentials, you might want to assign credential maintenance to a user or group of users on the My SnapCenter Assets page.

Adding hosts and installing plug-in packages on remote hosts

You must use the SnapCenter Add Host page to add hosts, and then install the plug-in packages. The plug-ins are automatically installed on the remote hosts. You can add a host and install the plug-in packages either for an individual host or for a cluster.

Before you begin

- You must be a user that is assigned to a role that has the plug-in install and uninstall permissions, such as the SnapCenter Admin role.
- You should ensure that the message queueing service is running.

About this task

If you install plug-ins on a cluster (WSFC), the plug-ins are installed on all of the nodes of the cluster.

The *Administration Guide* contains more information on managing hosts.

[Performing administrative tasks](#)

Steps

1. In the left navigation pane, click **Hosts**.
2. Verify that the **Managed Hosts** tab is selected at the top.
3. Click **Add**.
4. On the **Hosts** page, perform the following actions:

For this field...	Do this...
Host Type	Select the type of host: <ul style="list-style-type: none"> • Windows • Linux Note: The custom plug-ins can be used in both Windows and Linux environments.

For this field...	Do this...
Host name	<p>Enter the fully qualified domain name (FQDN) or the IP address of the host.</p> <p>SnapCenter depends on the proper configuration of the DNS. Therefore, the best practice is to enter the FQDN.</p> <p>For Windows environments, the IP address is supported for untrusted domain hosts only if it resolves to the FQDN.</p> <p>You can enter the IP addresses or FQDN of a stand-alone host.</p> <p>If you are adding a host by using SnapCenter and the host is part of a subdomain, you must provide the FQDN.</p>
Credentials	<p>Either select the credential name that you created, or create new credentials.</p> <p>The credentials must have administrative rights on the remote host. For details, see the information about creating credentials.</p> <p>You can view details about the credentials by positioning your cursor over the credential name that you specified.</p> <p>Note: The credentials authentication mode is determined by the host type that you specify in the Add Host wizard.</p>

5. In the **Select Plug-ins to Install** section, select the plug-ins to install.
6. (Optional) Click **More Options**.

For this field...	Do this...
Port	<p>Either retain the default port number, or specify the port number. The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port.</p> <p>Note: If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.</p>

For this field...	Do this...
Installation Path	<p>The custom plug-ins can be installed on either a Windows system or a Linux system.</p> <ul style="list-style-type: none"> For the SnapCenter Plug-ins Package for Windows, the default path is <code>C:\Program Files\NetApp\SnapCenter</code>. Optionally, you can customize the path. For SnapCenter Plug-ins Package for Linux, the default path is <code>/opt/NetApp/snapcenter</code>. Optionally, you can customize the path. For the SnapCenter Custom Plug-ins: <ul style="list-style-type: none"> a. In the Custom Plug-ins section, click Browse, and then select the zipped custom plug-in folder. The zipped folder contains the custom plug-in code and the descriptor <code>.xml</code> file. b. Click Upload. The descriptor <code>.xml</code> file in the zipped custom plug-in folder is validated before the package is uploaded. The custom plug-ins that are uploaded to the SnapCenter Server are listed. If you want to manage MySQL or DB2 applications, you can use the MySQL and DB2 custom plug-ins that are provided by NetApp. The MySQL and DB2 custom plug-ins are available at the NetApp Tool Chest. NetApp Tool Chest
Skip preinstall checks	Select this check box if you already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.

7. Click **Submit.**

If you have not selected the **Skip prechecks** checkbox, the host is validated to verify whether the host meets the requirements for installing the plug-in. The disk space, RAM, PowerShell version, .NET version, location (for Windows plug-ins), and Java version (for Linux plug-ins) are validated against the minimum requirements. If the minimum requirements are not met, appropriate error or warning messages are displayed.

If the error is related to disk space or RAM, you can update the `web.config` file located at `C:\Program Files\NetApp\SnapCenter WebApp` to modify the default values. If the error is related to other parameters, you must fix the issue.

Note: In an NLB setup, if you are updating `web.config` file, you must update the file on both nodes.

8. If host type is Linux, verify the fingerprint, and then click **Confirm and Submit.**

In a cluster setup, you should verify the fingerprint of each of the nodes in the cluster.

Note: Fingerprint verification is mandatory even if the same host was added earlier to SnapCenter and the fingerprint was confirmed.

9. Monitor the installation progress.

The installation-specific log files are located at `/custom_location/snapcenter/logs`.

Result

When the host is added, the configuration checker operation is triggered automatically and provides alerts for recommendations, corrective actions, and notifications to resolve the issues.

Related tasks

[Setting up credentials for SnapCenter Custom Plug-ins](#) on page 113

[Viewing Configuration Checker alerts](#) on page 124

[Running Configuration Checker on the plug-in hosts](#) on page 124

[Managing the Configuration Checker Schedules](#) on page 125

Related references

[Prerequisites for adding hosts and installing SnapCenter Custom Plug-ins](#) on page 109

[Host requirements to install SnapCenter Plug-ins Package for Windows](#) on page 53

[Host requirements for installing the SnapCenter Plug-ins Package for Linux](#) on page 79

Related information

[NetApp Knowledgebase Answer 1087846: Validation of adding a host fails](#)

Installing SnapCenter Plug-in Packages for Linux or Windows on multiple remote hosts by using cmdlets

You can install the SnapCenter Plug-in Packages for Linux or Windows on multiple hosts simultaneously by using the `Install-SmHostPackage` PowerShell cmdlet.

Before you begin

The user adding a host should have the administrative rights on the host.

Steps

1. Launch PowerShell.
2. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
3. Install the plug-in on multiple hosts using the `Install-SmHostPackage` cmdlet and the required parameters.

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

You can use the `-skipprecheck` option when you have installed the plug-ins manually and do not want to validate whether the host meets the requirements to install the plug-in.

4. Enter your credentials for remote installation.

Related tasks

[Setting up your credentials for the SnapCenter Plug-ins Package for Linux](#) on page 80

[Configuring credentials for an Oracle database](#) on page 81

[Setting up credentials for the SnapCenter Plug-in for SAP HANA Database](#) on page 100

Related references

[Prerequisites for adding hosts and installing SnapCenter Plug-in for SAP HANA Database](#) on page 96

[Prerequisites for adding hosts and installing SnapCenter Custom Plug-ins](#) on page 109

Adding resources to SnapCenter Custom Plug-ins

You must add the resources that you want to back up or clone. Depending on your environment, resources might be either database instances or collections that you want to back up or clone.

Before you begin

- You must have completed tasks such as installing the SnapCenter Server, adding hosts, creating storage system connections, and adding credentials.
- You must have created a custom plug-in.
[Developer Guide for Creating Custom Plug-ins](#)
- You must have uploaded the plug-ins to SnapCenter Server.

About this task


You can also add resources for MySQL and DB2 applications. These plug-ins can be downloaded from the [NetApp Storage Automation Store](#).

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the **Resources** page, click **Add Resource**.
3. In the **Provide Resource Details** page, perform the following actions:

For this field...	Do this...
Name	Enter the name of the resource.
Host name	Select the host.
Type	<p>Select the type.</p> <p>Type is user defined as per the plug-in description file. For example, database and instance.</p> <p>In case the type selected has a parent, enter the details of the parent. For example, if the type is Database and the parent is Instance, enter the details of the Instance.</p>
Credential name	(Optional) Select Credential or create a new credential.
Mount Points	<p>Enter the mount paths where the resource is mounted.</p> <p>This is applicable only for a Windows host.</p>

4. In the **Provide Storage Footprint** page, select a storage system and choose one or more volumes, LUNs, and qtrees, and then click **Save**.

Optional: Click the  icon to add more volumes, LUNs, and qtrees from other storage systems.

Note: SnapCenter Custom Plug-ins does not support automatic discovery of the resources and the storage details for physical and virtual environments. You must provide the storage information for physical and virtual environments while creating the resources.

5. In the **Resource Settings** page, provide custom key-value pairs for the resource.

Use the custom key-value pairs if you want to pass resource-specific information. For example, when you are using the MySQL plug-in, you must specify a HOST as `HOST=hostname`, Port as `=port-no used for MySQL` and master-slave configuration as `MASTER_SLAVE = "YES"` or `"NO"` (name is MASTER_SLAVE and value is "YES" or "NO").

Resource settings ⓘ

Custom key-value pairs for MySQL plug-in ^

Name	Value	
HOST	localhost	✕
PORT	3306	✕
MASTER_SLAVE	NO	+ ✕

- Review the summary, and then click **Finish**.

Result

The resources are displayed along with information such as type, host or cluster name, associated resource groups and policies, and overall status.

After you finish

If you want to provide access to the assets to other users, the SnapCenter administrator must assign assets to those users. This enables users to perform the actions for which they have permissions on the assets that are assigned to them.

After adding the resources, you can modify the resource details. If a custom plug-in resource has backups associated with it, the following fields cannot be modified: resource name, resource type, and host name.

Related tasks

[Assigning users access to assets](#) on page 23

Installing SnapCenter Plug-in for VMware vSphere

If your database is stored on virtual machines (VMs), or if you want to protect VMs and datastores, you must deploy the NetApp Data Broker virtual appliance and enable the SnapCenter Plug-in for VMware vSphere.

The NetApp Data Broker, SnapCenter Plug-in for VMware vSphere, documentation has more information.

[Deployment Guide for SnapCenter Plug-in for VMware vSphere](#)

Managing SnapCenter plug-ins






You can modify the port details, monitor the installation of SnapCenter plug-ins, identify available resources, remove a host, and update the hypervisor configuration settings.

Monitoring SnapCenter plug-in package installation status

You can monitor the progress of SnapCenter plug-in package installation by using the Jobs page. You might want to check the progress of installation to determine when it is complete or if there is an issue.

About this task

The following icons appear on the Jobs page and indicate the state of the operation:

-  In progress
-  Completed successfully
-  Failed
-  Completed with warnings or could not start due to warnings
-  Queued

Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. On the **Jobs** page, to filter the list so that only plug-in installation operations are listed, do the following:
 - a. Click **Filter**.
 - b. Optional: Specify the start and end date.
 - c. From the Type drop-down menu, select **Plug-in installation**.
 - d. From the Status drop-down menu, select the installation status.
 - e. Click **Apply**.
4. Select the installation job and click **Details** to view the job details.
5. In the **Job Details** page, click **View logs**.

Managing Configuration Checker

You can create a new schedule, view, modify, delete, disable, or run the schedules for multiple hosts simultaneously.

After installing SnapCenter Server when you log in for the first time, a default configuration checker schedule is created with the following characteristics:

- You cannot create additional schedules for SnapCenter Server.
- You cannot delete the default schedule.
- Only a SnapCenter administrator can modify or disable the default schedule.

When a plug-in host is added to the SnapCenter Server, Configuration Checker is triggered and alerts are generated. You can create only one schedule for the plug-in host, which you can modify, delete, or disable.

Viewing Configuration Checker alerts

You can view a list of Configuration Checker alerts that are generated when the configuration checker operation is performed on SnapCenter Server or plug-in hosts. You can view the alert details and delete the alerts when you no longer need them.

About this task

- The SnapCenter Server alerts can be deleted only by the SnapCenter administrator.
- You can use the `Set-SmConfigSettings` PowerShell cmdlet to modify the number of days that the new and resolved alerts are retained in the system.

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)


Steps

1. In the left navigation pane, click **Alerts**.
2. Optional: In the **Alerts** page, filter the alerts according to their severity levels.
3. If you want to see the alert details, click the **Alert Name** link.
4. If you want to delete the alert, select the alert, and then click **Delete**.
5. Monitor the operation progress by clicking **Monitor > Jobs**.

Running Configuration Checker on the plug-in hosts

The Configuration Checker operation is triggered when a plug-in host is added to SnapCenter Server and provides alerts. After resolving the issues, you can either perform an on-demand configuration check, or you can schedule recurring configuration checks of the host from the Host Details page.

Steps

1. In the left navigation pane, click **Hosts**.
2. Select the host whose configuration you want to check.
If you want to perform an on-demand configuration check, or schedule a configuration check for multiple hosts simultaneously, select multiple hosts, and then click the  icon.
3. Optional: In the **Host Details** page, click either **See All** or the alert to see the alert details.
4. Click the **Configuration Checker** link.
5. In the **Set Configuration Checker** page, select when to check the configuration:
 - If you want to check the configuration immediately, select **Run now**.
 - If you want to schedule the configuration check, select **Configure schedule**.
6. Monitor the operation progress by clicking **Monitor > Jobs**.

7. Optional: In the left navigation pane, click **Alerts**, and then select an alert to see the details.

Managing the Configuration Checker Schedules

You can create a new schedule, modify, delete, disable, or run the schedules for multiple hosts simultaneously. The SnapCenter administrator can modify or disable the SnapCenter Server.

About this task

- The SnapCenter Server default schedule cannot be deleted.

Steps

1. In the left navigation pane, click **Settings > Scheduled Configuration Checker**.
2. Optional: In the **Scheduled Configuration Checker** page, filter the schedules according to the entity type.
3. Select the entity name to create, modify, disable, or run the Configuration Checker schedule.
4. Monitor the operation progress by clicking **Monitor > Jobs**.
5. Optional: In the left navigation pane, click **Alerts**, and then select an alert to see the details.

Identifying available resources

Resources are the databases and similar components that are maintained by the plug-ins you have installed. You can add those resources to resource groups to perform data protection jobs, but first you must identify available resources. Identifying resources also verifies that the installation of plug-in packages is completed successfully.

About this task

SnapCenter Custom Plug-ins does not allow you to refresh resources.

Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. From the drop-down list, select the application (File Systems, Microsoft Exchange Server, Microsoft SQL Server, Oracle Database, or SAP HANA) that you want to manage.
3. To filter the resources, select the host from the **Host** drop-down menu.
If you have installed SnapCenter Plug-ins Package for Windows, you can also filter the resources based on the resource types such as database, instance, and availability group.
4. Click **Refresh Resources**.

The new resources added to the SnapCenter inventory are displayed.

Modifying plug-in hosts

After installing a plug-in, you can modify the plug-in hosts details if required. You can modify credentials, installation path, plug-ins, log directory details for SnapCenter Plug-in for Microsoft SQL Server and the plug-in port.

Before you begin

Ensure that the plug-in version is the same as that of the SnapCenter Server version.

About this task

You can modify a plug-in port only after the plug-in is installed. If you are 2.x or earlier versions of SnapCenter Server and SnapCenter plug-ins, you must upgrade both SnapCenter Server and SnapCenter plug-ins to be able to modify the plug-in port. You cannot modify the plug-in port while upgrade operations are in progress.

While modifying a plug-in port, you must be aware of the following port rollback scenarios:

- In a standalone setup, if SnapCenter fails to change the port of one of the components, the operation fails and the old port is retained for all of the components.
If the port was changed for all of the components but one of the components fails to start with the new port, then the old port is retained for all of the components. For example, if you want to change the port for two plug-ins on the stand-alone host and SnapCenter fails to apply the new port to one of the plug-ins, the operation fails (with an appropriate error message) and the old port is retained for both the plug-ins.
- In a clustered setup, if SnapCenter fails to change the port of the plug-in that is installed on one of the nodes, the operation fails and the old port is retained for all of the nodes.
For example, if the plug-in is installed on four nodes in a clustered setup, and if the port is not changed for one of the nodes, the old port is retained for all of the nodes.

Steps

1. In the left navigation pane, click **Hosts**.
2. Verify that **Managed Hosts** is selected at the top.
3. Select the host for which you want to modify and modify any one field.
Only one field can be modified at a time.
4. Click **Submit**.

Result

The host is validated and added to SnapCenter Server.

The configuration checker operation is triggered automatically and provides alerts for recommendations, corrective actions, and notifications to resolve the issues.

Related tasks

[Viewing Configuration Checker alerts](#) on page 124

[Running Configuration Checker on the plug-in hosts](#) on page 124

[Managing the Configuration Checker Schedules](#) on page 125

Adding an ONTAP RBAC role using security login commands

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

Before you begin

Before you create an ONTAP RBAC role for storage systems running clustered ONTAP, you must identify the following:

- The task (or tasks) that you want to perform

- The privileges required to perform these tasks

About this task

Configuring an RBAC role requires that you perform the following actions:

- Grant privileges to commands and/or command directories.
There are two levels of access for each command/command directory: all-access and read-only.
You must always assign the all-access privileges first.
- Assign roles to users.
- Vary your configuration depending on whether your SnapCenter plug-ins are connected to the Cluster Administrator IP for the entire cluster or directly connected to a SVM within the cluster.

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

[NetApp Community Document: RBAC User Creator for Data ONTAP](#)

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

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

More information about setting up ONTAP RBAC roles is in the ONTAP administration information.

[ONTAP 9 SAN Administration Guide](#)

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

Steps

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

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

svm_name is the name of the SVM. If you leave this blank, it defaults to cluster administrator.

role_name is the name you specify for the role.

command is the ONTAP capability.

Note: You must repeat this command for each permission.

Note: Remember that all-access commands must be listed before read-only commands.

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

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

user_name is the name of the user you are creating.

<password> is your password. If you do not specify a password, the system will prompt you for one.

svm_name is the name of the SVM.

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

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

<user_name> is the name of the user you created in Step 2. This command lets you modify the user to associate it with the role.

<svm_name> is the name of the SVM.

<role_name> is the name of the role you created in Step 1.

<password> is your password. If you do not specify a password, the system will prompt you for one.

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

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

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

This command displays information about the user and the role.

ONTAP CLI commands for creating SVM roles

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

ONTAP CLI command list

Command to run
security login role create -role <i>SVM_Role_Name</i> -cmddirname "snapmirror list-destinations" -vserver <i>SVM_Name</i> -access all
security login role create -role <i>SVM_Role_Name</i> -cmddirname "event generate-autosupport-log" -vserver <i>SVM_Name</i> -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "job history show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "job stop" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun delete" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun igroup add" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun igroup create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun igroup delete" -access all

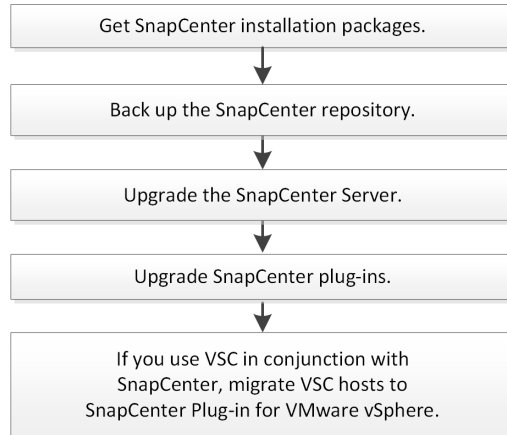
Command to run
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun igroup rename" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun igroup show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun mapping add-reporting-nodes" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun mapping create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun mapping delete" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun mapping remove-reporting-nodes" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun mapping show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun modify" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun move-in-volume" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun offline" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun online" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun resize" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun serial" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "lun show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "network interface" -access readonly
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "snapmirror policy add-rule" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "snapmirror policy modify-rule" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "snapmirror policy remove-rule" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "snapmirror policy show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "snapmirror restore" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "snapmirror show" -access all

Command to run
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "snapmirror update" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "snapmirror update-ls-set" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "version" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume clone create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume clone show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume clone split start" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume clone split stop" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume destroy" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume file clone create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume file show-disk-usage" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume modify" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume offline" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume online" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume qtree create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume qtree delete" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume qtree modify" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume qtree show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume restrict" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume snapshot create" -access all

Command to run
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume snapshot delete" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume snapshot modify" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume snapshot rename" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume snapshot restore" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume snapshot restore-file" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume snapshot show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume unmount" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver cifs share create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver cifs share delete" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver cifs share show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver cifs show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver export-policy create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver export-policy delete" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver export-policy rule create" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver export-policy rule show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver export-policy show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver iscsi connection show" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver" -access readonly
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver export-policy" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "vserver iscsi" -access all
security login role create -vserver <i>SVM_Name</i> -role <i>SVM_Role_Name</i> -cmddirname "volume clone split status" -access all

Upgrading SnapCenter Server and plug-ins

Each release of SnapCenter contains an updated SnapCenter Server and plug-in package updates. Plug-in package updates are distributed with the SnapCenter installer. You can configure SnapCenter to check for available updates. Then, you must install them.



Related concepts

[Preparing for the SnapCenter Server installation](#) on page 8

Related tasks

[Backing up the SnapCenter repository](#) on page 133

Configuring SnapCenter to check for available updates

SnapCenter periodically communicates with the NetApp Support Site to notify you of available software updates. You can also create a schedule to specify the interval in which you want to receive information about available updates.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Software**.
The Available Software page displays the available plug-in packages, versions available, and their installation status.
3. Click **Check for updates** to see if any newer versions of plug-in packages are available.
4. Click **Schedule Updates** to create a schedule to specify the interval in which you want to receive information about available updates:
 - a. Select the interval in **Check for updates**.
 - b. Select the Windows credential and click **OK**.

Backing up the SnapCenter repository

Backing up the SnapCenter Server repository helps protect it from data loss. You can back up the repository by running the `Protect-SmRepository` cmdlet.

About this task

The `Protect-SmRepository` cmdlet accomplishes the following tasks:

- Creates a resource group and a policy
- Creates a backup schedule for the SnapCenter repository

Steps

1. Launch PowerShell.
2. On the SnapCenter Server host, establish a session using the `Open-SmConnection` cmdlet, and then enter your credentials.
3. Back up the repository using the `Protect-SmRepository` cmdlet and the required parameters.

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

Related information

[Performing administrative tasks](#)

Upgrading the SnapCenter Server

You can use the SnapCenter Server installer executable file to upgrade the SnapCenter Server. You can upgrade either from SnapCenter 4.0 or 4.1.x to SnapCenter 4.2 or 4.2.1.

Before you begin

- The SnapCenter Server host must be up to date with Windows updates, with no pending system restarts.
- You should ensure that no other operations are in running state before initiating the upgrade operation.
- You should back up the SnapCenter repository (MySQL) database after ensuring that no jobs are in running state.
- You should back up all the SnapCenter configuration files that you have modified either on the SnapCenter Server host or the plug-in host.
Examples of SnapCenter configuration files: `SnapDriveService.exe.config`, `SMCoreServiceHost.exe.config`, and so on.

About this task

The upgrade procedure places the host in maintenance mode, which prevents the host from running any scheduled jobs.

Steps

1. Download the SnapCenter Server installation package from the NetApp Support Site.
NetApp Downloads: SnapCenter Software
2. In the left navigation pane, click **Hosts**., and in the **Managed Hosts** list, select the host that you want to upgrade.
3. Create a copy of the `web.config` located at `C:\Program Files\NetApp\SnapCenter\WebApp`.
4. Export the SnapCenter schedules related to SnapCenter plug-in for Oracle host from windows task schedule so that you can use it to restore the schedules if upgrade fails.

```
md d:\SCBackup  
schtasks /query /fo CSV /v >> "D:\SCBackup\sch.csv"
```
5. Create the SnapCenter MySQL database dump if the repository backup is not configured.

```
md d:\SCBackup  
mysqldump --all-databases --single-transaction --add-drop-database --triggers --routines --events -u root -p > D:\SCBackup\SCRepoBackup.dmp
```

When prompted, enter the password.
6. Initiate the SnapCenter Server upgrade by double-clicking the downloaded `.exe` file.

After you initiate the upgrade, all the prechecks are performed, and if the minimum requirements are not met, appropriate error or warning messages are displayed. You can ignore the warning messages and proceed with the installation. However, errors should be fixed.

Note: SnapCenter will continue to use the existing MySQL Server repository database password provided during installation of the earlier version of SnapCenter Server.
7. Click **Upgrade**.

At any stage if you click the **Cancel** button, the upgrade workflow will be cancelled. It will not rollback the SnapCenter Server to previous state.
8. After the upgrade is successful, log in to SnapCenter and then, on the left navigation pane, click **Hosts > Activate Schedule** to bring the host out of maintenance mode so that operations can resume.

After you finish

Best Practice: You should either log out and then log into SnapCenter, or close and then open a new browser to access SnapCenter GUI.

- If the plug-in is installed using a sudo user, you should copy the sha224 keys available at `C:\ProgramData\NetApp\SnapCenter\Package Repository\oracle_checksum.txt` to update the `/etc/sudoers` file.
- You should perform a fresh discovery of resources on the hosts.
- If the upgrade fails, you should clean up the failed installation, reinstall the earlier version of SnapCenter, and then restore the NSM database to its previous state.
- After upgrading the SnapCenter Server host, you must also upgrade the plug-ins before adding any storage system.

Upgrading your plug-in packages

The plug-in packages are distributed as part of the SnapCenter upgrade.

Before you begin

- If you are a non-root user with access to the Linux machines, you should update the `/etc/sudoers` file with the latest checksum values before performing the upgrade operation.
- You should back up all the SnapCenter configuration files that you have modified either on the SnapCenter Server host or the plug-in host.
Examples of SnapCenter configuration files: `SnapDriveService.exe.config`, `SMCoreServiceHost.exe.config`, and so on.


About this task

- You can only upgrade from plug-in 4.0 or later to 4.2 or 4.2.1.
- You can only upgrade one host at a time.
Note: If your hosts are in a Microsoft cluster, you can upgrade the SQL and Windows plug-ins on all the hosts in the cluster at one time.
- The upgrade procedure places your Windows or Linux host in maintenance mode, which prevents the host from running any scheduled jobs.

For information about upgrading the SnapCenter Plug-in for VMware vSphere, see the NetApp Data Broker SnapCenter Plug-in for VMware vSphere documentation.

[Deployment Guide for SnapCenter Plug-in for VMware vSphere](#)

Steps

1. In the left navigation pane, select **Hosts > Managed Hosts**.
2. Select the host that for which you want to upgrade the plug-in.
3. Upgrade the host by performing one of the following tasks:
 - If the Overall Status column displays Upgrade available, click the host name and perform the following:
 - a. Click **More Options**.
 - b. Select **Skip prechecks** if you do not want to validate whether the host meets the requirements to upgrade the plug-in.
 - c. Click **Upgrade**.
Note: After upgrading SnapCenter Plug-in for Microsoft SQL Server, you must refresh the resources to view the Availability Group type and you must also provide new values for “Repeat every” option for monthly schedules because the values of “Repeat every” option are not retained.
 - If the Overall Status column does not display Upgrade available, click  and then click **Upgrade > OK**.

Note: All the plug-ins in the package gets selected, but only the plug-ins that were installed with the earlier version of SnapCenter are upgraded and the remaining plug-ins are not installed. You must use the **Add plug-ins** option to install any new plug-in.

If you have not selected the **Skip prechecks** check box, the host is validated to see if it meets the requirements to install the plug-in. If the minimum requirements are not met, appropriate error or warning messages are displayed. After fixing the issue, click **Validate** to re-validate the requirements.

Note: If the error is related to disk space or RAM, you can either update the `web.config` located at `C:\Program Files\NetApp\SnapCenter WebApp` or PowerShell config files located at `C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SnapCenter\` to modify the default values. If the error is related to remaining parameters you must fix the issue and then validate the requirements again.

After you finish

After the plug-in package is upgraded, bring the host out of maintenance mode by clicking **Activate Schedule**.

Related information

[NetApp Knowledgebase Answer 1086820: Upgrading SnapCenter Plug-in Package for Microsoft Windows or SnapCenter Plug-in for Microsoft SQL Server might fail on hosts with SQL databases on VMDK](#)

Uninstalling SnapCenter plug-ins and plug-in packages

You can remove hosts and uninstall individual plug-ins or plug-in packages using the SnapCenter GUI. You can also uninstall individual plug-ins or plug-in packages on remote hosts using the command-line interface (CLI) on your SnapCenter Server host or using the Windows **Uninstall a program** option locally on any host.

For information about uninstalling the SnapCenter Plug-in for VMware vSphere, see the NetApp Data Broker, SnapCenter Plug-in for VMware vSphere, documentation.

[Deployment Guide for SnapCenter Plug-in for VMware vSphere](#)

Removing a host from SnapCenter Server

You can remove a host if you no longer want to use SnapCenter to manage its data protection jobs. For example, you might want to remove a host if it no longer has data that needs to be protected.

Prerequisites for removing a host

You can remove a host if you no longer want to use SnapCenter to manage its data protection jobs. For example, you might want to remove a host if it no longer has data that needs to be protected. Before you remove a host from SnapCenter Server, you must perform the prerequisite tasks.

- You must log in as an administrator.
- If you are using SnapCenter Custom Plug-ins, you must delete from SnapCenter all clones that are associated with the host.
- You must ensure that discovery jobs are not running on the host.

Prerequisites to remove a host using role-based access control

- You must have logged in using an RBAC role that has read, delete host, installation, uninstallation of plug-in, and delete objects permissions.
Objects can be clone, backup, resource group, storage system, and so on.
- You must have added the RBAC user to the RBAC role.
- You must assign the RBAC user to the host, plug-in, credential, resource groups, and storage system (for clones) that you want to delete.
- You must have logged in SnapCenter as an RBAC user.

Prerequisites to remove a host with clones created from clone lifecycle operation

- You must have created clone jobs using clone lifecycle management for SQL databases.
- You must have created an RBAC role with clone read and delete, resource read and delete, resource group read and delete, storage read and delete, provision read and delete, mount, unmount, plug-in installation and uninstallation, host read and delete permissions.
- You must have assigned the RBAC user to the RBAC role.
- You must have assigned the RBAC user to the host, SnapCenter Plug-in for Microsoft SQL Server, credential, clone lifecycle resource group, and storage system.

- You must have logged in SnapCenter as an RBAC user.

Removing a host

When the SnapCenter Server removes a host, it first removes the backup, clones, clones jobs, resource groups, and resources listed for that host in the SnapCenter Resources page, and then it uninstalls the plug-in packages on the host.

Before you begin

- You must be assigned a role with permissions to remove all of the objects associated with the host. Otherwise, the remove operation fails.
- You should confirm the fingerprint if the SSH key was modified after adding the host to SnapCenter.
- You should confirm the fingerprint if the SnapCenter host is upgraded to a later version of SnapCenter but the plug-in host is still running an earlier version of the plug-in.

About this task

- If you delete a host, the backups, clones, and resource groups associated with the host are also deleted.
- When you remove the resource groups, all the associated schedules are also removed.
- If the host has a resource group that is shared with another host and you delete the host, then the resource group is also deleted.
- You must use PowerShell cmdlet to remove the decommissioned or unreachable SnapCenter Server hosts.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Managed Hosts**.
3. Select the host you want to remove, and then click **Remove**.
4. For Oracle RAC clusters, to remove SnapCenter software from all the hosts in the cluster, select **Include all the hosts of cluster**.

You can also remove one node of a cluster and in that way remove all the nodes one by one. However, if there are no backups associated with a node, select **Delete backups** to remove the host from the RAC cluster.

5. Click **OK**.

Uninstalling plug-ins from a host using the SnapCenter GUI

When you decide that you no longer require an individual plug-in or a plug-in package, you can uninstall it using the SnapCenter interface.

Before you begin

- You must have removed the resource groups for the plug-in package that you are uninstalling.
- You must have detached the policies associated with the resource groups for the plug-in package that you are uninstalling.

About this task

You can uninstall an individual plug-in. For example, you might need to uninstall the SnapCenter Plug-in for Microsoft SQL Server because a host is running out of resources and you want to move that plug-in to a more powerful host. You can also uninstall an entire plug-in package. For example, you might need to uninstall the SnapCenter Plug-ins Package for Linux, which includes SnapCenter Plug-in for Oracle Database and SnapCenter Plug-in for UNIX.

- Removing a host includes uninstalling all plug-ins.
When you remove a host from SnapCenter, SnapCenter uninstalls all the plug-in packages on the host before removing the host.
- SnapCenter GUI removes plug-ins from one host at a time.
When you use the SnapCenter GUI, you can uninstall plug-ins on only one host at a time. However, you can have several uninstall operations running at the same time.
You can also uninstall a plug-in from multiple hosts by using the command-line interface (CLI).

Attention: Uninstalling the SnapCenter Plug-ins Package for Windows from a host on which the SnapCenter Server is installed will damage the SnapCenter Server installation. Do not uninstall the SnapCenter Plug-ins Package for Windows unless you are certain that you no longer require the SnapCenter Server.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the **Hosts** page, click **Managed Hosts**.
3. In the **Managed Hosts** page, select the host from which you want to uninstall the plug-in or plug-in package.
4. Adjacent to the plug-in that you want to remove, click **Remove > Submit**.

After you finish

After you uninstall a plug-in, you must wait for 5 minutes before you reinstall the plug-in on that host. This time period is sufficient for the SnapCenter GUI to refresh the status of the managed host. The installation fails if you immediately reinstall the plug-in.

If you are uninstalling SnapCenter Plug-ins Package for Linux, uninstallation-specific log files are available at: `/custom_location/snapcenter/logs`.

Uninstalling Windows plug-ins using the PowerShell cmdlet on the SnapCenter Server host

You can uninstall individual plug-ins or uninstall plug-ins packages from one or more hosts by using the `Uninstall-SmHostPackage` cmdlet on the SnapCenter Server host command-line interface.

Before you begin

You must have logged in to SnapCenter as a domain user with local administrator rights on each host on which you want to uninstall the plug-ins.

Steps

1. Launch PowerShell.
2. On the SnapCenter Server host, enter:

`Open-SMConnection -SMSbaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME`
command, and then enter your credentials.

3. Uninstall the Windows plug-ins using the `Uninstall-SmHostPackage` cmdlet and the required parameters.

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

[SnapCenter Software 4.2 Windows Cmdlet Reference Guide](#)

Uninstalling plug-ins locally on a host

You can uninstall SnapCenter plug-ins locally on a host if you cannot reach the host from the SnapCenter Server.

About this task

The best practice for uninstalling individual plug-ins or plug-in packages is to either use the SnapCenter GUI or use the `Uninstall-SmHostPackage` cmdlet on the SnapCenter Server host command-line interface. These procedures help the SnapCenter Server to stay up to date with any changes. However, you might have a rare need to uninstall plug-ins locally. For example, you might have run an uninstall job from the SnapCenter Server but the job failed, or you uninstalled your SnapCenter Server and orphan plug-ins remain on a host.

Attention: Uninstalling a plug-in package locally on a host does not delete data associated with the host; for example scheduled jobs and backup metadata.

Attention: Do not attempt to uninstall the SnapCenter Plug-ins Package for Windows locally from the Control Panel. You must use the SnapCenter GUI to ensure that SnapCenter Plug-in for Microsoft Windows is properly uninstalled.

Steps

1. On the host system, navigate to the **Control Panel** and click **Uninstall a program**.
2. In the list of programs, select the SnapCenter plug-in or plug-in package you want to uninstall and click **Uninstall**.

Windows uninstalls all plug-ins in the selected package.

Uninstalling SnapCenter Plug-ins Package for Linux using the command-line interface

You should uninstall SnapCenter Plug-ins Package for Linux by using the SnapCenter user interface. However, if you cannot uninstall it for some reason, you can uninstall SnapCenter Plug-ins Package for Linux using the command-line interface.

Before you begin

You must have deleted the scheduled jobs and running jobs must have been completed.

Step

1. Enter the following command:

```
/custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
```

Related information

[NetApp Knowledgebase Answer 1086824: SnapCenter Plug-ins Package for Linux installation fails](#)

Uninstalling the SnapCenter Server

If you no longer wish to use the SnapCenter Server to manage data protection jobs, you can uninstall SnapCenter Server using the Programs and Features Control Panel on the SnapCenter Server host. Uninstalling the SnapCenter Server removes all its components.

Before you begin

- Ensure that you have at least 2 GB of free space on the drive where the SnapCenter Server is installed.
- Ensure that the domain in which the SnapCenter Server is installed is not removed.
If you remove the domain where the SnapCenter Server was installed and then try to uninstall, the operation fails.
- You should have backed up the repository database because the repository database will be cleaned up and uninstalled.

Steps

1. On the SnapCenter Server host, navigate to the **Control Panel**.
2. Make sure you are in the **Category** view.
3. Under **Programs**, click **Uninstall a program**.
Programs and Features window opens.
4. Select NetApp SnapCenter Server, and then click **Uninstall**.

From SnapCenter 4.2, when you uninstall the SnapCenter Server, all its components including the MySQL Server repository database is uninstalled.

After you finish

- Removing the NLB node from an NLB cluster requires that you restart the SnapCenter Server host. If you do not restart the host, you might experience a failure if you attempt to reinstall the SnapCenter Server.
- You should manually uninstall .NET Framework which is not removed during uninstallation.

Minimum ONTAP privileges required

The minimum ONTAP privileges that are required vary according to the SnapCenter plug-ins you are using for data protection.

All SnapCenter plug-ins require the following minimum privileges, except where noted in the information following these tables.

All-access commands: Minimum privileges required for ONTAP 8.2.x and later
event generate-autosupport-log
job history show job stop
lun lun create lun delete lun igroup add lun igroup create lun igroup delete lun igroup rename lun igroup show lun mapping add-reporting-nodes lun mapping create lun mapping delete lun mapping remove-reporting-nodes lun mapping show lun modify lun move-in-volume lun offline lun online lun persistent-reservation clear lun resize lun serial lun show
snapmirror policy add-rule snapmirror policy modify-rule snapmirror policy remove-rule snapmirror policy show snapmirror restore snapmirror show snapmirror show-history snapmirror update snapmirror update-ls-set
version

All-access commands: Minimum privileges required for ONTAP 8.2.x and later
<pre> volume clone create volume clone show volume clone split start volume clone split stop volume create volume destroy volume file clone create volume file show-disk-usage volume offline volume online volume modify volume qtree create volume qtree delete volume qtree modify volume qtree show volume restrict volume show volume snapshot create volume snapshot delete volume snapshot modify volume snapshot rename volume snapshot restore volume snapshot restore-file volume snapshot show volume unmount </pre>
<pre> vserver cifs vserver cifs share create vserver cifs share delete vserver cifs shadowcopy show vserver cifs share show vserver cifs show vserver export-policy vserver export-policy create vserver export-policy delete vserver export-policy rule create vserver export-policy rule show vserver export-policy show vserver iscsi vserver iscsi connection show vserver show </pre>

Read-only commands: Minimum privileges required for ONTAP 8.2.x and later

```
network interface
network interface show
vserver
```

Additional information for SnapCenter Plug-in for Microsoft SQL Server

All-access command privilege that is not required: `lun persistent-reservation clear`.

Additional information for SnapCenter Plug-in for Oracle Database

- All-access command privileges that are not required:

```
vserver cifs share create
vserver cifs share delete
vserver cifs share show
vserver cifs show
vserver export-policy
vserver export-policy create
vserver export-policy delete
vserver export-policy rule create
vserver export-policy rule show
vserver export-policy show
vserver iscsi
vserver iscsi connection show
```

- Read-only command privileges that are not required:

```
network interface
network interface show
vserver
```

- Additional all-access command privileges that are required:

```
lun attribute show
lun geometry
network interface
network interface show
vserver
```

Additional information for SnapCenter Plug-in for Microsoft Windows

All-access command privilege that is not required: `lun persistent-reservation clear`.

Additional information for SnapCenter Custom Plug-ins

- All-access command privileges that are not required:

```
lun
lun persistent-reservation clear
vserver export-policy
vserver iscsi
```

- Read-only command privileges that are not required:

```
network interface show
```


vserver

- Additional all-access command privileges that are required:

lun attribute show

lun geometry

network interface

vserver cifs shadowcopy show

Features enabled on your Windows host during installation

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

Category	Feature
Web Server	<ul style="list-style-type: none"> • Internet Information Services • World Wide Web Services • Common HTTP Features <ul style="list-style-type: none"> ◦ Default Document ◦ Directory Browsing ◦ HTTP Errors ◦ HTTP Redirection ◦ Static Content ◦ WebDAV Publishing • Health and Diagnostics <ul style="list-style-type: none"> ◦ Custom Logging ◦ HTTP Logging ◦ Logging Tools ◦ Request Monitor ◦ Tracing • Performance Features <ul style="list-style-type: none"> ◦ Static Content Compression • Security <ul style="list-style-type: none"> ◦ IP Security ◦ Basic Authentication ◦ Centralized SSL Certificate Support ◦ Client Certificate Mapping Authentication ◦ IIS Client Certificate Mapping Authentication ◦ IP and Domain Restrictions ◦ Request Filtering ◦ URL Authorization ◦ Windows Authentication • Application Development Features <ul style="list-style-type: none"> ◦ .NET Extensibility 4.5 ◦ Application Initialization ◦ ASP.NET 4.5 ◦ Server-Side Includes ◦ WebSocket Protocol • Management Tools <ul style="list-style-type: none"> ◦ IIS Management Console
IIS Management Scripts and Tools	<ul style="list-style-type: none"> • IIS Management Service • Web Management Tools

Category	Feature
.NET Framework 4.5.2 Features	<ul style="list-style-type: none">• .NET Framework 4.5.2• ASP.NET 4.5.2• Windows Communication Foundation (WCF) HTTP Activation45<ul style="list-style-type: none">◦ TCP Activation◦ HTTP Activation◦ Message Queuing (MSMQ) Activation
Message Queuing	<ul style="list-style-type: none">• Message Queuing Services• Microsoft Message Queue (MSMQ) Server
Windows Process Activation Service	<ul style="list-style-type: none">• Process Model
Configuration APIs	All

Copyright

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277